ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

REDISEÑO DE LA RED DE VOZ, DATOS Y VIDEO PARA LA UNIDAD EDUCATIVA "SANTA MARÍA D. MAZZARELLO"

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

OSCAR VICENTE AGUILAR GONZAGA
oscarin_aguilar@hotmail.com

DIRECTOR:
ING. RODRIGO CHANCUSIG CHUQUILLA
rodrigch@panchonet.net

Quito, Abril 2012

DECLARACIÓN

Yo, Oscar Vicente Aguilar Gonzaga, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Oscar Vicente Aguilar Gonzaga

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Oscar Vicente Aguilar Gonzaga, bajo mi supervisión.

_____

ING. RODRIGO CHANCUSIG

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

A mi Dios por darme unos padres tan maravillosos que gracias a su apoyo incondicional y confianza he culminado mis estudios mediante la terminación de este proyecto.

A mis hermanos porque siempre encontré en ellos apoyo y confianza a más de buenos consejos para superar algunas adversidades.

A mis amigos y profesores por permitir compartir con ellos esta carrera contribuyendo en mi formación y en especial al Ing. Chancusig porque encontré en él un amigo que gracias a su disposición y conocimientos he terminado este proyecto con éxito.

A la Escuela Politécnica Nacional por abrir sus puertas y brindarme la oportunidad de seguir una carrera profesional para tener un mejor futuro.

DEDICATORIA

Dedico este proyecto a mis padres Florentino y Lidia por su amor, compresión y por estar junto a mí en todo momento apoyándome y guiándome por un buen camino. Gracias papi y mami por inculcar en mi, valores y principios para ser un hombre de bien y darme una carrera para mi futuro. Los quiero y admiro mucho

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS:

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto se desarrolló para cubrir la necesidad de la Unidad Educativa Santa María D. Mazzarello en el ámbito de tecnologías de la información, para lo cual se realizó el diseño de la red convergente en la que va a cursar tráfico de voz, datos y video.

En el capítulo, 1 se da una visión breve de conceptos básicos requeridos para realizar el diseño de la red LAN y WLAN. Además, se describe las diferentes tecnologías, telefonía IP, video vigilancia y seguridad.

En el capítulo 2, se realiza un análisis del estado actual de la red, abarcando todo lo que es cableado estructurado, equipos de networking, estaciones de trabajo, servidores, impresoras y central telefónica. Además, del respectivo análisis de tráfico que se genera en la Institución.

El capítulo 3 está centrado al rediseño de la red convergente de acuerdo a los datos obtenidos en el capítulo 2, para realizar el rediseño se calculó el nuevo tráfico de red separándolo por servicio a más del análisis y dimensionamiento de los equipos requeridos para solventar los actuales y futuros requerimientos. Además, del rediseño de la red inalámbrica, telefonía IP y video vigilancia IP.

Adicionalmente, se sugiere algunas políticas que deben ser implementadas para mayor seguridad y óptimo desempeño de la red, a más de un sistema centralizado utilizando un equipo UTM para brindar seguridad perimetral, antivirus y un sistema de administración para mejorar el tiempo de respuesta en caso de que ocurra alguna anomalía en la red.

En el capítulo 4 se realiza la selección de los equipos que se van a utilizar luego de haber comparado 3 alternativas que se ofrecen en el mercado, para ello se consideró las características técnicas mínimas que debían cumplir cada equipo en el capítulo 3.

En el último capítulo están las conclusiones y recomendaciones más importantes de este proyecto.

PRESENTACIÓN

De acuerdo a la evolución tecnológica las redes de telecomunicaciones deben estar diseñadas no solo para transmitir datos sino también deben soportar varias aplicaciones como voz y video, entre otras. Debido a esto es necesario que las Instituciones cuenten con una infraestructura física flexible, escalable centralizada para brindar varios servicios utilizando la misma red.

En este sentido varias Instituciones Educativas han visto la necesidad de reestructurar sus redes de comunicación para brindar un mejor servicio a la Comunidad, invirtiendo en nueva tecnología de comunicación debido a las ventajas que se tiene al contar con redes convergentes recuperando la inversión en cortos periodos de tiempo.

El principal objetivo que se tiene para el desarrollo del presente proyecto es ofrecer a la Comunidad Educativa un servicio de comunicación eficiente y de calidad para el desarrollo diario de sus actividades. Además, de ofrecer seguridad centralizada para el monitoreo continuo de sitios críticos que tiene la Institución

CAPÍTULO 1

FUNDAMENTOS TEÓRICOS

CAPÍTULO 1

FUNDAMENTOS TEÓRICOS

1.1 REDES LAN[1]

Una red LAN es un conjunto de dispositivos interconectados entre sí, utilizando un medio físico para proporcionar una compartición de recursos físicos y lógicos dentro de un área determinada.

Existen dos formas en la que los elementos que constituyen una red de datos se interconecten entre sí, de manera física y lógica, a la cual se le llama topología de red.

Topología Física.- es la forma real como están conectadas las máquinas, los dispositivos de interconexión y el cableado en la red.

Topología Lógica.- es la manera como se comunican los dispositivos a través del medio físico, es decir muestra el comportamiento de la red.

1.1.1 TOPOLOGÍAS DE RED

La topología de red se define como la cadena de comunicación usada por los nodos que conforman una red para comunicarse.

Existen las topologías de red: bus, árbol, anillo, estrella, entre otras.

[1] [FT1] Redes de Área Local, Ing. Pablo Hidalgo, ESCUELA POLITÉCNICA NACIONAL, Marzo 2008
[PW1] http://es.wikipedia.org/wiki/Red_de_computadoraS

1.1.1.1 Topología de bus

Esta topología utiliza un medio de transmisión compartido y está relacionada con la transmisión broadcast en la que se utiliza la técnica de acceso al medio por contención. Ver figura 1.1

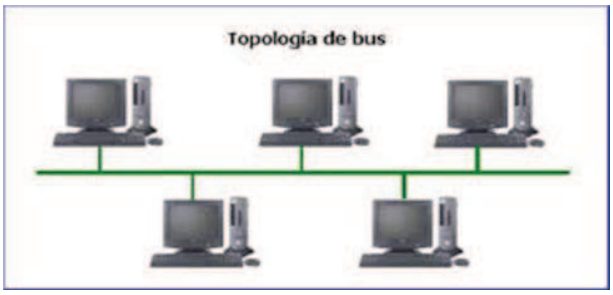


Figura 1. 1 Topología Bus [1]

1.1.1.2 Topología de árbol

Actualmente esta topología es poco utilizada, era empleada para redes que cumplen con el estándar IEEE 802.3/10Broad36 con una técnica de transmisión de banda ancha.

Esta topología al igual que la de bus utiliza un único segmento de cable, pero se diferencia en que utiliza un dispositivo al final del segmento de la red, conocido como *headend*. Ver figura 1.2

Figura 1. 2 Topología Árbol. [2]

1.1.1.3 Topología de anillo

Está basada en un conjunto de repetidores los cuales están unidos en un enlace punto a punto dentro de un bucle cerrado. Esta topología normalmente es utilizada con las tecnologías Token Ring y FDDI, utilizando tokens como técnica de acceso al medio. Ver figura 1.3

Figura 1. 3 Topología Anillo. [3]

1.1.1.4 Topología de estrella

Es una de las topologías más antiguas, la cual está formada por un concentrador al cual converge todo el tráfico generado por los dispositivos que se encuentran conectados.

La gran mayoría de redes actuales utilizan este tipo de topología física con diferente topología lógica que difiere en el método de acceso al medio. Ver figura 1.4

Figura 1. 4 Topología estrella. [4]

1.1.2 MODELO DE REFERENCIA OSI [2]

Este modelo fue creado con la necesidad de tener un estándar con el cual se tenga compatibilidad e interoperabilidad entre equipos de diferentes fabricantes. Es un modelo de referencia de interconexión de sistemas abiertos.

El modelo OSI solo especifica los protocolos que se deberían usar en cada una de las capas y está dividido en 7 como se indica en la figura 1.5, donde cada una realiza una función para la comunicación.

Figura 1. 5 Modelo de referencia OSI. [5]

1.1.2.1 Capa Física

Aquí se realiza la transmisión y recepción del flujo bits a través del medio físico conectado y cumple las siguientes funciones: mecánicas, eléctricas y funcionales.

Características Mecánicas. Descripción de las caracteristicas físicas del interfaz de red y del medio de transmisión utilizado.
Características Eléctricas. Describe la forma en que se representan los bits y la velocidad de transmisión.

[2] [PW2] www.ie.itcr.ac.cr/marin/mpc/redes/Modelo_osi_tcp_ip(oficial).pdf

Características Funcionales. Define las funciones que realiza la interfaz como establecimiento, mantenimiento y liberación del enlace físico.

1.1.2.2 Capa de Enlace de Datos

Es la encarga del acceso al medio de transmisión, convierte un medio de transmisión no confiable en un enlace libre de errores, se ocupa del direccionamiento físico, control del flujo y de la distribución en forma ordenada de las tramas. Además resuelve problemas de duplicidad y borrado de tramas.

1.1.2.3 Capa de Red

Realiza el direccionamiento y la selección de la mejor ruta para la transferencia de información entre sistemas finales a través de algún tipo de red.

Esta capa es la encargada de interconectar redes heterogéneas y de realizar la conmutación, control de flujo y de la recuperación de fallas que tiene la capa de enlace.

1.1.2.4 Capa de Transporte

Conocida como extremo – extremo y es la encargada de recibir los datos de la capa de sesión, los fragmenta si es necesario y los pasa a la capa de red. Además, realiza control de flujo entre los dos extremos y optimiza el uso de todos los servicios de la red.
En este nivel se proporciona mecanismos de intercambio de datos extremo a extremo asegurando que dichos datos lleguen correctamente a su destino.

1.1.2.5 Capa de Sesión

Esta capa es la encargada del establecimiento de sesiones entre diferentes aplicaciones para que los usuarios se puedan comunicar. Además, realiza la sincronización de puntos de comparación y recuperación durante una transferencia de archivos.

1.1.2.6 Capa de Presentación

Maneja el formato de los datos que se van a intercambiar entre las aplicaciones de manera que estos sean legibles a los procesos de aplicación. Cabe mencionar que esta capa solo se encarga del formato pero no del significado de los datos. Además proporciona el servicio de codificación de datos en modo estándar a más de realizar funciones de compresión y cifrado.

1.1.2.7 Capa de Aplicación

Mediante los mecanismos que tiene esta capa los procesos de aplicación acceden al entorno OSI. Además, proporciona el interfaz final entre el usuario y la red.
En este nivel se realiza la administración y la implementación de las diferentes aplicaciones.

1.1.3 MODELO DE REFERENCIA TCP/IP [3]

Este modelo se utiliza para la conexión de Internet porque permite que equipos de diferentes marcas puedan interconectarse usando la misma pila de protocolos TCP/IP. Fue desarrollado por la red ARPANET, existen 6 versiones siendo una de

[3] [PW2] www.ie.itcr.ac.cr/marin/mpc/redes/Modelo_osi_tcp_ip(oficial).pdf

las más importantes en su desarrollo la IPv4, este modelo consta de cuatro capas o niveles los cuales son: Aplicación, Transporte, Internet y Acceso de Red. Como se indica en la figura 1.6

Figura 1. 6 Modelo de referencia TCP/IP. [6]

1.1.3.1 IPv4[4]

En relación al direccionamiento, IPv4 está limitado a 32 bits y consta de 4 octetos donde cada octeto está dentro del rango de 0 a 255. En esta versión se especifica 3 tipos de direcciones las cuales son: públicas, privadas y reservadas.

1.1.3.1.1 Direcciones Públicas

Son aquellas que se utilizan para navegar en la red Internet.

1.1.3.1.2 Direcciones Privadas

Estas direcciones son utilizadas en redes LAN en un área domestica o corporativa, no pueden ser utilizadas para enrutamientos hacia la Internet. El rango detallado en la tabla 1.1 es el designado para las direcciones privadas.

[4] [FT1] Redes TCP/IP, Ing. Pablo Hidalgo, ESCUELA POLITÉCNICA NACIONAL, Marzo 2008
[PW3] http://www.albertnogues.com/attachments/014_IntroIp.pdf

Clase	Rango
A	10.0.0.0 a 10.255.255.255
B	172.16.0.0 a 172.31.255.255
C	192.168.0.0 a 192.168.255.255

Tabla 1. 1 Rango de direcciones Privadas. [1]

1.1.3.1.3 Direcciones reservadas

Estas direcciones están designadas para un uso específico, entre las más importantes están las siguientes:

0.0.0.0 Esta dirección es utilizada para referirse a la red.
255.255.255.255 Se utiliza esta dirección para broadcast.
127. X.X.X Estas direcciones son utilizadas para Loopback es decir direcciones para diagnóstico.

127.0.0.1 Esta dirección es utilizada para hacer referencia a nuestra propia maquina de forma local.

1.1.3.2 IPv6

IPv6 es una versión del protocolo de Internet (IP), diseñada para remplazar a IPv4. Debido a que el número de direcciones de red está empezando a restringir el crecimiento de Internet y su uso. Por este motivo, y previendo la situación, el organismo que se encarga de la estandarización de los protocolos de Internet (*IETF, Internet Engineering Task Force*), ha desarrollado IPv6, que posee direcciones con una longitud de 128 bits, es decir 2^{128} posibles direcciones.

1.1.4 ELEMENTOS DE UNA RED LAN[5]

1.1.4.1 Servidor

Son equipos que tienen mejores características que las computadoras y son capaces de compartir diferente tipo de recursos, existen diferentes tipos de servidores de acuerdo al recurso o aplicación que se quiera compartir o administrar.

1.1.4.2 Clientes o terminales

Son dispositivos finales los cuales pueden trabajar en de manera independiente o conectados a una red compartiendo alguna aplicación específica.

1.1.4.3 Sistema operativo de la red

El sistema operativo en una red permite que se puedan comunicar las estaciones de trabajo y así poder compartir recursos y aplicaciones entre estas.

1.1.4.4 Tarjeta adaptadora de red (NIC)

Las NIC permiten transformar la señal analógica que recibe del medio de transmisión en una secuencia de bits, estas tarjetas son dispositivos que permiten la conexión física entre las PCs y el cable de la red.

Existen diferentes tipos de NICs pero la más utilizada en la actualidad es la Ethernet la cual utiliza los conectores RJ45. Ver figura 1.7

---

[5] [PW4] http://www.ie.itcr.ac.cr/marin/mpc/redes/01_RedesIntroduccion.pdf

Figura 1. 7 NIC. [7]

1.1.4.5 Medios de transmisión

Son utilizados para la conexión física de todos los dispositivos de la red, ya que por ellos se transmite la señal la cual transporta la información de un dispositivo a otro. Existen diferentes medios de transmisión de acuerdo a los requerimientos de la red como son: ancho de banda, velocidad máxima de transmisión y distancia.

Los medios de transmisión se dividen en dos grupos: medios guiados y los no guiados. Dentro de los medios guiados están fibra óptica y cobre (cable coaxial y par trenzado), y de los no guiados están los que utilizan radiofrecuencia, infrarrojos y microondas. Ver figura 1.8

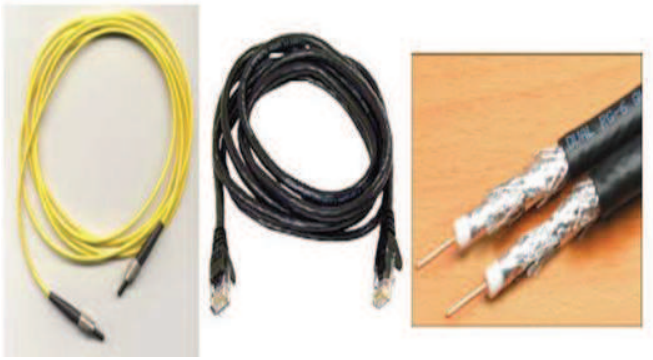


Figura 1. 8 Medios de transmisión Guiados. [8]

1.1.4.6 Equipos periféricos compartidos

Estos equipos pueden trabajar de forma local conectados directamente al pc o de forma compartida conectados a la red, dentro de estos equipos están las impresoras y escáner etc. Como se indica en la figura 1.9

Figura 1. 9 Equipos Periféricos. [9]

1.1.4.7 Equipos de conectividad

Son los que realizan la interconexión de la red. A través de estos equipos los diferentes dispositivos se pueden comunicar entre ellos, entre estos equipos están los puentes, concentradores, repetidores, puntos de acceso, conmutadores y enrutadores. Ver como ejemplo la figura 1.10

Figura 1. 10 Equipos de Conectividad. [10]

1.1.5 TECNOLOGÍAS DE REDES LAN[6]

Al inicio de las redes LAN existieron algunas versiones, las cuales se diferenciaron por el método de acceso al medio, topología, medio de transmisión y velocidad de

[6] [LB1] William Stallings, "Comunicaciones y Redes de Computadores", 6ª edición, Prentice Hall, 2000.

transmisión. Pero este tipo de redes no eran flexibles ya que dependían de los fabricante, por lo que fue necesario la creación de un estándar que permita la interconexión de equipos de diferentes fabricantes. Para solventar esta necesidad se creó el estándar IEEE 802.3 que está basado en la red Ethernet.

Ethernet es una tecnología desarrollada en los años ochenta por las empresas Digital Equipment Corporation, Intel y Xerox.

El estándar IEEE 802.3 utiliza como técnica de control de acceso al medio, el acceso múltiple con detección de portadora y de colisiones CSMA/CD con esto realiza un sondeo del canal de transmisión o escucha para detectar alguna portadora que se esté transmitiendo. Además, realiza detección de colisiones.

Actualmente, en redes LAN las tecnologías que más se utilizan son: Fast Ethernet, Gigabit Ethernet, 10Gigabit Ethernet, 40Gigabit Ethernet y 100Gigabit Ethernet.

1.1.5.1 Fast Ethernet[7]

Cuando se fueron creando aplicaciones con nuevos servicios como multimedia se requería tener una red de mayor velocidad que la que tiene Ethernet original que es de 10 Mbps pero que conserve algunos parámetro como la técnica de acceso al medio CSMA/CD y la longitud del medio de transmisión, para ello se creó la nueva versión conocida como Ethernet de alta velocidad que alcanza una tasa de transmisión de 100 Mbps.

En esta versión se tienen dos variantes de acuerdo al medio físico de transmisión, una es 100Bas-X, que utiliza los medios de transmisión STP, UTP Cat 5 o superior y

[7] [PW6] http://es.wikipedia.org/wiki/100BASE-X

para fibra óptica, la otra variante es la 100Base-T4 que es utilizada para transmitir voz por medio de cable UTP Cat 3. En la tabla 1.2 se especifica las diferencias entre estas dos tecnologías.

TECNOLOGÍA		VELOCIDAD DE TRANSMISIÓN	MEDIO DE TX	DISTANCIA MÁXIMA	CODIFICACIÓN DE LÍNEA
100Base-X	100Base-TX	100Mbps	STP o UTP Cat. 5	100 m	4B4B + MLT-3
	100Base-FX	100Mbps	Fibra óptica	2000 m	4B5B
100Base-T4		100Mbps	UTP Cat. 3 o 5	100 m	8B6T

Tabla 1. 2 Estándares Fast Ethernet. [2]

1.1.5.2 Gigabit Ethernet[8]

Esta tecnología es la evolución de Fast Ethernet, es conocida como GigaE y esta estandarizada en IEEE 802.3ab y 802.3z, alcanza una velocidad de 1000 Mbps.

IEEE 802.3ab (1000Base-T) es soportada sobre cable UTP Cat. 5, 5E, 6 y 6A, también trabaja sobre fibra óptica, este estándar a diferencia de las anteriores versiones 10Base-T y 100Base-T transmite en los dos sentidos en modo full dúplex con extensión de portadora y utiliza modulación PAM-5.

IEEE 802.3z (1000Base-X) tiene algunas versiones y utiliza el método de codificación 8B10B, es utilizado para fibra óptica y para cable apantallado STP.

El la tabla 1.3 se especifica algunas características de la tecnología Gigabit Ethernet

[8] [T1] Ing. Josue Quelal, Rediseño de la Red de Comunicaciones de la empresa metropolitana de obras públicas (EMOP-Q) para soportar aplicaciones de voz sobre IP (VoIP), pág 7

	1000BASE-T	**1000BASE-X**		
		1000Base-SX	1000Base-LX	1000Base-CX
Medio de Transmisión	UTP Cat. 5,5E o 6	Fibra Multimodo	Fibra Multimodo y Mono modo	STP (2 pares)
Longitud máxima	100 m	220 a 550 m	550 m y 5 Km	25 m
Codificación	4D-PAM5	8B10B	8B10B	8B10B

Tabla 1. 3 GigaE. [3]

1.1.5.3 10 Gigabit Ethernet[9]

10Gigabit Ethernet fue estandarizada como IEEE 802.3ae en el año 2002 con una velocidad de 10 Gbps, al inicio fue creado como 10GBase-R solo para trabajar en fibra óptica en los año 2004 y 2006 se crearon nuevos estándares para que pueda trabajar en cable de cobre los cuales son 10GBase-X y 10GBase-T.

Esta tecnología fue desarrollada para que trabaje en ambientes LAN y WAN por lo que la IEEE especificó dos tipos de capa física, una para LAN y otra para WAN. La utilizada por las redes WAN añade una encapsulación extra y se la conoce como 10GBASE-W. En la tabla 1.4 se especifica las principales características de 10GBase-R y 10GBASE-W.

	10GBASE-R				**10GBASE-W**	
	10GBase SR	**10GBase LX4**	**10GBase LR**	**10GBase ER**	**10GBase SW**	**10GBase LW**
Medio de Transmisión	Fibra Multimodo	Fibra Multimodo Monomodo	Fibra Monomodo	Fibra Monomodo	Fibra Multimodo	Fibra Monomodo
Codificación	64B66B	8B10B	64B66B	64B66B	64B66B	64B66B

[9] [PW27] http://standards.ieee.org/resources/glance.html
[PW28] www.10gea.org

	10GBase SR	10GBase LX4	10GBase LR	10GBase ER	10GBase SW	10GBase LW
Longitud Máxima	26 a 82 m	240 a 300 m 10 Km	10 Km	40 Km	300 m	10 Km

Tabla 1. 4 10GBase-R, 10GBase-W. [4]

En la siguiente tabla se detallan los estándares creados para que 10Gbit Ethernet pueda trabajar sobre cobre.

	10GBASE-CX4	10GBASE-T
Medio de Transmisión	InfiniBand	UTP Cat 6a o 7
Codificación	8B10B	8B10B
Longitud Máxima	15 m	100 m

Tabla 1. 5 Estándar para cable de Cobre. [5]

1.1.5.4 40Gigabit Ethernet y 100Gigabit Ethernet[10]

Con el desarrollo de la tecnología y de los nuevos servicios es necesario contar con redes de alta velocidad para los enlaces entre los equipos a nivel de core de la red, para que no se genere cuellos de botella en los sitios críticos de la red.

Para cumplir con los nuevos requerimientos el grupo HSSG (*Higher Speed Study Group*) creó el nuevo estándar IEEE 802.3ba ratificado en junio del 2010, con este estándar se tiene velocidades de transmisión de 40 Gbps y 100 Gbps alcanzando un distancia de 40 Km con fibra monomodo y 100 m con fibra multimodo.

[10] [PW29] http://www.ethernetalliance.org/wp-content/uploads/2011/10/document_files_40G_100G_Tech_overview.pdf

En la figura 1.11 se especifica una arquitectura simple de la capa física, donde la capa MAC[11] corresponde a la capa 2 del modelo OSI y se puede usar fibra o cobre como medio de transmisión.

La capa física (PHY) corresponde al nivel 1 del modelo OSI, se divide en las subcapas PMD[12], PMA[13] y PCS[14]. Además, incluye una subcapa para auto negociación (AN) y una subcapa para corrección de errores FEC.

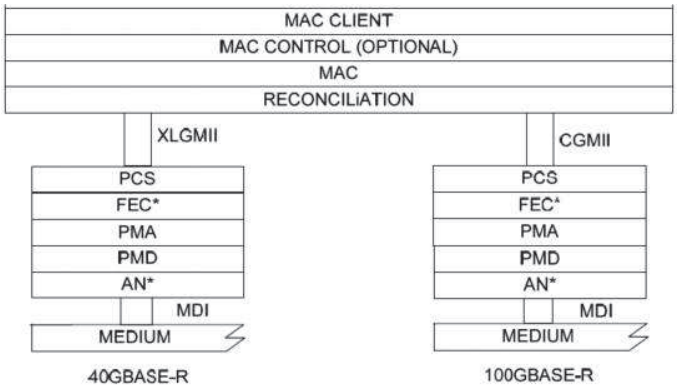


Figura 1. 11 Arquitectura 802.3ba. [11]

En la tabla 1.6 se especifica los tipos de tecnologías definidas para 40 Gigabit Ethernet y 100Gigabit Ethernet.

TECNOLOGÍAS 40 GIGABIT ETHERNET Y 100GIGABIT ETHERNET				
Medio de Transmisión	**Longitud máxima**	**40 Gigabit**	**100 Gigabit**	**Codificación**
Backplane	1 m	40GBase-KR4	---	64B/66B
Cobre	7 m	40GBase-CR4	100GBase-CR10	64B/66B

[11] Media Access Controller
[12] Physical Medium Dependent
[13] Physical Medium Attachment
[14] Physical Coding Sublayer

Medio de Transmisión	Longitud máxima	40 Gigabit	100 Gigabit	Codificación
Fibra multimodo OM3	100 m	40GBase-SR4	100GBase-SR10	64B/66B
Fibra multimodo OM4	150 m	40GBase-SR4	100GBase-SR10	64B/66B
Fibra monomodo	10 Km	40GBase-LR4	100GBase-LR4	64B/66B
Fibra monomodo	40 Km		100GBase-ER4	64B/66B

Tabla 1. 6 Tecnologías 40 Gigabit Ethernet y 100Gigabit Ethernet. [6]

1.2 REDES INALÁMBRICAS DE ÁREA LOCAL WLAN[15]

Las redes inalámbricas WLAN prestan los mismos servicios que las redes cableadas tales como Ethernet y Token Ring, no están limitadas a conexiones físicas, las WLAN utilizan un medio no guiado como luz infrarroja (IR) o radiofrecuencias (RFs).

Al utilizar luz infrarroja están limitadas por los obstáculos por lo que tienen poco alcance a diferencia de las que utilizan radiofrecuencia con las cuales se atraviesa la mayoría de obstáculos por lo que tienen mayor alcance.

Las WLAN permiten alta disponibilidad y movilidad para que los usuarios puedan conectarse en cualquier lugar en tiempo real y acceder a las aplicaciones locales de la Institución y navegar en Internet. Estas redes a más de ser otra alternativa de red son un complemento sustancial de las redes cableadas ya que se pueden utilizar estas dos tecnologías en conjunto y crear una red hibrida donde la red cableada es la red principal y la inalámbrica sería utilizada para acceder a lugares inaccesibles.

[15] [PW30] http://senet.wikispaces.com/file/view/REDES_INALAMBRICAS_UCC.pdf

Las WLAN trabajan en las bandas de 2.4 GHz y 5GHz las cuales son bandas no licenciadas IMS especificadas en el estándar IEEE 802.11, el cual realiza una descripción de los protocolos utilizados en la capa física y en la capa de control de acceso al medio. Ver figura 1.12 como ejemplo de una red WLAN

Figura 1. 12 Redes WLAN. [12]

1.2.1 TÉCNICAS DE MODULACIÓN[16]

El estándar IEEE 802.11 especifica las siguientes técnicas de modulación en las que se tiene una eficiente codificación para tener un mayor flujo de bits utilizando el mismo ancho de banda.

1.2.1.1 FHSS (*Frequency Hopping Spread Spectrum*)

Esta técnica de modulación se basa en cambiar de forma aleatoria la frecuencia de transmisión, para lo cual cuenta con señales de sincronización en las que se envía el tipo de secuencia y la duración de cada salto, para el caso de IEEE 802.11 utiliza bandas de frecuencia ISM en el rango de frecuencias de 2,400 hasta los 2,4835 GHz. Este rango de frecuencia está dividido en 79 canales y el tiempo de duración de cada salto es de 300 a 400 ms.

[16] [PW16] http://multingles.net/docs/Manual%20-%20Redes%20WiFi%20inalambricas.pdf

1.2.1.2 DSSS (*Direct Sequence Spread Spectrum*)

En esta técnica se genera un patrón de bits redundante para cada uno de los bits que componen la señal. Cuanto mayor sea este patrón de bits, mayor será la resistencia de la señal a las interferencias. El estándar IEEE 802.11 recomienda un tamaño de 11 bits, pero el óptimo es de 100.

HR-DSSS es una extensión de DSSS, con el fin de incrementar la velocidad de transmisión, utiliza un esquema de modulación por código complementario (*CCK, Complementary Code Keying*) que consiste en dividir la secuencia de chips en palabras código de 8 bits por símbolo, en comparación de DSSS que utiliza 11 bits.

1.2.1.3 OFDM (*Orthogonal Frequency-Division Multiplexing*)

OFDM está basada en FDM, envía los datos por ondas de radio para lo cual divide la señal portadora en múltiples subportadoras y las transmite simultáneamente utilizando diferentes frecuencias. Las subportadoras son moduladas de forma independiente utilizando QAM o PSK, esta técnica es mayormente utilizada en la actualidad.

1.2.2 PROTOCOLOS DE LA CAPA FÍSICA Y DE LA CAPA MAC[17]

Los protocolos que especifica el estándar IEEE 802 son para las capas inferiores del modelo de referencia OSI como se detalla en la tabla 1.7.

[17] [T2] Ing. Emilio Bolaños, Diseño de la Red Inalámbrica de área local para los edificios la tribuna y villafuerte de Petroproducción bajo el Estándar IEEE 802.11g y su Interconectividad, pág 3

	802.2 LOGICAL LINK CONTROL (LLC)				**SUB CAPA LLC**	**CAPA MAC**
MAC	802.11 MAC				Sub Capa MAC	
Estándar	802.11	802.11a	802.11b	802.11g	802.11n	
PHY (Modulación)	FHSS DSSS	OFDM	HR-DSSS	OFDM DSSS	OFDM MIMO	Capa Física

Tabla 1. 7 Protocolos 802.11. [7]

1.2.3 PRINCIPALES ESTÁNDARES DE IEEE 802.11

Este es el primer estándar creado para el uso de redes inalámbricas que especifica una velocidad de transmisión de 1 a 2 Mbps, utilizando la técnica de modulación DSSS o FHSS. Además, utiliza CSMA/CA como técnica de acceso al medio.

1.2.3.1 802.11a

Este estándar trabaja en la banda de 5GHz y establece una velocidad de hasta 54 Mbps utilizando canales de 20 MHz con modulación OFDM, permite dividir una señal portadora en 52 subportadoras de las cuales 4 son utilizadas para la sincronización.

Además, específica 12 canales de los cuales 8 son utilizados para la parte inalámbrica y los 4 para las conexiones punto a punto.

1.2.3.2 802.11b

Este estándar es conocido como WiFi. Trabaja en la banda de 2.4 GHz con una velocidad de transmisión de hasta 11, utiliza DSSS como técnica de modulación con codificación CCK (Complementary Code Keying).

Es uno de los estándares más difundidos en la actualidad para la implementación de redes WLAN, por trabajar en la banda de 2.4 causa interferencia con otros dispositivos que trabajan en esta banda como los microondas o telefonía fija inalámbrica.

1.2.3.3 802.11g

Este estándar trabaja en la banda de 2.4 GHz alcanzando una velocidad de 54 Mbps empleando OFDM como técnica de modulación, tiene gran aceptación en el mercado debido a la interoperabilidad con el estándar 802.11b.

1.2.3.4 802.11n

Con este estándar se tiene una mejora en el rendimiento de las redes inalámbricas ya que alcanza una tasa de transmisión de 600 Mbps utilizando Channel Bonding lo que permite tener un canal de 40 MHz. Este estándar se basa en las versiones anteriores pero adiciona MIMO con multiplexado de división espacial (SDM).

1.2.4 TOPOLOGÍAS DE REDES WLAN [18]

En las redes WLAN se tiene dos tipos de topologías que son: redes Ad Hoc y redes de infraestructura.

1.2.4.1 Redes Ad-Hoc

Es un conjunto de ordenadores que tiene la misma jerarquía, que realizan una comunicación entre ellos sin utilizar un punto de acceso común, solo necesitan usar

[18] [PW17]www.cantv.com.ve/Portales/Cantv/Data/Eventos/SemanaSeguridad_2k8/Mendillo_SEMANADELA_SEGURIDAD_Cantv .pdf

las señales de radio con un mismo canal y un identificador especifico de WiFi ESSID. Ver figura 1.13 que es un ejemplo de una red Ad-Hoc

Figura 1. 13 Redes Ad Hoc. [13]

1.2.4.2 Red de Infraestructura

En esta topología es primordial el uso de un punto de acceso (AP) para que dos ordenadores se puedan comunicar. La topología es más eficaz que la Ad – Hoc y es la que se utiliza para implementar redes híbridas a más de tener mayor velocidad de transmisión.

La configuración del canal para las señales de radio se la realiza automáticamente en el dispositivo llamado tarjeta de red para que se conecte con el AP más cercano. Ver figura 1.14 donde se indica el área de cobertura de los AP.

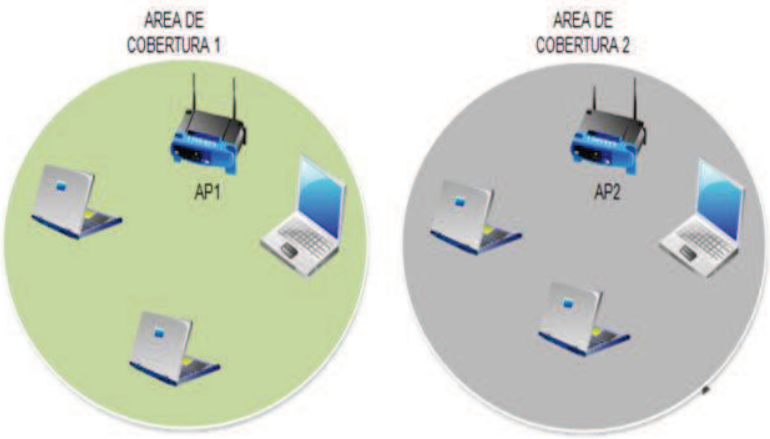


Figura 1. 14 Red Modo Infraestructura. [14]

1.2.5 SEGURIDAD EN REDES INALÁMBRICAS[19]

Con la creación de las redes inalámbricas se tiene mayor flexibilidad y movilidad para los usuarios, pero con esto aparecieron nuevos riesgos y amenazas que afecta la seguridad. Para prevenir estos riesgos se utiliza algunos mecanismos de seguridad para proteger la información de los intrusos.

1.2.5.1 WEP (*Wired Equivalent Protocol*)

WEP es un protocolo utilizado para la encriptación de la información que se implementa en la capa MAC y realiza la compresión y cifrado de los datos.

Este protocolo trabaja con el campo CRC de la trama 802.11, utiliza RC4 que es un algoritmo de encriptación simétrica, sin embargo con la utilización de WEP solo se proporciona una seguridad mínima a la red.

Este tipo de mecanismo es utilizado comúnmente en la configuración de una red inalámbrica de hogar debido a que no se requiere de un alto grado de seguridad en este tipo de redes.

1.2.5.2 WPA (*Wifi Protect Access*)

WPA o TSN es un mecanismo de control de acceso para una red inalámbrica que fue desarrollado para eliminar las debilidades de WEP. Trabaja de forma similar a WEP pero utiliza claves dinámicas y para la gestión de claves dinámicas utiliza TKIP (*Temporal Key Integrity Protocol*). La autenticación de usuario la realiza mediante el

[19] [PW18] http://trajano.us.es/~fornes/RSR/2005/SeguridadWIFI/Trabajo%20WIFI.pdf

uso de un servidor que almacena las credenciales y contraseñas de todos los usuarios.

WPA puede trabajar de dos formas ya sea utilizando claves compartidas PSK la cual es débil a los ataques de fuerza bruta ó haciendo uso de un servidor de autenticación como Radius que es la más segura y óptima para implementar en una Institución.
Existe dos versiones donde la que ofrece mayor seguridad es la versión 2 porque utiliza el algoritmo AES para el cifrado de datos.

1.3 CABLEADO ESTRUCTURADO

Un sistema de cableado estructurado es una infraestructura que soporta múltiples servicios como: voz, datos y video, en su estructura utiliza un punto central donde se conectan todos los dispositivos utilizando una topología física de estrella facilitando la interconexión y administración del sistema. Además, se tiene flexibilidad, cumplimiento de las normas y estándares internacionales. Además, es un sistema de arquitectura abierta.

1.3.1 MEDIOS DE TRANSMISIÓN[20]

Los medios de transmisión son una parte primordial de una red, dado que estos hacen posible la interconexión y el intercambio de información y de recursos de los diferentes componentes de red, la elección del medio de transmisión depende de los servicios y aplicaciones requeridas, porque cada medio cuenta con sus propias características como son: ancho de banda, tasa de transmisión, distancia máxima soportada y atenuación. Se clasifican en dos grupos que son. Medios de transmisión guiados y los medios de transmisión no guiados.

[20] [PW19] http://es.wikipedia.org/wiki/Medio_de_transmisi%C3%B3n

1.3.1.1 Medios de Transmisión Guiados

Los medios de transmisión guiados son aquellos que transmiten la señal por medio de un estructura física, es decir, a través de cables de cobre o fibra óptica.

1.3.1.2 Cable de Par Trenzado

Este tipo de cable es el más utilizado, existen dos versiones, uno con apantallamiento llamado STP y el UTP sin apantallar.

El cable UTP (*Unshielded Twisted Pair)* es utilizado para redes de pequeñas y medianas empresas, la velocidad de transmisión y el ancho de banda dependen de la categoría del cable a utilizar, existen algunas variantes estandarizados que van desde el utilizado para telefonía analógica hasta la categoría 6A que es empleado para transmisión de datos. Ver figura 1.15 que representa un cable UTP

Figura 1. 15 Cable UTP. [15]

Una de las desventajas al utilizar este tipo de cable es que es susceptible a interferencias eléctricas por lo que no es utilizado en estos entornos.

El cable UTP tiene una impedancia característica de 100 ohms, utiliza un conector RJ-45 y está limitado a 100 m de distancia. Ver figura 1.16

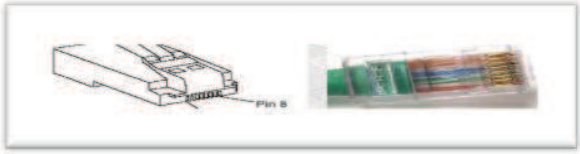


Figura 1. 16 Conector RJ-45. [16]

STP es un cable de par trenzado similar al UTP con la diferencia de que cada par tiene una pantalla protectora, además de tener una lámina externa de aluminio o de cobre trenzado alrededor del conjunto de pares, diseñada para reducir la absorción de ruido eléctrico.

1.3.1.2.1 Tipos de conexiones para el cable de par Trenzado

Existen dos tipos de conexiones que se pueden realizar de acuerdo al dispositivo que se desea conectar que son: cable recto y cruzado de acuerdo a la norma 568 A/B de la configuración de pines en un conector RJ-45. Ver figura 1.17 donde se especifica la conexión que se debe realizar en cada norma.

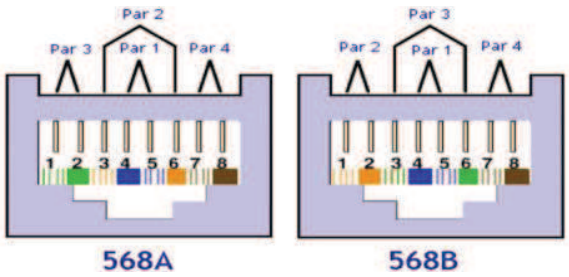


Figura 1. 17 Norma 568 A/B. [17]

1.3.1.2.2 Cable Coaxial

El cable coaxial está compuesto por un conductor solido de cobre envuelto con un aislante y por una malla, tiene un alto nivel de resistencia a las interferencias externas. Existen dos categorías de cable coaxial.

Para transmisión en banda ancha.

Con una impedancia característica de 75 ohmios. Utilizado para transmisión de señales de televisión por cable (CATV, "Cable Televisión").

Para transmisión en banda base.

Con una impedancia característica de 50 ohmios. Utilizado en redes LAN. Dentro de esta categoría, se emplean dos tipos de cable: coaxial grueso (*thick*) y coaxial fino (*thin*).

A diferencia de UTP este cable se puede utilizar en ambientes con un alto nivel de interferencias. En la figura 1.18 se detallan los componentes del cable.

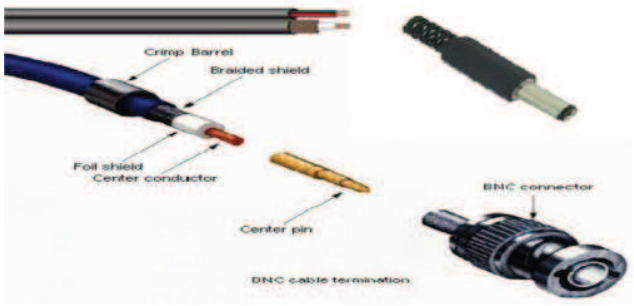


Figura 1. 18 Cable Coaxial. [18]

1.3.1.2.3 Fibra óptica[21]

Este es el mejor medio de transmisión físico, está compuesto de hilos muy finos de cristal o de materiales de plásticos. Las señales se envían por estos hilos mediante pulsos de luz que representan los datos enviados.

Con la fibra óptica se tiene velocidades en unidades de Mbps hasta Gbps, se puede cubrir grandes distancias y es inmune a las interferencias electromagnéticas por lo que es muy utilizada en el sector de las telecomunicaciones.

El cable de fibra óptica está formado por un núcleo central, Buffer y un revestimiento con material similar al del núcleo pero el revestimiento tiene menor índice de

[21] [PW20] http://es.wikipedia.org/wiki/Fibra_%C3%B3ptica

refracción. Para obtener una reflexión interna total es necesario tener mayor diferencia de índices y ángulo de incidencia. En la figura 1.19 se detalla los componentes de la fibra.

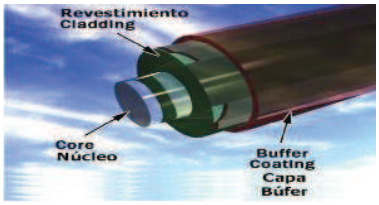


Figura 1. 19 Fibra Óptica. [19]

Existen dos tipos de fibras ópticas que son la Multimodo y la Monomodo.

Fibra Óptica Multimodo

Este tipo de fibra puede transmitir múltiples modos simultáneamente los cuales se supone que no llegan todos en el mismo tiempo porque viajan a diferentes velocidades, a diferencia de la fibra Monomodo el núcleo es de mayor diámetro, que es de 50 µm y 62.5 µm. Sin embargo la fibra multimodo alcanza menores distancias y tiene un ancho de banda reducido.

Existen dos tipos de fibra óptica Multimodo que son: de índice gradual y de índice escalonado. Como se indica en la figura 1.20.

La fibra óptica Multimodo de índice gradual es la más utilizada porque su índice de refracción no es constante y tiene menor dispersión modal.

Figura 1. 20 Fibra Óptica Multimodo. [20]

Fibra Óptica Monomodo

La fibra Monomodo tiene un núcleo de menor diámetro por el cual transmite un único modo como se puede observar en la figura 1.21, es utilizada para cubrir mayores distancias, a diferencia de las fibras multimodo, tiene menor atenuación y soportan una mayor tasa de transmisión.

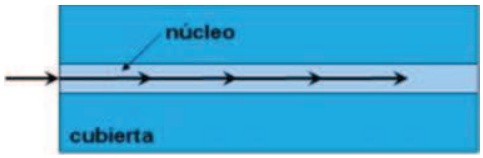


Figura 1. 21 Fibra Óptica Monomodo. [21]

1.3.2 NORMAS Y ESTÁNDARES ACTUALES[22]

Todo sistema de cableado estructurado cumple con normas y estándares dictados por los siguientes organismos.

ANSI (*American National Standards Institute*)

Esta organización es privada sin fines de lucro fundada en 1918, encargada de administrar y coordinar la estandarización del sector privado de los Estados Unidos.

EIA (*Electronics Industry Association*)

Es la encargada de desarrollar normas y publicaciones sobre componentes eléctricos, información electrónica y telecomunicaciones.

[22] [FT3] Folleto Sobre Cableado Estructurado. Ing Soraya Sinche, 2008

TIA (*Telecommunications Industry Association*)

Es una asociación de comercio que desarrolla normas para cableado industrial y para algunos productos de telecomunicaciones.

IEEE (*Institute of Electrical and Electronics Engineers*)

Es la más grande que existe a nivel mundial, fue creada en el año de 1884 para trabajar sin fines de lucro, está formada por ingenieros con conocimiento en las nuevas tecnologías de las diferentes especialidades.

ISO (*International Organization for Standardization*)

Esta organización tiene una sede en cada país miembro que la representa a nivel nacional, estos países miembros desarrollan estándares a nivel local.

El modelo de referencia OSI para conexión de redes de datos fue creado por la ISO.

Las normas que se utilizan para el diseño e implantación de un sistema de cableado estructurado son ANSI/EIA/TIA. Dentro de estas están los siguientes estándares:

ANSI/EIA/TIA 568C: este es el estándar actual utilizado para realizar el diseño e implantación de un SCE, el cual tiene todas las especificaciones del anterior estándar que es ANSI/EIA/TIA 568B y sus versiones.

ANSI/EIA/TIA 569 A: esta norma es utilizada para el enrutamiento del cableado en edificios comerciales.

ANSI/EIA/TIA 606: este es el estándar para la administración de las telecomunicaciones en los edificios comerciales.

ANSI/EIA/TIA 607: requerimientos para conexiones y puesta a tierra para telecomunicaciones.

1.3.3 ELEMENTOS DE UN SISTEMA DE CABLEADO ESTRUCTURADO[23]

En la figura 1.22 se detalla los subsistemas que tiene un sistema de cableado estructurado.

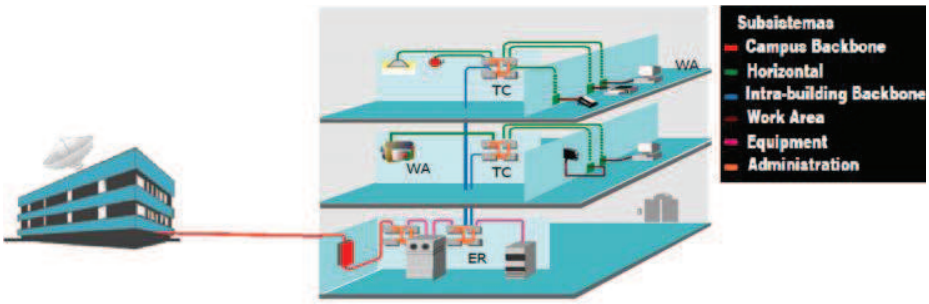


Figura 1. 22 Subsistemas de un Sistema de Cableado Estructurado. [22]

1.3.3.1 Área de trabajo

El área de trabajo comprende desde la salida de telecomunicaciones hasta las tarjetas NIC de los equipos los cuales pueden ser. Computadoras, impresoras, scanner etc.

Este subsistema no está diseñado de forma permanente por lo que tiene flexibilidad a la restructuración de los equipos de comunicación.

---

[23] [PW21] http://materias.fi.uba.ar/6679/apuntes/CABLEADO_ESTRUC.pdf
[PT3] Folleto Sobre Cableado Estructurado. Ing Soraya Sinche, 2008
[PW22] http://www.uazuay.edu.ec/estudios/electronica/proyectos/cableado_estructurado.pdf

Los componentes de este subsistema no se encuentran regulados por los estándares. Dentro de los cuales están los patch cord y los adaptadores.

Patch Cord es el cable que conecta los dispositivos con la salida de telecomunicaciones, es multifilar y debe tener las mismas características de transmisión del cableado horizontal a diferencia de su atenuación, tiene una longitud máxima de 3 metros y utiliza conectores RJ-45. Ver figura 1.23

Patch Cord de fibra óptica que puede ser monomodo o multimodo de acuerdo al utilizado en todo el sistema de cableado.

Figura 1. 23 Área de Trabajo. [23]

1.3.3.2 Cableado Horizontal

El cableado horizontal está definido desde el armario de telecomunicaciones hasta el área de trabajo.

Este subsistema tiene una topología estrella y está formado por cables de cobre o fibra óptica, salidas de telecomunicaciones, equipos o hardware de conexión y cross connects.

Al realizar el diseño y la implementación del cableado horizontal se debe tomar en cuenta que no se puede realizar puentes o empalmes a lo largo del trayecto del

cableado. Además, se debe verificar que el cableado de datos esté alejado del cableado eléctrico porque genera altos niveles de interferencia electromagnética.

En el cableado horizontal se puede tener una distancia máxima de 90 m independiente del tipo de medio de transmisión, tomando en cuenta las respectivas holguras que se deben dejar tanto en el armario de telecomunicaciones que es de 2 a 3 metros como en la salida de telecomunicaciones donde se debe dejar 30 centímetros si es cobre o 1 metro si se trata de fibra óptica.

Algunas de las características que tiene este subsistema es que solo puede existir un punto de consolidación o uno de transición desde closet de telecomunicaciones hasta el área de trabajo. La diferencia entre estos dos puntos es que el PC requiere de una conexión adicional. En la figura 1.24 se detalla las máximas distancias.

Los “puntos de Consolidación” son lugares de interconexión entre cableado horizontal proveniente del closet de telecomunicaciones y cableado horizontal que termina en las áreas de trabajo.

Dado que el cableado horizontal es “rígido”, la idea es tener un punto intermedio que permita, en caso de reubicaciones de oficinas, re-cablear únicamente parte del cableado horizontal (el que va desde el punto de consolidación hasta las nuevas estaciones de trabajo).

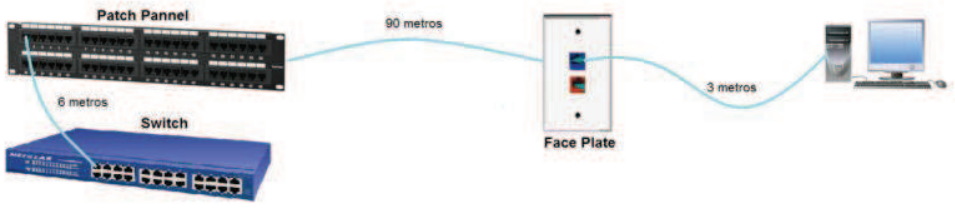


Figura 1. 24 Cableado Horizontal. [24]

1.3.3.2.1 Elementos del cableado Horizontal

El cableado horizontal está compuesto por elementos tales como: Patch Pannels o paneles de conexión, los que permiten la interconexión entre el cableado horizontal con los equipos activos de la red como switches, routers y hubs usando patch Cords de máximo 6 metros.

Existen una gran variedad de patch panels en el mercado que van desde 12, 24, 48 y 96 conexiones, los más utilizados por mayor flexibilidad y seguridad son los de 24 puertos. Como se indica en la figura 1.25

Figura 1.25 Patch Panel y Jack RJ-45. [25]

Salida de telecomunicaciones también conocida como *face plate* está ubicada en el Área de Trabajo y debe tener como mínimo dos salidas: una para datos y otra para voz. Como se muestra en la figura 1.26

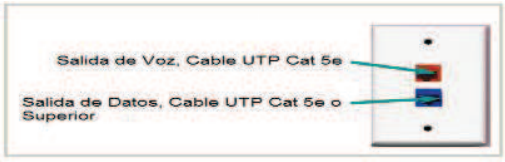


Figura 1. 26 Face Plate. [26]

Patch Cord para interconexión tienen una longitud máxima de 6 metros y permiten conectar los equipos activos de la red a los paneles de conexión. Ver figura 1.27

Figura 1. 27 Patch Cord de cobre y fibra. [27]

El tipo de cable utilizado en el cableado horizontal según la norma ANSI/TIA/EIA 568 es el siguiente.

- UTP Cat 5e, 6 y 6A con una impedancia característica de 100 Ω y una distancia máxima de 100 metros
- Fibra óptica multimodo de 62.5/125 µm

1.3.3.3 Cableado Vertical

Este subsistema es también conocido como cableado de BACKBONE, es el que interconecta los closets de telecomunicaciones con el cuarto de equipos y la infraestructura de entrada como se indica en la figura 1.28.

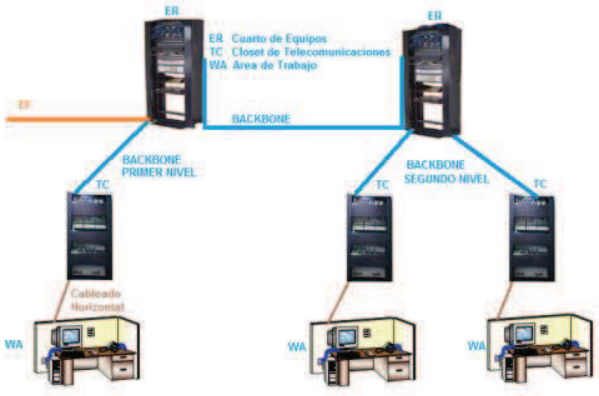


Figura 1. 28 Cableado vertical. [28]

Los elementos que forman el cableado vertical son: Cable de cobre o fibra óptica, conexiones cruzadas, hardware de conexión y cables de enlace.

Según la norma ANSI/TIA/EIA 568C los tipos de cables reconocidos son los siguientes.

- Cable UTP de 100 Ω
- Fibra óptica multimodo de 62.5/125μm o 50/125μm
- Fibra óptica monomodo

Las máximas longitudes que especifica el estándar con estos cables dependen del tipo de servicio de voz o datos, como se especifica en la tabla 1.8

TIPO DE CABLE	LONGITUD (M)	
	Voz	Datos
UTP	800	90
Fibra óptica monomodo	3000	
Fibra óptica multimodo	2000	

Tabla 1. 8 Longitud Máxima de los cables para BACKBONE. [8]

1.3.3.4 Closet de telecomunicaciones

El closet de telecomunicaciones debe tener un espacio exclusivo dentro del edificio, en este se realizan las interconexiones primarias y se encuentran algunos equipos activos de la red como: switches y hubs.

En el closet se realizan las conexiones cruzadas mediante el uso de hardware de conectividad para poder conectar el cableado horizontal con el vertical y tiene los siguientes elementos:

- Cable horizontal y vertical
- Regletas 110 o patch pannel
- Patch Cord

- Racks
- Organizadores horizontales y verticales
- Regleta de alimentación AC

El dimensionamiento del closet de telecomunicaciones según la norma EIA/TIA 568 específica que se debe tener un closet por cada 200 estaciones de trabajo y si se excede los 90 metros que es la máxima distancia.

1.3.3.5 Cuarto de equipos

En cuarto de equipos es la parte central del cableado estructurado porque a éste llega todo el cableado vertical que conecta a los closets de telecomunicaciones. Además, se encuentran los equipos más importantes de telecomunicaciones como son centrales telefónicas, servidores y routers. Por lo que se debe tomar en cuenta algunos parámetros como son: ventilación, control de fuego, control de acceso e iluminación.

1.3.3.5.1 Área del cuarto de equipos

En la tabla 1.9 se especifica el área que debe tener un cuarto de equipos de acuerdo al número de estaciones de trabajo que estén conectadas.

ESPACIO DESIGNADO DE ACUERDO AL NÚMERO DE ESTACIÓN DE TRABAJO	
Número de estaciones de trabajo	**Área del cuarto de equipos (m^2)**
1-100	14
101-400	38
401-800	74
801-1200	111

Tabla 1. 9 Área del Cuarto de equipos. [9]

Sistema de ventilación.- Debe disponer con un sistema HVAC (Heating, Ventilating and Air Conditioning) para obtener la temperatura recomendada que está en el rango de 18°C a 27°C con un porcentaje de humedad del 30 al 55% según la norma EIA/TIA 569.

Dimensiones de altura.- No se deben instalar techos falsos en un cuarto de equipos y tiene que tener una altura de 2.4 a 3 metros.

Localización.- El lugar donde se va a implementar el cuarto de equipos debe estar lejos de fuentes que puedan causar interferencia electromagnética como son motores, transformadores, etc.

Adicionalmente, un cuarto de equipos debe contar con un sistema de seguridad, ups, sistema de puesta a tierra, pararrayos, ventilación y tener una instalación eléctrica dedicada.

1.3.3.6 Acometida de Entrada

Son las conexiones por las que ingresan los servicios de comunicación de otros edificios, pueden estar localizadas en el Cuarto de Equipos y utiliza una conexión cruzada para conectarse con el backbone principal.

1.3.3.7 Sistemas de Puesta a Tierra

Los sistemas de comunicación requieren de un sistema de aterrizaje que les permita descargar las corrientes indeseables, electrostáticas, de ruido y alta frecuencia.

Según la norma EIA/TIA 607 se debe tener un TGB (Telecommunications Grounding Busbar) por cada cuarto de telecomunicaciones y conectarse mediante un TBB (Telecommunications Bonding Backbone) al TMGB (Telecommunications Main Grounding Busbar) principal.

1.4 CALIDAD DE SERVICIO (QoS)

QoS o Calidad de Servicio garantiza la transmisión de información a ciertas aplicaciones tales como voz y vídeo en un tiempo dado (*throughput*). Es la capacidad de dar un buen servicio. La calidad de servicio se logra en base a los siguientes criterios:

- La supresión de silencios otorga más eficiencia a la hora de realizar una transmisión de voz, porque se aprovecha mejor el ancho de banda.
- Compresión de cabeceras aplicando los estándares RTP/RTCP.
- Priorización de los paquetes que requieran menor latencia. Las tendencias actuales son:

  - ☐ CQ (*Custom Queuing*). Asigna un porcentaje del ancho de banda disponible.
  - ☐ PQ (*Priority Queuing*). Establece prioridad en las colas.
  - ☐ WFQ (*Weight Fair Queuing*). Asigna la prioridad al tráfico de menos carga.
  - ☐ DiffServ (*Differentiated Services*): proporcionan mecanismos de calidad de servicio para reducir la carga en dispositivos de la red a través de un mapeo entre flujos de tráfico y niveles de servicio.

1.5 TELEFONIA IP[24]

Con el avance de la tecnología y especialmente de las redes IP actualmente existen técnicas que permiten integrar múltiples servicios en una sola infraestructura de red. La telefonía IP permite realizar llamadas telefónicas sobre la red de datos utilizando un computador, un gategay y teléfonos IP como se indica en la figura 1.29.

Al realizar una llamada utilizando telefonía IP se realizan los siguientes pasos básicos, la señal de voz es digitalizada y encapsulada en paquetes IP para luego ser enviada por la red hasta su destino donde los paquetes son ensamblados y la señal digital es transformada en señal analógica.

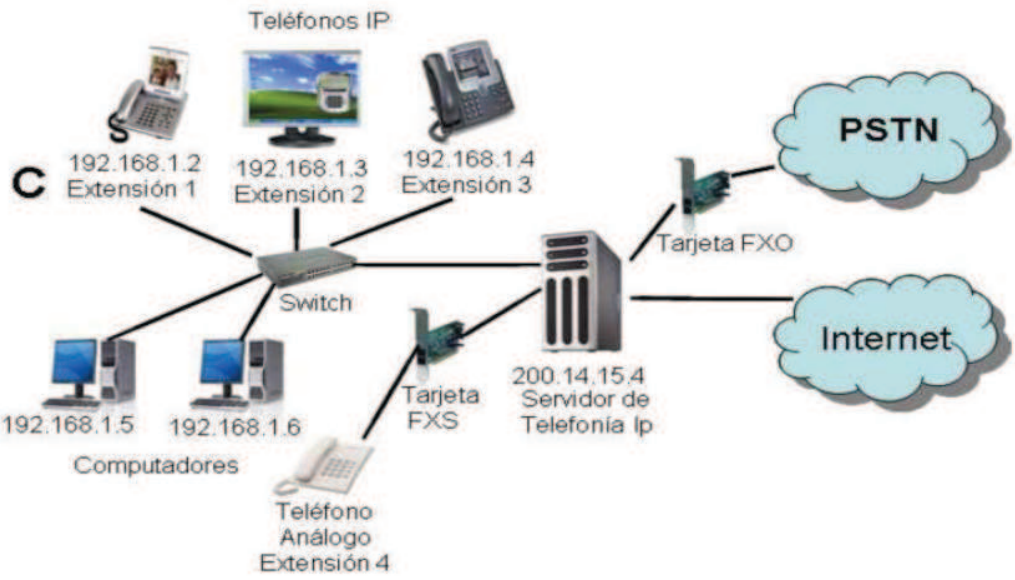


Figura 1. 29 Telefonía IP. [29]

[24] [T3] Ings. Diana Lovato y Luis Cadena, Diseño de la Red de Telefonía IP y su integración con la red de datos para la comunicación de la matriz con las sucursales de Importadora Vega S.A., pág 21
http://www.telefoniavozip.com/voip/que-es-la-telefonia-ip.htm

1.5.1 CLASES DE TELEFONÍA IP

Dentro de la telefonía IP se puede tener telefonía IP Privada que es utilizada en una Intranet y telefonía IP pública que es utilizada en conjunto con la red PSTN.

1.5.1.1 Telefonía IP Privada

Es implementada en la intranet de las empresas para dar servicio solo a los usuarios internos como se muestra en la figura 1.30

Figura 1. 30 Telefonía IP Privada. [30]

1.5.1.2 Telefonía IP Pública

En esta telefonía se hace la interconexión entre la PSTN y la red Internet para realizar y recibir llamadas desde y hacia cualquier teléfono ya sea analógico o teléfono IP. Como se indica en la figura 1.31

Figura 1. 31 Telefonía IP Pública. [31]

1.5.2 INTERFACES ATA

Son interfaces utilizadas en la telefonía IP para convertir la señal analógica a digital y viceversa, se tiene dos clases de interfaces que son: FXO y FXS.

1.5.2.1 FXO (*Foreign Exchange Office*)

Este interfaz es el que realiza la comunicación entre la PSTN y la red IP por lo que es conocido como Gateway, se encarga de la conversión de la señal analógica a digital y viceversa, generalmente se encuentra localizado en el servidor IP.

1.5.2.2 FXS (*Foreign Exchange Station*)

Este interfaz o tarjeta permite la conversión analógica a digital y viceversa por lo que es utilizado para conectar un teléfono convencional a una red IP.

1.5.3 PROTOCOLOS DE SEÑALIZACIÓN[25]

Estos protocolos son los encargados de gestionar el establecimiento de la comunicación y la administración de los mensajes. En VoIP existe una gran variedad de protocolos pero los más relevantes son SIP y H323.

1.5.3.1 H.323

El estándar H.323 define un conjunto de normas y protocolos recomendados por la ITU-T que permiten el envió de contenidos multimedia por una red IP, por lo que es

[25] [PW8] www.it.uc3m.es/~jmoreno/articulos/protocolssenalizacion.pdf

utilizado para telefonía IP y videoconferencia sobre IP. Este estándar no garantiza calidad de servicio pero si admite pasarelas con lo que se puede usar más de un canal para cada aplicación. Además, es independiente de la topología de red utilizada.

1.5.3.1.1 Componentes de H.323

H.323 define algunos componentes como terminales que son los encargados de negociar el canal y su capacidad, Gateway, gatekeeper y MCU (*Multipoint Control Unit*), la definición de estos componentes y sus funciones se las realiza a continuación. Como se indica en la figura 1.32

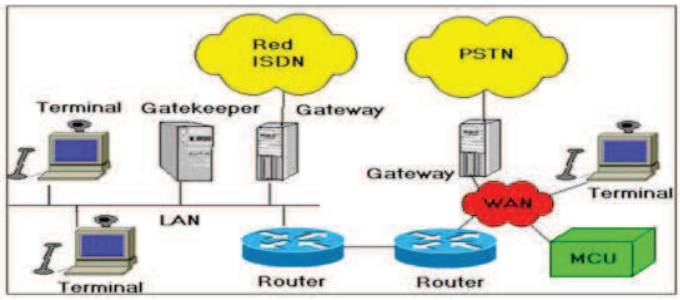


Figura 1. 32 Componentes de H.323. [32]

Terminales.- Estos son los puntos finales también llamados ***Endpoints***, estos dispositivos permiten establecer comunicación bidireccional en tiempo real de voz, datos y video.

Los terminales H.323 deben soportar codificación y decodificación de los formatos de audio y algunos códec como son H.261.

Gateways.- El Gateway H.323 trabaja en conjunto con el gatekeeper para realizar la interconexión de los terminales H.323 de la red IP con los terminales de una red

PSTN o red VoIP basada en el protocolo SIP. En general el propósito del Gateway es permitir la comunicación entre los diferentes protocolos.

Gatekeeper.- Es la parte principal de la estructura de VoIP, realiza la administración de los terminales, gateways y MCU dentro de una zona. Además, es el encargado de la traducción de las direcciones, control de ancho de banda y autorización de llamada.

MCU.- Es un punto final encargado de realizar una videoconferencia entre diferentes terminales, asignando los diferentes canales para voz, datos y video. Además, realiza la negociación de los códec para la transmisión de audio o video utilizados en la videoconferencia.

1.5.3.1.2 Protocolos de H.323

El estándar H.323 especifica los protocolos detallados en la figura 1.33 que son utilizados para realizar diferentes funciones como la administración de los mensajes, utilización de códec, establecimiento y finalización de la comunicación.

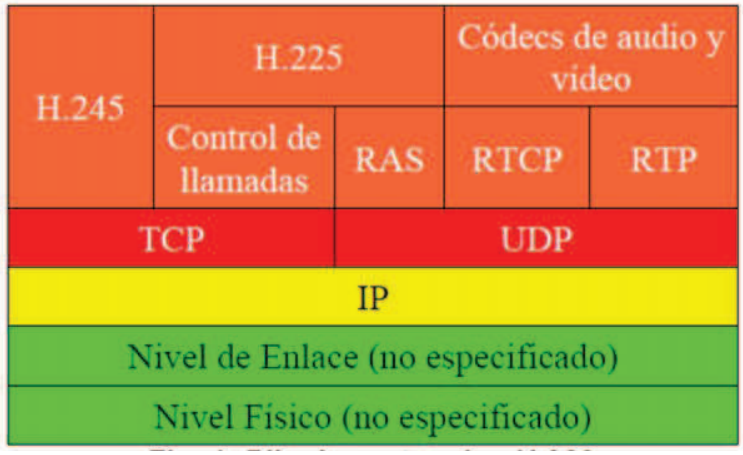


Figura 1. 33 Stack de protocolos utilizados por H.323. [33]

1.5.3.1.3 Protocolo H.245

Este protocolo de señalización es utilizado para el control de comunicación multimedia y realiza las siguientes funciones que son: apertura y cierre de los canales lógicos, negociación sobre la capacidad de transmisión entre el transmisor y el receptor, determina que terminal actúa como maestro o como esclavo.

1.5.3.1.4 Protocolo H.225

Es un protocolo de comunicación utilizado para VoIP y videoconferencia encargado de la señalización de llamadas y señalización RAS (*Registration, Admision and Status*).

En la señalización de llamadas realiza todos los procesos involucrados en el establecimiento, control y finalización de una llamada, se basa en la recomendación Q.903.

En la señalización RAS realiza las siguientes funciones como son, control de ancho de banda, descubrir todos los gatekeeper conectados, localización, registrar puntos finales, establecer y verificar el estado de la comunicación entre el Gateway y un Gatekeeper.

1.5.3.1.5 Protocolos RTP y RTCP

Estos protocolos son utilizados para el transporte y control de medios, trabajan en tiempo real y sobre el protocolo UDP.

RTCP (*Protocolo de Control en Tiempo Real*) realiza un monitoreo de las conexiones RTP obteniendo información de los paquetes enviados y recibidos para verificar la calidad de servicio (QoS). Mientras RTP (*Protocolo en Tiempo Real*) transporta flujos de audio y video de un terminal a otro.

1.5.3.2 SIP (*Session Initiation Protocol*)

Este protocolo trabaja en la capa aplicación del modelo OSI y se encarga de los procesos que conllevan el establecimiento, mantenimiento y finalización de las sesiones entre los usuarios. Se encuentra definido en el RFC 3261.

SIP no especifica un sistema de comunicación, solo ofrece un conjunto de primitivas que las aplicaciones pueden utilizar para implementar algún servicio de voz o videoconferencia. A continuación se detallan los componentes lógicos de SIP que son implementados por TCP y UDP

1.5.3.2.1 Agente de Usuario

Este agente es el encargado de la inicialización y de la terminación de las sesiones, trabaja con una arquitectura cliente-servidor, donde el cliente y el servidor realizan las siguientes funciones; el cliente hace las peticiones al servidor y el servidor envía un mensaje de notificación de la petición enviada por el cliente y responde a las peticiones solicitadas por los usuarios.

1.5.3.2.2 Servidor de Redirecciones

Este servidor trabaja en conjunto con el agente cliente, es el encargado de recibir, aceptar y responder a las peticiones realizadas por los agentes clientes.

1.5.3.2.3 Servidor Proxy

Este servidor es el encargado de realizar el encaminamiento de las peticiones hacia su destino para lo cual realiza un análisis de la cabecera de los mensajes y adiciona información indicando que es el que realiza la petición y la envía al cliente, al recibir la respuesta del cliente quita la información adicional de la cabecera de los mensajes y la reenvía al cliente que realizó la petición.

1.5.3.2.4 Servidor de Registro

Utiliza una base de datos para almacenar información relacionada a la localización de los usuarios que realizan las peticiones para lo cual los terminales tienen que registrarse en este servidor permitiendo flexibilidad.

1.5.3.2.5 B2BUA (Back to Back User Agent)

Realiza funciones similares al servidor proxy procesando peticiones de invitación y determina como realizar llamadas salientes, se diferencia del proxy en que realiza un mayor control del estado de las llamadas mediante el envió de peticiones y respuestas.

1.5.4 VENTAJAS DE LA TELEFONÍA IP

Utilizar telefonía IP en lugar de la telefonía tradicional tiene las siguientes ventajas.

- Como gran ventaja es utilizar una sola infraestructura de red para enviar voz y datos sin necesidad de hardware adicional disminuyendo costo y centralizando la administración de la red.

- Se tiene mayor flexibilidad y movilidad para los usuarios que pueden realizar y recibir llamadas desde cualquier lugar donde exista conectividad a la red de Internet.

- Se tiene mayor seguridad y privacidad en la realización de las llamadas gracias a las nuevas tecnologías que permiten autenticación y codificación de los datos enviados por la red.

- Es una arquitectura que permite flexibilidad y escalabilidad, con poca inversión se puede incrementar el número de usuarios.

1.5.5 DESVENTAJAS DE LA TELEFONÍA IP

En la actualidad existen pocas desventajas al usar telefonía IP esto es debido al constante desarrollo de las nuevas tecnologías que permiten optimizar el envió de datos por la red.

- Como principal desventaja son los retrasos y perdida de datos que pueden existir debido a que los paquetes son enviados por diferentes rutas.

- Al utilizar software de teléfonos en lugar de teléfonos IP la comunicación se ve limitada a las características que tenga la PC.

- VoIP requiere de una conexión eléctrica. En caso de un corte eléctrico a diferencia de los teléfonos VoIP los teléfonos de la telefonía convencional siguen funcionando.

1.6 VIDEO VIGILANCIA IP[26]

El uso de vigilancia IP se ha incrementado notablemente como una solución de seguridad y control para las Instituciones. Antes de la aparición de la tecnología digital de vigilancia IP, se la realizaba utilizando CCTV (*Circuito cerrado de TV*) que es analógica y requiere infraestructura adicional para su instalación generando un alto costo utilizando un deficiente sistema de almacenamiento.

Con el uso de las cámaras IP se tiene mejor resolución en las imágenes, se cubre mayor cobertura y permiten enviar señales de control que son utilizadas para el manejo del zoom. Además, existen cámaras con sensores de movimiento con lo cual se optimiza el almacenamiento del video requiriendo menor capacidad en los discos.

1.6.1 COMPARACIÓN DE CCTV Y VIGILANCIA IP

En la tabla 1.10 se realiza una comparación entre estas dos tecnologías que pueden ser empleadas para la implementación de un sistema de seguridad.

	CCTV	**VIGILANCIA IP**
Coste	Esta tecnología utiliza como medio de transmisión cable coaxial y de acuerdo al lugar donde se quiera implementar la seguridad se necesita mayor cantidad de cable.	Utiliza el mismo medio de transmisión de la red de datos como el cable UTP. Además, permiten la conexión mediante medios inalámbricos con lo que se puede cubrir sitios sin acceso sin necesidad de utilizar grandes cantidades de cable.

[26] [PW31] http://www.dlink.es/cs/Satellite?c=Guide_P&childpagename=DLinkEuropeES/DLGeneric&cid=1197380409000&p=1197318960420&packedargs=locale=1195806681347&pagename=DLinkEurope-ES/DLWrapper

	CCTV	VIGILANCIA IP
Resolución	Tiene una baja resolución en las imágenes.	Soporta una alta resolución de las imágenes, además estas cámaras tienen resolución en megapixeles lo que no es soportado por CCTV
Escalabilidad	No es adaptable fácilmente a nuevas tecnologías por lo que se requiere una gran inversión.	Es adaptable a nuevas tecnologías, es un sistema muy flexible porque se pueden instalar cámaras en cualquier lugar de la red que se requiera.
Funcionalidad	Muchas de las cámaras no tienen aplicaciones actuales como el manejo de zoom que es muy importante al instante de grabar un evento importante.	Permiten controlar control de acceso, alarmas y gestión de tráfico mediante el uso de cámaras inteligentes. Se puede enviar señales de control las cuales permiten la rotación de las cámaras y el manejo del zoom Se puede acceder de forma remota a las cámaras en tiempo real desde cualquier parte donde exista conexión a Internet.

Tabla 1. 10 Comparación de CCTV con Vigilancia IP. [10]

1.7 SERVIDORES[27]

1.7.1 SERVIDOR DE ARCHIVO

Este servidor almacena múltiples tipos de archivos para que estén disponibles para todos los usuarios que requieran este servicio.

[27] http://es.wikipedia.org/wiki/Servidor

1.7.2 SERVIDOR DE IMPRESIONES

Este servidor controla varias impresoras y permite la compartición de este dispositivo a toda la red. Disminuyente el costo de adquirir una impresora por cada usuario.

1.7.3 SERVIDOR DE CORREO

Se encarga de la administración de los mensajes internos y externos de la red local. Existen plataformas gratuitas para brindar este servicio como Zimbra que es un servidor de correo que ofrece las mismas o mejores características que un servidor propietario

1.7.4 SERVIDOR DE LA TELEFONÍA IP

Realiza funciones relacionadas a la telefonía IP, como almacenar los mensajes de voz, contestador automático, enrutamiento de las llamadas, control de la red entre otras. Este servidor debe ser dedicado solo para la central IP

1.7.5 SERVIDOR PROXY

Un Servidor Proxy se define como un PC o dispositivo que ofrece un servicio de red que consiste en permitir a los clientes realizar conexiones de red indirectas hacia otros servicios de red.

Este servidor generalmente trabaja simultáneamente como firewall operando en el nivel de red, actúa como filtro de paquetes, como en el caso de iptables, o también opera en el nivel de aplicación, controlando diversos servicios.

Una aplicación común es funcionar como caché de contenido de red principalmente HTTP, proporcionando en la proximidad de los clientes un caché de páginas y ficheros disponibles a través de la red en servidores HTTP remotos, permitiendo a los clientes de la red local acceder hacia éstos de forma más rápida y confiable.

1.7.6 SERVIDOR WEB

Permite el almacenamiento de imágenes y archivos para compartirlos en la red mediante la web, para que los usuarios tengan acceso a esta información de forma local o remota.

1.7.7 SERVIDOR DE VIDEO

Este dispositivo permite tener varias funciones en lo relacionado a la vigilancia IP como: almacenar video, enviar y recibir señales de audio, enviar señales de control para utilizar el zoom de las cámaras. Además, permite convertir una señal analógica en digital.

1.8 ANALIZADORES DE TRÁFICO

1.8.1 ETHERAPE[28]

Este es un software open source de Unix que permite realizar un monitoreo del tráfico que cursa por la red de forma gráfica, trabaja en la capa de enlace con los protocolos IP y TCP. Con esta herramienta se puede realizar un filtrado de tráfico.

[28] [PW32] http://insecure.org/tools/tools-es.html

1.8.2 IPTRAF[29]

IPtraf es un software libre que permite obtener información del tráfico IP y de las conexiones TCP de la red así como de sus interfaces, con lo cual se puede verificar el tráfico TCP y UDP

1.8.3 NMAP[30]

Es una herramienta multiplataforma que se utilizada para evaluar la seguridad que tiene una red de datos mediante el escaneo de puertos. Además, obtiene información del hardware, software y de puertos abiertos que hay en la red

1.8.4 NTOP[31]

Ntop es una herramienta que trabaja tanto en la plataforma de Linux como en Windows y permite controlar los usuarios, las aplicaciones y ayuda a detectar malas configuraciones en los equipos, mediante el monitoreo en tiempo real de la red.

Ntop tiene un servidor web donde se puede visualizar las estadísticas de tráfico que circula por la red, esta herramienta monitoriza algunos protocolos como TCP, UDP, ICMP, SNMP, POP, IMAP, ARP, entre otros.

1.8.5 NAGIOS[32]

Esta herramienta trabaja en la plataforma de UNIX, es utilizado para monitorizar y analizar equipos y servicios de la red.

---

[29] [PW33] http://es.wikipedia.org/wiki/IPTraf
[30] [PW23] http://nmap.org/
[31] [PW12] http://www.ntop.org/OpenSourceConf_Athens2008.pdf
[32] [PW24] http://www.nagios.org/documentation

Realiza la monitorización de los servicios y aplicaciones de la red, recursos de los host y de los servidores, estado de los puertos y monitorización remota, brindando a los administradores de la red datos suficientes para que puedan tomar decisiones con relación al crecimiento de red, vulnerabilidades actuales de los equipos, tráfico actual, eficiencia del sistema y gestión de los recursos.

1.8.6 WIRESHARE[33]

Esta herramienta multiplataforma que trabaja tanto en Unix como en Windows es un analizador de paquetes que circulan por la red, con wireshare se analiza el tráfico que circula por la red mediante el filtrado de información.

[33] http://www.ftp.ucv.ve/Documentos/Wireshark/Manual.doc

CAPÍTULO 2

ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED

CAPÍTULO 2

ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED

2.1 LA INSTITUCIÓN

La Unidad Educativa SANTA MARÍA D. MAZZARELLO es una Institución que ofrece a la comunidad una educación de calidad para los niveles de jardín hasta tercero de bachillerato.

Cuenta con la matriz ubicada al Sur de Quito entre las calles Delfín Treviño y Willian Shunk, como se muestra en las figura 2.1

Figura 2. 1 Ubicación de la Unidad Educativa Santa María D. Mazzarello. [1]

La Institución está constituida por 52 profesores, 11 trabajadores y 1000 estudiantes entre primaria y secundaria[34]. Cabe indicar que sólo se toma en cuenta como trabajadores al personal administrativo que son los que requieren de los servicios de la red de comunicación

2.1.1 MISIÓN INSTITUCIONAL[35]

La Unidad Educativa "Santa María Mazzarello" de Quito, forma niñas, niños y jóvenes del sector sur, como ciudadanas (os) activas (os), propositivas (os), autónomas (os), abiertas (os) y optimistas de la realidad cotidiana, con alto nivel académico vinculado a las tecnologías actuales, corresponsables con la familia, con la comunidad y cristianas (os) comprometidas (os) en la construcción de un orden social más humano; bajo la responsabilidad de todos los miembros de la Comunidad Educativa, iluminados por la vivencia de valores, la preventividad de Don Bosco y María Mazzarello.

2.1.2 VISIÓN INSTITUCIONAL[36]

La Unidad Educativa "Santa María Mazzarello" de Quito, será en los próximos 5 años, líder entre los centros educativos de las Hijas de María Auxiliadora y del país, mediante el dominio de la tecnología y la práctica de valores; con un equipo profesionalmente formado, competente, productivo y comprometido con la praxis salesiana.

Acorde a las innovaciones educativas y tecnológicas, haciendo de las estudiantes y los estudiantes el centro de toda intervención educativa; con una formación científica, técnica y con actitudes dinámicas críticas frente a la realidad y a los

[34] Rectora 2011, Sor Mercy Sanchez
[35] Agenda de la Unidad Educativa Santa María Mazzarello
[36] Agenda de la Unidad Educativa Santa María Mazzarello

acontecimientos, con capacidad de comprometerse en opciones de servicio a los demás.

2.2 DESCRIPCIÓN DE LA RED DE LA INSTITUCIÓN

2.2.1 TOPOLOGÍA DE LA RED ACTUAL

La red de datos tiene una topología en estrella que se detalla en la figura 2.2, el sistema de cableado estructurado en los departamentos de Secundaria y Primaria está diseñado de acuerdo a la norma ANSI/EIA/TIA 568-B pero no la cumple en su totalidad, la norma ANSI/EIA/TIA 568-B es la que se utiliza para el diseño de sistemas de cableado estructurado aplicable para edificios comerciales y oficinas.

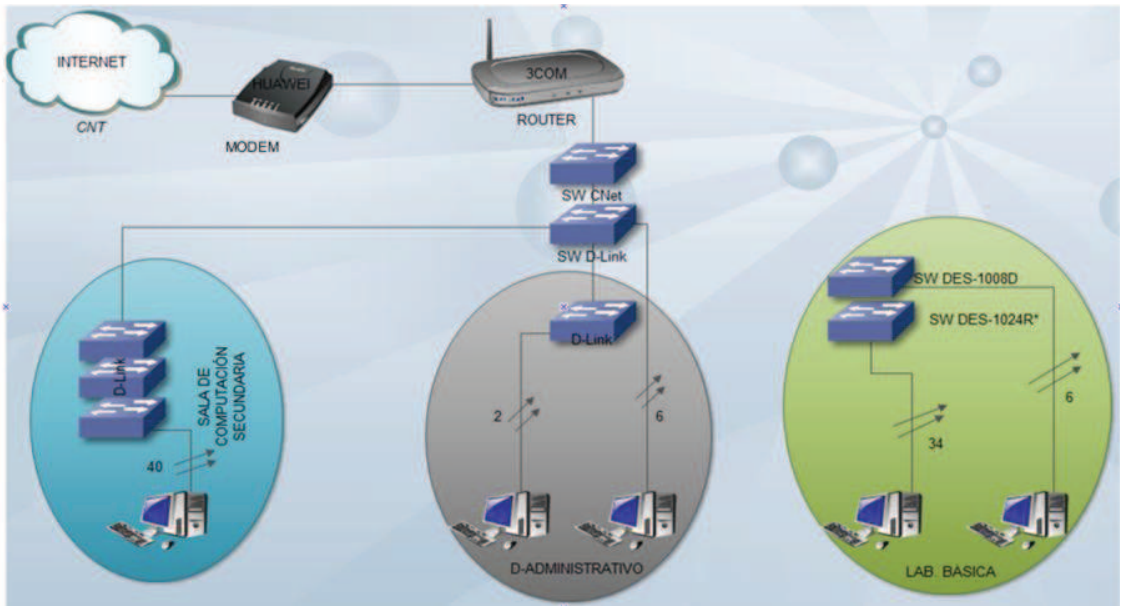


Figura 2. 2 Red de datos Actual. [2]

El laboratorio de Básica no está conectado a la red de la Institución por lo que no cuenta con Internet, CNT presta el servicio de Internet utilizando la línea telefónica

conectada a un modem Huawei el cual se conecta mediante un cable UTP Cat 5e al router.

El cuarto de equipos ubicado en el departamento administrativo está el router inalámbrico de marca 3com el cual provee los servicios Dns y Dhcp, a este dispositivo está conectado un switch Cnet que está conectado a un switch de marca D-Link que conecta el Backbone del laboratorio de Secundaria y todos las computadoras de los usuarios administrativos.

2.2.2 CABLEADO ESTRUCTURADO

El análisis del cableado estructurado se lo realizará describiendo el estado en que se encuentra cada elemento del mismo.

2.2.2.1 Área de Trabajo (WS)[37]

En el departamento administrativo existen 6 puntos de datos con cable UTP Cat 5E que no cumplen con las normas TIA/EIA-569 y TIA/EIA-606 ya que no cuentan con el respectivo enrutamiento horizontal. Además las salidas de telecomunicaciones están directamente conectadas a los equipos activos de la red (switch). Este departamento no cuenta con etiquetación para su administración. Ver imagen 2.3

Figura 2. 3 Red de datos Actual. [3]

[37] Informe 2010 sobre los equipos que están en red, Ing. Mirian Sarango

Los laboratorios de Secundaria y Primaria tienen instalado 40 y 34 puntos de datos mediante cable UTP Cat 5E, utilizan como enrutamiento canaletas empotradas en el piso, sin embargo no cumplen con la norma TIA/EIA-606. Cabe indicar que no todos los puntos están ocupados ya que algunas estaciones de trabajo no están conectadas.

En la tabla 2.1 se detalla el numero de *Jacks y Face* plates que están instalados en la Institución.

Departamentos	Jacks	Face Plate Dobles	Face Plate Simple
Administrativos	6	0	6
Lab. Secundaria	40	20	0
Lab. Básica	34	17	0
TOTAL	80	37	6

Tabla 2. 1 Número de host por Departamento. [1]

2.2.2.2 Equipos Activos de la Red

La Institución es una construcción de 3 pisos donde tiene distribuida la red de datos de acuerdo a la tabla 2.2, en ésta se especifica la distribución de host por departamento. Cabe, mencionar que no todos los host están conectados a la red de la de datos.

DEPARTAMENTOS	NÚMERO DE HOST
Administrativos	10
Lab. Secundaria	40
Lab. Primaria	40
Biblioteca	1
Catequesis	1
Salón	1
Trabajo Social	1

DEPARTAMENTOS	NÚMERO DE HOST
Inglés	1
Inspección	1
Nuevo laboratorio	12

Tabla 2. 2 Número de host por Departamento. [2]

Se realizó un análisis de los hosts que están actualmente conectados a la red de datos, obteniendo las características más importantes, que se detallan en la tabla 2.3.

DEPARTA_MENTO	NOMBRE	PROCESADOR	PLACA	MEMORIA	DISCO DURO	S.O
Administrativo	Colecturía	Intel Pentium 4	Biostar P4M800-MTA	512 MB DDR	250 GB Samsung	Windows XP
	Secretaría	DualCore 1600 MHz	Intel AAD79951-407	1024 MB DDR2	250 GB Samsung	Windows XP
	Rectorado	Intel(R) Core™2	Intel AAD78647-300	1024 MB DDR2	250 GB Samsung	Windows XP
	Vicerrectorado	Intel Pentium 4, 1600 MHz	ECS Versión. 1.0	1024 MB DDR	40 GB Samsung	Windows XP
	Coord. E. Básica	Intel Wolfale DualCore 2600 MHz	Intel AAD97573-306	2048 MB DDR	298 GB Samsung	Windows XP
	SIS1 (Internet)	Intel DualCore Pentium D	Intel AAD66165-302	512 MB DDR2	372 GB Samsung	Windows XP
	Dobe2	Intel Pentium 4, 1600 MHz	ECS Versión 1.0	1024 MB DDR	40 GB Samsung	Windows XP
	Dobe1	Intel Pentium 4, 1700 MHz	ECS Versión 1.0	1024 MB DDR	40 GB Maxtor	Windows XP
Laboratorio Secundaria	PC1	Intel Celeron 800 MHz	Biostar P4M90-M74	2048 MB DDR	40 GB Samsung	Windows XP
	PC2	Intel DualCore 2200 MHz	Intel AAD97573-205	1536 MB DDR	160 GB Samsung	Windows XP
	PC3	Intel DualCore 2200 MHz	Intel AAD97573-205	2048 MB DDR	160 GB Samsung	Windows XP

DEPARTA_ MENTO	NOMBRE	PROCESADOR	PLACA	MEMO RIA	DISCO DURO	S.O
Laboratorio Secundaria	PC4	Intel Pentium D DualCore	Intel AAD78647-300	2048 MB DDR2	160 GB Samsung	Windows XP
	PC5	Intel Pentium D DualCore	Intel AAD66165-302	2048 MB DDR2	160 GB Samsung	Windows XP
	PC6	Intel Pentium D DualCore	Intel AAD66165-303	512 MB DDR2	160 GB Samsung	Windows XP
	PC7	Intel Celeron 1600 MHz	Biostar Versión 1	2048 MB DDR2	232 GB Samsung	Windows XP
	PC8	Celeron 1600 MHz	Biostar Versión 1.0	1536 MB	232 GB Samsung	XP
	PC9, PC10	Intel Wolfale DualCore 2600 MHz	Intel AAD97573-306	4096 MB DDR	298 GB Samsung	Windows XP
	PC11-PC20	Intel (R) Core™ i3 3070 MHz	Intel AAE70933-501	2048 MB DDR	500 GB Samsung	Window s Vista
	PC21-PC29	Intel Wolfale DualCore 2600 MHz	Intel AAD97573-306	4096 MB DDR	298 GB Samsung	Windows XP
	PC31	Intel Pentium 4 3066 MHz	Biostar P4M800-M7A	1024 MB DDR	298 GB Samsung	Windows XP
	PC32, PC33	Intel Pentium D DualCore	Intel AAD78647-300	1536 MB DDR2	160 GB Samsung	Windows XP
	PC34, PC35	Intel DualCore	Intel AAE54511-205	2048 MB DDR2	80 GB Samsung	Windows XP
	PC36	Intel Pentium 4, 3000MHz	ECS Versión 1.0	1024 MB DDR	149 GB Maxtor	Windows XP
	PC37	Intel Pentium 4, 2800MHz	Intel AAC45439-301	2048 MB DDR	37 GB Maxtor	Windows XP
	PC38	Intel Celeron, 1800MHz	Biostar P4M266-PM12-TL	2048 MB DDR	80 GB Maxtor	Windows XP
	PC39	Intel Pentium 4, 2100MHz	ECS Versión 1.0	2048 MB DDR	250 GB Maxtor	Windows XP
	PC40	Intel Pentium 4, 1700MHz	ECS Versión 1.0	2048 MB DDR	40 GB Maxtor	Windows XP

Tabla 2. 3 Características de los Hosts. [3]

La Institución realizó una adquisición de nuevos computadores para la implementación de un nuevo laboratorio y para cambiar algunos que están obsoletos en el laboratorio de Básica, estos equipos tiene buenas características por lo que pueden trabajar con varias aplicaciones requeridas por los estudiantes.

Actualmente en algunas áreas de trabajo no se utiliza patch Cord, los computadores esta conectados directamente a los switches por lo que no cumplen con el estándar de cableado estructurado.

2.2.2.3 Equipos periféricos compartidos

La Institución cuenta con cuatro impresoras, que se encuentran ubicadas en el departamento administrativo, sus principales características se detallan en la tabla 2.4. Cabe, indicar que dichas impresoras no están conectadas en red por lo que es uso del usuario en particular.

UBICACIÓN	MARCA	MODELO	CARACTERÍSTICAS	IMAGEN
Coordinación	Epson Stylus	TX410	Documento con texto negro Hasta 34 ppm/cpm Documento con texto color Hasta 33 ppm/cpm Resolución Óptica 1200 x 2400 dpi Interpolada 9600 x 9600 dpi Interface y conectividad	
Rectorado	LexMark	X1185	Resolución (Scanner) = 600x1200 dpi Tipo de Impresora = Inyección térmica de tinta Interface = USB - Conector "B" Velocidad Impresión B/N [PPM] = 8.00 Velocidad Impresión Color [PPM] = 14.00 Resolución Horizontal Impresión B/N [DPI] = 2400 dpi Resolución Vertical (Impresión B/N) = 1200 dpi	

UBICACIÓN	MARCA	MODELO	CARACTERÍSTICAS	IMAGEN
Secretaría	Hp	P2015dn	Velocidad de Impresión: 27 ppm Resolución: 1200 dpi Procesador: 400 MHz Memoria: 32 MB Interfaces: Puerto Hi-speed USB 2.0 y Fast Ethernet Protocolos de red: TCP/IP	
Colecturía	Sharp	AL-2031	**Tipo escritorio** Capacidad de papale: 300 hojas Memoria: 32 MB **Copiadora** Velocidad max: 20cpm Resolución: 600 dpi Escala de grices: 256 niveles **Impresión** Velocidad max: 20ppm Resolución: 600 dpi Interfaces: USB 2.0 **Escaner de Color** Resolución: 600x600 dpi Protocolos: TWAIN,WIA y STI Interface: USB 2.0	

Tabla 2. 4 Equipos periféricos. [4]

2.2.2.4 Equipos de Conectividad[38]

Se dispone de los equipos de interconexión que están detallados en la tabla 2.5.

TIPO	UBICACIÓN	MARCA	MODELO	CANTIDAD	IMAGEN
Modem	Cuarto de Equipos	HUAWEI	Echolife HG250c Home Gateway	1	
Router	Cuarto de Equipos	3COM	Wireless 11N Cable/DSL Firewall Router	1	

[38] [PW35] www.3com.com

TIPO	UBICACIÓN	MARCA	MODELO	CANTIDAD	IMAGEN
Switch	Cuarto de Equipos	CNET	CNSH-800	1	
Switch	Cuarto de Equipos	D-Link	DES-1016D	4	
Switch	Lab. Secundaria	D-Link	DES-1016D	1	
			DES-1024R*	2	
Switch	Internet	D-Link	DES-1008D	2	
Switch	Lab. Básica	D-Link	DES-1024R*	1	
			DES-1008D	1	

Tabla 2. 5 Equipos de Conectividad. [5]

2.2.2.4.1 Características de los Equipos de Conectividad[39][40]

EQUIPO	CARACTERÍSTICAS	
Router	Requerimiento del sistema	Interfaces Ethernet 10/100BASE Soporta IEEE 802.11n 802.11g y 802.11b
	Número de Usuarios simultaneos Soportados	Total 253 de los cuales 32 son inalámbricos, la administración de los usuarios inalámbricos la realiza por filtrado MAC
	Configuración de Hardware	LAN: 4 autosensing 10BASE-T/100BASE-TX ports WAN: 1 autosensing 10BASE-T/100BASE-TX port
	WIRELESS NETWORKING	Wireless distribution system (WDS); WDS con WEP y WPA/WPA2 Soporta canales de 20 Mhz y 40 Mhz Soporta WMM (IEEE 802.11e) Filtrado de direcciones MAC

[39] [PW36] www.cnetusa.com
[40] [PW31] www.dlink.com

EQUIPO	CARACTERÍSTICAS	
Router	Banda de Operación	2.4 GHz
	Modulación	OFDM CCK
	Técnica de acceso al medio	CSMA/CA
	Pila de protocolos	Direccionamiento IP estático y dinámico DHCP server IP to MAC address binding NAT/PAT (with TCP and UDP), PPPoE, PPTP, IP, PAP, CHAP, MS CHAP, IPCP, SNTP, L2TP
	Routing y Networking	RIP 1 y 2 Ruteo estático IGMP snooping Puertos basados en VLANs
	Calidad de Servicio (QoS)	WMM Diferenciación de servicio (DiffServ); mark/remark up para 16 regles de mapeo
	Seguridad	Utiliza 128-bit WPA/WPA2 con TKIP/AES 40-/64-bit y 128-bit WEP para encriptación Soporta ACL Proxy ARP Virtual DMZ support (up to 8 servers) SSID Broadcast Disable MAC address filtering Full stateful packet inspection (SPI) firewall with DoS/DDoS protection NAT-T draft 2.0 SIP ALG
	VPN	IPSec, PPTP y L2TP/IPSec Encryption: DES, 3DES, AES-128, AES-256 Key management: IKE (main and aggressive modes) IKE keep-alive FQDN support PFS
	Administración	Browser-based administration Administración remota via HTTP E-mail alerts SNMP v1/2c (MIBII)
Switch CNet	Estándar	IEEE 802.3u: 100BASE-TX IEEE 802.3: 10BASE-T
	Número de puertos	8 puertos 100BASE-TX/10BASE-T
Switch DES-1016D	Estándar	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX ANSI/IEEE 802.3 IEEE 802.3x
	Número de puertos	16 puertos Fast Ethernet
	Modo de transmisión	Store and forward
Switch DES-1008D	Estándar	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX

EQUIPO	CARACTERÍSTICAS	
Switch DES-1008D	Estándar	ANSI/IEEE 802.3 IEEE 802.3x
Switch DES-1008D	Número de puertos	8 puertos
	Modo de transmisión	CSMA/CA
Switch DES-1024R*	Estándar	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE802.3x
	Número de puertos	DES-1024R: 24 x 10/100 Mbps
	Modo de transmisión	Store and forward

Tabla 2. 6 Características de los Equipos de Conectividad. [6]

En la tabla 2.6 se realiza una descripción de las características más importantes de los equipos de la red activa.

2.2.2.5 Servidores

Actualmente la red de la Institución no está utilizando servidores debido a que los dos servidores disponibles que tiene están apagados por daños técnicos. Las características de dichos servidores se detallan en la tabla 2.7.

MARCA	HP
Modelo	ProLiant ML350G5
RAM	Estándar: 512 MB (modelos entrada), 1 GB (modelos base); Máximo: 16 GB
Tipo/Velocidad de la RAM	PC2-5300F FB-DIMMs 667 MHz
HD	Tres discos de 146 GB
Procesador	Intel Xeon 5160 de doble núcleo, 3,00 GHz, Bus frontal (FSB) 1333 MHz [modelo base]
cache	4 MB L2 (1 x 4 MB) para procesadores Xeon Serie 5100
Ranuras de Expansión	3 PCI Express x8 (velocidad x4) 1 PCI-X 133 MHz de 64 bits 2 PCI-X 100 MHz de 64 bits
Sistema Operativo	Microsoft® Windows® Server 2003/R2, Centos 4.5

Tabla 2. 7 Servidores. [7]

Cabe indicar que no se tiene instalados servidores de correo, proxy, DHCP, DNS, firewall, web, base de datos, entre otros, que son indispensables para la seguridad como para la administración de la red.

El servidor DHCP y firewall están habilitados en el router 3Com.

2.2.2.6 Equipos UPS

Existen 3 ups localizados en el cuarto de equipos y en el departamento administrativo, los cuales se detallan en la tabla 2.8. Cabe, indicar que todos los computadores cuentan con regulador de voltaje individual de marca CAP y TDE.

MARCA	MODELO	POTENCIA	SALIDAS	IMAGEN
APC 1500	Back-UPS-RS	1500 W	8	
APC 1500	Back-UPS-RS	1500 W	8	
APC 1500	Back-UPS-RS	1500 W	8	
TDE	1000 W		6	
CDP	1200 W		6	

Tabla 2. 8 Características de los UPS. [8]

2.2.2.7 Listado de los Equipos

La Institución actualmente dispone de los siguientes equipos detallados en la tabla 2.9. En esta tabla se hace un listado de todos los equipos utilizados en la red de datos.

CANTIDAD	TIPO DE EQUIPO
108	Estaciones de trabajo
8	Switches
1	Router Inalámbrico
1	Modem
2	Servidores
3	UPS
3	Impresora
1	Central telefónica

Tabla 2. 9 Total de equipos utilizados. [9]

2.2.2.8 Cableado Vertical

La Institución no cuenta con cableado vertical o Backbone para todos los departamentos sólo para el laboratorio de Secundaria y en la sala de equipos para conectar el switch D-link con el router 3com.

El Backbone que une la sala de equipos con Secundaria es un cable UTP Cat 5E que está instalado sin elementos de enrutamiento.

Existe una instalación de Backbone entre la sala de equipos y el laboratorio de Primaria que excede la longitud máxima permitida que es de 100 m, está enrutada mediante una manguera de ¾ que se utiliza para instalaciones eléctricas. Cabe indicar que esta desconectada debido a las caídas recurrentes del servicio.

2.2.2.9 Sala de Equipos

El espacio físico disponible para el cuarto de equipos es de 4.25 m^2 en el cual se encuentran los servidores, Router, modem y switches como se muestra en la figura 2.4.

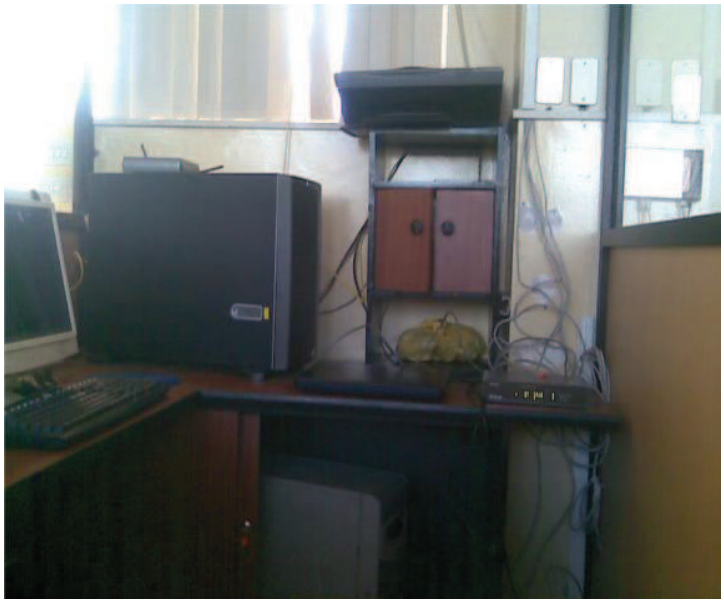


Figura 2. 4 Cuarto de Equipos. [4]

Como se puede apreciar este cuarto no cuenta con un rack ni con un adecuado sistema de etiquetación para el cableado, por lo que no cumple con la norma EIA/TIA-606, carece de organización tanto del cableado vertical como del horizontal para su administración. Además, no tiene instalado un sistema HVAC para mantener una adecuada temperatura para los equipos electrónicos.

Adicionalmente, cabe indicar que no cuenta con un sistema de puesta a tierra por lo que no cumple con la norma EIA/TIA-607: Sin embargo para la alimentación eléctrica de los dispositivos se utiliza dos UPS.

La acometida de entrada de Internet llega a esta sala mediante un cable telefónico que provee la CNT y termina en un modem al cual se conecta el router 3com para brindar el servicio de Internet.

Utiliza una dirección clase c para su direccionamiento que es la 192.168.1.0 con máscara de 24, se lo realiza de forma dinámica que ofrece el router 3com.

2.2.2.10 Armario de Telecomunicaciones

Existe un Armario de telecomunicaciones en los laboratorios de Secundaria y Primaria pero no cuentan con regletas ni organizadores. Además carecen de etiquetación para su administración. Como se indica en la figura 2.5

Figura 2. 5 Armario de Telecomunicaciones. [5]

2.3 SOFTWARE

En todos los computadores de la institución se tiene instalado el sistema operativo Windows en sus diferentes versiones como sistema principal. Además, todos tienen instalado las aplicaciones básicas como office en sus diferentes versiones, Adobe Acrobat y WinRar entre otras.

La Institución optó por el Sistema operativo ofertado por Microsoft debido a la fácil manipulación del software por su aplicación gráfica que tiene, esto facilita el aprendizaje de los estudiantes y el fácil manejo de esta herramienta para los docentes y administrativos.

Para proteger a los computadores de virus, gusanos y troyanos a los que están expuestos diariamente por estar conectados a la Internet, se utiliza el antivirus NOD32 en cada una de las estaciones de trabajo.

2.4 APLICACIONES

Actualmente, la Institución no cuenta con aplicaciones para el mejor desempeño de la administración de la Institución, como son correo electrónico interno, bases de datos y servidor para almacenamiento de archivos entre otras.

2.5 ANÁLISIS DE TRÁFICO DE LA RED

En la Institución se utiliza una dirección de red clase C que es la 192.168.1.0 con máscara 255.255.255.0, asignado mediante un servidor DHCP del router para el direccionamiento dinámico de las estaciones de trabajo conectadas a la red de datos.

Para analizar el tráfico interno se bebe tomar en consideración que no todas las estaciones de trabajo están conectadas a la red y que la Unidad Educativa no cuenta actualmente con aplicaciones internas, esto hace que el tráfico dentro de la red LAN sea bajo.

2.5.1 ANÁLISIS DEL ANCHO DE BANDA

La Unidad Educativa tiene contratado un enlace simétrico con CNT de 512 Kbps, el cual le asignó las siguientes direcciones públicas 190.152.0.146 hasta la 150 con la siguiente máscara 255.255.255.248 y para el Gateway se le asignó la dirección 190.152.0.145 mientras que para los DNS primario y secundario se le asignó las siguientes direcciones 200.107.10.52 y la 200.107.10.62, para verificar cual es el ancho de banda utilizado en cierto tiempo se utilizó IP Scanner, el cual dio como resultado lo detallado en la figura 2.6

Figura 2. 6 Análisis de la velocidad de transmisión. [6]

2.5.2 UTILIZACIÓN DE ALGUNAS HERRAMIENTAS PARA ANALIZAR EL TRÁFICO Y SEGURIDAD DE LA RED.

Para la determinación del tráfico y las vulnerabilidades de la red se utilizó algunas herramientas tales como con Ntop, wireshark, IP Scanner y nmap obteniendo los resultados detallados a continuación.

2.5.2.1 Utilizando la Herramienta WireShark

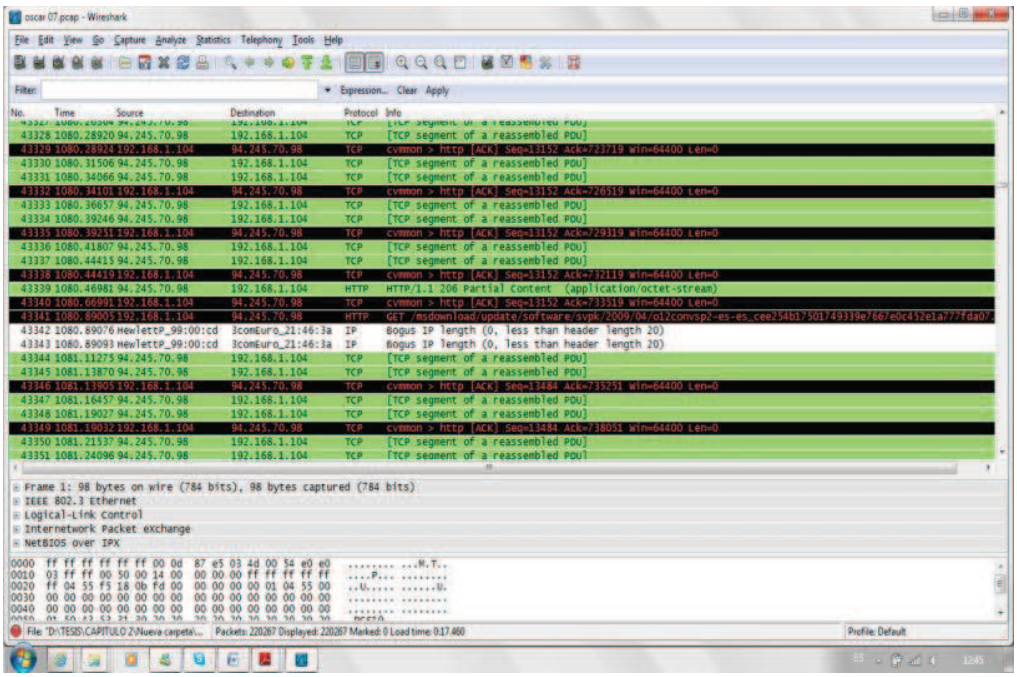


Figura 2. 7 Tráfico capturado con WireShark. [7]

Para ver el tráfico utilizando WireShark se realizó la siguiente conexión, se conectó una laptop al switch D-Link que está conectado al router 3Com y desde ahí se realizó las mediciones.

Cabe indicar que las mediciones se las realizó desde las 10:09 H hasta las 13:02 H, porque en este tiempo es cuando se tiene tráfico en la red, esto es debido a que la Unidad Educativa trabaja en horario diurno.

La medición se la realizó durante una semana, teniendo como resultado los datos especificados en la tabla 2.10

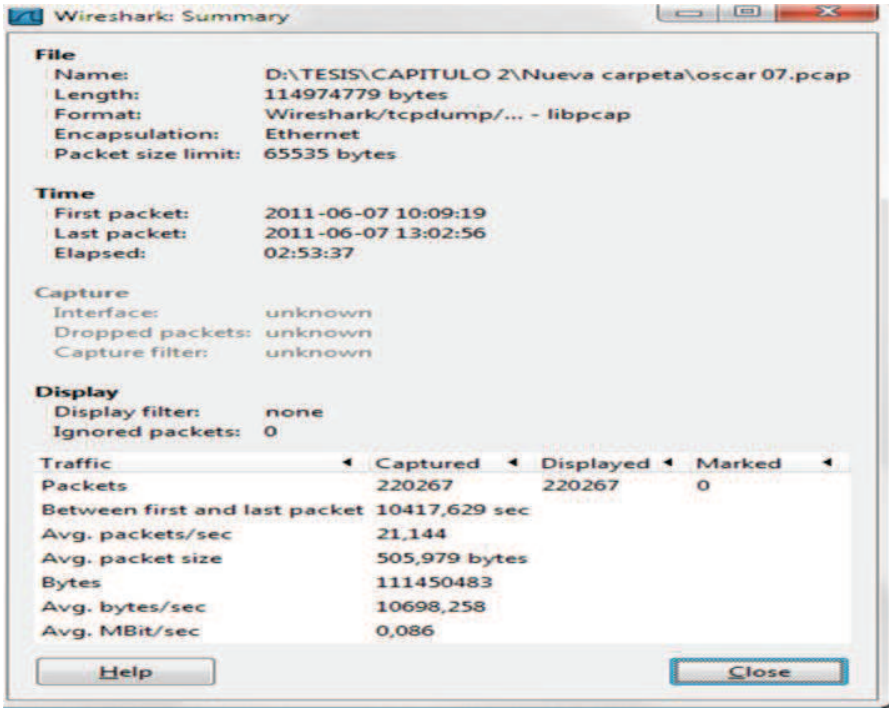


Figura 2. 8 Tráfico de la red. [8]

Con los valores obtenidos se calcula el valor pico utilizando la ecuación (2.1)[41].

[41] [T4] Ings. Darwin Cortez y Jaime López, Rediseño de la red de comunicaciones para la Universidad Estatal de Bolívar que soporte aplicaciones de voz, datos y videoconferencia. Año 2004.

$$\text{Capacidad} = \frac{\#\text{bits}}{\text{tiempo transmisión}} \quad (\text{Ec } 2.1)$$

$$\text{Capacidad} = \frac{\#\text{paquetesxtamaño(paquete)x8}}{\text{tiempo transmisión}}$$

$$\text{Capacidad} = \frac{220267\text{x}505.979\text{x}8}{10417.629}$$

$$\text{Capacidad} = 85.58 \text{ Kbps}$$

	LUNES	MARTES	MIÉRCOLES	JUEVES	VIERNES
Capacidad (Kbps)	76.84	74,56	85,58	67,49	59,87

Tabla 2. 10 Tráfico. [9]

CAPACIDAD DEL CANAL

Figura 2. 9 Capacidad del Canal. [9]

2.5.2.2 Utilizando la Herramienta Ntop

Utilizando la herramienta Ntop se obtuvo los siguientes valores de tráfico y el número de estaciones de trabajo conectadas con su respectivo tráfico generado.

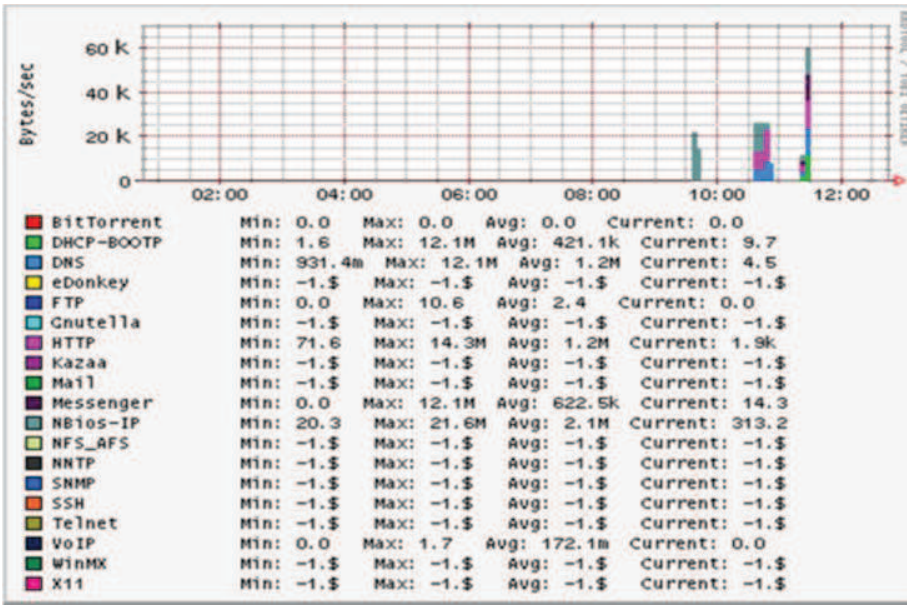


Figura 2. 10 Tráfico. [10]

Como se puede apreciar en la tabla y figura anterior se tiene un bajo tráfico esto es debido a que no se tiene servicios locales en la red. Cabe mencionar que el mayor tráfico se tiene en la hora que los estudiantes tienen computación en el laboratorio de Secundaria.

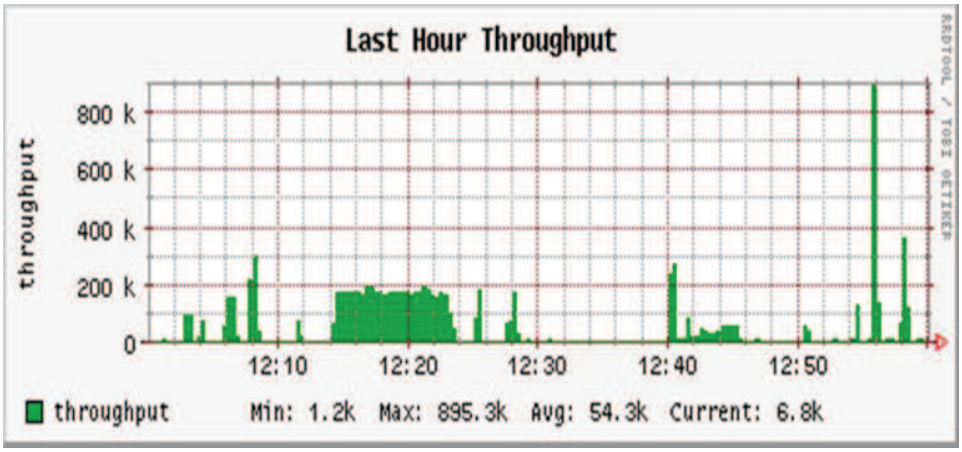


Figura 2. 11 Throughput de la red durante una hora. [11]

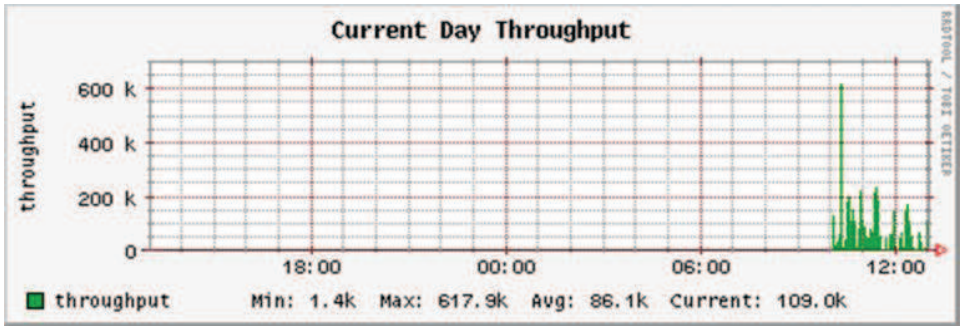


Figura 2. 12 Throughput de la red durante todo el día. [12]

En las figurar anteriores se puede observar el Throughput que se tiene en una hora determinada (figura 2.9) y durante todo un día (figura 2.10), es bajo debido a que son pocas las estaciones de trabajo que están conectadas en red.

En el **ANEXO A** se tiene algunos gráficos ilustrativos del Throughput de la red en diferentes horas del día en los que se puede observar el bajo tráfico de la red.

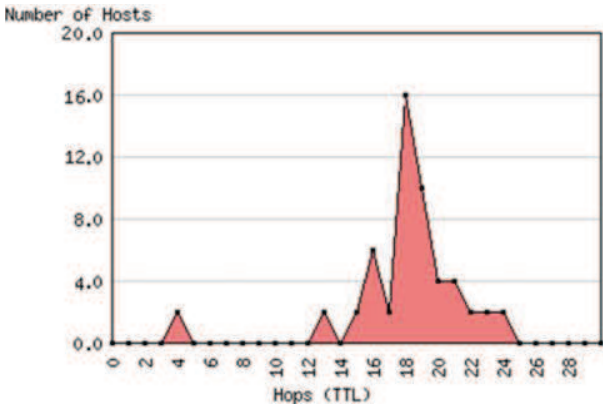


Figura 2. 13 Estaciones de trabajo conectadas. [13]

En esta figura se indica la estadística de saltos (*hops*) necesarios para que un paquete llegue a su destino, se puede ver gráficamente el número de estaciones de trabajo conectadas con su respectivo salto. La prueba se realizó desde una laptop conectada al router 3com.

2.5.2.2.1 Tráfico IP

En la tabla 2.11 se detalla el tráfico IP capturado con la herramienta Ntop. Se visualiza el tráfico generado por cada una de las estaciones de trabajo que están conectadas a la red LAN. Se puede observar la cantidad de datos que se transmiten con su respectivo porcentaje.

HOST	DIRECCIÓN IP	DATOS	
Dns	192.168.1.1	273.9 KB	12.3 %
66-188-54-11.dhcp.bycy.mi.charter.com	66.188.54.11	340 B	0.0 %
clients1.google.com	74.125.47.113	15.8 KB	0.7 %
colecturia	192.168.1.31	5.5 KB	0.2 %
coordinacion	192.168.1.45	42.0 KB	1.9 %
cpe-65-27-197-155.cinci.res.rr.com	65.27.197.155	60 B	0.0 %
crl.microsoft.com	216.66.8.161	1.0 KB	0.0 %
dlink-9e7ad1	192.168.1.159	186.9 KB	8.4 %
g.ceipmsn.com	207.46.193.112	16.4 KB	0.7 %
googleads.g.doubleclick.net	74.125.47.154	21.9 KB	1.0 %
mscrl.microsoft.com	94.245.70.21	832 B	0.0 %
pagead2.googlesyndication.com	74.125.47.166	271.4 KB	12.2 %
pele.backup.com	67.148.75.44	413.5 KB	18.6 %
ratings-wrs.symantec.com	143.127.102.125	41.0 KB	1.8 %
secretaria	192.168.1.43	4.9 KB	0.2 %
sn105ds.mail.services.live.com	65.55.85.74	36.9 KB	1.7 %
msg3020326.sn1.gateway.edge.messenger.live.com	65.55.71.218	165.8 KB	7.4 %
toolbarqueries.google.com.ec	209.85.157.99	14.0 KB	0.6 %
urs.microsoft.com	157.55.60.189	48.8 KB	2.2 %
www.google-analytics.com	74.125.47.102	2.4 KB	0.1 %
www.google.com	74.125.115.106	53.3 KB	2.4 %
www.quebajar.com	209.172.61.102	180.7 KB	8.1 %
mazz-27b059b26d [NetBIOS]	192.168.0.199	1.6 KB	0.1 %
66.229.196.11	66.229.196.11	246 B	0.0 %
69.204.232.64	69.204.232.64	68 B	0.0 %
71.237.0.143	71.237.0.143	68 B	0.0 %
77.245.96.34	77.245.96.34	60 B	0.0 %
157.100.62.8	157.100.62.8	29.3 KB	1.3 %
187.2.117.2	187.2.117.2	68 B	0.0 %
192.168.0.1	192.168.0.1	13.9 KB	0.6 %
212.161.8.3	212.161.8.3	6.4 KB	0.3 %
Tráfico Total	1.85 MB		
Ancho de banda Usado	82.93 Kbps		
Periodo de Tiempo	10:09 am a 13:02 pm		

Tabla 2. 11 Tráfico IP. [11]

En la tabla 2.11 lo más importante es el tráfico que genera colecturía, coordinación y secretaría, este tráfico es debido a que comparten archivos sobre información de los estudiantes. Mientras que las otras direcciones son las visitadas por otros usuarios.

2.5.2.3 Utilizando la herramienta Nmap

Esta herramienta fue utilizada para descubrir las estaciones de trabajo que están conectadas y los puertos que tienen habilitados y deshabilitados, en la tabla 2.12 se detalla un ejemplo de lo que se encontró al realizar un escaneo. Esta información se en encuentra en el **ANEXO A.1**

Comando	**nmap -v sn 192.168.1.0/24**
Estaciones de trabajo no encontradas	**Estaciones de trabajo encontradas**
Starting Nmap 5.51 (http://nmap.org) at 2011-05-19 10:59 Failed to resolve given hostname/IP: sn. Note that you can't use '/mask' AND '1-4,7,100-' style IP ranges Initiating Ping Scan at 10:59 Scanning 256 hosts [2 ports/host] Completed Ping Scan at 10:59, 2.22s elapsed (256 total hosts) Initiating Parallel DNS resolution of 256 hosts. at 10:59Completed Parallel DNS resolution of 256 hosts. at 10:59,0.04s elapsed	Discovered open port 80/tcp on 192.168.1.1 Discovered open port 80/tcp on 192.168.1.159 Discovered open port 135/tcp on 192.168.1.104 Nmap scan report for (192.168.1.1) Host is up (0.0029s latency). Not shown: 999 filtered ports PORT STATE SERVICE 80/tcp open http
Comando	**nmap -v sn 192.168.1.0/24**
Nmap scan report for 192.168.1.0 [host down] Nmap scan report for 192.168.1.2 [host down] Nmap scan report for 192.168.1.3 [host down] Nmap scan report for 192.168.1.4 [host down]	Nmap scan report for 192.168.1.104 Host is up (0.0034s latency). Not shown: 992 filtered ports PORT STATE SERVICE 80/tcp open http 135/tcp open msrpc

Tabla 2. 12 Host escaneados. [12]

Al realizar el escaneo de las estaciones de trabajo conectadas a la red se ingresó como parámetro la dirección IP 192.168.1.0/24, buscando cada una de las direcciones dentro de esta red, debido a que no todas las PC están conectadas se tiene el resultado de "host down" y en donde se encuentra respuesta son todas las conectadas a la red.

Por ejemplo la dirección 192.168.1.1/24 es la del router 3Com el cual tiene abierto solo el puerto 80/TCP para http como se muestra en la anterior tabla.

2.5.2.4 Utilizando la herramienta IP Scanner

Utilizando la herramienta IP Scanner se obtuvo las direcciones IP y MAC de los computadores que estaban conectados en red los cuales se detallan en la figura 2.14. Cabe indicar que los computadores que están siempre conectados son los del departamento administrativo y algunas del laboratorio de Secundaria.

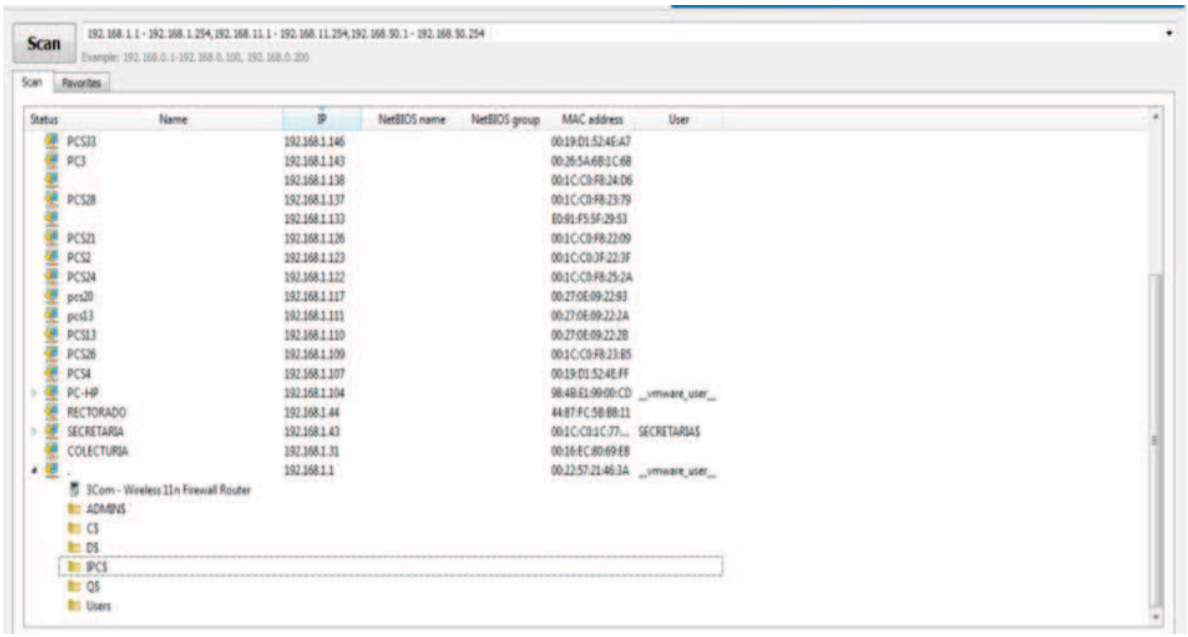


Figura 2. 14 Host Conectados. [14]

2.5.3 ANÁLISIS DE SEGURIDAD EN LA RED LAN Y WLAN

Al analizar la seguridad que se tiene en la red, se encontró las siguientes vulnerabilidades:

- Los usuarios ingresan a los computadores como administradores, lo que es un riesgo para la seguridad.

- No existen VLAN, por lo que los estudiantes pueden ver los archivos compartidos por los docentes y administrativos.

- Al ingresar como administradores los usuarios pueden instalar cualquier software lo cual es riesgoso para la seguridad de la red.

- El router tiene habilitado el DHCP para la red WLAN lo cual no es recomendable por seguridad.

- Si se realiza un ataque al router la red queda sin funcionamiento ya que es el encargado del direccionamiento dinámico.

- No existe un antivirus centralizado el cual este actualizado continuamente para brindar mayor seguridad.

- No se tiene instalado un proxy para que los usuarios no ingresen a sitios no deseados.

- Para el acceso inalámbrico se requiere de una contraseña, al adquirir dicha contraseña el usuario ingresa con todos los privilegios lo cual es un riesgo para la seguridad de la red LAN.

- No existen políticas de seguridad.

- Los puertos de los switch que no son utilizados están habilitados por lo que cualquier usuario puede conectarse y tener acceso a toda la red.

- No se tiene instalado ningún sistema de administración de red, con el cual se pueda realizar un monitoreo continuo en busca de vulnerabilidades.

- Para configurar el router se ingresa a la dirección //192.168.1.1, dentro del interfaz web se solicita usuario y contraseña del administrador.

- El router soporta firewall por lo que se tiene habilitada esta opción.

2.5.4 RED TELEFÓNICA

La red telefónica de la Institución trabaja en forma independiente de la red de datos y está conformada por una central telefónica de marca Panasonic que tiene 4 puertos RJ-11, las características técnicas se las especifica en la tabla 2.13.

TIPO	MARCA	MODELO	CARACTERÍSTICAS	IMAGEN
Central Telefónica	Panasonic	308 Easa - Phone	Toma, desvío, transferencia y captura de llamadas Conferencia Servicio Diurno/Nocturno Bloqueo de llamadas Conector para portero y abre puertas	

Tabla 2. 13 Característica de la Central Telefónica. [13]

Actualmente tiene conectado solo 3 extensiones debido a que una está dañada, las extensiones están distribuidas en los siguientes departamentos: rectorado, comunidad, secretaría y colecturía, la extensión de colecturía está dañada por lo que este departamento no tiene acceso a la red de voz.

Adicionalmente, es necesario indicar que la central telefónica solo puede tener como máximo 4 extensiones y una línea telefónica (troncal).

La CNT es la empresa que le provee el servicio de telefonía fija, la Institución solo tiene contratado una línea telefónica para brindar el servicio dentro de sus instalaciones la cual es la 022-653-242.

La central telefónica o PBX no está ubicada en el cuarto de equipos, se encuentra ubicada en recepción sin contar con un nivel de seguridad físico adecuado. En la figura 2.15 se tiene un esquema físico de la red telefónica que tiene la Institución.

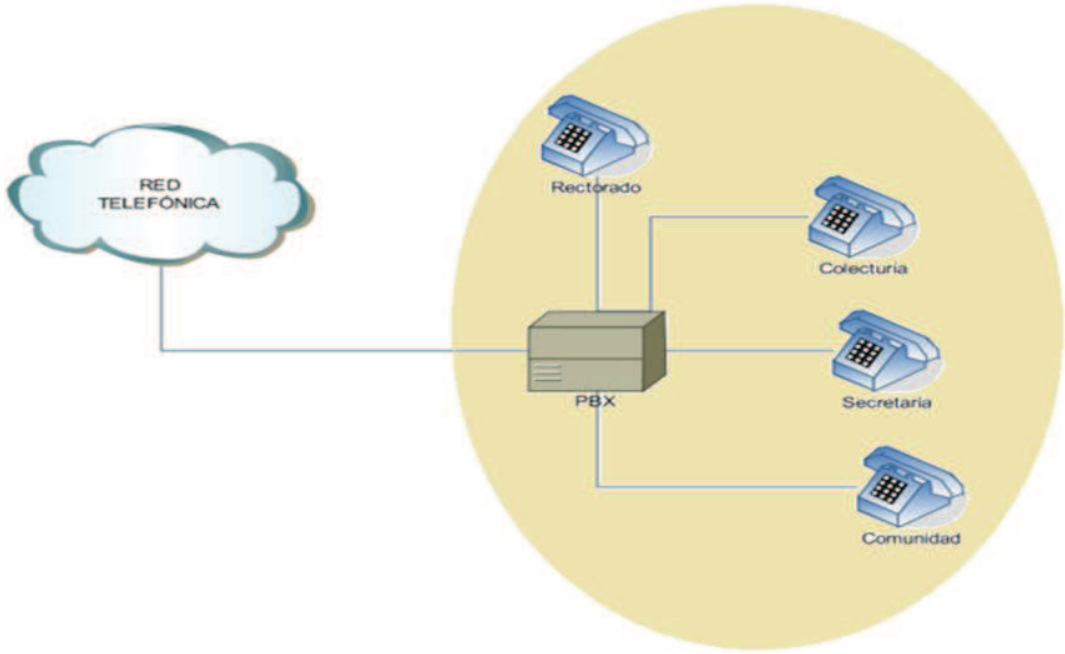


Figura 2. 15 Red telefónica. [15]

2.5.4.1 Tráfico de la Red Telefónica

En la Institución actualmente no existe un administrador de la red por lo que para obtener información acerca del tráfico telefónico se realizó una consulta a la señora recepcionista, la cual explico que recibe entre 30 y 40 llamadas diarias con una duración promedio de 3[42] minutos.

[42] Fuente, consulta al Rectorado, Secretaria y Colecturia

Además, La central telefónica no cuenta con un software para verificar el tráfico entrante y saliente que se tiene, por lo que no se puede saber con exactitud cuál es el tráfico que circula diariamente.

2.5.4.2 Costo mensual de teléfono

La Unidad Educativa paga por el uso de la línea telefónica un valor promedio mensual de 30 dólares, esta línea telefónica es la troncal que se encuentra conectada a la central telefónica Panasonic de donde salen 3 exenciones hacia el departamento administrativo.

2.6 ANÁLISIS TOTAL DEL DIAGNÓSTICO DE LA RED

2.6.1 RED DE DATOS

La mayoría de estaciones de trabajo que tiene la Institución no están conectadas a la red por lo que no cuentan con el servicio de Internet y aplicaciones locales.

Los dos servidores están fuera de servicio por falta de mantenimiento, uno requiere una fuente de poder mientras que el otro tiene dañado el kernel del sistema operativo Linux.

De acuerdo al análisis de tráfico realizado en el literal 2.5.2, éste es bajo debido a que sólo un porcentaje de estaciones de trabajo están conectadas.

El esquema de direccionamiento IP es de forma dinámico. Sin embargo las estaciones de trabajo del departamento Administrativo tienen asignadas direcciones estáticas debido a que utilizan un software de administración para subir las notas de los estudiantes.

No existe un software para realizar la administración de la red debido a que los equipos de networking no soportan el protocolo básico SNMP.

2.6.2 RED TELEFÓNICA

La red telefónica está compuesta por una central telefónica ubicada en el departamento Administrativo, soporta máximo una línea telefónica y 4 extensiones, de las cuales sólo 3 están en funcionamiento una se encuentra dañada: sin embargo los usuarios no tienen restricción de llamadas por lo que pueden hacer llamadas a teléfonos celulares, locales y nacionales.

2.6.3 EQUIPOS DE COMUNICACIÓN

Dentro de los equipos activos de la red están los switch D-link detallados en el literal 2.2.2.4 y un router 3com, los switch no son equipos administrables.

Las funcionalidades de los equipos de red utilizados actualmente no cumplen con los requerimientos de las nuevas tecnología que se pretende implementar en la Institución: VoIP, video vigilancia IP, etc. Además, los switch utilizados en los laboratorios no tienen suficientes puertos disponibles para incrementar mas estaciones de trabajo que se requieren para la demanda estudiantil que existe.

2.6.4 CABLEADO ESTRUCTURADO

El cableado de toda la Institución no está desarrollado en su totalidad bajo los estándares ANSI/EIA-TIA. Además no cuenta con certificación de los puntos de red del cableado estructurado.

No existe un rack en la sala de equipos para organizar tanto el cableado horizontal, vertical y los equipos de networking. Además no cuenta con un sistema de puesta a tierra para proteger a los equipos y caídas de tensión en la red eléctrica.

Los armarios de telecomunicaciones no cuentan con organizadores ni regletas para la conexión y organización de los cables.

Algunos departamentos no tienen cableado vertical por lo que no tienen acceso al Internet y a servicios internos que presta la red de Institución como son revisión y subida de notas por parte de los profesores y estudiantes.

2.6.5 SEGURIDAD

No existen políticas de seguridad definidas o documentadas con relación a las normas de uso y acceso a la red.

Para la parte correspondiente a la seguridad física no existe un registro de las personas que acceden a la sala de equipos y a realizar cambios en los armarios de telecomunicaciones.

Para la seguridad lógica no cuenta con un servidor proxy para bloquear páginas y aplicaciones que no deben acceder los usuarios.

La Institución no dispone de un antivirus centralizado para mantener las estaciones de trabajo libres de gusanos, virus y troyanos.

CAPÍTULO 3

REDISEÑO DE LA RED LAN Y WLAN

CAPÍTULO 3

REDISEÑO DE LA RED LAN Y WLAN

3.1 VISIÓN GENERAL

Para un buen desempeño de la Institución se requiere contar con una red convergente, escalable y segura que cumpla con los requerimientos actuales y tenga una proyección de crecimiento futuro, ofreciendo a la comunidad interna de la Institución servicios de fácil acceso y de calidad.

Se realizará el rediseño de la red, que ofrezca una solución completa de conectividad de los diferentes laboratorios. Para esto se contempla los diferentes servicios que debe soportar la red como son telefonía IP, video vigilancia, Internet, correo Interno entre otros.

3.2 REQUERIMIENTOS DE LA INSTITUCIÓN

Con el análisis, fruto del capítulo 2, se ha determinado que la UESMDM[43] tiene los siguientes requerimientos tales como: conectividad total, nuevos servicios y seguridad los cuales están detallados a continuación:

- Se requiere que todas las estaciones de trabajo estén conectadas a la red local de la Institución para que los estudiantes, administrativos y profesores tengan acceso a aplicaciones locales y a servicios de Internet.

[43] UESMDM (Unidad Educativa Santa María D. Mazzarello)

- Para mayor seguridad del ingreso a la Institución por parte de profesores, administrativos y de los estudiantes, así como el acceso a algunos departamentos se requiere de cámaras de vigilancia.

- Para optimizar la comunicación de voz utilizando la misma infraestructura de red de datos y para tener acceso a un dispositivo que permita la transmisión de voz en todas las áreas donde se requiere, es necesario realizar el diseño de telefonía IP.

- En algunos departamentos como son: biblioteca, equipo pastoral, sala de profesores y el administrativo se requiere contar con una red inalámbrica para dar servicios locales y navegación al Internet a los usuarios visitantes.

- Se requiere contar con políticas de seguridad para el acceso a la red, en las cuales se restrinja el ingreso de algunos usuarios a aplicaciones que no son de su competencia.

- Es necesario contar con servidores tales como DNS, DHCP, Proxy, Impresión, Web, correo y base de datos entre otros para brindar un servicio de calidad y con seguridad necesaria dentro y fuera de la Institución.

- Para mayor seguridad, flexibilidad y mejora en la red es necesario crear VLANs (redes virtuales) para segmentar los siguientes servicios, una VLAN para datos, otra para video y otra para VoIP.

- Contar con un sistema de cableado estructurado que cumpla los estándares internaciones para tener flexibilidad y escalabilidad en la red para futuras aplicaciones.

3.2.1 INFRAESTRUCTURA DE LA RED

Con base al estudio realizado en el capítulo 2, y de acuerdo a los requerimientos que tiene la Institución, se realiza un análisis de los servicios que se brindará en la red con lo que se procede con el diseño de la infraestructura de la red.

3.3 SERVICIOS QUE BRINDARÁ LA RED LAN Y WLAN

3.3.1 SERVICIO DE VIDEO VIGILANCIA IP

El avance tecnológico ha permitido que en una sola infraestructura de red se pueda brindar varios servicios utilizando la pila de protocolos TCP/IP, esto hace posible la conexión de una cámara de video en cualquier lugar donde se requiera seguridad y exista un puerto disponible para brindar dicho servicio.

Las cámaras capturan el video y audio transmitiendo información hacia el servidor de video, al cual se tiene acceso desde cualquier parte dentro de la Intranet y también se puede acceder desde la red Internet para lo cual se debe tomar en cuenta algunos parámetros de seguridad.

El objetivo de brindar este servicio en la UESMDM es proveer un monitoreo de seguridad en el ingreso a la Institución y algunos departamentos, esto es necesario por el alto índice de inseguridad que existe en la ciudad de Quito.

3.3.2 SERVICIO DE TELEFONÍA IP

Es un servicio adicional que se puede brindar en la red mediante el uso del protocolo IP, con lo que se usa la misma infraestructura para aprovechar los siguientes beneficios:

- No se requiere de conexiones adicionales lo cual conlleva a tener un menor gasto en la implementación.
- La configuración de la central IP tiene menor costo que adquirir una central telefónica analógica.
- Tiene mayor escalabilidad que la telefonía tradicional.
- Se puede utilizar teléfonos de diferentes fabricantes, siempre y cuando se cumpla con algunos parámetros técnicos.
- Se puede brindar el servicio de telefonía a todos los usuarios que requieran sin necesidad de realizar nuevas instalaciones de cableado.
- Se tiene un menor costo de administración de toda la red, esto es debido a que existe una sola infraestructura de red, por lo que se tiene una administración centralizada.
- Los usuarios contarán con mejores servicios de los que brinda la telefonía tradicional.
- Se ofrece mayor seguridad a los usuarios, mediante la autenticación y codificación de la información.

Este servicio es requerido por la Institución, debido a que actualmente cuenta con una central telefónica analógica que sólo puede dar servicio a 4 usuarios, teniendo la necesidad del servicio para 16 usuarios.

3.3.3 SERVICIO DE CORREO ELECTRÓNICO

La Unidad Educativa actualmente no cuenta con correo electrónico Institucional, los usuarios para enviar un archivo dentro de la Institución utilizan correos externos como Hotmail, gmail entre otros.

El correo electrónico es requerido para dar servicio a todos los usuarios de la Institución para que puedan enviar, recibir mensajes y archivos dentro y fuera de

la UESMDM de forma rápida y simple con la utilización de una aplicación cargada en cada uno de los computadores.

Se debe considerar que este servicio en la mayoría de los casos es proporcionado por las empresas proveedoras de Internet, sin embargo puede ser implementado dentro de la Intranet mediante el uso de un servidor de correo y con la utilización de aplicaciones clientes de correo en cada uno de los usuarios.

3.3.4 SERVICIO DE INTERNET

Este servicio será proporcionado para todos los usuarios conectados a la red local, ofreciéndoles calidad y una alta disponibilidad, con el objetivo de mejorar el acceso a la información contribuyendo con el desarrollo académico de los estudiantes.

Además, los estudiantes mediante la utilización de este servicio tendrán la facilidad de adquirir nuevas destrezas por medio de la investigación mejorando su nivel académico.

También los docentes podrán investigar y adquirir nuevas destrezas mediante la actualización contínua de sus conocimientos, lo cual hace que se mejore el nivel académico de los estudiantes.

3.3.5 SERVICIOS VARIOS

Adicionalmente, se ofrecerá otros servicios como son la implementación de un servidor de impresión, fax y servidor de archivos.

3.3 6 DIMENSIONAMIENTO DE TRÁFICO POR SERVICIO

El dimensionamiento de tráfico se lo realizará para cada servicio que va a ofrecer la Institución. Es fundamental tener un aproximado de la cantidad y tipo de tráfico que va a circular por la red.

3.3.6.1 Tráfico para Video Vigilancia IP

Antes de realizar el análisis de ancho de banda, se va a realizar una descripción general de los protocolos utilizados para la transmisión de video en redes IP. Los protocolos se detallan en la tabla 3.1.

Protocolos Utilizados Para Video IP	Protocolos de Transporte	Puerto	Características
FTP	TCP	21	Transfiere las imágenes desde la cámara hacia el servidor
SNMP	TCP	25	Es utilizado para enviar notificaciones de alarma al correo electrónico
HTTP	TCP	80	Es el encargado de transferir el video desde el dispositivo de red (cámara), el cual funciona básicamente como servidor web que pone el video a disposición del usuario o del servidor de aplicaciones que lo solicita.
HTTPS	TCP	443	Tiene las mismas funciones que el protocolo HTTP pero proporciona seguridad.
RTP	UDP/TCP	No está definido	Es utilizado para la entrega de audio y de video en la red IP, utilizado en sistemas multimedio o videoconferencia Transmite video basado en el estándar H.264/MPEG. Además, RTP proporciona numeración y señalización de paquetes para el ensamblado de forma correcta de los paquetes en el destino.
RTSP	TCP	554	Permite la configuración y el control de sesiones multimedia RTP:

Tabla 3. 1 Protocolos utilizados para transmitir video sobre redes IP[44]. [1]

[44] [PW38] http://www.axis.com/files/brochure/bc_techguide_33337_es_0902_lo.pdf

3.3.6.1.1 Parámetros que se deben considerar para transmitir video sobre redes IP

Para realizar el análisis de ancho de banda requerido en la transmisión de video sobre una red IP, se consideran algunos parámetros fundamentales tales como:

- Número de imágenes por segundo
- Algoritmo de compresión
- Encapsulamiento de video
- Número de cámaras IP

Los procesos básicos para implementar un sistema de video vigilancia IP son:

- **Codificación y Decodificación**

  La codificación es el proceso mediante el cual una señal analógica se digitaliza y comprime para luego ser transmitida por la red IP. Este proceso se realiza ya sea en la cámara IP ó en el servidor de video, mientras que la decodificación de video es la traducción de la información con el fin de ser visualizada desde una PC normal mediante la utilización de un software de gestión de video.

  La compresión se basa en aplicar un algoritmo al video original para crear un archivo comprimido. Para obtener el archivo original se aplica el algoritmo inverso. El tiempo que se tarda en comprimir, enviar, descomprimir y mostrar un archivo es lo que se denomina "latencia". De acuerdo a esto, cuanto más avanzado sea el algoritmo de compresión, menor será el ancho de banda requerido para transmitir video sobre la red.

Al codificador y decodificador se los denomina códecs de video. Los códecs de video de estándares diferentes no suelen ser compatibles entre sí.

- **Transmisión IP**

Es la transmisión que se realiza desde la cámara de video, la cual captura las imágenes y las envía a través de la red hacia un servidor de almacenamiento, para luego ser visualizado o monitoreado desde un PC.

- **Grabación**

La grabación o almacenamiento del video se lo realiza en servidores tales como NAS o RAS. Un esquema de funcionamiento sería como el detallado en la figura 3.1

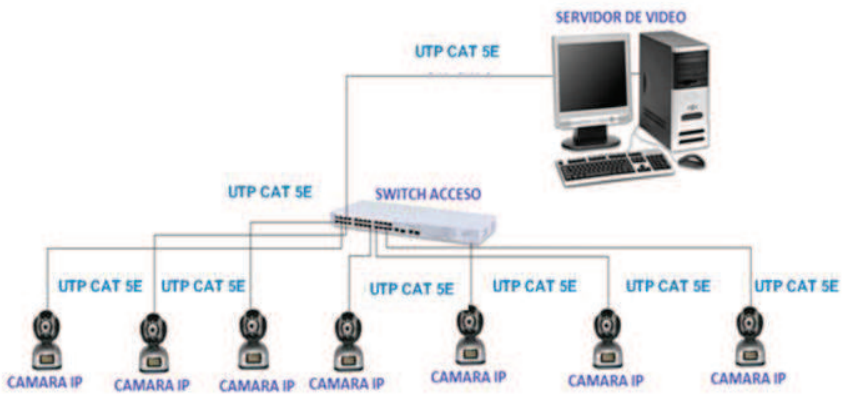


Figura 3. 1 Modelo del sistema de video vigilancia. [1]

3.3.6.1.2 Algoritmos de Compresión

Cada sistema de vigilancia o cámara IP utiliza diferentes tipos de compresión, la mayoría de los dispositivos soportan varios tipos de compresión dando la

flexibilidad de elegir el más adecuado, entre los formatos de compresión de video más utilizados se tiene:

- M-JPEG
- MPEG-4
- H.264 que es la versión 10 de MPEG-4.

Para este caso se escogió la compresión que proporciona MPEG-4 debido a que este sistema permite un alto grado de compresión manteniendo una buena calidad de video y utilizando un menor ancho de banda en relación a M-JPEG.

Cabe indicar que el algoritmo de compresión H.264 o MPEG-4 AVC, proporciona mejores características que MPEG-4 aumentando la compresión, manteniendo la calidad de video, disminuyendo el uso de ancho de banda y utilizando un menor espacio de almacenamiento: sin embargo no está muy difundido en el mercado por lo que se tiene pocos equipos que soporten este tipo de compresión. Esta es la razón principal por la que no se escogió este algoritmo de compresión.

	M-JPEG	**MPEG**	**H.264**
Compresión	Espacial	Espacial/Temporal	Espacial/Temporal
Calidad de la imagen	Grande	Pequeña	Pequeña
Pérdida	Con pérdidas	Con pérdidas	Con pérdidas
Tamaño de los Archivos	Grande	Pequeño	Pequeño
Resolución	640X480	720X576	352X288
Tamaño de la Matriz	8X8	16X16	8X8
Ratio	20:1 y 40:1	100:1 variable	100:01:00
Capacidad (Mbps)	2.5	1.86	0.546
Ips (Imágenes x segundo)	25	30	20
Aplicaciones	Transmisión de video	Transmisión de video, TV	Video conferencia

Tabla 3. 2 Características de los algoritmos de compresión de video. [2]

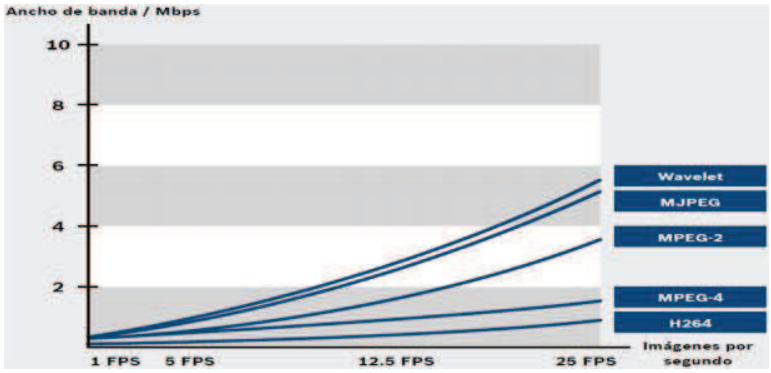


Figura 3. 2 Utilización de AB de algunos algoritmos de compresión de video. [2]

3.3.6.1.3 Dimensionamiento de Tráfico para video

De acuerdo a los factores descritos en la tabla 3.2, que se utilizan para determinar la capacidad requerida para enviar video por la red, con la siguiente ecuación.

$$C_{video} = \left[\frac{width * heighth * color * color\ bit\ depth * Ips}{Factor\ de\ compresión}\right] bps$$

***Ecuación 3.1*[45]**

Descripción de las variables utilizadas en la ecuación.

- **width * heighth** = tamaño de la imagen (pixeles)
- **Color bit depth** = Profundidad del color utilizado para las imágenes, 8 bits para codificar cada uno de los tres colores RGB.
- **Ips** = Número de Imágenes por segundo
- **Factor de compresión** = Factor de compresión de imágenes de video.
- **C =** Capacidad

[45] [T5] Ing. Diego Pozo, Estudio y Diseño de una Red de Voz y Datos para la Unidad Educativa Municipal Quitumbe utilizando la tecnología Gigabit Ethernet para soportar servicios en tiempo real de VoIP, Video seguridad y Videoconferencia, tesis EPN, 2009, Pág. 79

En el mercado se puede encontrar diferentes alternativas en cámaras IP, las que en gran parte cumplen con las mismas características técnicas requeridas.

- 25/30 Ips con una resolución de 160X120
- 25/30 Ips con una resolución de 320X240
- 10/25 Ips con una resolución de 640X480
- Compresión M-JPEG y MPEG-4

El estándar de compresión MPEG-4 soporta un factor de compresión que está en el rango de 70:1 (Movimiento) a 200:1(Estático), considerando que no va a existir un movimiento continuo se va a seleccionar un factor de compresión de 140.

Se toma como referencia 640x480 porque es una resolución que permite ver adecuadamente el video. Además no genera mucho tráfico en la red.

El valor de 24 es debido a que se necesitan 8 bits para codificar los tres colores RGB y las 15 imágenes por segundo es una secuencia adecuada para ver un video.

$$C_{video\ (bps)} = \left[\frac{640 * 480 * 24 * 15}{140}\right] bps$$

$$C_{video} = 789.94\ kbps$$

$$C_{video} = Capacidad(Video) + Capacidad(Voz)$$

$$C_{video} = 789.94 + 64$$

$$C_{video} = 853.94\ kbps$$

Se consideró 64 kbps de voz debido a que existen cámaras de bajo presupuesto que ofrecen el servicio de grabacion de voz a más del video.

La capacidad requerida es de 853.94 Kbps por cada cámara a utilizar, tomando en cuenta que son 8 cámaras se obtiene lo siguiente.

$$C_{total} = Número\ Total\ de\ Cámaras * C_{video}$$

$$C_{total} = 8 * (853.94) kbps$$

$$C_{total} = 6831.52\ kbps$$

3.3.6.1.4 Dimensionamiento de Almacenamiento

En base a la capacidad requerida, se procede a calcular el espacio de almacenamiento necesario.

$$6831.52 \frac{bits}{segundo} * \frac{1\ Byte}{8\ bits} * \frac{3600\ segundos}{1\ hora} * \frac{1}{1000} * \frac{1}{1000} = 3.07\ GB \frac{GB}{hora}$$

Se necesita 3.07 GB por cada hora de actividad, para la adquisición de las cámaras IP una de las características principales es que se enciendan y capturen video solo si hay actividad caso contrario se deben poner en estado de reposo.

Tomando en cuenta que las cámaras IP solo capturan video si existe actividad y que la UESMDM está abierta frecuentemente de 6:30 am a 5:00 pm, donde se tiene un flujo continuo de grabación de 6:30 am a 2:00 pm, obteniendo un tiempo promedio de grabación de 10 horas por día los 30 días al mes, se necesita un disco duro de almacenamiento de:

$$3.07\ GB \frac{GB}{hora} * \frac{10}{día} * \frac{30}{mes} = 922.25\ GB$$

Para el almacenamiento de video se puede utilizar un servidor normal el cual tenga una capacidad de 1 TB, sin embargo existen servidores especiales para almacenamiento de información tales como los NAS y los SAN.

3.3.6.2 Tráfico para Telefonía IP

Para realizar el dimensionamiento de tráfico de voz sobre una red IP se han considerado cuatro factores principales:

- Códec a utilizar
- El tamaño del paquete de datos de voz
- Utilización de compresión de la cabecera RTP
- Supresión de silencio.

Los códecs de voz son dispositivos que convierten la señal analógica en digital. Además, permiten comprimir la señal, disminuyendo significativamente el ancho de banda requerido para enviar paquetes de voz por la red IP.

Otra forma de ahorrar ancho de banda es utilizando supresión de silencio, esto es no enviar paquetes de voz de silencio durante la conversación.

En la tabla 3.3 se realiza una descripción de los códecs más utilizados para transmitir VoIP.

CÓDEC	MODULACIÓN	CAPACIDAD (KBPS)	FRECUENCIA DE MUESTREO (KHZ)	OBSERVACIONES
G.711	PCM	64	8	Existen 2 versiones para muestrear la señal u-law (US y Japón) y a-law (Europa)
G.721	ADPCM	32	8	Obsoleta

CÓDEC	MODULACIÓN	CAPACIDAD (KBPS)	FRECUENCIA DE MUESTREO (KHZ)	OBSERVACIONES
G.722	7 kHz codificación de audio dentro de 64 kbit/s	64	16	Se basa en dividir La frecuencia de muestreo en dos bandas cada una usando ADPCM
G.722.1	Codificación a 24 y 32 kbit/s	24/32	16	Describe un algoritmo Wideband proporcionando un AB de 50 a 7000 Hz
G.723	Codificación de 24 y 40 kbit/s para aplicaciones en circuitos digitales.	24/40	8	Obsoleta y diferente de G.723.1.
G.723.1	Codec de audio de baja velocidad en aplicaciones multimedia.	5.6/6.3	8	Es parte de H.324. y es utilizada para videoconferencia
G.726	ADPCM	16/24/32/40	8	Reemplaza a G.721 y G.723.
G.727	ADPCM	variable		Relacionada con G.726.
G.728	Codificación de señales de voz mediante la utilización de la técnica de predicción lineal con excitación por código de bajo retardo	16	8	CELP.
G.729	CS-ACELP	8	8	Tiene un bajo requerimiento de ancho de banda y Bajo retardo (15 ms)

Tabla 3. 3 Códecs utilizados en VoIP[46]. [3]

De acuerdo a las características de los códecs más utilizados en telefonía IP el que cuenta con un ancho de banda relativamente bajo y mantiene una buena calidad de voz es el G.729 por lo que será utilizado para este diseño.

Para el envío de voz sobre redes IP es necesario estructurar la información mediante paquetes, donde el ancho de banda requerido dependerá de la sobrecarga que generen estos paquetes.

[46][PW39] http://www.ozvoip.com/codecs.php

3.3.6.2.1 Protocolos de Encapsulamiento para enviar Voz sobre una red IP

Para enviar VoIP sobre una red LAN mediante tramas Ethernet se utiliza el protocolo RTP (*Real Time Protocol*). El cual es encapsulado en el protocolo UDP (*User Datagram Protocol*), para luego ser encapsulado sobre IP, el que es encargado de llevar la información sobre Ethernet. Como se detalla en la figura 3.3

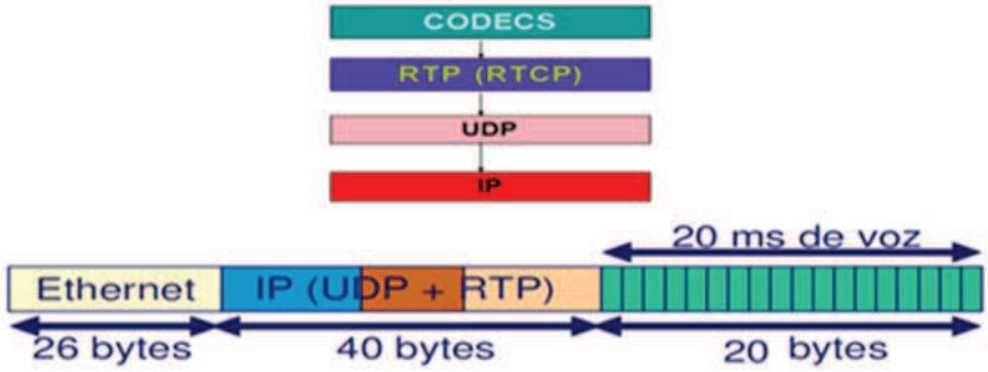


Figura 3. 3 Cabecera de los protocolos para voz sobre redes IP. [3]

Con la siguiente ecuación se puede determinar la capacidad necesaria para transmitir paquetes de voz sobre una red IP.

$$C_{canal} = AB_{codec} \frac{longitud\ de\ sobrecarga + longitud\ de\ encapsulamie}{longitud\ de\ sobrecarga} \quad bps)$$

***Ecuación 3.2*[47]**

Donde cada variable representa lo siguiente:

- **$C_{códec}$** = Ancho de banda del códec seleccionado.
- **Longitud de sobrecarga** = Tamaño del payload de la trama.
- **Longitud de encapsulamiento** = Tamaño de la cabecera de la trama.

[47] [T5] Ing. Diego Pozo, Estudio y Diseño de una Red de Voz y Datos para la Unidad Educativa Municipal Quitumbe utilizando la tecnología Gigabit Ethernet para soportar servicios en tiempo real de VoIP, Video seguridad y Videoconferencia, Tesis EPN, Pág. 79

Con la ecuación anterior se obtiene la capacidad requerida por canal: sin embargo, la capacidad real para cada conversación será el doble del valor obtenido, debido a que la conversación se la realiza en sentido bidireccional.

Para obtener la capacidad real por conversación se va a utilizar la siguiente ecuación.

$$C_{capacidad\ real\ por\ conversación} = 2 * C_{canal}$$

En la tabla 3.4 se tiene una descripción detallada de las cabeceras de los protocolos que se encapsulan en el protocolo IP.

Cabecera RTP	**12 Bytes**
Cabecera UDP	8 Bytes
Cabecera IP	20 Bytes
Payload (Voz)	20 Bytes
Sobrecarga Ethernet	26 Bytes
Longitud de Sobrecarga	20 Bytes
Longitud de Encapsulamiento	66 Bytes
Ancho de banda del codec	8 Kbps

Tabla 3. 4 Cabecera de los protocolos utilizados para enviar voz sobre redes IP. [4]

$$C_{canal} = 8\ kbps \frac{20\ Bytes + 66\ Bytes}{20\ Bytes}$$

$$C_{canal} = 34.4\ kbps$$

$$C_{capacidad\ real\ por\ conversación} = 2 * 34.4\ kbps$$

$$C_{capacidad\ real\ por\ conversación} = 68.8\ kbps$$

Tomando en cuenta que la Unidad Educativa tiene un requerimiento de 16 puntos para voz, por lo que la capacidad mínimo mínima requerida es:

$$C_{Total} = 16 * 68.8\ kbps$$

$$C_{Total} = 1100.8\ kbps$$

3.3.6.2.2 Líneas troncales hacia la PSTN

Para determinar el flujo de tráfico que circula a través de la central telefónica se va a utilizar la siguiente ecuación.

A=C*T (Erlang)

Ecuación 3.3[48]

Definición de las variables utilizadas en la ecuación.

- **A** = Intensidad de tráfico o velocidad de flujo de llamadas, este valor es dado en Erlangs.
- **C** = Número de llamadas originadas durante horas pico
- **T** = Tiempo promedio que dura una llamada.

Con los datos obtenidos en el capítulo 2, se va a realizar una aproximación del tráfico que va a circular por la central telefónica. Además, cabe mencionar que la Institución solo tiene 3 extensiones, teniendo la necesidad de 13 extensiones adicionales, por lo que los datos obtenidos serán una aproximación del tráfico real.

Los datos obtenidos fueron de entre 30 y 40 llamadas por día, tomando como referencia que las horas laborables donde se tiene mayor tráfico es de 8:00h a 13:00 H se tendría un promedio de 8 llamadas por hora con una duración promedio de 3 minutos.

[48] [T1] **QUELAL**, Josué, "Rediseño de la Red de Comunicaciones de la empresa metropolitana de obras públicas (EMOP-Q) para soportar aplicaciones de voz sobre IP (VoIP)", pág 87

$$A = 8\frac{llamadas}{hora} * \frac{1\ hora}{60\ minutos} * 3\frac{minutos}{1\ llamada}\ (Erlangs)$$

$$A = 0.4\ (Erlangs)$$

La intensidad de tráfico calculado es de 0.4 Erlangs[49], tomando en cuenta el valor 0.01 (este valor es recomendado para telefonía) de la probabilidad de pérdida (GoS)[50] y utilizando la gráfica de Erlang B de la figura 3.4, se determina 3 canales de voz necesarios para la Unidad Educativa.

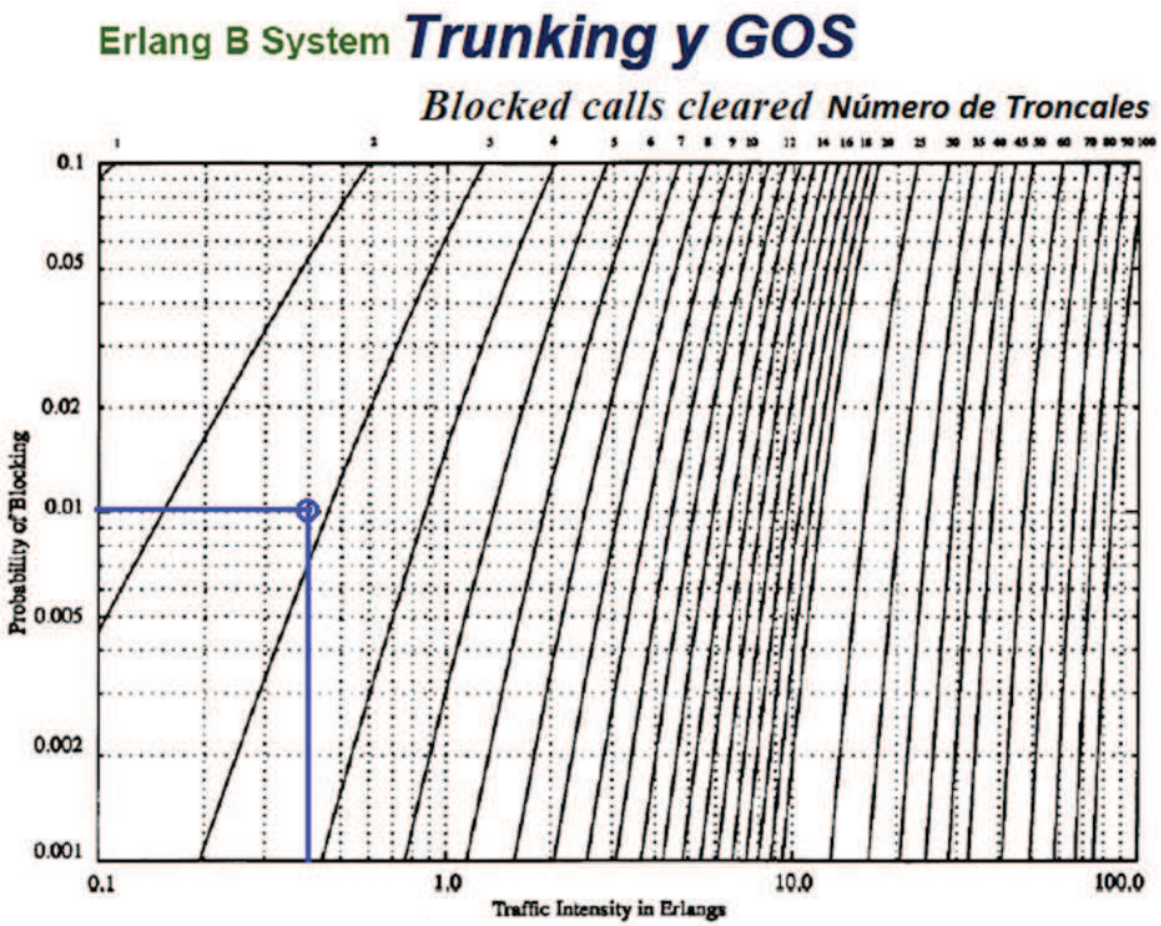


Figura 3. 4 Erlang B. [4]

[49] Erlang representa la cantidad de intensidad de tráfico transportado por un canal de voz.
[50] GoS (Grade of Service) Es una medida de la habilidad del usuario para acceder a un sistema que utiliza Trunking.

Se observa en el gráfico que se requieren de 3 líneas troncales para distribuir todo el tráfico generado por los 16 usuarios que requieren del servicio de telefonía.

De acuerdo a los datos obtenidos se procederá a proyectar el tráfico telefónico a un periodo de 5 años para lo cual se utiliza la ecuación 3.4.

El índice[51] de contratación de personal administrativo o trabajadores de la Institución es de máximo una persona por año. Cabe indicar que se toma como referencia sólo los trabajadores ya que ellos son los que contarán con una extensión telefónica. En la tabla 3.5 se detalla el crecimiento de extensión a 5 años.

AÑO	2007	2008	2009	2010	2011	2012	2013	2014	2015
EXTENSIONES	4	3	3	3	3	16	17	18	19

Tabla 3. 5 Proyección de crecimiento de extensiones. [5]

$$A_f = A_0(1 + f_c)^n$$

Ecuación 3.4

Variables de la ecuación.

- A_f = Tráfico final
- A_o = Tráfico inicial
- f_c = Factor de crecimiento anual
- n = Número de años

De acuerdo a la tabla 3.4 se tiene un crecimiento anual aproximado del 1% durante un periodo de 5 años se tendrá un tráfico de 0.42 Erlangs, por lo que los tres canales de voz soportarán esta cantidad de tráfico generada.

[51] Rectora de la UESMDM 2011, Sor Mercy Sanchez

$$A_f = 0.4(1 + 0.01)^5$$

$$A_f = 0.42\ Erlangs$$

En la tabla 3.6 se detalla la cantidad de tráfico proyectado por año durante los 5 primeros años.

Año	A (Erlangs)	Número de Troncales
0	0.40	3
1	0.404	3
2	0.408	3
3	0.412	3
4	0.416	3
5	0.42	3

Tabla 3. 6 Tráfico Proyectado para 5 años. [6]

3.3.6.3 Tráfico para Correo Electrónico

Para calcular el ancho de banda necesario para enviar y recibir un correo electrónico, se toma como referencia lo siguiente. Un mensaje de correo electrónico Institucional tiene un peso promedio de 50 KB[52] y que el usuario revise el mail cada 30 minutos.

Cabe indicar que los usuarios que dispondrán de correo electrónico Institucional son 14 dentro de los cuales se encuentran los administrativos.

A continuación se detalla el cálculo utilizado para determinar el volumen de correo electrónico:

$$AB_{(por\ usuario)} = \frac{50\ KB}{1\ mail} * \frac{8\ bits}{1\ byte} * \frac{1\ mail}{30\ minutos} * \frac{1\ minuto}{60\ segundos}$$

$$AB_{(por\ usuario)} = 0.22\ Kbps$$

$$AB_{(total\ correo\ electrónico)} = 0.22 * (14)\ Kbps$$

[52] [PW40] Referirse a la página Web http://technet.microsoft.com/es-es/library/cc745931.aspx

$$AB_{(total\ correo\ electrónico)} = 3.11\ Kbps$$

3.3.6.4 Tráfico generado por páginas web[53]

Todos los usuarios que estén conectados a la red de la UESMDM contarán con el servicio de acceso a Internet, se estima que cada usuario visite 10 páginas web por hora y considerando la información detallada en la figura 3.5 donde se detalla el tamaño promedio de una página web con relación al número de objetos que tiene. De acuerdo a lo anterior una página web simple tiene un peso promedio de 350 KB.

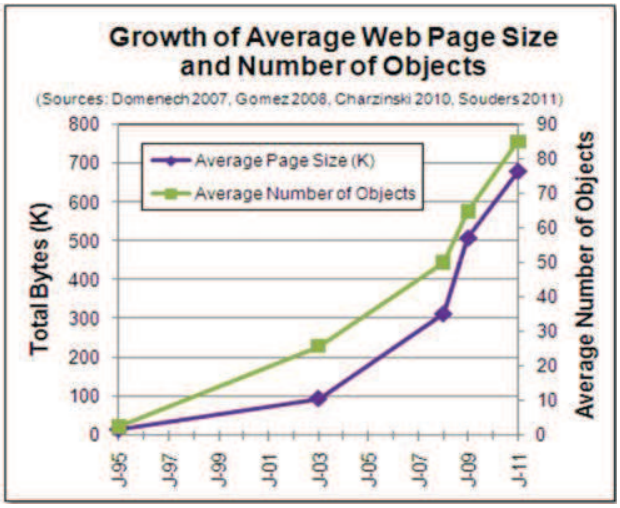


Figura 3. 5 Crecimiento promedio de una página web[54]. [5]

A continuación se realiza el cálculo para determinar el ancho de banda requerido.

$$AB_{(por\ usuario\ conectado\ al\ internet)} = \frac{350\ KB}{1\ página} * \frac{8\ bits}{1\ byte} * \frac{10\ página}{1\ hora} * \frac{1\ hora}{3600\ segundos}$$

$$AB_{(por\ usuario\ conectado\ al\ internet)} = 7.8\ Kbps$$

[53] [T6] Ing. Herrera Myriam, Ingeniería de detalle para el diseño de una Intranet con conexión a Internet para aplicaciones de voz, Datos y Video utilizando la arquitectura TCP/IP, Octubre 2004, Quito. Tesis E.P.N., pág. 52

[54] [PW41] Referirse a la página http://www.maxglaser.net/el-tamano-de-las-paginas-web-se-ha-triplicado-desde-el-2003/

Una vez calculado el ancho de banda requerido por cada usuario para visitar una página web se procede a calcular la correspondiente para todos los usuarios que tendrán acceso a este servicio. Sin embargo, no todos los usuarios estarán navegando en Internet de forma simultánea por lo que se utiliza un índice de simultaneidad del 40% del total de puntos de datos que son 142. Ya que todos realizan diferentes actividades.

$$AB_{(total\ para\ navegar\ en\ internet)} = 57 * 7.8\ Kbps$$

$$AB_{(total\ para\ navegar\ en\ internet)} = 444.6Kbps$$

3.3.6.5 Tráfico generado por acceder a la base de datos

Antes de calcular el tráfico que se genera al subir las notas a la base de datos, es necesario indicar que los profesores actualmente no cuentan con este servicio, por lo que las calificaciones son entregadas en colecturía para que sean almacenadas en la base de datos. Sin embargo: en este diseño se considera este tráfico ya que la Institución requiere dicho servicio.

Los docentes para subir la información al Sistema de Gestión Académica contarán con la siguiente infraestructura, 22 computadores del nuevo laboratorio, 3 en la sala de profesores y 2 en Biblioteca. Los computadores del nuevo laboratorio solo estarán disponibles a la hora de recreo, por lo que se considera esta hora para calcular el tráfico. Esta hora se asigna a los profesores porque no es utilizada por los estudiantes.

En base al estudio realizado en el capítulo 2, donde se indica que existen 52 profesores los cuales están distribuidos en primaria y secundaria. Cabe indicar

que el recreo tanto para secundaría como para primaria está en diferente horario, por lo que no todos los profesores estarán libres.

La duración de recreo es de 40 minutos y el número de profesores posibles es aproximadamente 27 que es número de docentes de secundaria y representa más del 50%, tomando como referencia un peso promedio de 50 KB[55] para cada consulta a la base de datos.

$$AB_{(Académico)} = \frac{50\ KB}{1\ usuario} * \frac{8\ bits}{1\ byte} * \frac{27\ usuarios}{40\ minutos} * \frac{1\ minuto}{60\ segundos}$$

$$AB_{(Académico)} = 4.5Kbps$$

3.3.6.6 Tráfico generado por mensajería instantánea.

En la actualidad el uso de chat es muy utilizado tanto por los administrativos como por los estudiantes por lo que será considerado para el diseño de la red. Se tiene 142 puertos para datos y un mensaje tiene un peso aproximado promedio de 1KB[56] por cada mensaje donde cada usuario envía uno cada minuto aproximadamente se requiere el ancho de banda detallado a continuación.

$$AB_{(Messenger)} = \frac{1KB}{1\ mensaje} * \frac{8\ bits}{1\ byte} * \frac{1\ mensaje}{1minutos} * \frac{1\ minuto}{60\ segundos}$$

$$AB_{(Messenger)} = 0.13\ Kbps$$

$$AB_{(Total)} = 142 * 0.13\ Kbps$$

$$AB_{(Total)} = 18.9\ Kbps$$

[55] [T5] Ing. Diego Pozo, Estudio y Diseño de una Red de Voz y Datos para la Unidad Educativa Municipal Quitumbe utilizando la tecnología Gigabit Ethernet para soportar servicios en tiempo real de VoIP, Video seguridad y Videoconferencia, Tesis EPN, Pág. 78

[56] [PW42] http://www.movistar.com.ve/particulares/Internet/soporte_preguntas_frecuentes.asp

3.3.6.7 Tráfico generado por impresión

Para determinar el ancho de banda ocupado para enviar una hoja de datos a imprimir se realizó un análisis del peso de diferentes hojas de Word, dicho análisis está detallado en el **ANEXO B** obteniendo los datos detallados en la tabla 3.7.

	Peso (KB)
Peso de una hoja de Word con diferente contenido	153
	33.1
	24.3
	25
Peso promedio	**47.08**

Tabla 3. 7 Peso de hojas de word. [7]

Para el servicio de impresión se hace una estimación de que cada usuario imprimirá 8 hojas por hora donde cada hoja tiene un peso aproximado de 47.08KB y que son 8[57] usuarios que utilizarán este servicio se necesitará el siguiente ancho de banda.

$$AB_{(Impresión)} = 8\ \frac{47.08\ KB}{1\ hoja} * \frac{8\ bits}{1\ byte} * \frac{8\ hojas}{1\ hora} * \frac{1\ hora}{3600\ segundos}$$

$$AB_{(Impresión)} = 6.7Kbps$$

3.3.6.8 Tráfico generado por descargar archivos de Internet

Para calcular el ancho de banda necesario para descargar un archivo desde Internet se utiliza 2 factores importantes que son: tamaño del archivo y el tiempo de descarga de dicho archivo. Un archivo de 1MB se descarga en un tiempo aceptable de un minuto, por lo que se requiere del siguiente ancho de banda.

[57] Rectora, Sor Mercy Sanchez, 2011

$$AB_{(Descarga)} = T_{archivo} * t_{descarga}$$

$$AB_{(Descarga)} = \frac{1000\ KB}{1\ minuto} * \frac{8\ bits}{1\ byte} * \frac{1\ minuto}{60\ segundos}$$

$$AB_{(Descarga)} = 16.7\ Kbps$$

Cabe indicar que no todos los usuarios conectados a Internet descargarán un archivo de forma simultánea, razón por la cual solo se calcula el ancho de banda requerido por los usuarios de la biblioteca que son 9 y la sala de profesores que son 3. Se toma como referencia este departamento porque es utilizado para que los estudiantes realicen investigación utilizando Internet.

$$AB_{(Descarga)} = 12 * 16.7\ Kbps$$

$$AB_{(Descarga)} = 200.4\ Kbps$$

3.3.6.9 Tráfico por Aplicación y Servicio

En la tabla 3.8 se realiza un detalle del tráfico total requerido para todos los servicios y aplicaciones que se prestarán en la red de la Unidad Educativa.

APLICACIÓN	CAPACIDAD REQUERIDA (Kbps)
Correo Electrónico	3.11
Páginas Web	444.6
Base de Datos	4.5
Mensajería Instantánea	18.9
Impresión	6.7
Descargar Archivos de Internet	200.4
TOTAL APLICACIONES	***678,21***
SERVICIO	
Telefonía IP	1100.8
Video Vigilancia IP	6831.52
TOTAL SERVICIOS	***7932.32***
TOTAL GENERAL	***8610.53***

Tabla 3. 8 Ancho de banda total requerido de la red interna. [8]

Se requiere una capacidad para la red interna de la Institución de **8.61 Mbps** para prestar todos los servicios requeridos.

3.3.6.10 Conexión a Internet

Para calcular la capacidad requerida para el enlace a Internet, se toma en cuenta el tráfico generado por acceder a las páginas web, descargas de Internet y mensajería instantánea. Lo cual se detalla en la tabla 3.9.

APLICACIÓN	CAPACIDAD REQUERIDA (Kbps)
Páginas Web	444.6
Mensajería Instantánea	18.9
Descargar Archivos de Internet	150.3
TOTAL	***663.9***

Tabla 3. 9 Capacidad requerida para el enlace a Internet. [9]

De acuerdo al análisis realizado en la tabla 3.9 se requiere un enlace con una capacidad de 663.9 Kbps: sin embargo, los ISPs (*proveedores de servicio de Internet*) ofrecen enlaces con capacidades estándar de 1 Mbps el cual puede ser simétrico (1:1) y sin compartición con otros usuarios.

La UESMDM tiene contratado un enlace de 512 Kbps simétrico (1:1) con la empresa CNT por lo que se sugiere contratar un enlace de 1 Mbps simétrico para cubrir las necesidades que tiene al conectar todas las computadoras a la red local.

3.3.6.11 Proyección de Tráfico

Al realizar un diseño de red se debe tomar en cuenta una estimación de tráfico futuro. Esto es primordial para asegurar un correcto funcionamiento de la red. El

crecimiento de tráfico se da debido al aumento de personal y actualización tecnológica.

El rediseño se lo realizó para todos los usuarios actuales: sin embargo, cada año se puede tener un aumento del personal administrativo o docente, para lo cual se considera un crecimiento del 1% anual como se indicó anteriormente.

El tráfico que va existir en la red de acuerdo al análisis anterior es de 8.6 Mbps y para calcular el crecimiento futuro se utiliza la siguiente ecuación la cual fue especificada en el punto 3.3 .6.2.2.

$$A_f = A_0(1 + f_c)^n$$

$$A_f = 8.61(1 + 0.01)^5$$

$$A_{f0-5} = 9.05\ Mbps$$

En la tabla 3.10 se detalla el tráfico proyectado durante 5 años.

Años	Tráfico Final (Mbps)
1	8,69
2	8,78
3	8,87
4	8,96
5	9.05

Tabla 3. 10 Proyección de Tráfico. [10]

En la figura 3.6 se realiza el incremento de tráfico durante los próximos 5 años

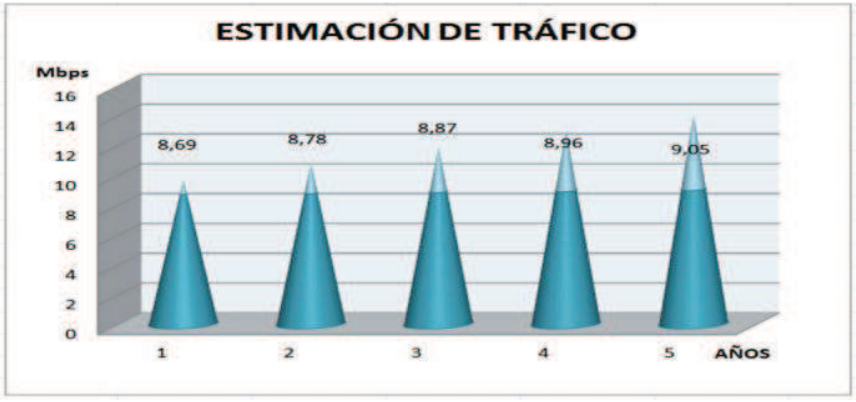


Figura 3. 6 Estimación de Tráfico a 5 años. [6]

3.4 REDISEÑO DE LA RED PASIVA

La UESMDM requiere contar con una red eficiente para prestar los servicios internos y externos optimizando recursos y mejorando el nivel educativo de los estudiantes.

De acuerdo a los servicios y aplicaciones que requiere la UESMDM no necesita contar con un medio de comunicación que soporte un gran ancho de banda por lo que se va a utilizar cable UTP CAT 5E con tecnología Fast Ethernet.

3.4.1 CABLEADO ESTRUCTURADO

El diseño del cableado estructurado está dimensionado para conectar a todas las estaciones de trabajo de la Institución. Además, permitir la conexión entre los departamentos.

En el diseño del cableado primero se elige el medio de transmisión a utilizar, para lo cual se considera: ancho de banda, alcance máximo y velocidad de transmisión, en este caso en particular la inmunidad al ruido no es importante debido a que el cableado no está cerca de fuentes que puedan causar interferencia.

Actualmente, la Institución tiene implementado cable UTP Cat 5E en todas las áreas de trabajo y en el cableado vertical, como se mencionó en el capítulo 2.

De acuerdo al análisis realizado de las nuevas necesidades que tiene la UESMDM y por las nuevas aplicaciones como video vigilancia y telefonía IP, se puede seguir utilizando cable UTP CAT 5E, el cual esta estandarizado según la norma TIA/EIA 568 B-2 y ratificada en la norma TIA/EIA 568 C, este tipo de cable ofrece altas

tasas se transmisión, escalabilidad, es fácil de instalar, y un alcance máximo de 100 m.

Cabe indicar que la distancia entre el cuarto de equipos y los diferentes departamentos no sobrepasa los 100 m por lo que es adecuado utilizar cable UTP CAT 6 como Backbone para cubrir la demanda de la Unidad Educativa.

En la tabla 3.11 se especifica los diferentes estándares que se van a utilizar para realizar el rediseño del cableado estructurado.

ESTÁNDAR	DESCRIPCIÓN
ANSI/TIA/EIA 568 B	Descripción de cableado de telecomunicaciones en Edificios comerciales, está dividido en tres partes de las cuales en este proyecto solo son necesarias las dos primeras, debido a que no se utilizará fibra óptica en el diseño.
	ANSI/TIA/EIA 568 B.1 –especificación de los requisitos generales.
	ANSI/TIA/EIA 568 B.2 –componentes para cableado utilizando cable UTP de 100 ohm.
ANSI/TIA/EIA 569 A	Esta norma es utilizada para realizar el enrutamiento y selección espacios de telecomunicaciones para Edificios Comerciales.
ANSI/TIA/EIA 606 A	Esta norma se refiere a la administración de la Infraestructura de Telecomunicaciones en Edificios Comerciales.
ANSI/TIA/EIA 607	Utilizada para establecer los requerimientos para Conexiones y Puestas a tierra para Telecomunicaciones en Edificios Comerciales.
TSB 67	Son especificaciones de rendimiento de transmisión para pruebas de campo de Sistemas de Cableado UTP

Tabla 3. 11 Estándares de Cableado Estructurado. [11]

3.4.1.1 Área de Trabajo

En este subsistema se especifica la cantidad de patch cords por departamento que se van a utilizar para conectar las estaciones de trabajo, teléfonos IP y las cámaras IP a la red de la Institución.

En la tabla 3.12 se detalla el número de *patch cords* necesarios por departamento, los cuales tendrán una longitud de 3 metros. Cabe indicar, que el *patch Cord* a utilizar tiene que tener las mismas o mejores características que el cableado horizontal según la norma ANSI/TIA/EIA-568 B.2, por lo que se va a utilizar CAT 5E.

DEPARTAMENTOS	NÚMERO DE PATCH CORDS (U)
Administrativos	20
Lab. Secundaria	42
Lab. Primaria	46
Nuevo laboratorio	22
Biblioteca	10
Salón	2
Trabajo Social	2
Inspección	2
Equipo Pastoral	2
Departamento Médico	2
Sala de profesores	4
Inglés	2
Catequesis	2
AP	3
Cámaras IP	8
TOTAL	**169**

Tabla 3. 12 Número de Patch Cords Requerido. [12]

Se requiere 169 *patch cords* para conectar a todas las estaciones de trabajo, cámaras IP, teléfonos IP y AP de la Institución para dar servicio a los usuarios que son: estudiantes, docentes y trabajadores.

3.4.1.2 Cableado Horizontal

Para el cableado horizontal se va a utilizar cable UTP CAT 5E según la norma ANSI/TIA/EIA-568-B.2. La distribución de puntos de red será de acuerdo al

departamento, para los laboratorios sólo se tendrá puntos de datos, esto es debido a que los usuarios en este caso los estudiantes solo requieren este servicio. Mientras que para el área administrativa se proveerá dos puntos de red por usuario: uno para datos y otro para voz IP.

Para la conexión de los puntos de acceso para la red inalámbrica se ubicarán los puntos de red necesarios para dar servicio a visitantes, docentes, administrativos y estudiantes que requieran conectarse al Internet.

Para brindar mejor seguridad en lugares críticos de la UESMDM se ubicarán puntos de red para conectar las cámaras IP, con las que se realizará un monitoreo continuo.

Para la asignación de puntos de red se tomo en cuenta un crecimiento total del 5% por áreas donde se cuenta con espacio suficiente para incrementar equipos si así lo requiere la Institución. En la tabla 3.13 se detallan los puntos de red que se designarán por departamento.

DEPARTAMENTOS	**PUNTOS DE RED**			**TOTAL**
	DATOS	VOZ	CAMARAS	
Administrativos	10	10	5	25
Lab. Secundaria	42	0	1	43
Lab. Básica	46	0	1	47
Nuevo laboratorio	22	0	1	23
Biblioteca	9	1	0	10
Inglés	2	0	0	2
Catequesis	2	0	0	2
Salón	2	0	0	2
Trabajo Social	1	1	0	2
Inspección	1	1	0	2
Equipo Pastoral	1	1	0	2

DEPARTAMENTOS	PUNTOS DE RED			TOTAL
	DATOS	VOZ	CAMARAS	
Médico	1	1	0	2
Sala de profesores	3	1	0	4
AP	3	0	0	3
TOTAL	**145**	**16**	**8**	**169**

Tabla 3. 13 Asignación de puntos de red. [13]

La figura 3.7 es un esquema gráfico de como están distribuidos los deparatementos en el edificio de la Institución.

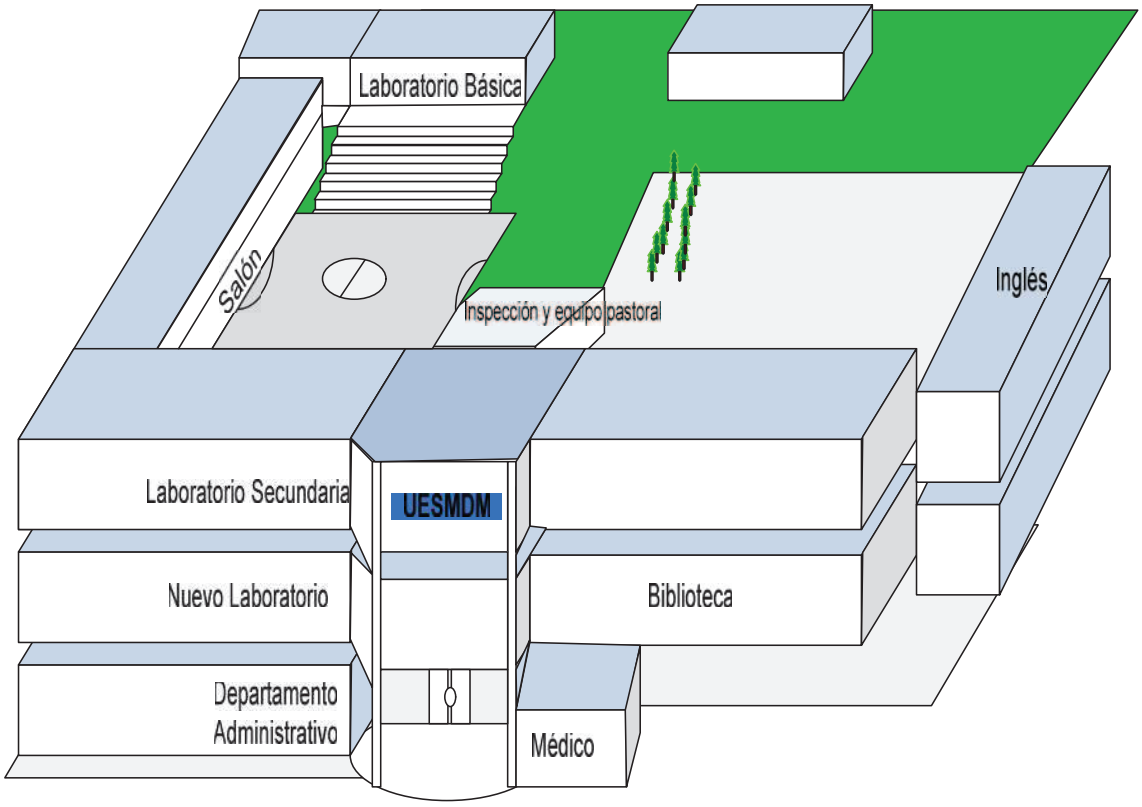


Figura 3. 7 Localizaciones de los Departamentos. [7]

En la tabla 3.14 se detalla en número de face plates y jacks necesarios para todos los puntos que se van a instalar. Cabe indicar que los face plates simples serán utilizados para conectar las cámaras y los AP.

Departamentos	Jacks	Face Plate Dobles	Face Plate Simple
Administrativos	15	5	5
Lab. Secundaria	43	21	1
Lab. Básica	47	23	1
Nuevo laboratorio	23	11	1
Biblioteca	10	5	0
Inglés	2	1	0
Catequesis	2	1	0
Salón	2	1	0
Trabajo Social	2	1	0
Inspección	2	1	0
Equipo Pastoral	2	1	0
Médico	2	1	0
Sala de profesores	4	2	0
AP	3	0	3
TOTAL	159	74	11

Tabla 3. 14 Face Plate a utilizar. [14]

Figura 3. 8 Face Plate y Jack's a utilizar. [8]

3.5.1.2.1 Cálculo de la Longitud del Cable

En el **ANEXO C** se encuentra los planos correspondientes al rediseño del sistema de cableado estructurado de la Unidad Educativa; en estos, se ubican los puntos de red para datos, voz y video vigilancia IP que son considerados en este proyecto.

Para calcular la distancia máxima y mínima del cableado horizontal se utilizó los planos de cada departamento y de acuerdo a estas distancias se calculó la cantidad de cable necesario por departamento y el total.

Adicionalmente, se realiza el etiquetado correspondiente a cada punto de red de acuerdo al siguiente formato D/V/VV/APX. D se utiliza para representar un punto de datos, V un punto de voz, VV un punto para video vigilancia, X es el número de departamento. La localización de éstos se la realizó en base a la ubicación donde se encuentre el punto de red.

Longitud máxima: Lmax
Longitud mínima: Lmin
Longitud media: Lmed

Fórmulas para calcular el número de rollos necesarios por cada departamento[58]

$$Lmed = \frac{L\max + L\min}{2}[m] \qquad \textbf{Ecuación 3.5}$$

$$L'med = Lmed + Lmed * 0.1 + 2.5[m] \qquad \textbf{Ecuación 3.6}$$

$$\#Corridas = \frac{305}{L'med} \qquad \textbf{Ecuación 3.7}$$

$$\#Rollos = \frac{\#Puntos}{\#Corridas} \qquad \textbf{Ecuación 3.8}$$

Un ejemplo del uso de las fórmulas para determinar la cantidad de cable UTP Cat 5E en cada departamento, para este caso el Administrativo.

$$Lmed = \frac{27.98 + 6.4}{2}[\mathrm{m}]$$

[58] [FT3] Folleto sobre Cableado Estructurado, Ing. Soraya Sinche

$$Lmed = 17.19[\text{m}]$$

$$L'med = 17.19 + 17.19 * 0.1\ 2.4[\text{m}]$$

$$L'med = 21.41[\text{m}]$$

$$\#corridas = \frac{305}{21.41}$$

$$\#corridas = 14.24$$

$$\#rollos = \frac{25}{14.41}$$

$$\#rollos = 1.75$$

En la tabla 3.15 se detalla la cantidad de cable utilizado en cada departamento.

DEPARTAMENTOS	Lmáx (m)	Lmín (m)	# Corridas	# Rollos
Administrativos	27.98	6.4	14	2
Lab. Secundaria	14.74	6.38	21	2
Lab. Básica	18.4	5.5	19	2
Nuevo laboratorio	16.7	6.5	20	1
Biblioteca	15.58	5.2	22	1
Longitud (m) considerando los puntos de red que existen en cada departamento				
DEPARTAMENTOS	**Longitud (m)**	**Número de puntos de red**		
Inglés	125	2		3
Catequesis	126	2		
Trabajo Social	44	2		
Inspección	50	2		
Equipo Pastoral	54	2		
Médico	110	2		
Salón	90	2		
Sala de profesores	120	2		
AP	40	3		
TOTAL		**11**		

Tabla 3. 15 Total de Rollos de cable UTP CAT 5E para Cableado Horizontal. [15]

Para el caso como el departamento de inglés se realizó las mediciones para los 2 puntos de red que se instalarán, dando como resultado 125 m, de igual forma se realizó las medidas en los departamentos que no tienen datos tales como longitud máxima y mínima, debido a que las fórmulas no serían aplicables.

3.4.1.3 Elementos para el Enrutamiento y Terminación

3.5.1.3.1 Subsistema Horizontal

La norma ANSI/EIA/TIA 569 A específica los ductos a utilizar en cableado estructurado para tendido de cable horizontal y vertical, para este diseño se recomiendan utilizar canaletas decorativas para todo el cableado horizontal las cuales estarán sujetas a la pared mediante pernos con tacos Fisher. Además, las canaletas deben ser instaladas con sus respectivos accesorios y acopladores cumpliendo con el radio de curvatura de 27 mm que es el utilizado para cable UTP CAT 5E.

Para la elección del tamaño de las canaletas se toma en cuenta solo el 60% de su capacidad según la norma de cableado estructurado. La cantidad de elementos requeridos se detalla en la tabla 3.16

Material	Dimensión (mm)	Longitud (m)/Unidad (U)	Cantidad de Material
Canaleta Decorativa	32X12	2 m	18
	40X22	2 m	16
	40X40	2 m	12
	60X40	2 m	5
Codo Interno	32X12	1 U	6
	40X22	1 U	16
	40X40	1 U	16
	60X40	1 U	6

Material	Dimensión (mm)	Longitud (m)/Unidad (U)	Cantidad de Material
Codo Externo	32X12	1 U	6
	40X22	1 U	13
	40X40	1 U	11
	60X40	1 U	5
Codo Plano	32X12	1 U	5
	40X22	1 U	3
	40X40	1 U	2
Derivación en T	40X22 a 32X12	1 U	1
	40X40 a 32X12	1 U	2
	60X40 a 32X12	1 U	2
	60X40	1U	2
Terminación	32X12	1U	18

Tabla 3. 16 Elementos a Utilizar. [16]

3.5.1.3.2 Subsistema Vertical

Para el cableado vertical se va a utilizar cable UTP CAT 6, con el cual se puede tener una distancia máxima de 100 m, con una velocidad de transmisión de hasta 1Gbps.

La utilización del cable UTP CAT 6 es debido a que sobre este subsistema converge todo el tráfico generado por cada área de trabajo; cabe indicar, que se utilizará redundancia para optimizar el tiempo de respuesta en caso de un daño en el cable principal.

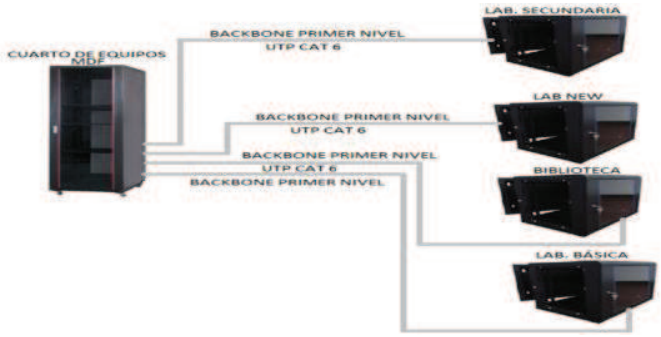


Figura 3. 9 Diagrama del cableado vertical. [9]

En la tabla 3.17 se especifica la cantidad de cable necesario para la implementación del cableado vertical, para unir los armarios de telecomunicaciones con el cuarto de equipos.

DEPARTAMENTOS	CABLE UTP	CONDUIT		CAJETÍN DE PASO	CODOS	ABRAZADERAS
	Long (m)	Diámetro (pulg)	Long (m)	(U)	(U)	(U)
Lab básica	180	¾	90	3	6	90
		1	20		7	20
Lab Secundaria	90	¾	4	3	5	4
		1 1/4	30		3	30
Lab New	75	¾	4	-	2	4
Biblioteca	150	1	17	3	4	17
		¾	18		4	18
Total	***495***	***¾***	***116***	***9***	***17***	***116***
		1	***37***		***11***	***37***
		1 1/4	***30***		***3***	***30***

Tabla 3. 17 Materiales utilizados para el cableado vertical. [17]

Para el cableado vertical se va a utilizar 2 rollos de cable UTP CAT 6 de 24 AWG esto se debe a la redundancia de enlaces.

3.4.1.4 Closet de Telecomunicaciones

En los departamentos tales como; nuevo Laboratorio, Lab Secundaria, Biblioteca y Lab Básica se utilizará closets de telecomunicaciones, los cuales serán dimensionados de acuerdo a los elementos y equipos que serán instalados en cada uno de ellos.

Para el dimensionamiento de los closets se tomará en cuenta las medidas en unidades (U) para cada elemento, como se detalla en la tabla 3.18. Además, se debe considerar que los equipos no se pueden colocar montados por lo que se debe dejar espacio que permita la libre circulación del aire para que los equipos trabajen con una temperatura adecuada.

Adicionalmente, es recomendable dejar un espacio de crecimiento de 2 (U) para la ubicación de nuevos equipos si así lo requiere el crecimiento de la Unidad Educativa.

DEPARTAMENTO	ELEMENTO	CANTIDAD	UNIDADES (U)
NEW LABORATORIO	Switch de Acceso 24p	2	2
	Organizador horizontal	2	4
	Organizador vertical	2	0
	Patch Panel 24p	2	2
	Panel de Alimentación AC	1	1
	Separación	2	2
	Crecimiento	2	2
TOTAL			**13**
LAB SECUNDARIA	Switch de Acceso 24p	2	2
	Organizador horizontal	2	4
	Organizador vertical	2	0
	Patch Panel 24p	2	2
	Panel de Alimentación AC	1	1
	Separación	2	2
	Crecimiento	2	2
TOTAL			**13**
LAB BÁSICA	Switch de Acceso 24p	3	3
	Organizador horizontal	3	6
	Organizador vertical	2	0
	Patch Panel 24p	3	3
	Panel de Alimentación AC	1	1
	Separación	2	2
	Crecimiento	2	2
TOTAL			**17**
BIBLIOTECA	Switch de Acceso 24p	1	1
	Organizador horizontal	1	2
	Organizador vertical	2	0
	Patch Panel 24p	1	1
	Panel de Alimentación AC	1	1
	Separación	2	2
	Crecimiento	2	2
Total			**9**

Tabla 3. 18 Dimensionamiento del los Closets de Telecomunicaciones. [18]

3.4.1.5 Sala de Equipos

Este subsistema está ubicado en el departamento administrativo y deberá cumplir con las especificaciones de acuerdo a las normas ANSI/TIA/EIA 568-B y ANSI/TIA/EIA 569-A.

En la sala de equipos se utilizará un rack abierto con sus respectivos organizadores horizontales y verticales, este rack tiene mayor tamaño de los detallados anteriormente, las características se las detalla en la tabla 3.19.

Para el diseño de este rack se debe considerar si es el caso, servidores y otros dispositivos utilizados en el cuarto de equipos.

DEPARTAMENTO	ELEMENTO	CANTIDAD	UNIDADES (U)
ADMINISTRATIVO	Switch de Acceso 24p	2	2
	Switch de Core 24p	1	1
	Organizador horizontal	5	10
	Organizador vertical	2	0
	Patch Panel 24p	4	4
	Panel de Alimentación AC	1	1
	Separación	2	2
	Crecimiento	2	2
TOTAL			**22**

Tabla 3. 19 Dimensionamiento del rack de la Sala de Equipos. [19]

3.4.1.6 Etiquetación

La etiquetación y administración de todo el sistema de cableado estructurado se la realiza de acuerdo a la norma ANSI/TIA/EIA606.

La etiquetación facilita la administración de la infraestructura del cableado estructurado la cual se debe implementar en los extremos y en un punto intermedio del cableado. Además para mejor administración del cableado se utiliza código de color, en la UESMDM se va a utilizar el código de color detallado en la tabla 3.20

Color	Utilización
Azul	Cableado Horizontal
Blanco	Backbone de primer nivel
Morado	Conexiones cruzadas
Naranja	Proveedor Externo

Tabla 3. 20 Código de Color. [20]

La nomenclatura utilizada en la UESMDM es la detallada a continuación.

RE-R1A-PV01

RE = Rectorado

R1A = Rack uno en el Patch pannel A

PV01 = Puerto de voz número uno

PD01 = Puerto de datos número uno

Para realizar todo la etiquetación se va a utilizar la siguiente identificación para cada departamento la cual se detalla a continuación:

DEPARTAMENTO	IDENTIFICACIÓN
Dobe 1	DOB1
Dobe 2	DOB2
Bodega	BO
Coordinación E. Básica	CEB
Vicerrectorado	VR
Rectorado	RE
Secretaria	SE

DEPARTAMENTO	IDENTIFICACIÓN
Almacén	AL
Colecturía	CO
Recepción	RC
Lab. Secundaria	LS
Lab. Básica	LB
Nuevo laboratorio	LN
Biblioteca	BI
Inglés	EN
Catequesis	CA
Salón	SA
Trabajo Social	TS
Inspección	IN
Equipo Pastoral	EP
Médico	ME
Sala de profesores	SP

Tabla 3. 21 Identificación de los departamentos de la UESMDM (Continuación). [21]

En el **ANEXO D** se detalla la ubicación de todos los puntos de datos y de voz con su respectiva nomenclatura.

3.4.1.7 Pruebas de certificación [59]

Para garantizar un correcto funcionamiento de la red LAN se debe realizar pruebas del cableado tanto vertical como horizontal.

La norma TIA/EIA TSB-67 es utilizada para especificaciones de rendimiento de transmisión para pruebas de campo solo para el medio de transmisión UTP. Dicha norma especifica las siguientes pruebas.

- Mapa de Alambrado

[59] [FT3]Folleto Sobre Cableado Estructurado. Ing Soraya Sinche, 2008

- Longitud.
- Atenuación
- Pérdidas de Inserción
- Next.
- PS Next
- ELFext
- PS ELFext
- Pérdidas por Retorno.
- Tiempo de Propagación.

En la figura 3.10 se especifica los valores mínimos aceptados para realizar las pruebas a realizarse de cable de cobre de 4 pares a 100 MHz

Category 5e Channel

Frequency (MHz)	Insertion Loss (dB)	NEXT (dB)	PSNEXT (dB)	ELFEXT (dB)	PSELFEXT (dB)	Return Loss (dB)
1.0	2.2	>60	>57	57.4	54.4	17.0
4.0	4.5	53.5	50.5	45.4	42.4	17.0
8.0	6.3	48.6	45.6	39.3	36.3	17.0
10.0	7.1	47.0	44.0	37.4	34.4	17.0
16.0	9.1	43.6	40.6	33.3	30.3	17.0
20.0	10.2	42.0	39.0	31.4	28.4	17.0
25.0	11.4	40.3	37.3	29.4	26.4	16.0
31.25	12.9	38.7	35.7	27.5	24.5	15.1
62.5	18.6	33.6	30.6	21.5	18.5	12.1
100.0	24.0	30.1	27.1	17.4	14.4	10.0

Category 5e Channel Requirements
Maximum channel propagation delay: 555 ns at 10 MHz
Maximum channel delay skew: 50 ns at 100 MHz

Category 5e Permanent Link

Frequency (MHz)	Insertion Loss (dB)	NEXT (dB)	PSNEXT (dB)	ELFEXT (dB)	PSELFEXT (dB)	Return Loss (dB)
1.0	2.1	>60	>57	58.6	55.6	19.0
4.0	3.9	54.8	51.8	46.6	43.6	19.0
8.0	5.5	50.0	47.0	40.6	37.5	19.0
10.0	6.2	48.5	45.5	38.6	35.6	19.0
16.0	7.9	45.2	42.2	34.5	31.5	19.0
20.0	8.9	43.7	40.7	32.6	29.6	19.0
25.0	10.0	42.1	39.1	30.7	27.7	18.0
31.25	11.2	40.5	37.5	28.7	25.7	17.1
62.5	16.2	35.7	32.7	22.7	19.7	14.1
100.0	21.0	32.3	29.3	18.6	15.6	12.0

Category 5e Permanent Link Requirements
Maximum link propagation delay: 518 ns at 10 MHz
Maximum link delay skew: 45 ns at 100 MHz

Category 5e Connecting Hardware

Frequency (MHz)	Insertion Loss (dB)	NEXT (dB)	FEXT (dB)	Return Loss (dB)
1.0	0.1	65.0	65.0	30.0
4.0	0.1	65.0	63.1	30.0
8.0	0.1	64.9	57.0	30.0
10.0	0.1	63.0	55.1	30.0
20.0	0.2	57.0	49.1	30.0
25.0	0.2	55.0	47.1	30.0
31.25	0.2	53.1	45.2	30.0
62.5	0.3	47.1	39.2	24.1
100.0	0.4	43.0	35.1	20.0

Figura 3. 10 Valores aceptables para realizar pruebas en cable UTP CAT 5E. [10]

3.4.1.8 Diagrama Lógico del Sistema de Cableado Estructurado

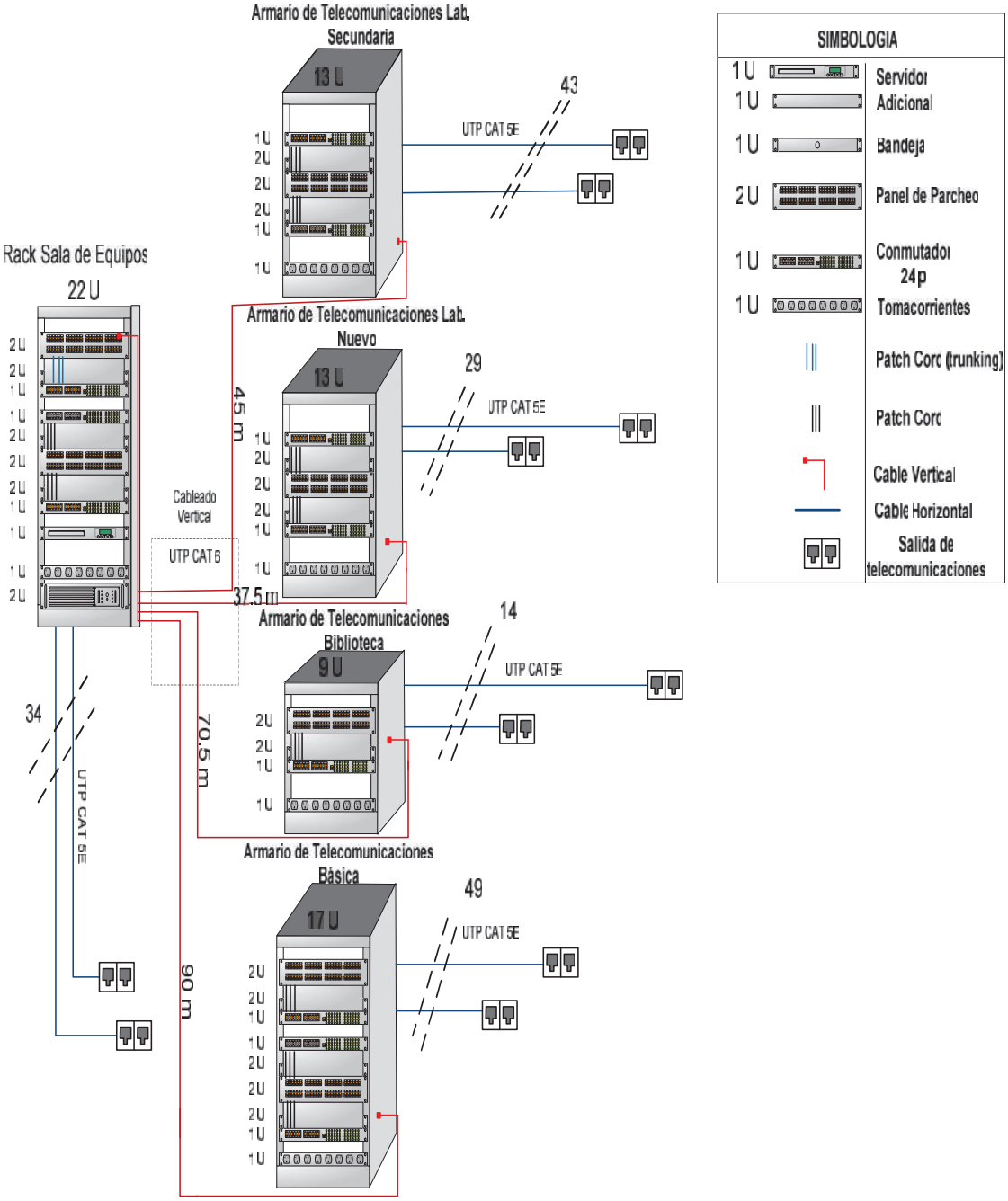


Figura 3. 11 Diagrama lógico del Sistema de cableado Estructurado. [11]

3.6 REDISEÑO DE LA RED ACTIVA

3.6.1 DISEÑO LÓGICO

El diseño lógico de la red activa se basa en la creación del direccionamiento IP para todos los departamentos de la UESMDM. Además, de definir las VLANs de acuerdo al tipo de servicio y departamento.

3.6.1.1 Breve descripción de VLANs

Las VLANs permiten crear redes de forma lógica y no física, reduciendo con esto el tamaño de los dominios de difusión, mejorando así la administración de los recursos prestados por una red.

Para tener un control óptimo, mejorar la gestión y administración de la red se crearán varias VLANs. De acuerdo al tipo de información que comparten en común cierto grupo de usuarios.

Las VLANs que se crearán están detalladas a continuación:

- **Administrativos**
  Está conformada por todo el personal administrativo el cual consta de 13 usuarios.
- **Telefonía**
  Incluye todos los usuarios que tienen una extensión telefónica. El número de usuarios que pertenecen a esta VLAN son 16.
- **Video vigilancia**
  Está conformada por todas las cámaras instaladas en puntos estratégicos de la UESMDA, consta de 8 usuarios.

- **Académica**

  Está conformada por los laboratorios y la biblioteca para prestar servicio al área estudiantil, consta de 119 estaciones de trabajo disponibles.

- **Inalámbrica**

  Esta VLAN es creada para todos los estudiantes y profesores que se conecten a la red de forma inalámbrica. La cantidad de posibles usuarios que utilizarán este servicio se lo detalla en el literal 3.7

- **Informática**

  Los usuarios que pertenecen a esta VLAN tienen acceso a la configuración de los equipos, tienen acceso total excepto a las paginas bloqueadas según las políticas de la Institución.

- **Servidores**

  Esta VLAN es la más importante para evitar que usuarios no autorizados tengan acceso a los servidores. Los cuales son aproximadamente 8.

3.6.1.2 Direccionamiento IP

Una vez definidas las VLANs principales que se deben crear en la Unidad Educativa y con el número de usuarios que pertenecen a cada una de éstas, se realiza el direccionamiento IP.

La UESMDM tiene un requerimiento de 169 direcciones IP privadas para direccionar a todos los equipos requeridos en el rediseño de la red. Para direccionar a todos los equipos excepto los servidores se va a utilizar un servidor DHCP, los servidores tendrán asignadas IPs estáticas.

Actualmente, la Institución está utilizando una dirección de clase C que es la 192.168.1.0 con máscara 255.255.255.0 por lo que se utilizará la misma dirección

pero se crearán subredes utilizando la técnica de asignación de direcciones denominada VLSM[60]

La UESMDM estará conformada por 7 VLANs. Las que permitirán proporcionar cierta clase de seguridad a los datos. Además, posibilitan la agrupación de dispositivos de red en una misma subred independientemente de que se encuentren o no en el mismo sector físico. En la tabla 3.22 se detalla las direcciones IP para cada subred y la asignación a cada VLAN.

VLAN	Subred	1° Dir. IP	Ult. Dir. IP	Broadcast	Mask Subred
Académica	**192.168.1.0**	192.168.1.1	192.168.1.254	192.168.1.255	255.255.255.0
Telefonía	**192.168.2.0**	192.168.2.1	192.168.2.30	192.168.2.31	255.255.255.224
Administrativos	**192.168.2.32**	192.168.2.33	192.168.2.62	192.168.2.63	255.255.255.224
V. Vigilancia	**192.168.2.64**	192.168.2.65	192.168.2.78	192.168.2.79	255.255.255.240
Servidores	**192.168.2.80**	192.168.2.81	192.168.2.94	192.168.2.95	255.255.255.240

[60] VLSM (VARIABLE LENGTH SUBNET MASK) es utilizada para direccionar subredes dentro de una red, empleando máscaras con diferente longitud.

VLAN	Subred	1° Dir. IP	Ult. Dir. IP	Broadcast	Mask Subred
Informática	**192.168.2.96**	192.168.2.97	192.168.2.102	192.168.2.103	255.255.255.248
Visitantes	**192.168.3.0**	192.168.3.1	192.168.3.254	192.168.3.255	255.255.255.0

Tabla 3. 22 Asignación de direcciones IP. [22]

La primera dirección IP de cada rango de host válidos se designa como dirección para el default Gateway.

Adicionalmente, en la tabla 3.23 se detalla la cantidad de direcciones IP designadas a cada VLAN considerando las direcciones IP que están libres para uso futuro. Cabe indicar que las VLANs serán por puerto.

VLAN	Cantidad de Direcciones IP			
	Totales	Utilizadas	Libres	% Utilización
Académica	**253**	129	124	50.98%
Telefonía	**29**	16	13	55.17%
Administrativos	**29**	13	16	44.8%
V. Vigilancia	**13**	8	5	61.53%
Servidores	**13**	6	7	53.85%
Informática	**5**	1	4	20%

Tabla 3. 23 Asignación de direcciones IP por VLAN Utilizadas y Libres. [23]

La figura 3.12 representa las VLANs que se deben crear en los switch de cada departamento, por lo que los dispositivos seleccionados deben soportar VLANs.

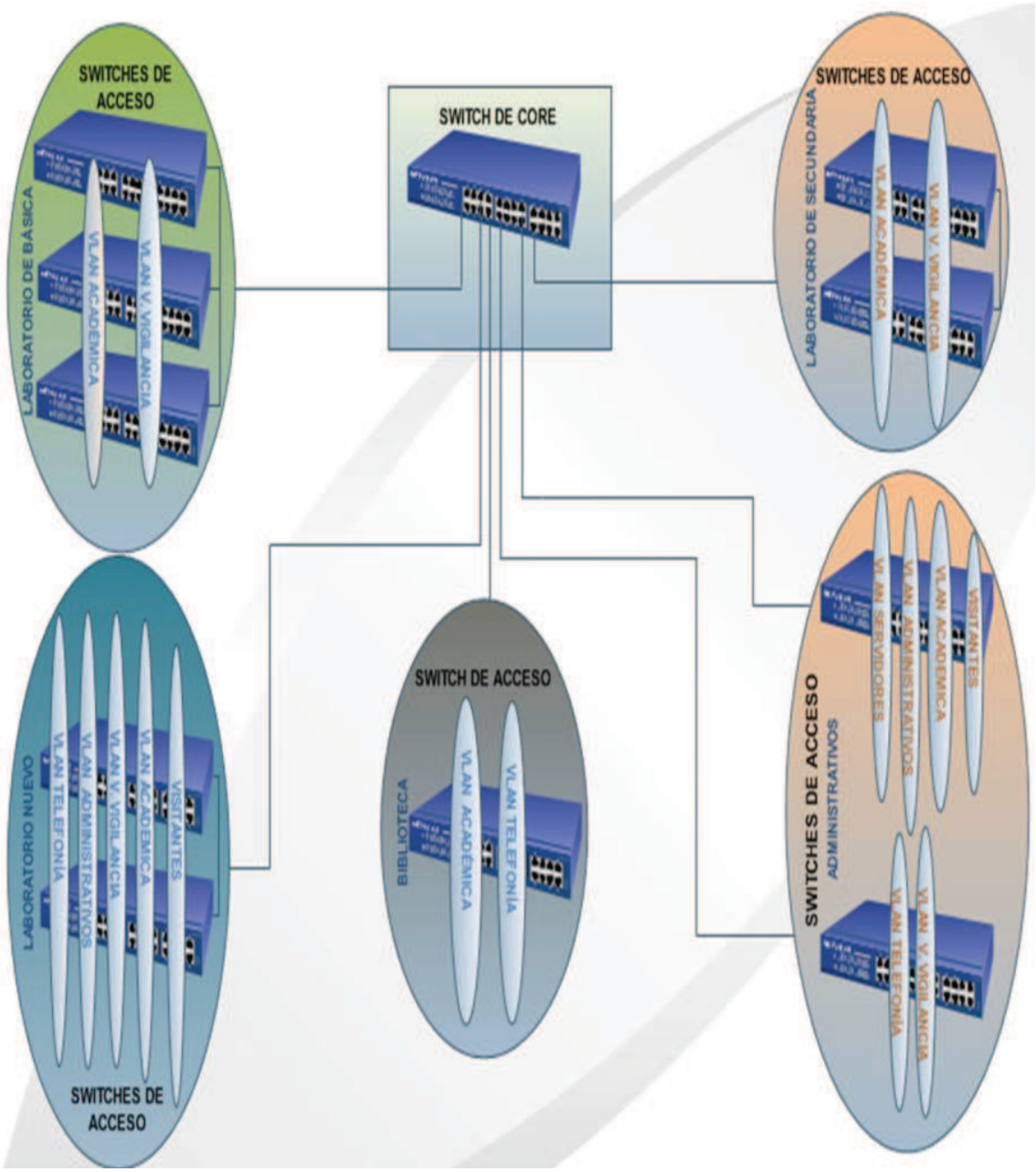


Figura 3. 12 Distribución de VLAN en los dispositivos de Red. [12]

La red de la Unidad educativa será una red convergente que permita transmitir voz, datos y video por una sola infraestructura, sin embargo para la selección y

ubicación de los equipos se realizará un análisis de sus caracteristicas por separado.

3.6.2 REDISEÑO DE LA RED PARA DATOS

Para realizar el diseño de la red de datos se consideran los equipos de networking, servidores y estaciones de trabajo que estarán conectados a la red interactuando entre sí para brindar un servicio de eficiente al usuario final.

3.6.2.1 Diagrama de la Red

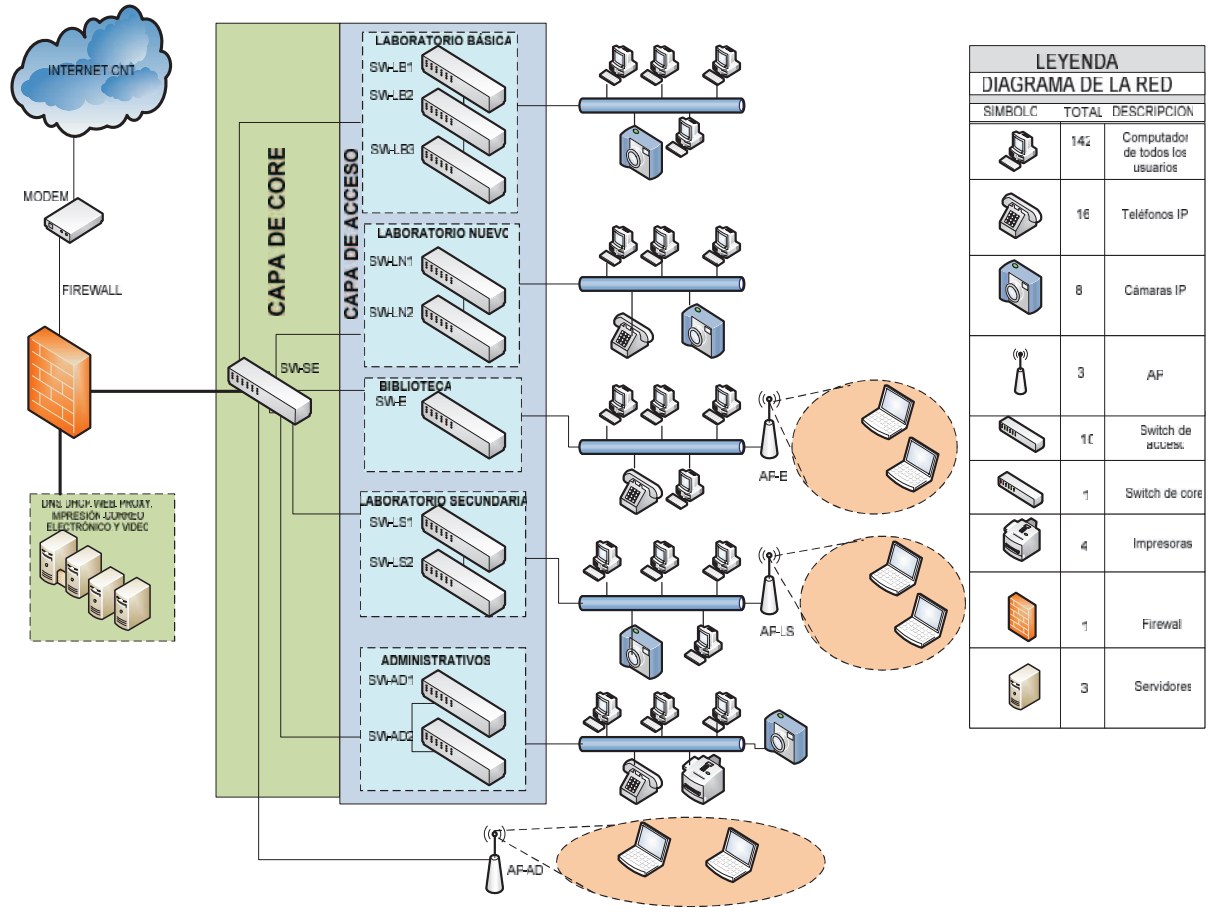


Figura 3. 13 Diagrama Físico de la red UESMDM. [13]

La red está estructurada en dos niveles que son: de acceso y de core, en el de acceso estarán conectados los hosts, cámaras IP y teléfonos. Cabe indicar que no se contará con redundancia de equipos por lo que se buscará un equipo con buenas características para el core de la red.

3.6.2.2 Estaciones de trabajo

Los host también conocidos como estaciones de trabajo son los dispositivos que interactúan de forma directa con los usuarios de la red, los cuales acceden a todos los servicios que presta la red mediante estos dispositivos.

La UESMDM está en un proceso de actualización de PCs por lo que está adquiriendo nuevos equipos de primera tecnología con excelentes características técnicas capaces de soportar aplicaciones actuales que requieren un óptimo desempeño de hardware y software de los equipos.

Como se mencionó en el capítulo 2 todos los equipos utilizan el Sistema Operativo Windows en sus diferentes versiones con sus respectivas aplicaciones de acuerdo al grupo de usuarios al que pertenezca.

3.6.2.3 Equipos de Conectividad

Para la elección del switch se tomará en cuenta dos parámetros técnicos tales como: velocidad de backplane y protocolos de la red.

Para calcular el backplane de los switch se considera el número de puertos y la velocidad que tenga cada uno de ellos. Es decir: para un switch de 24 puertos con una velocidad de 100 Mbps y 2 puertos Full dúplex a 1000 Mbps que es este caso el backplane de ser de (24x100 Mbps + 2x1000 Mbps)(2) = 8.8 Gbps.

Los switches deben soportar ciertos protocolos de red de acuerdo a si son o no administrables, para este caso en particular capa de acceso y de core. Los switch de core deben soportar los siguientes protocolos.

- STP (*Spanning Tree Protocol*)
  Este protocolo es utilizado para activar o desactivar de forma automática enlaces redundantes para no generar bucles locales en la red.
- TELNET (*Telecommunication Network*)
  Permite la administración remota de los switches.
- $SNMP_{V\ (1,2,3)}$ (*Simple Network Management Protocol*)
  Es un protocolo utilizado para administrar la red
- RIP (*Routing Information Protocol*)
  Es un protocolo de enrutamiento que permite intercambiar información sobre redes IP.
- OSPF(*Open Shortest Path First*)
  Es un protocolo de enrutamiento que permite determinar la ruta más corta.
- RMON(*Remote Monitoring*)
  Este protocolo permite monitorizar los switch de forma remota.
- DHCP (*Dynamic Host Configuration Protocol*)
  Es utilizado para asignar de forma dinámica las direcciones IP en la red.

3.6.2.3.1 Características de los Switches de Acceso

Después de realizar un análisis de requerimientos en la UESMDM se determinó que se requiere 169 puertos, se recomienda utilizar 9 switches de acceso de 24 puertos y uno de 12 puertos debido a que estarán distribuidos en diferentes puntos.

Se recomienda utilizar switches de 24 puertos para tener mayor disponibilidad del servicio, ya que si se daña uno solo quedarían sin servicio 24 estaciones de trabajo.

Este dispositivo es el encargado de conectar todos los host, teléfonos IP, cámaras IP, impresoras entre otros por lo que debe tener varios puertos para interconectar todo los equipos presentes en la UESMDM.

Las características que deben tener los switch de acceso están detalladas en la tabla 3.24.

	CARACTERÍSTICAS
Switch de Acceso	• 24 puertos *de* 10/100 Mbps full dúplex • Auto negociación de la velocidad de los puertos • Apilable • Administrable mediante consola o vía interfaz Web • Conmutación a nivel de capa 2 • Debe soportar el protocolos IP, DHCP, Telnet y SNMP V1, V2 y V3 (opcional) • Soporte de VLANs IEEE 802.1q • Debe soportar el estándar de seguridad IEEE 802.1X, listas de control de acceso (ACL), prevención mediante (DoS) y filtrado basado en MAC. • Soportar calidad de servicio (QoS) en base a IEEE 802.1p e IEEE802.1q. • Velocidad de backplane mínima de 8.8 Gbps • IP versión 4 y 6 • Soporte de 8000 direcciones MAC • Soporte de paquetes de telefonía IP (VoIP)

Tabla 3. 24 Características básicas de los Switch de Acceso. [24]

Los switch de acceso se requieren de 24 puertos con una velocidad de 10/100 Mbps ya que será una red Fast Ethernet, con autonegociasion para que se conecten con tarjetas de red que trabajen con 10 y 100 Mbps, apilables para conectar 2 ó 3 switch que se necesitan en algunos departamentos, soportar la creación de VLANs y ACLs porque se va a realizar segmentación y control de tráfico y principalmente soportar calidad de servicio para la telefonía IP.

3.6.2.3.2 Características del Switch de Core

Este dispositivo es el encargado de interconectar los switches de acceso que están distribuidos en toda la UESMDM, las características técnicas están detalladas en la tabla 3.25.

	CARACTERÍSTICAS
Switch de Core	• 24 puertos *de* 10/100 Mbps full dúplex • Auto negociación de la velocidad de los puertos • Apilable • Administrable mediante consola o vía interfaz Web • Conmutación a nivel de capa 2,3 y 4 • Debe soportar los protocolos IP, STP, RIPv1 y 2, DHCP, Telnet y $SNMP_{V\ (1,\ 2\ y\ 3)}$, $OSPF_{V\ (2\ y\ 3)}$, $RMON_{V\ (2\ y\ 3)}$ entre Otros. • Manejo y Administración de VLANs IEEE 802.1q • Debe soportar el estándar de seguridad IEEE 802.1X, listas de control de acceso (ACL) a nivel 2,3 y 4, prevención mediante (DoS) y filtrado basado en MAC. • Soportar calidad de servicio (QoS) en base a IEEE 802.1p e IEEE802.1q. • Velocidad de backplane mínima de 8,8 Gbps • IP versión 4 y 6 • Manejo, priorización y clasificación de tráfico VoIP

Tabla 3. 25 Características del Switch de Core. [25]

Este switch debe ser administrable que soporte los protocolos básicos SNMP, VLANS, ACLs y calidad de servicio para la VoIP

Este switch debe soportar los protocolos de administración porque se requiere implemetar una herramienta para realizar monitorización del tráfico.

La primordial que soporte calidad de servicio, manejo, priorización y clasificación de tráfico ya que por este pasará todo el tráfico de telefonía IP y video vigilancia IP a más de los datos.

Debe soportar creación de VLANS y ACL ya que se necesita realizar segmentación y administración de tráfico.

3.6.2.4 Dimensionamiento de Servidores.[61]

Una vez descritos anteriormente los servicios principales que requiere la UESMDM se procede a dimensionar los servidores necesarios para soportar dichos servicios.

En el capítulo 2 se especificó que UESMDM cuenta con 2 servidores HP ProLiant ML350 G5 los cuales se va a utilizar para configurar algunos servicios.

3.6.2.4.1 Primer Servidor

Este servidor será utilizado para implementar los siguientes servicios: DHCP, DNS, WEB y Proxy, se realizó esta agrupación debido a que estos servicios tienen algunas similitudes en cuanto a los servicios que prestan en la red.

Para implementar cada servicio se requiere como mínimo: un procesador de 250 Mhz, 256 MB de RAM y 8 GB de espacio en disco duro, tomando en cuenta que el servidor tiene un procesador de 2.66 GHz con una memoria que puede expandirse hasta 16 GB y un disco duro de 584 GB, todos los servicios trabajaran sin problema alguno.

A continuación se realiza el cálculo para determinar la velocidad de procesamiento y la capacidad de memoria requerida si se utiliza los 4 servicios de forma simultánea.

$$Procesador = 4x250\,GHz$$
$$Procesador = 1.000\,GHz$$
$$Memoria_{RAM} = 4x256\,MB$$

[61] [T7] Ings. Andrea Muños y Williams Leiva, Ingeniería de detalle para el diseño de la red para voz y datos, acceso remoto e intranet para la empresa Acurio & Asociados, Mayo 2011, Quito. Tesis E.P.N., pág. 160

$$Memoria_{RAM} = 1024\ MB$$

La capacidad de almacenamiento mínima necesaria es de 32 GB para implementar dichos servicios.

3.6.2.4.2 Segundo Servidor

Este servidor estará dedicado para los siguientes servicios: correo electrónico y servidor de impresión. Este servidor tiene las mismas características del primer servidor.

A continuación se realiza el cálculo para determinar la velocidad de procesamiento y la capacidad de memoria requerida si se utiliza los 2 servicios de forma simultánea.

$$Procesador = 2x250\ GHz$$

$$Procesador = 500\ GHz$$

$$Memoria_{RAM} = 2x256\ MB$$

$$Memoria_{RAM} = 512\ MB$$

Además, Con los datos obtenidos anteriormente se calcula la capacidad de almacenamiento necesario de correo electrónico requerido por los 14 usuarios que dispondrán de este servicio en 8 horas laborables los 22 días al mes.

$$AB_{(total\ correo\ electrónico)} = 3.78\ Kbps$$

$$C_{(Almacenamiento)} = 3.78\ Kbps \frac{1\ Byte}{8\ bits} * 3600s$$

$$C_{(correo\ electrónico)} = 1.7\ MB/hora$$

$$C_{(correo\ electrónico)} = 3.6\ GB/año$$

La capacidad de almacenamiento mínima necesaria es de 20 GB para implementar dichos servicios.

Este servidor también será utilizado para almacenar la información enviada por las 8 cámaras IP, la capacidad requerida es de 922.25 GB.

El servidor en la actualidad no tiene dicha capacidad, pero si dispone de 8 ranuras donde cada una soporta un disco duro de hasta 500 GB, por lo que se debe adquirir 2 discos duros de dicha capacidad.

3.6.2.4.3 Requerimiento mínimo del Sistema Operativo de los Servidores

Esta serie de servidores soportan sistemas operativos Linux y Windows por lo que se debe tomar en cuenta los requerimientos mínimos para instalar dichos sistemas operativos donde se van a implementar los servicios.

Linux (Red Hat, Suse)[62]

- **Procesador:** AMD Duron, Athlon o Intel Celeron, Pentium IV o superior
  Memoria RAM: Mínimo: 256 MB recomendado: 512 MB o superior
- **Disco duro:** Mínimo: 500MB Recomendado: 4GB o superior

Windows Server 2008

- **Procesador:** Mínimo: 1 GHz, Recomendado 2 GHz o superior
- **Memoria RAM:** Mínimo: 512 MB, Recomendado 1 GB o superior
- **Disco Duro:** Mínimo: 8 GB, Recomendado 40 GB o superior

En la tabla 3.26 se especifica en forma detallada las principales características requeridas para los servidores.

[62] [PW56] http://www.configurarequipos.com/doc835.html

Servidores	Procesador (Estándar)	Memoria RAM (Estándar)	HD
Primer	2.6 GHz	2 GB	80 GB
Segundo	2.6 GHz	2 GB	1 TB

Tabla 3. 26 Características de los servidores. [26]

La UESMDM tiene estos servidores pero dichos dispositivos no cuentan con las características técnicas requeridas por lo que se recomienda adquirir dos discos duros de 500 GB y dos memorias de de 1024 GB.

3.6.3 DISEÑO DE LA RED PARA TELEFONÍA IP

Para realizar el diseño de la red telefónica IP para la UESMDM se analizará dos esquemas de diseño, que se detallan a continuación.

Una solución que se plantea para prestar Telefonía IP es mediante el uso de software libre utilizando Trixbox CE que está basado en Asterisk y es de distribución gratuita. Por lo que se requiere solo un equipo para ser implementado.

La segunda solución que se plantea es utilizar centrales IP comerciales basadas en Asterisk.

3.6.3.1 Telefonía IP basada en software libre trixbox

En esta solución se utiliza de hardware un servidor equipado con tarjetas PCI[63] las cuales permiten la comunicación de la red telefónica interna con la red telefónica PSTN. Mientras, que de software se utiliza una herramienta de licencia GPL[64]

[63] *Peripheral Component Interconnect* (PCI): Es un bus de ordenador estándar que es utilizado para conectar dispositivos periféricos de forma directa a la placa base de un servidor o pc.
[64] General Public Licence

denominada Asterisk la cual es reconocida por sus excelentes características para implementar una Centralita IP.

En la figura 3.14 se presenta un diagrama de la red de Telefonía IP utilizando un servidor Asterisk el cual hace las funciones de una central telefónica IP.

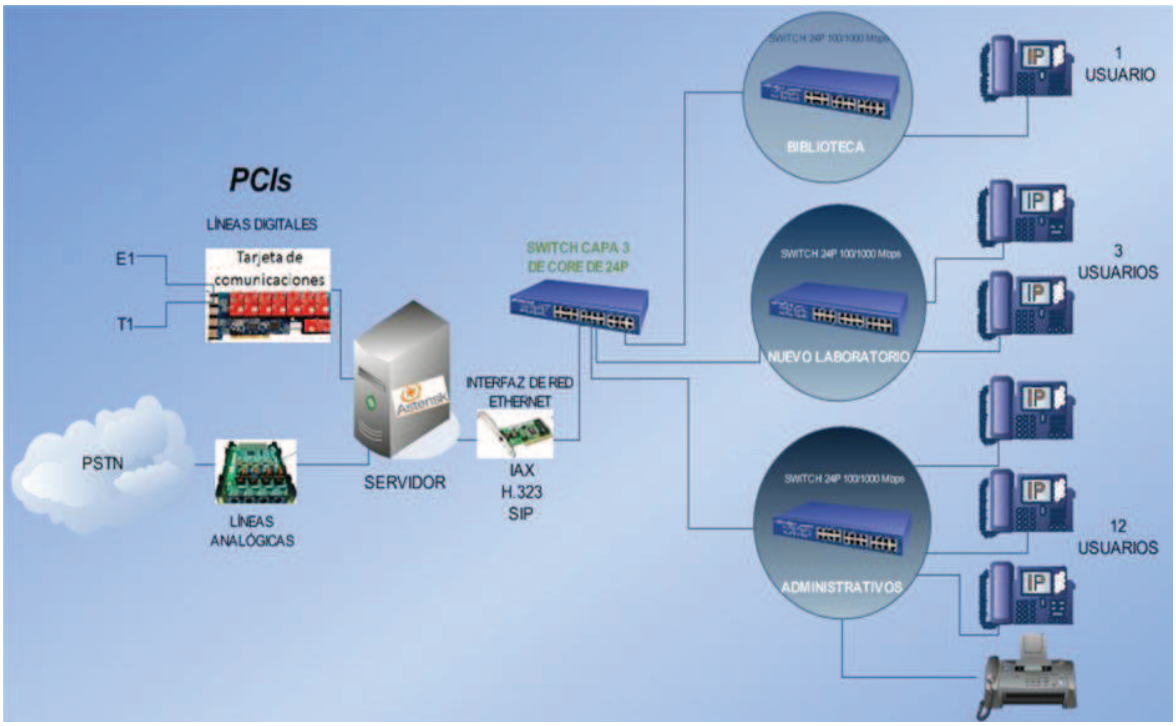


Figura 3. 14 Diagrama de la red de Telefonía IP de la UESMDM. [14]

Asterisk es una PBX en versión digital, fue creado utilizando la plataforma de Linux y Unix, permitiendo la conexión de diferentes interfaces de comunicación ya sean estas digitales o analógicas.

Esta herramienta provee algunos servicios tales como: directorios, cola de llamadas, conferencias, video conferencias, reconocimiento de voz, administradores únicos de llamadas, llamadas salientes y entrantes. Además, maneja varios tipos de protocolos para IP, SIP, H.323, ADSI, IAX, IVR.

3.6.3.1.1 Herramienta Trixbox CE

Empezó en el año 2004 como un proyecto IP-PBX llamado Asterisk@Home. El cual se convirtió en la distribución más popular para implementar centrales IP. Esta versión se caracteriza por dos pilares importantes; su flexibilidad para satisfacer las necesidades de los clientes, y por ser gratuita.

La herramienta está implementada en una distribución del sistema operativo Linux (Centos), es una central telefónica IP basada en software utilizando el código abierto Asterisk, al ser una central telefónica realiza las mismas funciones de una central convencional. Además, tiene varias características que solo utilizan sistemas propietarios. Además, Trixbox incluye lo siguiente:

- Servidor Web Apache, con soporte a PHP y Perl
- Administración de Base de Datos
- Correo de Voz e integración de este con el email
- Integración fax-a-email
- Autoconfiguración del hardware Zaptel de Digium
- Text-to-Speech en inglés.

La aplicación que se va a utilizar es Trixbox CE porque es la versión comunitaria de Trixbox y es un sistema basado en software libre, por lo que tiene algunas ventajas.

- No necesita licencia por lo que es una disminución de costos para la Institución
- Tiene una ambiente grafico facilitando la administración de la centralita IP
- Tiene soporte de la comunidad la cual se encuentra en continua investigación y desarrollo mejorando el esta aplicación

- Se tiene acceso al código fuente permitiendo el acceso a la configuración de acuerdo a las necesidades de la Institución

3.6.3.1.2 Requerimientos de hardware y Software para la implementación

Para la implementación de la centralita IP se requiere de un servidor o una PC que cumpla con las características detalladas a continuación.

- Sistema operativo Linux (Centos 5.x)
- Procesador 2 GHz o superior
- RAM 512
- Disco Duro 250 GB
- Tarjeta de red 10/100/1000 Mbps
- Software Trixbox CE
- Tarjeta PCI de 4 Puertos FXO y FXS.

3.6.3.2 Centrales Telefónicas Comerciales IP basadas en Asterisk

Existen algunas centrales telefónicas comerciales que se basan en el sistema Asterisk tales como Elastix, SwitchVox y Trixbox Pro, cada una de estas opciones posee excelentes características para trabajar como una central telefónica que incluso las hace competitivas con sistemas telefónicos propietarios tales como Cisco.

3.6.3.2.1 Elastix

Fue creado y actualmente es mantenido por la empresa PaloSanto Solution empezando como una interfaz de reporte de llamadas para Asterisk para posteriormente ser liberado en el 2006 para luego convertirse en una central

telefónica basada en Asterisk que no solo provee telefonía si no que también integra otros medios de comunicación para hacer más eficiente y productivo su entorno de trabajo. Elastix incluye en su paquete los siguientes medios de comunicación, los cuales se detallan en la figura 3.15.

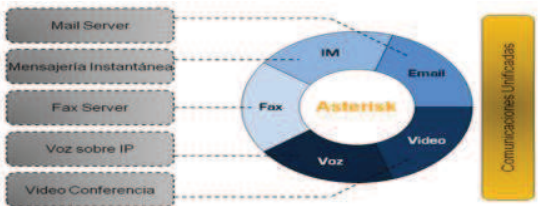


Figura 3. 15 Paquetes que incluye Asterisk. [15]

Elastix es una herramienta de código abierto distribuida bajo licencia GPLv2. Por lo que no tiene un costo relacionado con licenciamiento o funcionalidades haciendo que las versiones disponibles de Elastix sean versiones completas sin limitación de uso, permitiendo que cualquier empresa pueda utilizarlo sin ninguna restricción. En la tabla 3.16 se detalla las versiones disponibles de *Elastix*, detallando sus principales características técnicas.

	ELX-025	ELX-3000	ELX-5000
Telefonía			
Puertos Analógicos	Hasta 12	Hasta 24	Hasta 72
Puertos Digitales	Hasta 1 E1/T1/J1	Hasta 4 E1/T1/J1	Hasta 8 E1/T1/J1
Slots PCI de expansión	1	2	6: 3 PCI, 2(x8) PCIe, 1(x4)
Extensiones (SIP/IAX)	Hasta 100	Hasta 250	Hasta 600*
Llamadas concurrentes (máximo recomendado)	30	60	150*
Tiempo de soporte incluido	1 hora, 8x5 (-5GMT)	1 hora, 8x5 (-5GMT)	1 hora, 8x5 (-5GMT)
Hardware			
CPU	1.6 GHz Intel	2 x 1.6 GHz Dual Core Intel	1.86 GHz Dual Intel 64 bit Xeon
2do CPU	No	No	Si, hasta 4 núcleos Intel Xeon
RAM	1 GB	2GB	4 GB expandible a 48 GB
Hard Drive	250 GB	400 GB	1 TB de capacidad (2 x 500GB)
2do Hard Drive	No	Opcional	Opcional
RAID	No	Soft-RAID 1 (Opcional)	Soft-RAID por defecto
Tarjeta controladora de RAID	No	No	Opcional
Network Interface	10/100 Mbps	10/100 Mbps	2 x Gigabit Ethernet
Características de operación			
Potencia Nominal	90 W fanless, PSU eficiente	180 W PSU eficiente	Fuente redundante 500W HS
Voltaje de Operación	120-240 *Autoswitching*	120-240 *Autoswitching*	120-240 *Autoswitching*
Consumo de poder promedio	40 W *(low power)*	90 W	200 W
Fuente de poder redundante	No	No	Si
Sistema operativo	Elastix 32 bits	Elastix 32 bits	Elastix 64 bits
Características físicas			
Alto	1.75" (44.5 mm) - 1 U	2.63" (68 mm) - 1.5 U	3.46" (89 mm) - 2 U
Ancho	16.73" (425 mm)	16.73" (425 mm)	17.20" (437 mm)
Profundidad	11.96" (304 mm)	11.96" (304 mm)	14.45" (367 mm)
Montable en rack	Si	Si	Si - rack de 19"
Peso (Sistema básico)	4 Kg	5.5 Kg	9 Kg
Display LCD	No	20x4 chars. 5 botones de navegación	Si - Soporta Blacklight
Puertos USB	2 puertos en el panel frontal y 2 puertos en el panel posterior	4 puertos en panel posterior	4 puertos en panel posterior
Paneles LED frontales	Power/HDD	Power/HDD	Power/HDD

Figura 3. 16 Versiones disponibles de Elastix y sus características técnicas[65]. [16]

65 [PW43] http://store.palosanto.com/index.php/catalog/product_compare/index/

3.6.3.2.2 SwitchVox

El sistema SwitchVox® de Digium®, que es el creador de *Asterisk*, es más que un sistema telefónico tradicional, es un sistema de comunicaciones unificadas asequibles que tiene integrado todas las comunicaciones de una empresa, incluyendo teléfono, fax, chat y combinaciones en web.

SwitchVox es identificado como una de las centrales telefónicas IP más innovadoras y robustas que existen en el mercado, por la facilidad que ofrece para integrarse a servicios *web* tales como *Salesforce*, *Google Maps*, entre otras.

Imagen			
Función	**SwitchVox SMB AA65 Appliance**	**SwitchVox SMB AA305 Appliance**	**SwitchVox SMB AA355 Appliance**
Usuarios	Hasta 30	Hasta 150	Hasta 400
Llamadas simultaneas	Hasta 12	Hasta 45	Hasta 75
Ranuras de expansión	Dos	Tres	Tres
Grabaciones	"Hasta 5 llamadas grabadas simultáneamente	Hasta 10 llamadas grabadas simultáneamente	Hasta 20 llamadas grabadas simultáneamente
Conferencia	Hasta 5 usuarios de conferencia simultáneos	Hasta 15 usuarios de conferencia simultáneos	Hasta 30 usuarios de conferencia simultáneos
Slot para tarjetas de telefonía	2	2	2
Soporte de tarjetas de telefonía	B410P, TDM410, TDM800, TE122(only one TE122 supported)	TDM410, TDM800, TDM2400, TE122, TE205/207, TE405/407.	TDM410, TDM800, TDM2400, TE122, TE205/207,TE405/407
Opciones de garantía:	Garantía estándar de 1 año	Garantía estándar de 1 año	Garantía estándar de 1 año
Soporte de Idioma	Inglés, italiano y español	Inglés, italiano y español	Inglés, italiano y español

Tabla 3. 27 Versiones de SwitchVox y sus características técnicas[66]. [27]

[66] [PW44] http://www.digium.com/switchvox

3.6.3.2.3 Trixbox Pro

Trixbox Pro es una solución denominada "hibrid-hosted", esto significa que el cliente puede realizar un monitoreo 24/7, y le permite administrar la central desde cualquier lugar y actualizaciones del software de manera automática.

Trixbox Pro, es una versión empresarial la cual ha sido comercializada desde el 2004 permitiendo enviar/recibir más de 120 millones de llamadas por día. Trixbox Pro posee 3 versiones:

- **Standard Edition (SE)**

  Es una solución de telefonía IP basada en Asterisk mejorada para ofrecer mayor fiabilidad y escalabilidad. Además, Trixbox Pro SE incluye: una interfaz gráfica, voicemail basado en web, reportes de llamadas, clickto-call, integración con Outlook, gráficos de recursos en tiempo real, alertas del sistema, configuración auto-card y VoIP trunking.

- **Enterprise Edition (EE)**

  Trixbox Pro EE tiene todas las características de Trixbox Standard Edition. Sin embargo, incluye nuevas funcionalidades tales como: puentes para conferencia, múltiples auto attendants, paging, permisos de grupo entre otras. Además tiene incluido HUD Pro el cual añade administración presencial, control de llamadas drag and drop, chat corporativo privado, alertas interactivas y más.

- **Call Center Edition (CCE)**

  Trixbox Pro CCE fue desarrollado basándose en los anteriores estándares por lo que tiene todas sus funcionalidades añadiendo nuevas tales como:

ACD[67] e IVR[68] con colas ilimitadas, estadísticas en tiempo real de colas, reportes gráficos, acceso basado en web a grabaciones.

3.6.3.2.4 Requerimiento que debe cumplir la central comercial IP

En caso de que la elección sea adquirir una central telefónica comercial basada en Asterisk debe cumplir los siguientes requerimientos.

- 3 interfaces FXO con la red PSTN
- Soporte para más de 16 Usuarios
- Protocolos de señalización
- Control de llamadas
- IVR
- Correo de voz
- Administración vía web
- Distribución automática de llamadas
- Soporte de códecs G.729a
- Soporta Auto negociación de códec

3.6.3.2.5 Comparación de las dos soluciones propuestas

Luego de haber detallado las centrales IP comerciales basadas en Asterisk se realiza una comparación de aquellas que cumplen con las características requeridas por la UESMDM. Las que se detallan en la tabla 3.28

[67] Automatic Call Distributor (ACD): es un proceso utilizado para distribuir las llamadas que llegan a los sistemas de atención.
[68] Contestador Automático (IVR): guía a los que llamen según las opciones predeterminadas.

IPPBX	Elastix	SwitchVox	Trixbox Pro
			
Distribución	**ELX-025**	**SwitchVox SMB AA65 Appliance**	**Standard Edition (SE)**
Número de usuarios	100 máx	30 máx	200 máx
Llamadas concurrentes	30	12	23
Ranuras de expansión	1	2	6
Interfaces de red 10/100 Mbps	1	1	2
Soporte de protocolos SIP	si	si	si
Soporte de códecs G.729a	si	si	si
Grabación de llamadas	si	si	Si
Appliace	si	si	si
Garantia	1 año	1 año	1 año

Tabla 3. 28 Comparación de las centrales IP comerciales basadas en Asterisk. [28]

3.6.3.2.6 Selección de la solución a utilizarse en la UESMDM

Una vez presentadas y analizadas las dos propuestas utilizadas las cuales son: Trixbox CE y Centrales telefónicas IP comerciales basadas en Asterisk, se recomienda utilizar en la UESMDM una IPPBX comercial Elastix. Debido a que ésta ha sido desarrollada por ecuatorianos. Esto es una ventaja ya que cualquier

inconveniente que se presente los proveedores de ésta puede solucionarlos de forma inmediata a diferencia de un proveedor que se encuentre fuera del país.

Otra de las razones por la que se decidió por Elastix es la gran acogida que ha tenido a nivel nacional e internacional siendo nominada a premios de *software* libre.

3.6.3.2.7 Principales razones de la elección de Elastix

Elastix es un software aplicativo que tiene integrado las mejores herramientas disponibles para un central telefónica. Además cuenta con un conjunto de utilidades que permiten la creación de módulos haciendo de este uno de los mejores paquetes de software de código abierto ofreciendo confiabilidad, modularidad, robustez y una interfaz simple y fácil de usar.

La empresa PaloSanto Solution ofrece en sus productos un periodo de garantía, tiempo en el cual se evalúa la central telefónica y en caso de alguna eventualidad se puede reportar para solicitar una solución inmediata.

Al adquirir una central telefónica Elastix, PaloSanto Solution ofrece capacitación para los usuarios comunes y para el administrador. Además, la empresa ofrece soporte y mantenimiento continuo preventivo, este servicio incluye actualizaciones de archivos y consultas vía mail o telefónico.

3.6.3.3 Accesorios para la Telefonía IP

La UESMDM requiere 16 extensiones para dar servicio de telefonía a los usuarios administrativos de la Institución por lo que se debe adquirir 16 teléfonos IP los

cuales deben cumplir con las siguientes características básicas detalladas a continuación.

- 2 puertos Fast Ethernet (100Mbps)
- Soporte de códecs G.729
- Soporte DHCP
- QoS (802.1p)
- Soporte de capa 2 (802.1q VLAN, 802.1p)
- Soporte de cancelado de eco
- Calidad de voz
- Identificador de llamadas
- Llamada en espera
- Transferencia de llamadas

Adicionalmente, cabe mencionar que existe software cono Softphone que realiza las funciones de un teléfono IP, el cual puede ser instalado en cualquier estación de trabajo utilizando un micrófono con audífonos.

Si la UESMDM no desea adquirir todos los teléfonos IP necesarios para todos los usuarios que requieren este servicio debe utilizar esta opción adquiriendo únicamente los dispositivos mencionados anteriormente.

3.6.4 DISEÑO DE LA RED PARA VIDEO VIGILANCIA

El objetivo del sistema de video vigilancia es cubrir los lugares de mayor riesgo que tiene la UESMDM proporcionando monitoreo continuo porque contienen equipos costosos.

En el literal 3.6.2.4.2 se especificó que se va a utilizar el servidor dos para el almacenamiento y monitoreo de las cámaras IP que estarán conectadas a la red convergente de la Institución.

3.6.4.1 Ubicación Física de las Cámaras IP

Las cámaras IP estarán ubicadas de la siguiente manera: 3 en el acceso principal de la Institución para tener un mayor control del ingreso y salida del personal administrativo, estudiantes, docentes y padres de familia.

Una cámara se ubicará en el departamento Administrativo diagonal al cuarto de equipos, necesaria para monitorear el acceso y brindar mayor seguridad a los equipos de networking, servidores entre otros.

Otros lugares que son críticos y que requieren un monitoreo continuo son los laboratorios y biblioteca debido a que en estos se encuentra una alta concentración de computadores por lo que se colocará una cámara en cada sitio.

En las figuras 3.17 a las 3.21 se especifica los sitios donde estarán ubicadas las cámaras IP.

Figura 3. 17 Ubicación de las Cámaras IP Administrativos. [17]

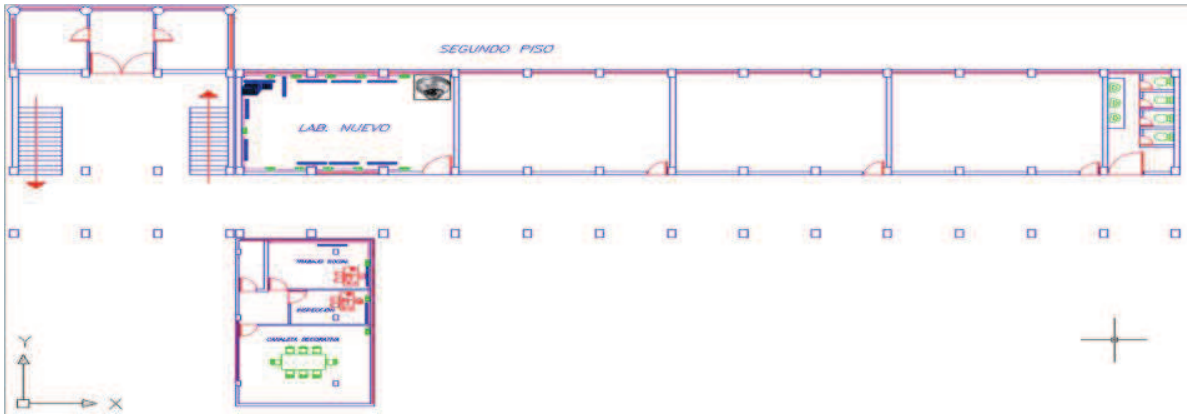


Figura 3. 18 Ubicación de las Cámaras IP Lab Nuevo. [18]

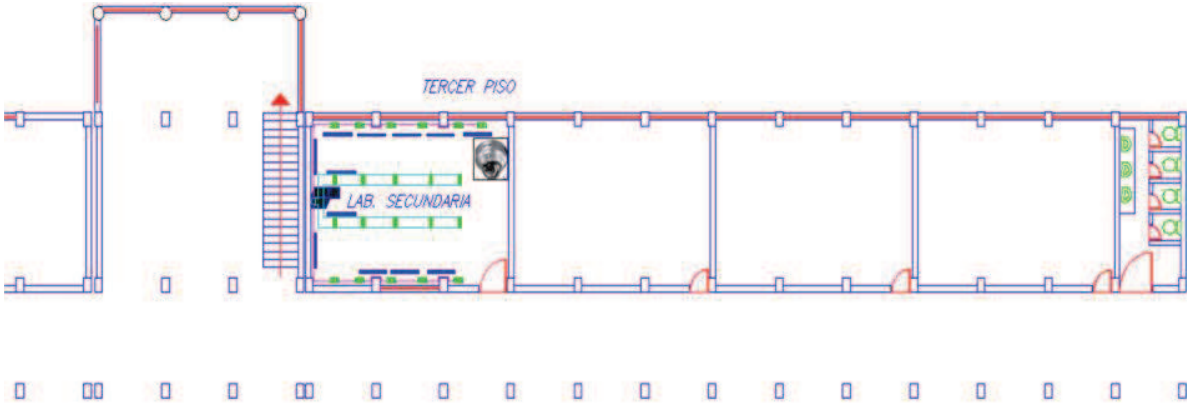


Figura 3. 19 Ubicación de las Cámaras IP Lab Secundaria. [19]

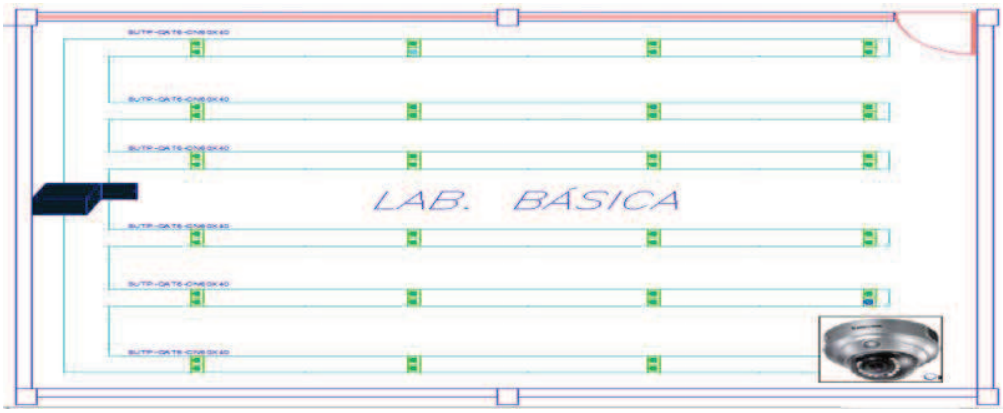


Figura 3. 20 Ubicación de las Cámaras IP Lab Básica. [20]

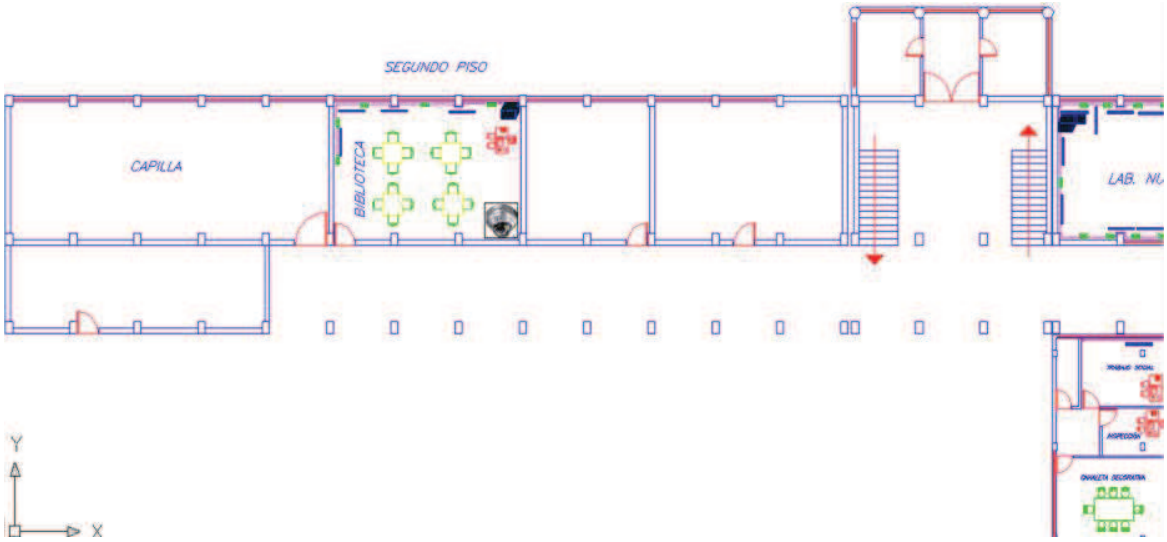


Figura 3. 21 Ubicación de las Cámaras IP Biblioteca. [21]

3.6.4.2 Diagrama de la red para video vigilancia

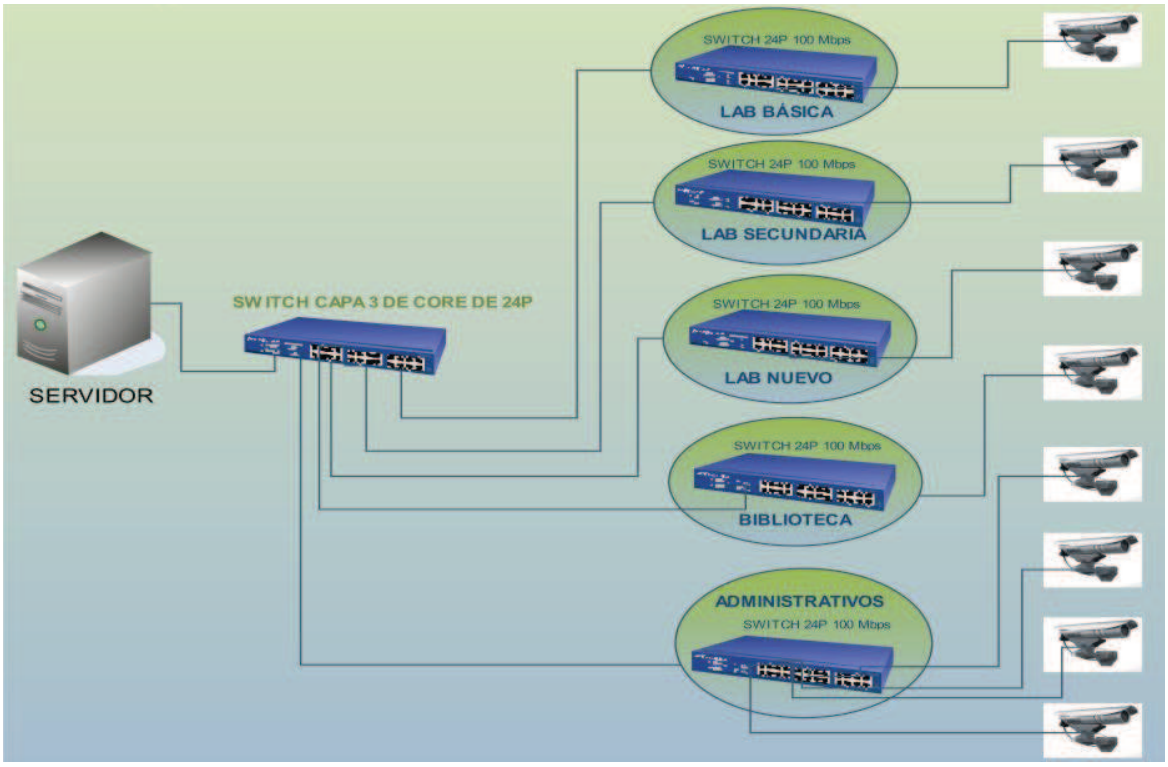


Figura 3. 22 Diagrama de la red de Video Vigilancia. [22]

Para la selección de las cámaras IP se tomará en cuentas los siguientes parámetros técnicos detallados a continuación.

- Un puerto 10/100 Fast Ethernet
- Protocolos TCP/IP, ARP, ICMP, HTTP, TELNET, SNMP Y DHCP
- Movimiento horizontal de cobertura 90°
- Detección de movimiento tanto de día como de noche (VMD) (Opcional)
- Formato de compresión MPEG-4 ó H.264
- Resolución de 640X480 pixeles ó superior
- Autenticación de usuario.

Las cámaras IP deben tener un interfaz de 10/100 Mbps porque se conectarán a una red Fast Ethernet, soportar los protocolos SNMP, HTTP para que permitan la administración via web y de forma remota, DHCP porque se les asignará las Ip desde un servidor, tener una cobertura de 90° para cubrir el área que requiere el monitoreo, soportar formatos de compresión MPEG-4 para consumir menor ancho de banda y autenticación de usuarios para mayor seguridad.

3.7 REDISEÑO DE LA RED WLAN

La red LAN inalámbrica será diseñada para brindar servicio de Internet a los visitantes, profesores y principalmente a los estudiantes. Estos usuarios tendrán acceso a los servicios internos de la red.

Antes de realizar el diseño de la red WLAN es necesario analizar la infraestructura del sitio donde va a ser implementada la red para saber algunos parámetros importantes como son: interferencia, distorsión, atenuación, área de cobertura etc.

3.7.1 REGLAS DE DISEÑO A CONSIDERAR

Para realizar el diseño se deben considerar las siguientes reglas.

- Separar lo máximo posible los puntos de acceso (AP) para asegurar una cobertura total del área y para reducir la interferencia co - canal.

- Cuando se tiene una red en un solo piso se recomienda utilizar los canales: 1, 6 y 11 para evitar toda interferencia inter-canal

3.7.2 ÁREA DE COBERTURA

La red inalámbrica WLAN no cubrirá en su totalidad la Institución, solo incluye algunos sectores importantes que son: sala de profesores, departamento administrativo, biblioteca y equipo pastoral, estos sectores se encuentran ubicados en el primer y segundo piso de la Institución. Además se contará con un AP para prestar dicho servicio en el tercer piso.

En la tabla 3.29 se detalla el área de los sitios donde se va a implementar la red inalámbrica.

SITIO	ÁREA DE COBERTURA (M^2)
Sala de profesores	50.00 (8.69x5.79)
Administrativo	180 (27.1x6.64)
Biblioteca	55.91 (8.82x6.34)
Equipo Pastoral	56.00 (10.19x5.50)

Tabla 3. 29 Área de Cobertura. [29]

El área de cobertura total requerida en el primer piso que abarca la sala de profesores y el departamento Administrativo es de 230 m^2: sin embargo el AP se

instalará en la sala de equipos con lo cual se requiere un radio de cobertura de 20.1 m.

Para el segundo piso donde se encuentran la biblioteca y el Equipo Pastoral se tiene un área de 111.91m^2, con un radio de cobertura 34.23 m. Cabe indicar que estos datos son requeridos para adquirir los AP de acuerdo al radio de cobertura y otros parámetros.

3.7.3 INTERFERENCIA Y ATENUACIÓN

Las ondas electromagnéticas al viajar por el aire están expuestas a sufrir algunos fenómenos que dificultan el diseño de la red, estos fenómenos son: desvanecimiento, reflexión y atenuación disminuyendo el alcance de la señal.

Algunos obstáculos como son: paredes, puertas, lozas atenúan la potencia de la señal disminuyendo la cobertura.

3.7.4 CARACTERÍSTICAS ARQUITECTÓNICAS DE LA UESMDM

La infraestructura de la Institución que es un edificio de 3 pisos está compuesta por: loza de cemento, delimitación de aulas es de ladrillo con un espesor de 24 cm y las oficinas están separadas por vidrio con madera de 10 cm.

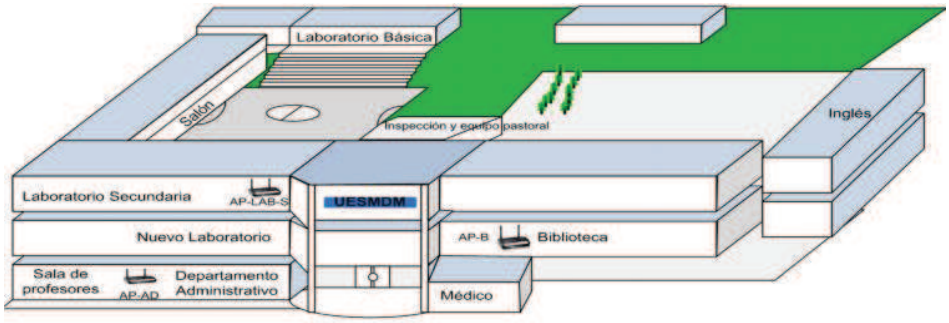


Figura 3. 23 Diagrama esquemático del edificio. [23]

En la tabla 3.30 se detalla la atenuación que sufre la señal al pasar por estos obstáculos.

MATERIAL	EJEMPLO	INTERFERENCIA
Madera	Tabiques	Baja
Vidrio	Ventanas	Baja
Amianto	Techos	Baja
Yeso	Paredes interiores	Baja
Ladrillo	Paredes interiores y exteriores	Media
Hojas	Árboles y plantas	Media
Agua	Lluvia / Niebla	Alta
Cerámica	Tejas	Alta
Papel	Rollos de papel	Alta
Vidrio con alto contenido en plomo	Ventanas	Alta
Metales	Vigas, armarios	Muy Alta

Tabla 3. 30 Materiales que causan Interferencia (Continuación)[69]. [30]

3.7.5 TIPO DE APLICACIONES

Los servicios y aplicaciones que se va a ofrecer en la red inalámbrica son: correo electrónico, acceso a Internet, mensajería instantánea y redes sociales.

Adicionalmente, cabe indicar que si es necesario instalar algún dispositivo tal como teléfono IP ó cámara IP dentro del rango de cobertura del AP la red debe soportar esta tecnología.

3.7.6 CANTIDAD DE USUARIOS

Al realizar el diseño de una red WLAN es importante conocer la cantidad de usuarios que se van a conectar a esta red para acceder a los servicios que proporciona.

69 [T8] GOMEZ Fernando, "Diseño, estudio y análisis de costos de una red inalambrica para el sistema de comunicaciones interno de PETROECUADOR "

Para determinar un aproximado de usuarios simultáneos que se conectarán a la red inalámbrica se considera los siguientes aspectos.

- El equipo pastoral se reúne dos veces a la semana, de los cuales 3[70] integrantes necesitan estar conectados a la red inalámbrica.

- La UESMDM tiene 53 docentes que requieren subir las notas a la base de datos a más de investigar y actualizarse para mejorar el nivel educativo de los estudiantes, para determinar el número de docentes que van a utilizar la red inalámbrica se toma en cuenta que no todos los profesores disponen de una computadora portátil y que el horario de recreo y salida es diferente tanto para la secundaria como para la primaria. Por lo que no todos los 53 docentes se conectarán de forma simultánea, sabiendo que son 19 docentes que conforman el grupo de profesionales en la secundaria. Además, se dispone de 3 computadores en la sala de profesores quedando la necesidad del servicio para 16 docentes.

- En el colegio trabajan un número fijo de personal administrativo y de acuerdo al espacio físico dedicado a este departamento es difícil asumir un crecimiento de personal.

- De todos los estudiantes, los secundarios son los que más utilizan la biblioteca para consultas, sabiendo que en la biblioteca se cuenta con 9 computadoras y que los estudiantes secundarios son un 50% aproximadamente de todos los estudiantes de la Institución. Sin embargo: en la actualidad los estudiantes no llevan computadores portátiles debido a que en esta no se presta este servicio.

[70] Información proporcionada por la UESMDM

- Este servicio será más utilizado por los estudiantes de bachillerato para realizar consultas y son aproximadamente 250 de los cuales no todos cuentan con equipos portátiles razón por la cual se toma un porcentaje del 25% dando un valor de 63 usuarios simultáneos.

De acuerdo a estas premisas, se tendrán aproximadamente 82 usuarios simultáneos conectados a la red inalámbrica en el peor de los casos.

3.7.7 SELECCIÓN DE LA TECNOLOGÍA A UTILIZAR

Los estándares de las redes inalámbricas IEEE 802.11 que se pueden utilizar para el diseño se detallan en la tabla 3.31.

Parámetros	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g
Frecuencia	5 GHz	2.4 GHz	2.4 GHz
Ancho de Banda	300 MHz	83.5 MHz	83.5 MHz
Modulación	OFDM	DSSS	OFDM
Número de Canales	6	3	3
AB por Canal	20MHz	22MHz	22MHz
Tasa de Transmisión	54 Mbps	Variada 1,2,5.5 y 11 Mbps	54 Mbps
U. Simultáneos	64	32	50
Distancia exteriores	30 m a 54 Mbps	120 m a 11 Mbps	Km con antenas parabólicas
	300m a 6Mbps	460 m a 1 Mbps	
Distancia interiores	12 m a 54 Mbps	30 m a 11 Mbps	30 Mbps a 50 m
	90m a 6Mbps	90 m a 1 Mbps	

Tabla 3. 31 Estándares IEEE 802.11. [31]

En este diseño se va a utilizar IEEE 802.11g por su radio de cobertura que es mayor al requerido de 34.23m y tasa de transmisión que ofrece el estándar en interiores y por el número de usuarios simultáneos especificados en el literal 3.7.6

Como no se encontraron otras redes inalámbricas en las cercanías se van a utilizar los canales 1, 6 y 11 para evitar las interferencias entre ellos. Para cumplir con las condiciones mínimas de diseño de la red WLAN se necesita tener por lo menos una velocidad de 4Mbps.

3.7.8 CANTIDAD Y UBICACIÓN DE LOS EQUIPOS (AP)

Para determinar el número de AP necesarios para cubrir los sitios que requiere la UESMDM consideró lo siguiente:

- El número de usuarios que se van a conectar en la red en cada departamento, el cual se detalló en el literal 3.7.6.

- Los obstáculos que se tienen por área de cobertura por los cuales tiene que atravesar la señal sufriendo cierto grado de atenuación disminuyendo el alcance de la señal.

- Elección de los AP, los cuales deben cumplir ciertos parámetros tales como: potencia de la señal la cual sea suficiente para cubrir el área a servir.

De acuerdo a las consideraciones anteriores se requiere de tres AP uno por piso los cuales utilizarán los canales de frecuencia 1, 6 y 11, y estarán ubicados de acuerdo a las figuras 3.23, 3.24 y 3.25

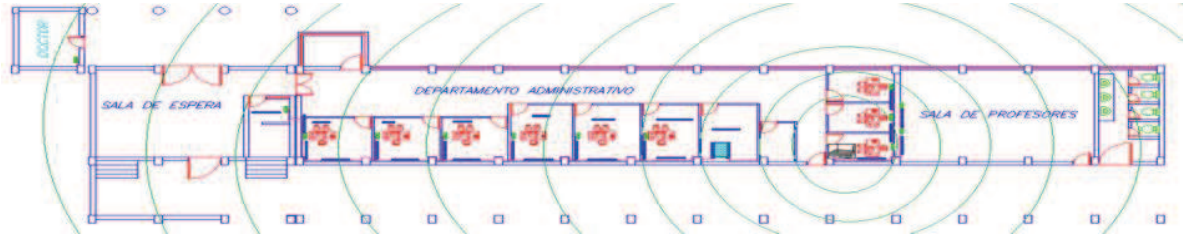


Figura 3. 24 Primer Piso. [24]

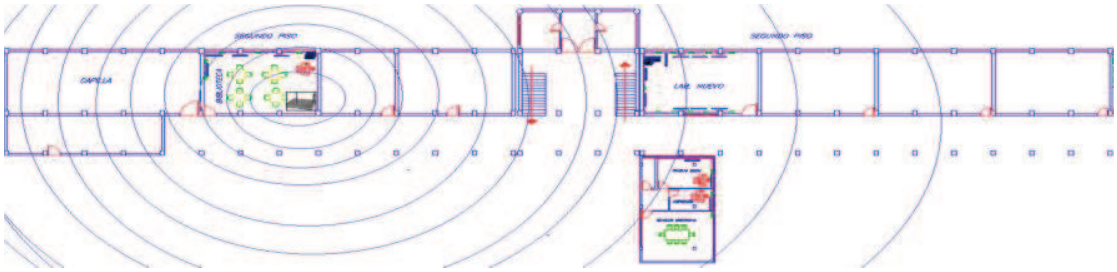


Figura 3. 25 Segundo Piso. [25]

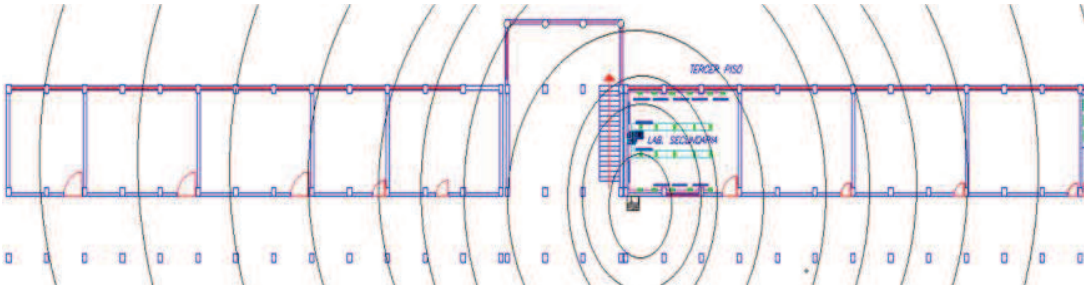


Figura 3. 26 Tercer Piso. [26]

3.7.9 DIAGRAMA DE LA RED WLAN

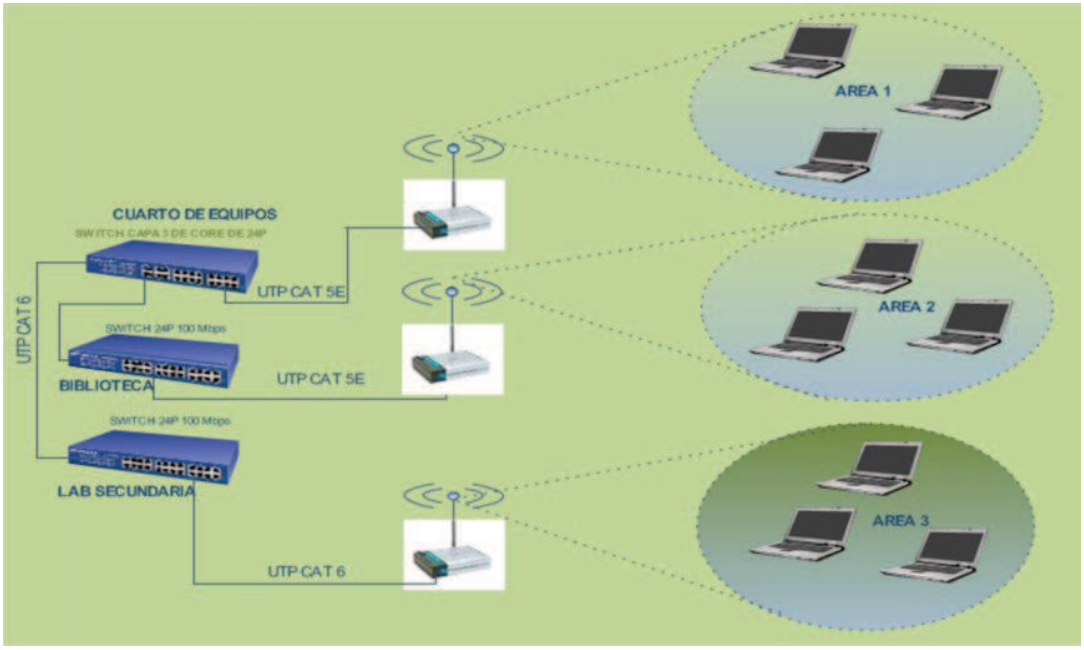


Figura 3. 27 Diagrama de la red WLAN. [27]

Los AP estarán conectados a los switch de Adminstración, Biblioteca y lab de Secundaria como se observa en la figura 3.27

3.7.10 CARACTERÍSTICAS MÍNIMAS QUE DEBEN CUMPLIR LOS AP

Para la elección de los AP se tomara en cuenta las siguientes características.

- Tasa de transmisión de 54 Mbps
- Trabajar en la banda de frecuencia de 2.4GHz
- Protocolo de gestión: SNMP (v1, v2, v3) (Opcional)
- Algoritmo de cifrado DES y AES
- Filtrado MAC
- Soporte estándares: IEEE 802.11g, IEEE 802.11e, IEEE 802.11q y IEEE 802.11x
- 1 interfaz Fast Ethernet
- Configuración de SSID
- Soporte de VLANs
- Certificación Wi-Fi

Se requiere AP tengan como mínimo un puerto Fast Ethernet, soporte de VLANs ya que la red inalámbrica estará configurada dentro de una, cifrado DES y AES para proteger el ingreso de personas que no pertenezcan a la Institución. Adicionalmente, configuración de SSID por seguridad.

La certificación es requerida para que se garantice una compatibilidad del equipo con otros debido a que se utilizara dispositivos de diferentes fabricantes.

3.8 UPS PARA EL CUARTO DE EQUIPOS Y CLOSET DE TELECOMUNICACIONES

Para realizar el dimensionamiento de los UPS es necesario considerar el tiempo que los UPS pueden suministrar energía a los dispositivos a este conectados después de que exista un corte del suministro eléctrico.

La capacidad del UPS es la suma de las potencias consumidas por los dispositivos a este conectados más un 40% adicional para que el equipo no trabaje al máximo de su capacidad; sin embargo, este es un sistema de emergencia por lo que no se puede seguir con las actividades normales en la Institución si existe un corte del suministro eléctrico.

3.8.1 CARACTERÍSTICAS MÍNIMAS DE LOS UPS

Los UPS requeridos deben cumplir los siguientes requerimientos mínimos para su adquisición.

- Deben ser para montaje sobre *rack.*
- *Smart.*
- La capacidad debe ser de al menos 1500 VA o superior
- Tener, una alimentación monofásica de 110 V y 60 Hz.

Los 1500 VA como mínimo es debido a que un switch consume en promedio 100 watts, un servidor 500 watts. Considerando un servidor y 3 switch se necesita 800 watts este valor no debe exceder el 60% del total de la capacidad del UPS.

Deben ser montables en rack porque se necesita para ser instalado el los closets de telecomunicaciones y en el rack.

3.8.2 PoE (*POWER OVER ETHERNET*)

Los AP y las cámaras son ubicados en lugares estratégicos donde no siempre existen puntos de alimentación eléctrica, provocando un mayor costo en cable y tomacorrientes. Para evitar estos gastos se utiliza equipos que soporten el estándar 802.3af, el cual especifica la utilización del cable de red de datos para suministrar energía a los dispositivos, eliminando la necesidad de suministrar por separado la energía eléctrica

3.9 SEGURIDAD DE LA RED

Para tener un buen nivel de seguridad en la UESMDM es necesario cumplir con los siguientes requisitos tales como confidencialidad, autenticación, integridad, y disponibilidad de los datos. Para lo cual se debe crear VLANs, ACLs y adquirir algunos equipos que proporcionen seguridad adicional a la red tales como: Firewall, antivirus y equipos de autenticación de usuarios. Sin embargo: nada de esto funciona correctamente, sin tener políticas de seguridad adecuadas en la Institución.

Implementar un esquema de seguridad en la Institución conlleva a crear políticas que permitan disminuir el riesgo de un ataque tanto interno como externo garantizando un correcto funcionamiento de los servicios y aplicaciones que ofrece la red.

Debido a que siempre existirán ataques a las redes informáticas se debe formular políticas que vayan acorde a la situación actual de la Institución y al desarrollo tecnológico. Además, dichas políticas deben ser evaluadas y actualizadas periódicamente para disminuir el riesgo de un posible ataque.

Antes de desarrollar las políticas de seguridad es necesario identificar los activos que deben ser protegidos para luego identificar las vulnerabilidades y los tipos de ataques a los que estarían expuestos.

3.9.1 ACTIVOS Y SUS VULNERABILIDADES

A continuación se detallan los activos y sus vulnerabilidades a los que se les implementarán ciertas políticas de acceso para protegerlos.

3.9.1.1 Estaciones de Trabajo:

- Todos los usuarios tienen permisos de administrador
- No tiene restricciones de instalación y uso de programas que pueden dañar el equipo.

3.9.1.2 Equipo Activo de la Red:

- Configuración por defecto
- Todos los puertos están habilitados.
- No soportan creación de ACL por lo que no se puede restringir el acceso de los usuarios normales a las computadoras de los administrativos.
- Los closets de telecomunicaciones donde están ubicados no cuentan con seguridad.
- Existen equipos a los cuales tiene acceso todos los usuarios

3.9.1.3 Router Inalámbrico 3COM:

- Tiene habilitado el servidor DHCP
- Un AP está ubicado en un lugar accesible para algunos usuarios

- Utiliza WEP para autenticar a los usuarios, el cual no es recomendable para una Institución.

3.9.1.4 Central Telefónica

- Está ubicada en la recepción por lo que no cuenta con ningún nivel de seguridad.
- No dispone de ningún software para administrar la red telefónica.

Después de haber encontrado algunas vulnerabilidades que tiene la red actual se determina las políticas de seguridad físicas y lógicas que deben ser implementadas en la UESMDM.

Las políticas físicas son aquellas que se aplican al hardware de la red y al acceso indebido de personal no autorizado a ciertas localidades de la Institución. Al hablar de hardware es referirse por ejemplo seguridad en los puertos o interfaces de los equipos de networking.

Las políticas lógicas son las que permiten o deniegan el acceso a los equipos mediante el uso de contraseñas, creación de usuarios con diferentes prioridades y configuración de los equipos de Internetworking

3.9.2 POLÍTICAS FÍSICAS Y LÓGICAS

3.9.2.1 Red LAN

Las políticas de seguridad físicas y lógicas sugeridas para la Institución son las siguientes:

- El cuarto de equipos y closets de telecomunicaciones tienen que estar cerrados con llave para controlar el acceso no autorizado a los equipos, y los usuarios con acceso deben llevar un registro de la hora de ingreso y salida detallando las modificaciones o monitoreo que realizaron.

- Los puertos de los switches (Acceso y Core) que no están siendo utilizados deben estar apagados, para evitar que cualquier usuario se conecte a la red sin autorización y si es requerido habilitar un puerto debe realizarse una solicitud por escrito al administrador de la red, el cual tiene que llevar un registro de la persona que solicitó dicho servicio y la modificación que realizó en el equipo.

- Se debe configurar los puertos o interfaces de los equipos de Internetworking de tal forma que no sea posible conectar AP o switch en las salidas de telecomunicaciones que están destinadas a conectar ya sea estaciones de trabajo o teléfonos IP.

- Se deben crear VLANS de acuerdo al esquema detallado anteriormente en el direccionamiento IP.

- El control de flujo de tráfico en los equipos de Internetworking debe realizarse mediante la creación de ACLs.

- Realizar de forma periódica respaldo de la configuración de los equipos y de la información de la UESMDM, esta información es necesario en caso de emergencia.

- Cuando exista cambio de personal administrativo o de administración de la red se debe quitar todos los privilegios que el usuario tenía anteriormente y

asignarle los nuevos permisos de acuerdo al tipo de usuario al que pertenezca.

- Los videos almacenados en el servidor de las cámaras IP sólo puede ser administrada por el administrador de la red, pero si puede ser monitoreada por el usuario a cargo de la seguridad física de la Institución.

- Todos los cambios que se realicen en los servidores y en la configuración de los equipos debe ser registrado con hora y fecha indicando la razón y el usuario responsable de dichos cambios.

- La actualización de datos, y de configuración de servidores y equipos debe ser realizada en un horario fuera del laboral para no causar pérdidas de tiempo a los trabajadores y estudiantes de la Institución.

- Se debe utilizar un mecanismo de autenticación de usuarios utilizando control de acceso (Active Directory), mediante el cual se pueda adherir a un dominio común todas las estaciones de trabajo, para tener un mejor control de los mismos.

- Configuración adecuada del perfil de usuario, debido a que en este se define los permisos para modificar las configuraciones, archivos, parámetros del sistema operativo, servidores y equipos de Internetworking; razón por la cual cada usuario es responsable de los cambios que realice según su permiso y de administrar su contraseña.

- Se debe configurar los equipos y sistemas para actualizar la contraseña de forma mensual, activando el número de intentos erróneos de contraseña a

tres veces pasado esto el equipo debe bloquearse temporalmente. Además determinar la longitud de la contraseña.

- La navegación en Internet debe ser exclusivamente para investigación o para cumplir algunas actividades de la Institución más no para algún uso comercial, utilizar un servidor proxy para limitar el acceso a páginas que no tengan relación a esta actividad.

- El uso del correo electrónico Institucional debe ser únicamente para labores relacionadas a la UESMDM, no se deben enviar ni recibir correos con contenido de imágenes y videos

- Mediante la utilización de un firewall se deben bloquear todos los puertos que no se van a utilizar para disminuir posibles ataques.

- Utilizar un antivirus centralizado de tipo empresarial para proteger a toda la red de virus, gusanos y troyanos, indicando a los usuarios que reporten cualquier anomalía que tenga que ver con el ingreso de virus en el sistema.
- Los usuarios deben analizar con el antivirus las unidades extraíbles antes de abrir cualquier archivo.

- El administrador de la red debe hacer un seguimiento continuo de los logs generados por el sistema para estar enterado de todo lo que sucede en la red.

- En cuanto a la información que se considere de un alto grado de privacidad se debe cifrar para evitar un posible robo o alteración del contenido.

- El administrador de la red debe crear un cronograma de mantenimiento preventivo de hardware y software de todos los equipos conectados a la red y los de la red para mantenerlos en un óptimo funcionamiento.

3.9.2.2 Red WLAN

- Cambiar el nombre por defecto SSID por otro que no tenga relación con la Institución.
- Desactivar el broadcast SSID para evitar que la red sea encontrada e identificada fácilmente.
- Configurar a los equipos (AP) para realizar autenticación mediante filtrado MAC y cifrado de datos utilizando WPA con PSK.
- Realizar mantenimiento continuo de los puntos de acceso
- Crear una VLAN.

Adicionalmente, cabe indicar que para obtener una mejor seguridad se contará con un firewall el cual será en encargado de filtrar el tráfico interno y externo de acuerdo a las políticas de seguridad que se mencionaron anteriormente.
La sanción por el incumplimiento de las políticas físicas será una llamado de atención a los responsables (el usuario que permitió el ingreso y el que ingresó), en caso de ser reincidente la falta se le realizará un llamado de atención escrita por parte de la rectora de la Institución.

Para el caso del incumplimiento de las políticas lógicas, el o los usuarios perderán momentáneamente el acceso a la red obligándolos a un cambio de la contraseña, en caso de ser reincidente la falta se realizará un llamado de atención verbal por parte de la rectora de la Institución.

3.9.3 SEGURIDAD PERIMETRAL

Para brindar seguridad perimetral a la red de la UESMDM se utilizará un UTM (*Unified Threat Management Security Appliance*) que es un dispositivo que tiene integrado varios servicios de seguridad. Los dispositivo UTM por lo general son equipos Appliance, lo que significa que son diseñados pasa realizar una función en concreto es decir equipos dedicados.

Estos equipos disponen de distintos interfaces de Red, que pueden utilizarse para diversas funciones o zonas que son:

- Zonas LAN
- Zonas WAN
- Zonas DMZ
- Zonas VPN

Son equipos que ofrecen una solución integrada compuesta de diversos módulos. A continuación se citan los módulos más comunes:

- Antivirus
- Antispam
- Antispyware
- IDS
- IPS
- Firewall
- QoS
- NAT
- VPN

Existen varias empresas en el mercado que ofrecen equipos UTM, a continuación se menciona algunas tales como:

- D-Link
- Fortigate
- Ziwall
- Astaro
- Security Point
- Check Point
- Cisco

Las características básicas que debe cumplir el UTM a elegir son:

- Firewall Throughput: 100 Mbps o superior
- 1 puertos WAN
- 3 puertos LAN
- 1 Puerto DMZ
- IPS
- Antivirus
- Antispam
- VLAN
- Políticas basadas en Routing
- Prioridad de ancho de banda

Se requiere que el equipo soporte un Throughput de 100 debido al número de usuarios que son 142 por lo que se recomienda utilizar un firewall de esta característica en Instituciones que sobrepasen los 100 usuarios.

El firewall debe soportar VLAN ya que la red estará segmentada por departamentos y servicios.

Tener un puerto para la zona DMZ para los servidores. Tres puertos LAN uno para administración y los otros para conectar la red interna.

Soportar administración de ancho de banda para distribuir adecuadamente los recursos de internet de acuerdo al usuario.

3.10 ADMINISTRACIÓN Y MONITORIZACIÓN DE LA RED

Para realizar la administración y monitorización de todos los equipos de red y estaciones de trabajo se puede utilizar software libre o comercial, el cual ayudará al administrador de la red a tener un menor tiempo de respuesta en caso de presentarse algún inconveniente con algún equipo. Manteniendo la red operable y segura.

En cuanto a herramientas para administrar una red existe una gran variedad en el mercado, pero para la Institución se va a tomar en cuenta Net Tools y WhatsUp Gold, las características de cada uno se detallan a continuación: sin embargo, en el **ANEXO E** se presenta un análisis de las dos alternativas de software mencionadas para la administración de redes.

3.10.1 AXENCE NETTOOLS PRO

Axence NetTools Pro es una herramienta de distribución gratuita utilizada para la monitorización, seguridad y administración de redes locales y tiene incluido las siguientes herramientas:

- NetWatch, esta herramienta es utilizada para monitorear la disponibilidad de hosts.

- WinTools, con esta herramienta se puede ver qué tiene instalado algún equipo en la red.
- NetStat, permite revisar los paquetes de entrada y salida en la red.
- Local info, para ver información detallada del equipo local.
- Network scanner, escanea la red para descubrir todos los nodos de la red.
- Service & port scanner, para obtener información sobre los servicios y puertos.
- TCP/IP workshop, prueba diferentes servicios con este tool
- SNMP Browser y otras herramientas para lanzar Trazas, Pings, entre otros.

Esta herramienta tiene una interfaz gráfica bien amigable por lo que es muy fácil su manipulación para monitorear la red local.

3.10.2 WHATSUP GOLD[71]

WhatsUp Gold ofrece monitoreo de aplicaciones y de redes de forma fácil mediante la interfaz web permitiendo un control total de la infraestructura y aplicaciones de la red. Además, provee una fácil configuración, escalabilidad y simplicidad.

WhatsUp Gold permite aislar los problemas de la red y proporciona visibilidad y comprensión sobre rendimiento y disponibilidad de la red. A continuación se detalla algunas funciones que realiza son:

- Identifica y mapea los dispositivos de la red
- Envía notificaciones cuando un dispositivo falla
- Almacena información de forma periódica de la red para generar reportes
- Proporciona monitoreo continuo de la red de forma local o remota.

[71] [PW45] http://www.ipswitch.com/international/spanish/whatsupgold.asp

- Identificación y Mapeo Dinámico descubriendo la red en minutos utilizando ayudantes de instalación intuitivos para rastrear routers, switches, servidores, impresoras, host y otros dispositivos conectados a la red. Toda la información obtenida es almacenada en una base de datos para luego ser utilizada para una mejor gestión y generación de reportes.
- Realiza la identificación y mapeo de direcciones MAC y direcciones IP, descubriendo la conectividad entre los puertos de un switch y los dispositivos conectados, optimizando la localización de recursos.
- Para una mejor administración envía alertas vía correo electrónico, beeper, SMS, audio y las respectivas alertas que son enviadas a la bandeja de tareas del Sistema.
- Monitoreo de SNMP y WMI

Además de utilizar SNMP v1/2/3 para monitoreo y reportes, también utiliza el WMI[72] de Microsoft para obtener información histórica y en tiempo real sobre todos los dispositivos Windows de la red.

En función de las características técnicas y económicas de cada una de las herramientas antes mencionadas se recomienda utilizar Axence *Net Tools Pro* para la administración de la red UESMDM.

Cabe, indicar que WhatsUp Gold tiene mejores características técnicas para administrar una red, pero se escogió Axence NetTools Pro porque es de libre distribución y fácil de manipular. Además, la red de la UESMDM es una red pequeña por lo que no requiere una herramienta avanzada para su administración.

[72] (WMI) Windows® Management Instrumentation: es un estándar de Microsoft Windows para obtener información de sistemas bajo Windows.

3.11 RECOMENDACIÓN PARA LA SELECCIÓN DEL ANTIVIRUS

Es recomendable adquirir un antivirus de tipo empresarial para mantener la UESMDM libre de virus, gusanos, spam, entre otros. Estos antivirus tienen la ventaja de gestionar las actualizaciones y buscar virus de manera centralizada disminuyendo la carga de la red.

La mayoría de riesgos en seguridad informática se encuentran al interior de la red empresarial, sea por infiltraciones exitosas originadas fuera de la organización, o por ataques internos. Estas amenazas pueden tomar múltiples formas, desde infecciones de virus hasta robo de información confidencial. Para controlarlas, hace falta amplia funcionalidad, incluyendo:

- Control antimalware
- Monitoreo de usuarios
- Administración de políticas
- Administración de Hardware y Software

En el **ANEXO F** se realiza un análisis de tres alternativas de antivirus del tipo empresarial, los cuales pertenecen a los fabricantes Panda, Kaspersky y Symantec.

En función de las características de cada uno de los antivirus antes mencionados se recomienda utilizar el antivirus Kaspersky en la red UESMDM.

3.12 EQUIPOS Y MATERIALES

Después de haber presentado todo los elementos que se requieren para implementar el cableado estructurado en la UESMDM, en la tabla 3.32, se detalla

la cantidad total de todos los accesorios que serán utilizados en la implementación del cableado estructurado. En la tabla 3.33 se detallan los equipos requeridos para la red activa de la UESMDM.

3.12.1 DISPOSITIVOS PARA LA RED PASIVA

NÚMERO	ÍTEMS	DESCRIPCIÓN	CANTIDAD (U)
1	Jacks	Cat 6	354
		Cat 6 A	30
2	Face Plate	Dobles	79
		Simples	8
3	Canaleta Plástica	32X12	18
		40X22	16
		40X40	12
		60X40	5
4	Codo Interno	32X12	6
		40X22	16
		40X40	16
		60X40	6
5	Codo Externo	32X12	6
		40X22	13
		40X40	11
		60X40	5
6	Codo Plano	32X12	5
		40X22	3
		40X40	2
7	Derivación en T	40X22	1
		40X40	2
		60X40	4
8	Terminación	32X12	18
9	Cable UTP CAT 5E	Bobina de 305 m	9
10	Cable UTP CAT 6	Bobina de 305 m	2

NÚMERO	ÍTEMS	DESCRIPCIÓN	CANTIDAD (U)
11	Conduit Metálico 3 m	¾	39
		1	13
		1 1/4	10
12	Codos Metálicos	¾	17
		1	11
		1 1/4	3
14	Cajetines	De paso 20x20	9
15	Patch Cord de 3m	Cat 6	158
	Patch Cord de 3m	Cat 6 A	30
16	Patch Pannel	Cat 6, 24 p	11
	Patch Pannel	Cat 6A, 24 p	1
17	Organizador	Horizontal	13
	Organizador	Vertical	10
18	Panel de Alimentación	AC	5
19	Closet de Telecomunicaciones	13 U	2
		17 U	1
		9 U	1
20	Rack abierto	22 U	1

Tabla 3. 32 Elementos para el Cableado Estructurado. [32]

3.12.2 EQUIPOS PARA LA RED ACTIVA

NÚMERO	ÍTEMS	DESCRIPCIÓN	CANTIDAD
1	**Switch de Acceso**	• 24 puertos *de* 10/100 Mbps full dúplex • Auto negociación de la velocidad de los puertos • Apilable • Administrable mediante consola o vía interfaz Web • Conmutación a nivel de capa 2 • Debe soportar el protocolos IP, DHCP, Telnet y SNMP V1, V2 y V3 (opcional) • Soporte de VLANs IEEE 802.1q • Debe soportar el estándar de seguridad IEEE 802.1X, listas	10

		de control de acceso (ACL), prevención mediante (DoS) y filtrado basado en MAC. • Soportar calidad de servicio (QoS) en base a IEEE 802.1p e IEEE802.1q. • Velocidad de backplane mínima de 8.8 Gbps • IP versión 4 y 6 • Soporte de 8000 direcciones MAC • Soporte de paquetes de telefonía IP (VoIP)	
2	**Switch de Core**	• 24 puertos *de* 10/100 Mbps full dúplex • Auto negociación de la velocidad de los puertos • Apilable • Administrable mediante consola o vía interfaz Web • Conmutación a nivel de capa 2,3 y 4 • Debe soportar el protocolos IP, STP, RIPv1 y 2, DHCP, Telnet y $SNMP_{V\ (1,\ 2\ y\ 3)}$, $OSPF_{V\ (2\ y\ 3)}$, $RMON_{V\ (2\ y\ 3)}$ • Manejo y Administración de VLANs IEEE 802.1q • Debe soportar el estándar de seguridad IEEE 802.1X, listas de control de acceso (ACL) a nivel 2,3 y 4, prevención mediante (DoS) y filtrado basado en MAC. • Soportar calidad de servicio (QoS) en base a IEEE 802.1p e IEEE802.1q. • Velocidad de backplane mínima de 8.8 Gbps • IP versión 4 y 6 • Manejo, priorización y clasificación de tráfico VoIP	1
3	**Access Point**	• Tasa de transmisión de 54 Mbps • Protocolo de gestión: SNMP (v1, v2, v3) (Opción) • Algoritmo de cifrado DES y AES • Filtrado MAC • Soporte estándares: IEEE 802.11g, IEEE 802.11e, IEEE 802.11q y IEEE 802.11x • 1 interfaz Fast Ethernet • Configuración de SSID • Soporte de VLANs • Certificación Wi-Fi	2

NÚMERO	ÍTEMS	DESCRIPCIÓN	CANTIDAD
4	**Servidores**	• Procesador: 2.6 GHz o superior, • Memoria RAM: 2 GHz o superior • Disco Duro: Mínimo: 640 GB o superior • Tarjeta de red 10/100/1000 Mbps	3
5	**Central Telefónica IP**	• Interfaces FXO (3) y FXS • Soporte mínimo para 16 Usuarios • Protocolos de señalización • Control de llamadas • IVR • Correo de voz • Administración vía web • Distribución automática de llamadas • Soporte de códecs G.729a • Soporta Auto negociación de códec • Software basado en Asterisk (Elastix)	1
6	**Teléfonos IP**	• 2 interfaces RJ45 • Soporte del protocolo SIP • Seguridad • Soporte de códecs G.729 • Soporte DHCP • QoS (802.1p) • Compatibilidad con protocolos de administración • Soporte de VLANs • Calidad de voz • Identificador de llamadas • Llamada en espera • Transferencia de llamadas	16
7	**Cámaras IP**	• Un puerto 10/100 Fast Ethernet • Protocolos TCP/IP, HTTP y DHCP • Movimiento horizontal de cobertura 90° • Detección de movimiento tanto de día como de noche (VMD) (Opcional) • Formato de compresión MPEG-4 ó H.264	8

		• Resolución de 640X480 pixeles ó superior • Autenticación de usuario.	
8	**Firewall**	• Firewall Throughput: 100 Mbps • 1 puertos WAN • 1 puertos LAN • 1 Puerto DMZ • IPS • Antivirus • Antispam • VLAN • Prioridad de ancho de banda	**1**

Tabla 3. 33 Elementos activos de la red. [33]

3.13 PROTOTIPO DE PRUEBA

El diagrama del prototipo de prueba se detalla en la figura 3.25

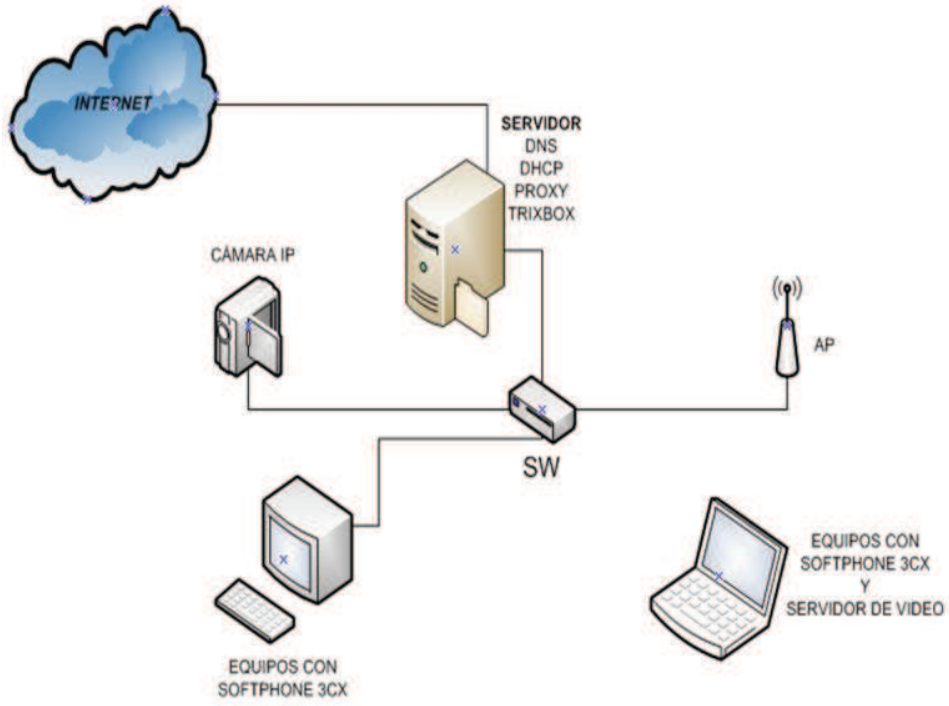


Figura 3. 28 Diagrama del Prototipo de Prueba. [28]

El prototipo de prueba se basa en configurar los servicios que se va a tener en la Institución, para ello se configura una central telefónica IP basada en asterisk, los servidores DHCP, DNS y Proxy.

Se utiliza una laptop hp, computador de escritorio, un router D-Link modelo DIR-600, una cámara IP D-Link modelo DCS-930L y un switch Advantek modelo ANS-05P

3.13.1 IMPLEMENTACIÓN DE LOS SERVIDORES DHCP, DNS Y PROXY

Para la instalación de los servidores DHCP, DNS y Proxy se utilizará el sistema operativo Red Hat 5

3.13.1.1 Instalación y Configuración del Sistema Operativo Red Hat 5

A continuación se detallan los pasos más importantes para instalar y configurar Red Hat 5.
Al empezar la instalación es recomendable presionar ***Enter*** para instalar desde cero el sistema operativo como se indica en la figura 3.29.

Figura 3. 29 Inicio de la Instalación de Red Hat. [29]

Otra parte importante en la instalación es la elección de los servidores que se desea instalar, para este caso se requiere los servidores DNS, DHCP y Proxy como se indica en la figura 3.30

Figura 3. 30 Selección de los servidores (Continuación). [30]

Al finalizar la instalación es importante seleccionar servicios específicos que el firewall deje pasar y para que filtre acceso no autorizado como se indica en la figura 3.31.

Figura 3. 31 Selección de servicios específicos (continuación). [31]

3.13.1.2 Configuración del servidor DHCP (Dynamic Host Configuration Protocol))

DHCP es un estándar TCP/IP creado para simplificar la configuración IP de los equipos de una red. Debido a que la asignación de direcciones IP es de forma automática sin necesidad de hacerlo manualmente.

Para configurar un servidor DHCP se modifica el archivo ubicado en /etc/**dhcpd.conf**

En la figura 3.32 se detalla la configuración realizada en el archivo. En el cual se utilizó la dirección IP privada 192.168.1.0 con máscara 255.255.255.0 con el rango de direcciones que va desde la 192.168.1.10 hasta la 192.168.1.20, la dirección broadcast es la 192.168.1.255 y la de Gateway será la 192.168.1.1

Los parámetros que se configuran son los siguientes:

- option routers (Esta es la dirección del servidor)
- option subnet-mask (Para la máscara de red)
- option domain-name (Nombre del dominio)
- Range (Rango de direcciones IP)

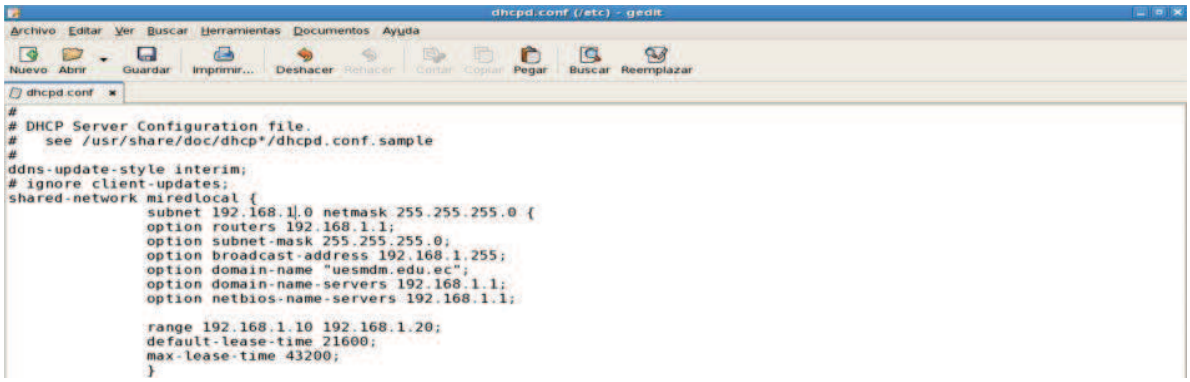


Figura 3. 32 Configuración del servidor DHCP. [32]

Para realizar la comprobación del servidor DHCP se utilizó el comando ***ipconfig*** en una computadora que tiene el sistema operativo Windows como se indica en la figura 3.33.

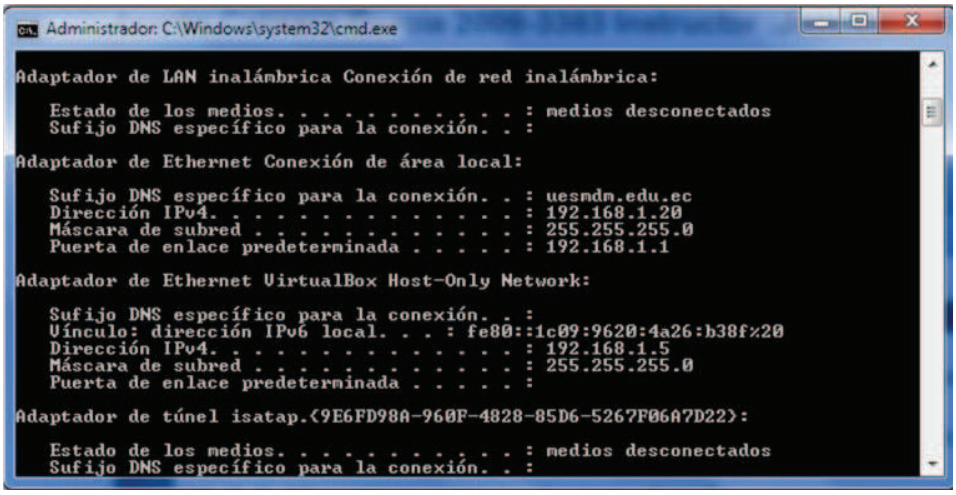


Figura 3. 33 Prueba realizada (Continuación). [33]

3.13.1.3 Configuración del servidor DNS

Un servidor DNS permite averiguar la IP de un PC a partir de su nombre. Para ello, el servidor DNS dispone de una base de datos en la cual se almacenan las direcciones IP y los nombres de las PCs pertenecientes a su dominio.

Los servidores DNS se encuentran de forma jerárquica de modo que si el servidor local no puede resolver una petición, este lo traslada al DNS superior.

Primero se realiza la configuración del fichero ***/etc/hosts***, agregando el nombre del equipo que desempeñara la función de servidor DNS así como también la dirección IP asignada a ese equipo como se detalla en la figura 3.34.

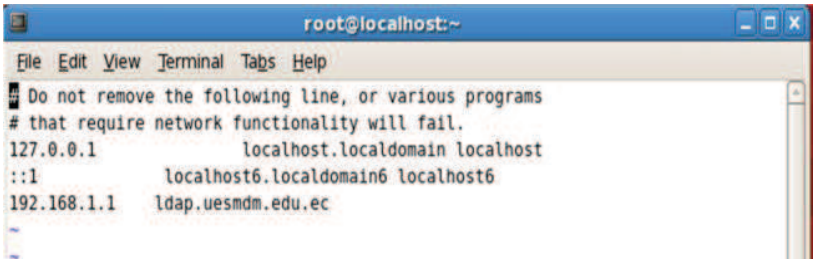
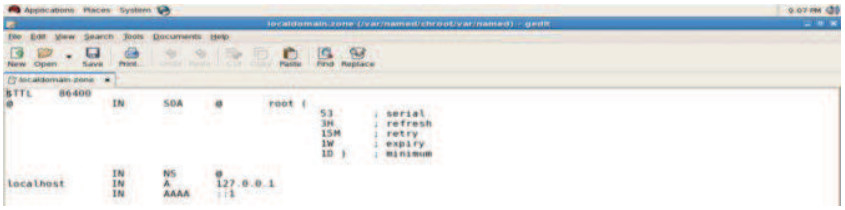


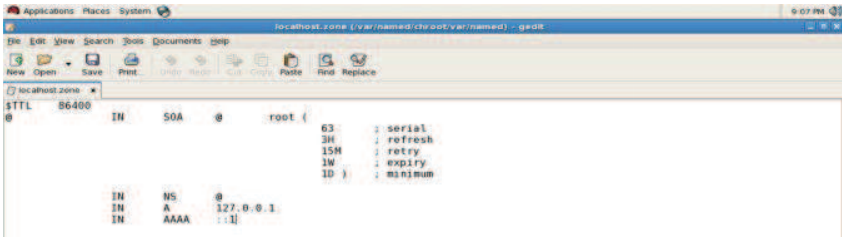
Figura 3. 34 Configuración del archivo ***/etc/hosts.*** [34]

Ficheros de configuración del DNS

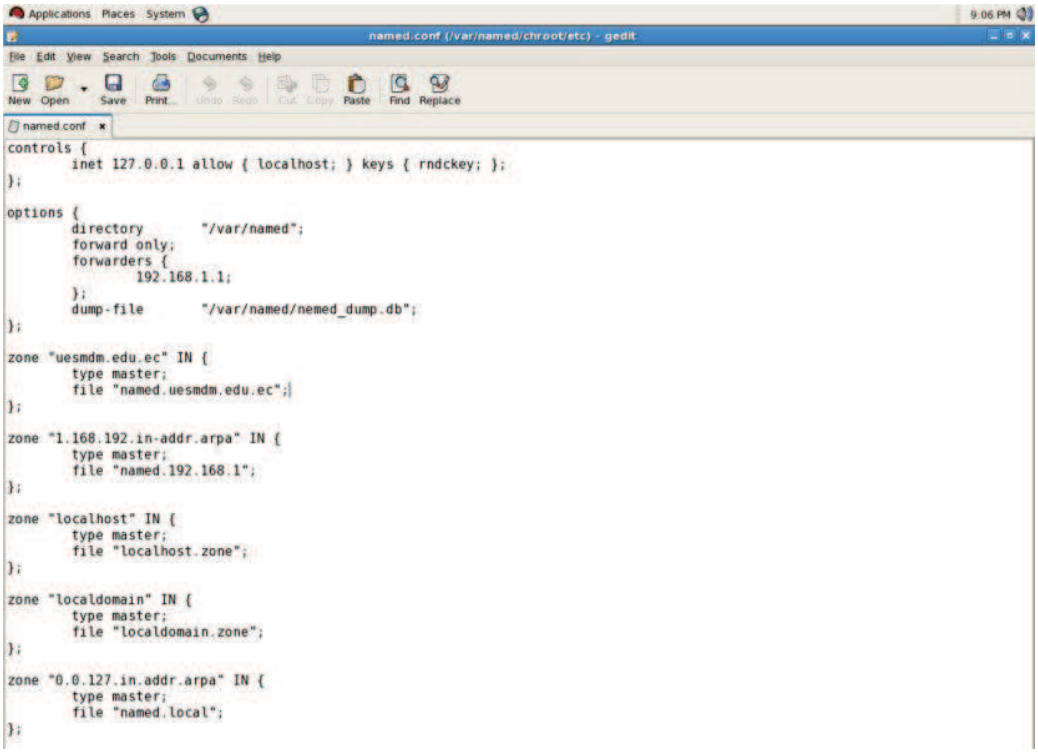
Los siguientes archivos deben ser creados y configurados como se detallan en la figuras a continuación.

- /var/named/chroot/etc: aquí se crea el archivo "named.conf".
- /var/named/chroot/var/named: creación de los ficheros de zona que son invocados por named.conf.

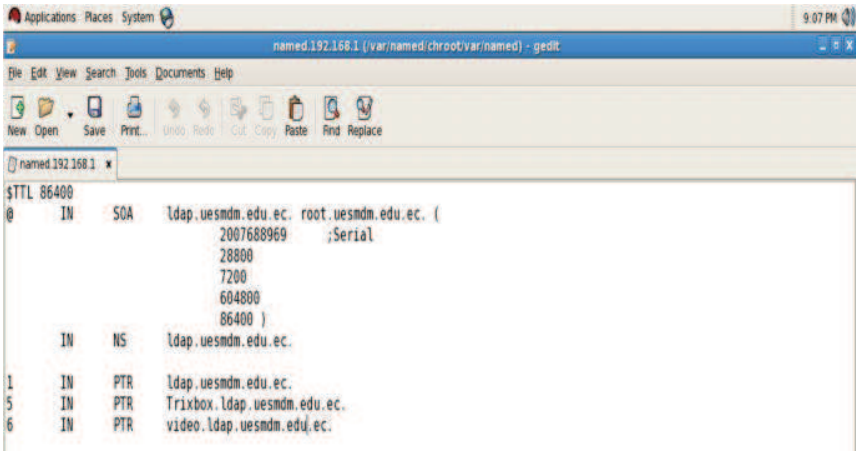




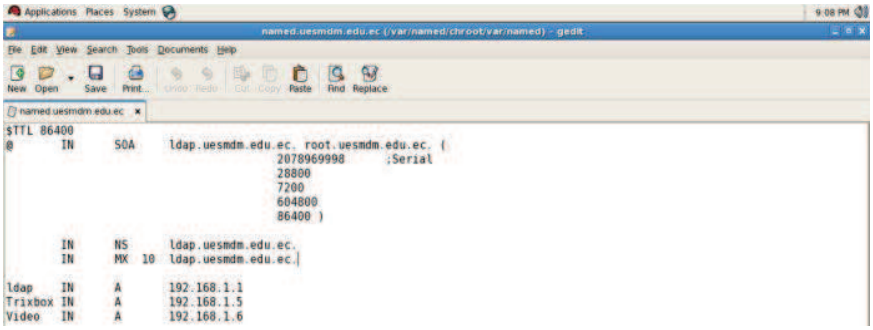
Generación del fichero "named.conf" dentro de la ruta "/var/named/chroot/etc/":



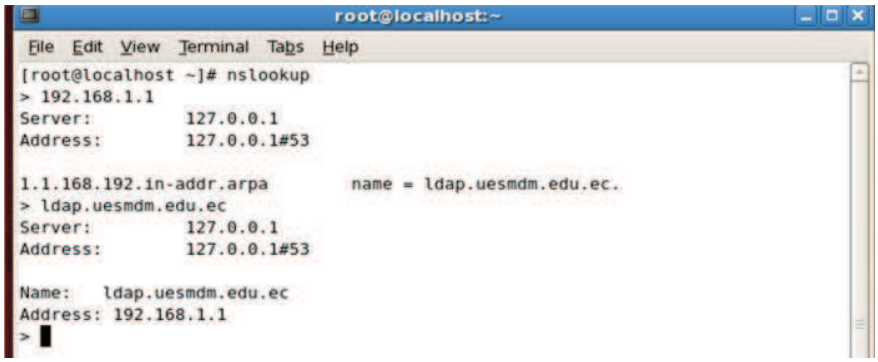
Generación del fichero para la resolución de la zona inversa "named.192.168.1" dentro de la ruta "/var/named/chroot/var/named/"



Generación del fichero para la resolución de la zona directa "named.uesmdm.edu.ec" dentro de la ruta "/var/named/chroot/var/named/"



Para comprobar el correcto funcionamiento del servidor se utiliza el comando ***nslookup***



3.13.1.4 Configuración del servidor Proxy (Squid)

Squid es un software utilizado como servidor proxy, es de libre distribución y está basado en UNIX. Además ofrece confiabilidad, robustez y versatilidad convirtiéndolo en uno de los más populares.

Squid también puede funcionar como Servidor Intermediario (Proxy) y caché de contenido de red para los protocolos HTTP, FTP, Proxy de SSL, caché transparente, WWCP, aceleración HTTP, caché de consultas DNS, filtración de contenido y control de acceso por IP y por usuario.

La configuración se la realizó en el fichero ***squid.conf*** localizado en la ruta ***/etc/squid/squid.conf*** como se detalla en la figura 3.35.

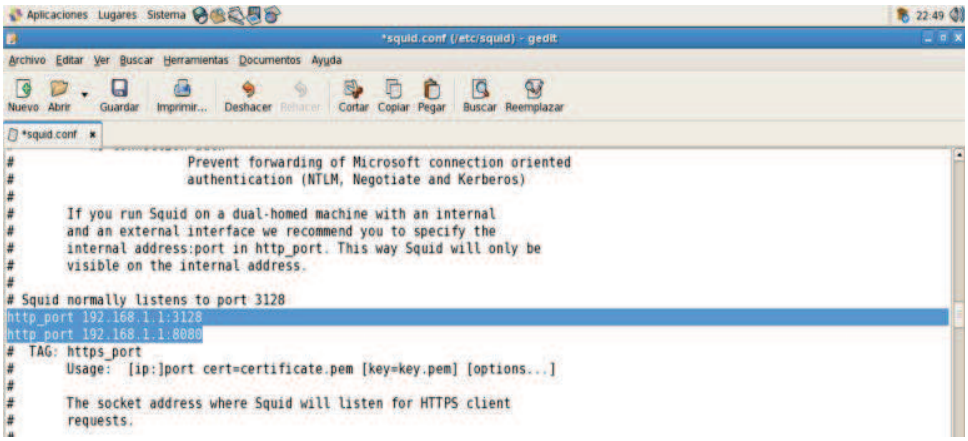


Figura 3. 35 Habilitación de los puertos. [35]

Creación de las ACLs para el control.

```
#Examples:
#acl macaddress arp 09:00:2b:23:45:67
#acl myexample dst_as 1241
#acl password proxy_auth REQUIRED
#acl fileupload req_mime_type -i ^multipart/form-data$
#acl javascript rep_mime_type -i ^application/x-javascript$
#
#Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl todalared src 192.168.1.0/255.255.255.0
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"
acl extensionesdenegadas urlpath_regex "/etc/squid/extensionesdenegadas"
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
```

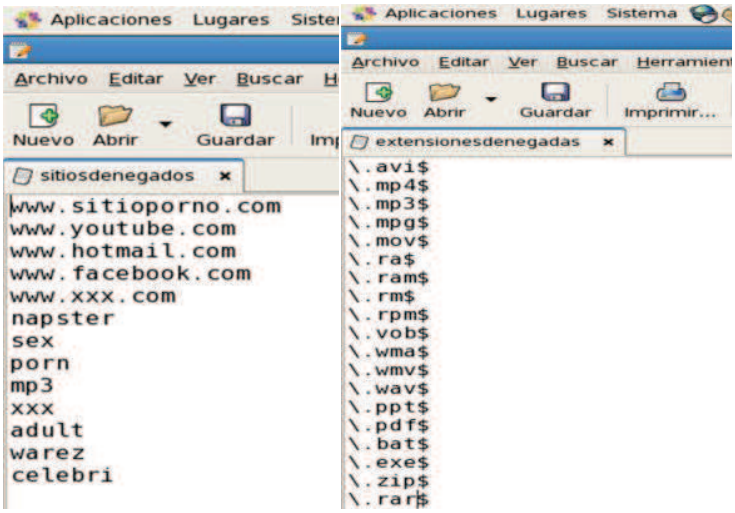
En la siguiente figura se crean las reglas para el control de acceso.

```
# Example rule allowing access from your local networks. Adapt
# to list your (internal) IP networks from where browsing should
# be allowed
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
#http_access allow our_networks

# And finally deny all other access to this proxy
http_access allow localhost
http_access allow todalared !sitiosdenegados !extensionesdenegadas
http_access deny all

#  TAG: http_access2
#       Allowing or Denying access based on defined access lists
#
#       Identical to http_access, but runs after redirectors. If not set
#       then only http_access is used.
#
```

Creación de los ficheros ***sitiosdenegados*** para restringir sitios web no deseados por la Institución y de extensiones denegadas para que los usuarios no puedan descargar archivos con las extensiones guardadas en dicho fichero.



3.13.2 IMPLEMENTACIÓN DE LA CENTRAL TELEFÓNICA IP TRIXBOX CE

Trixbox es una distribución ideal para pequeñas empresas donde no se requiere un gran número de extensiones. Además, su ambiente gráfico permite una fácil instalación y configuración sin necesidad de tener gran conocimiento en el sistema operativo Linux y mucho menos en Asterisk.

Los componentes que vienen incluidos en Trixbox son:

- Linux Centos como Sistema Operacional
- Asterisk el cual es el núcleo de la telefonía
- Drivers Zapata telephone
- Librería para soporte RDSI (Requerido para las tarjetas FXO/FXI)
- FreePBX entorno gráfico para la configuración mediante interfaz web

- FOP (Flap Operator Panel) para monitoreo de Asterisk
- Web Meet Control: es el administrador para salas de conferencias

La instalación se la realizará en una maquina utilizando VM VirtualBox en el sistema operativo Red Hat.

3.13.2.1 VM VirtualBox

VirtualBox es una aplicación que permite ejecutar diferentes Sistemas Operativos simultáneamente en el mismo equipo de manera virtual. La razón para usar VirtualBox es porque es libre (GNU/GPL) y ofrece un buen desempeño con servidores.

3.13.2.1.1 Instalación de VirtualBox en Red Hat

Para instalar VirtualBox en Red Hat se descarga la versión más reciente desde la dirección ***http://www.virtualbox.org*** y se realiza los siguientes pasos:

- rpm –ivh VirtualBox-4.1-4.1.4_74291_rhel5-1.i386.rpm (Para instalar el paquete rpm)
- rpm –ivh kernel-devel-2.6.18-92.1.18.SEL5.i386.rpm (paquete requerido para actualizar el kernel)
- Recompilar
- [root@localhost ~]# cd /etc/init.d/ (Ir al directorio para e iniciar el kernel)
- [root@localhost init.d]# ./vboxdrv setup Stopping VirtualBox kernel module [OK]
- Recompiling VirtualBox kernel module [OK]
- Starting VirtualBox kernel module [OK]

3.13.2.1.1 Crear y configurar la maquina virtual Trixbox

La creación de una maquina virtual en VirtualBox es bien sencillo solo se realiza los siguientes pasos:

- Hacer click en el icono 
- Nombre y tipo de Sistema Operativo
- Tamaño de la memoria RAM y HD
- Configurar la tarjeta de red
- Instalar e iniciar Trixbox

3.13.2.2 Requisitos mínimos de Hardware para la instalación

Se requiere de un PC o servidor que cumpla con las siguientes características:

- Pentium IV de 1.8 GHz
- Memoria de 512 MB
- HD de 8 GB
- Tarjeta de re 10/100 Mbps
- Unidad CD-ROM

3.13.2.3 Pasos para la instalación

Para una correcta instalación de Trixbox se efectúa 2 pasos previos que son importantes, primero saber el número de usuarios que requieren telefonía y el segundo consiste en definir qué tipo de servicios se brindará a los usuarios.

La primera actividad se le conoce como "Planificar el plan de marcación" ó DIAL PLAN, que para este caso se definirá de la forma que esta detallado en la tabla 3.34.

PLAN DE MARCADO		
EXTENSIONES POR DEFAULT	#	Directorio Telefónico del Sistema
	*43	Prueba de echo de llamadas
	*52	Extension no disponible OFF
	*53	Extension no disponible ON
	*60	Hora del sistema
	*65	Prueba de sonido audible de la extensión
	*69	Ultimo número que ha llamado
	*70	Llamada en espera ON
	*71	Llamada en espera OFF
	*72	Desvió de llamada ON
	*73	Desvío de llamada OFF
	*77	Grabar mensaje de IVR
	*78	Opción de "No molestar" ON
	*79	Opción de "No molestar" OFF
	*91	Teléfono ocupado no disponible ON
	*92	Teléfono ocupado no disponible OFF
	*97	Cambiar el mensaje de bienvenida del buzón
	*98	Acceso al buzón de mensajes
	*99	Oír la grabación de mensaje de IVR
	70	Poner en espera de transferencia de llamada PARKING
EXTENSIONES PROPIAS	**PLAN DE MARCADO**	
	220	Oscar Aguilar
	221	Vanesa Cruz
	222	Carlos Vaca

Tabla 3. 34 DIAL PLAN. [34]

Luego de tener bien claro los pasos previos mencionados en la tabla 3.36 se realiza la instalación de la central telefónica IP.

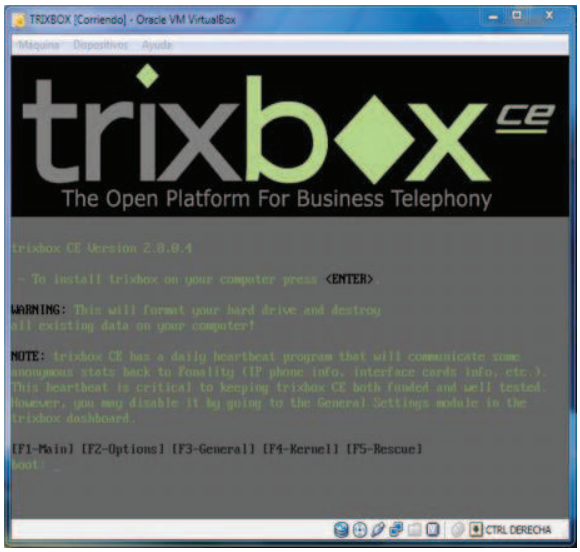


Figura 3. 36 Ventana de instalación de Trixbox. [36]

Instalar el sistema Trixbox es muy sencillo ya que no requiere ningún nivel avanzado porque solo pide se ingrese:

- Idioma del teclado
- Uso horario
- IP fija o estática la cual puede ser configurada luego de la instalación utilizando el comando ***system-config-network***
- Password para acceder al sistema

Una vez terminada la instalación, el sistema pide nombre de usuario y password que son: ***root*** y el password ingresado durante la instalación, el servidor está listo para ser configurado, para ello se ingresa desde un browser con la dirección IP que se asigno http://Dir IP. Acceder al sistema como usuario maint y password password como se indica en la figura 3.37.

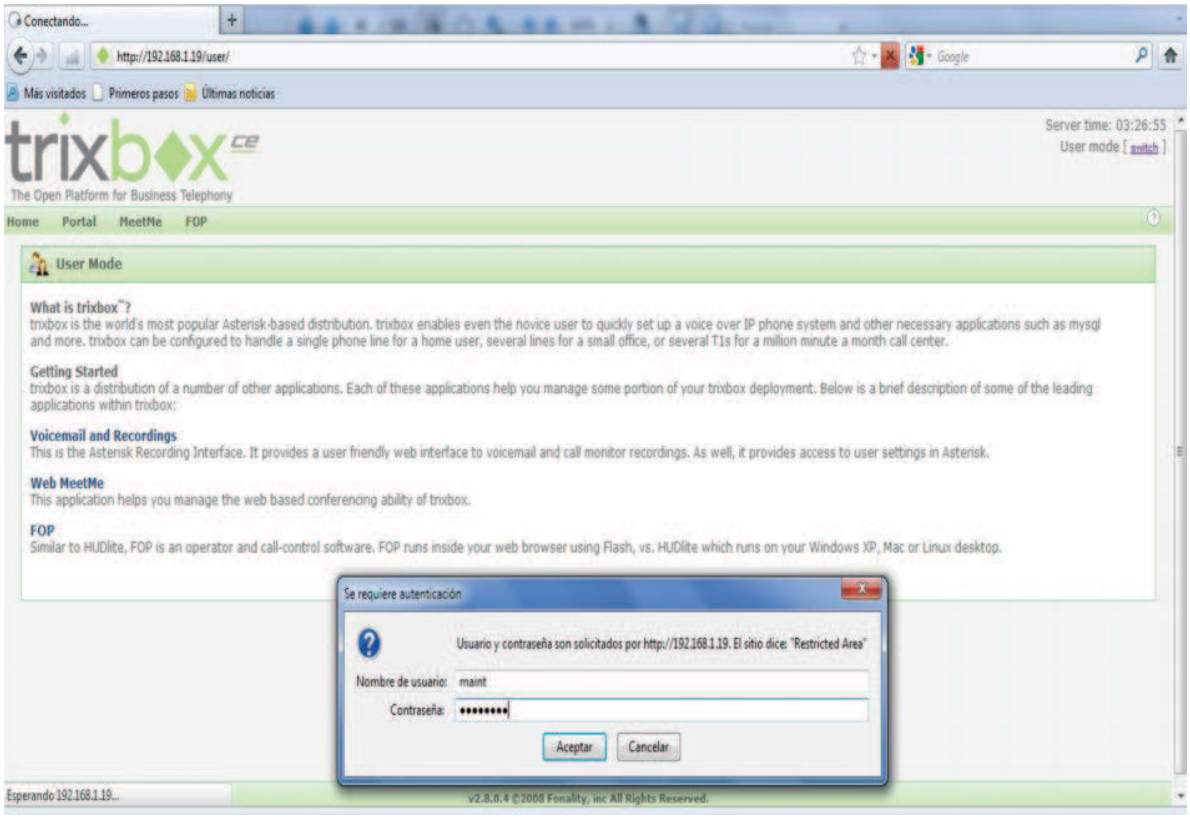
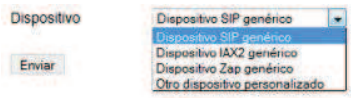


Figura 3. 37 Ingreso al sistema (continuación). [37]

3.13.2.4 Configuración de extensiones

Pasos para configurar una extensión

- Ingresar a PBX y setting PBX
- Ingresar a la opción de extensiones y seleccionar el tipo de extensión a crear



- Los datos básicos a ingresar son: extensión del usuario y nombre para mostrar en la pantalla del teléfono 3CX

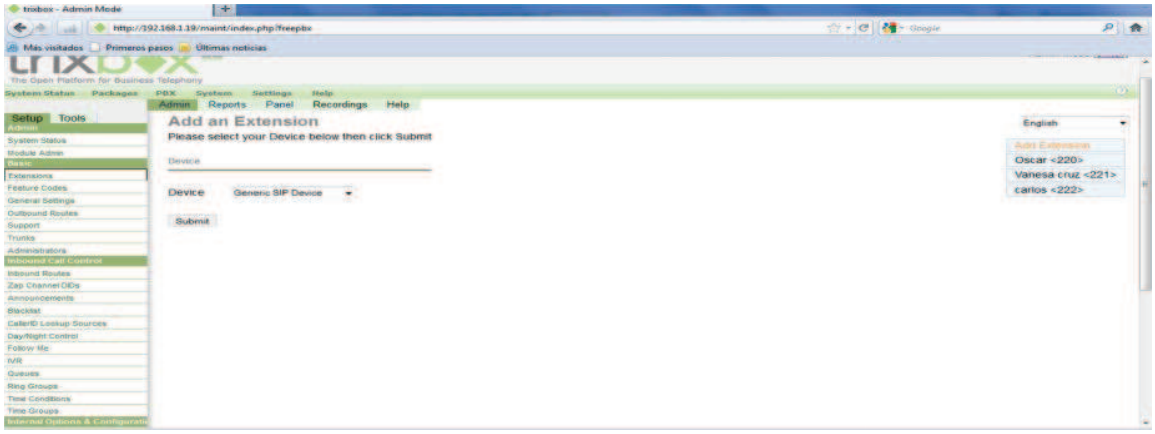


Figura 3. 38 Extensiones configuradas. [38]

3.13.2.5 Configuración de una Troncal

Trixbox CE tiene varias opciones para crear líneas troncales que son:

- Añadir línea troncal Zap (Modo de compatibilidad con DAHDI)
- Añadir línea troncal IAX2
- Añadir línea troncal SIP
- Añadir línea troncal ENUM
- Añadir línea troncal DUNDi

Para este proyecto se escoge la primera opción debido a que la tarjeta instalada en la PC es analógica

3.13.2.6 Teléfono 3CXPhone[73]

Teléfono 3CX es completamente gratuito para usuarios individuales y para empresas incluyendo entidades comerciales. Todas las características incluyendo

[73] [PW54] http://www.3cx.es

transferencia de llamada, están habilitadas. Esto facilita a las empresas, la instalación en cualquier escritorio de Windows, sin tener que preocuparse acerca del costo o problemas de administración de licencias. Además, cuenta con una interfaz intuitiva y fácil de usar.

Teléfono 3CX está disponible en 3 versiones:

- para Microsoft Windows XP, Vista y 7
- Dispositivos basados en Android 1.6, 2.1, 2.2 tales como Google Nexus, Sony Xperia, Motorola Droid o Samsung Galaxy y Iphone 3G, 3GS y 4.

3.13.2.6.1 Características del Teléfono 3CXPhone

Las características del teléfono 3CXPhone son:

- Habilidad para grabar llamadas al disco con un solo clic de un botón.
- Teléfono 3CX es un teléfono SIP que puede ser aprovisionado fácilmente en toda la red. A través de un URL,
- Aplicación pequeña y rápida
- Habilidad para trasferir llamadas o ponerlas en espera
- Multi-líneas (Windows)
- Soporta múltiples perfiles SIP
- Muestra registro / historial de llamadas personales
- Soporta & adhiere a los estándares RFC SIP
- Soporta G.711 (Ley-A y Ley-u), GSM y codecs Speex
- Soporte STUN para NAT/firewall traversal
- Archivo de instalación provisto como MSI para fácil despliegue (Windows)

- Funciona perfectamente como teléfono SIP con la Central Telefónica 3CX para Windows, la cual es una central SIP basada en software que reemplaza completamente una central telefónica propietaria tradicional.

3.13.2.6.2 Instalación del Teléfono 3CXphone

La instalación es bien sencilla, se descarga la aplicación desde http://www.3cx.es y se realiza los siguientes pasos:

- Ejecutar la aplicación y seleccionar Next (Pantalla de bienvenida)
- Aceptar las condiciones y Next
- Ingresar el directorio donde se va a instalar 3CXPhone
- Finalizar

3.13.2.6.3 Configuración del Teléfono 3CXphone

Para configurar 3CXPhone se realiza los siguientes pasos y se llena las opciones de la figura 3.39

- Click en la pestaña 
- En el menú ingresar a la opción Accounts 
- Crear una nueva cuenta
- Ingresar el nombre, número de extensión, password, ID y la dirección IP de la central telefónica.

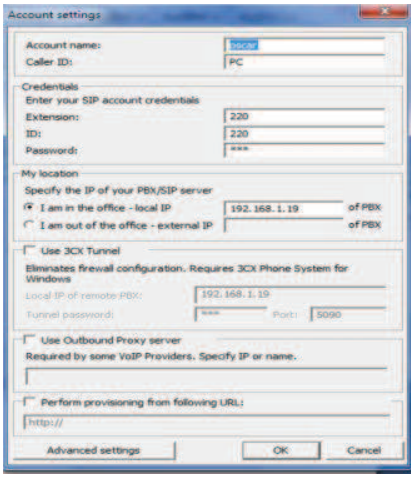


Figura 3. 39 Configuración de 3CXPhone. [39]

3.13.2.7 Pruebas de funcionamiento realizadas

Se realizó una llamada al usuario Oscar que tiene asignado la extensión 220, en la figura 3.40 se observa la recepción de la llamada.

Figura 3. 40 Prueba de Comunicación. [40]

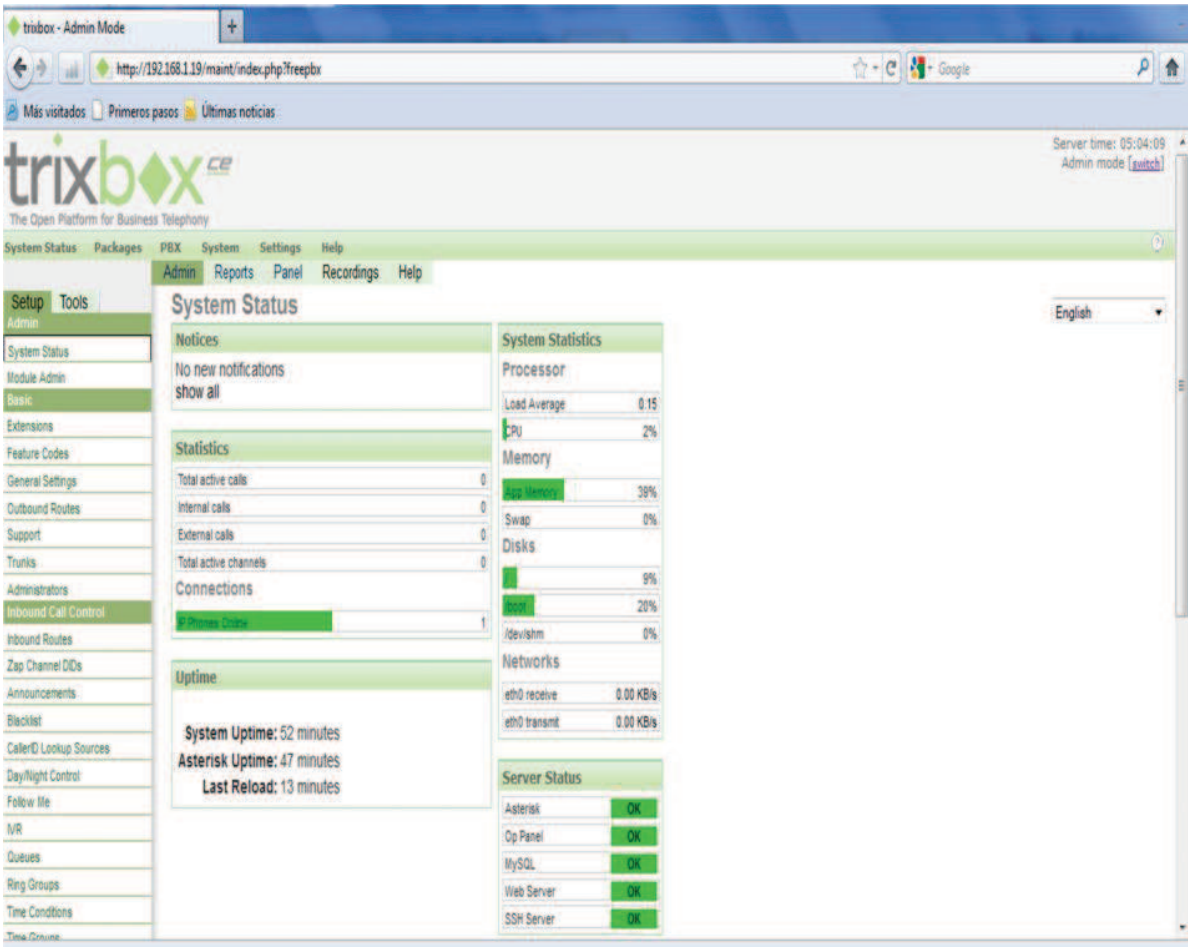


Figura 3. 41 Prueba de Estado del Sistema (Continuación). [41]

En la figura 3.41 se observa el estado del sistema, la pestaña de notificaciones indica si existen restricciones, en las estadísticas todo lo relacionado a las llamadas y los teléfonos conectados. Adicionalmente, en la parte de memoria y procesador nos da información del procentaje de utilización.

Además, se puede visualizar los servicios que están levantados en la central IP y los datos recibidos y transmitidos por la interfaz Ethernet.

3.13.3 VIDEO VIGILANCIA Y WLAN

Configuraciones básicas realizadas en los equipos para habilitar los servicios de video vigilancia y la WLAN.

3.13.3.1 Configuración de la Consola para Administrar las cámaras IP D-Link

Para instalar la consola de administración sólo se requiere de una pc que tenga una tarjeta de red, navegador y espacio en el disco duro para guardar el video.
Para este caso se utilizó una laptop hp y se realizó las siguientes configuraciones.

- Ubicar el directorio donde se guarda el video (F*:\CAMARAIP*). Ver figura 3.42
- Para registrar la cámara se ingresa la dirección IP y el usuario y contraseña como se indica en la figura 3.43
- Selección del número de imágenes por segundo, resolución y calidad de la imagen. Ver figura 3.44

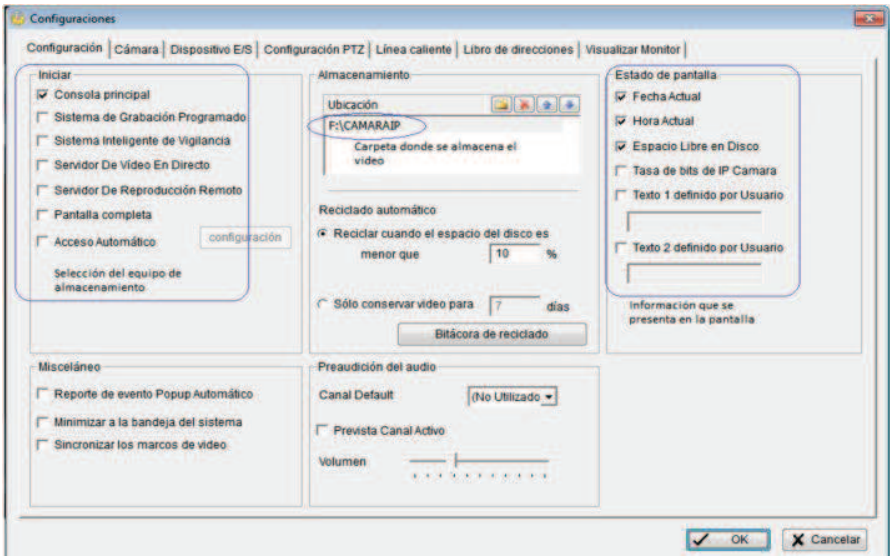


Figura 3. 42 Configuracion de Almacenamiento. [42]

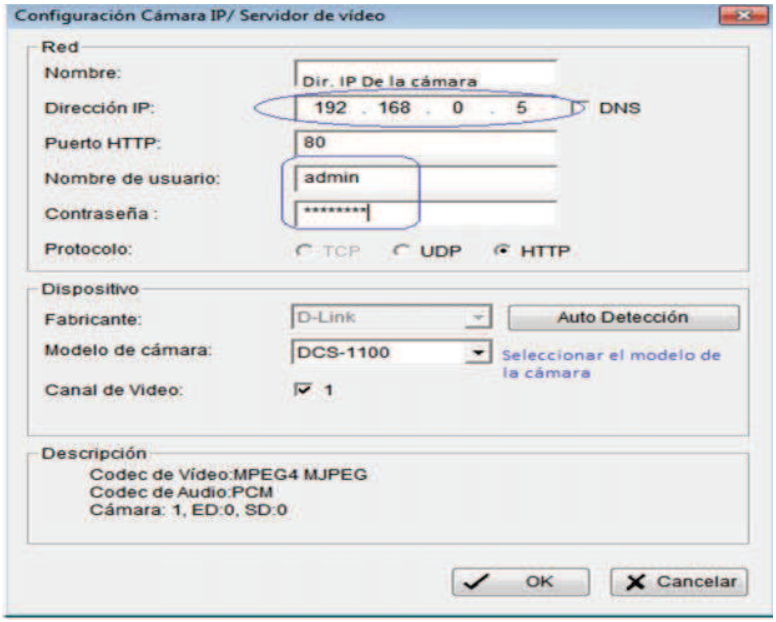


Figura 3. 43 Configuracion de Almacenamiento. [43]

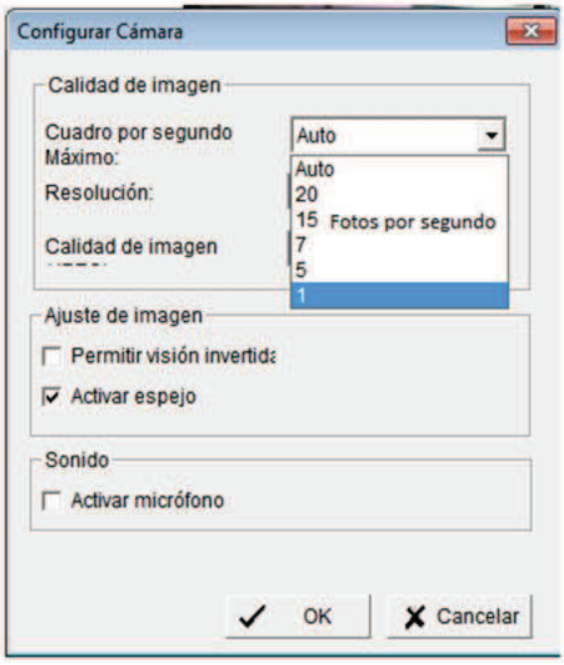


Figura 3. 44 Número de imágenes por segundo. [44]

En la figura 3.45 se indica los resultados obtenidos luego de haber realizado la configuración indicada anteriormente.

Figura 3. 45 Resultados obtenidos. [45]

3.13.3.2 Configuarción del Router D-Link Wireles N 150 Home

Para este caso sólo se realizó la siguiente configuración.

- Se configuró el acceso a Internet asignándole la dirección IP de forma dinámica. ver gráfico 3.46
- Configuración de la red Lan para que asigna un rango de direcciones desde la 192.168.0.5 hasta la 192.168.0.10 con máscara de 24. Ver figura 3.47
- Para la parte inalámbrica se le asigno el nombre UESMDM con cifrado AES como se detalla en la figura 3.48

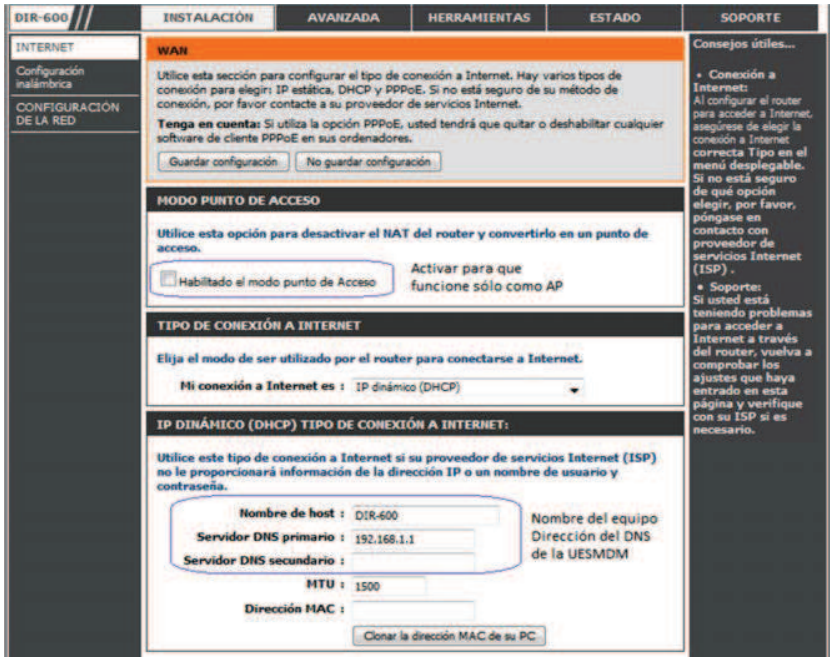


Figura 3. 46 Configuración de Acceso al Internet. [46]

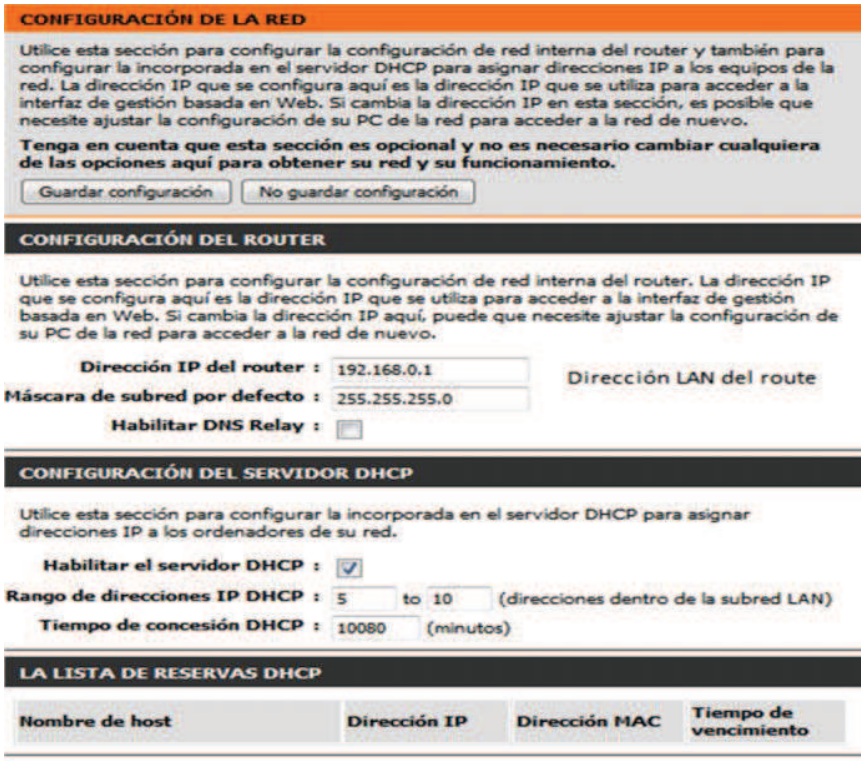


Figura 3. 47 Configuración de la red. [47]

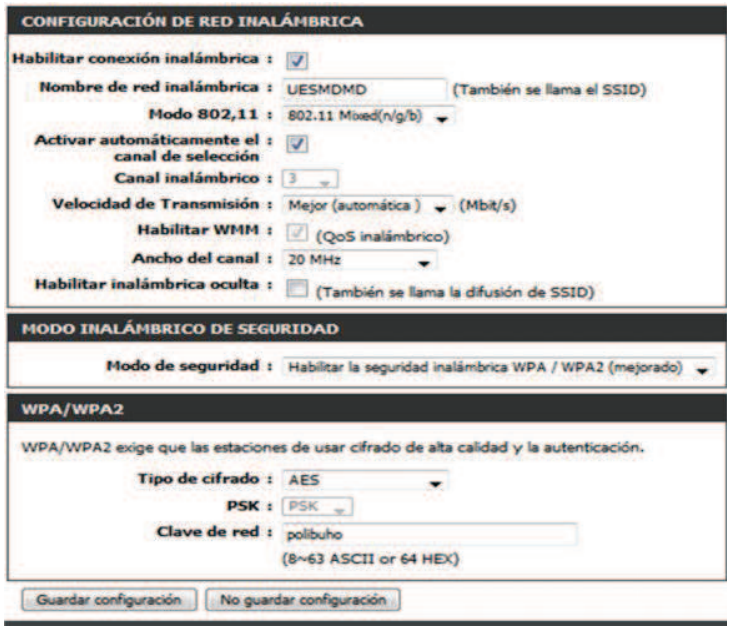


Figura 3. 48 Configuración de la red. [48]

3.13.3.2.1 Pruebas realizadas

En la figura 3.49 se puede observar la conexión inlámbrica a la red de la UESMDM con el tipo de seguridad que se configuró en el router.

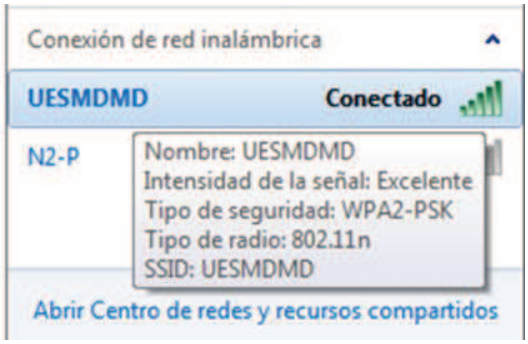


Figura 3. 49 Conexión a la red UESMDM. [49]

CAPÍTULO 4

ANÁLISIS DE COSTOS

CAPÍTULO 4

ANÁLISIS DE COSTOS

En este capítulo se realiza el análisis de costos y comparación de los equipos seleccionados para la implementación de la nueva red para la UESMDM.

Los equipos tomados en cuenta son para la red pasiva (Cableado Estructurado) y para la red activa (Equipos de networking). Además, de los equipos para la telefonía IP que se utilizan en el diseño de la red.

4.1 REUTILIZACIÓN DE EQUIPOS

La red de la UESMDM tiene varios equipos de networking, los cuales pueden ser reutilizados en el diseño disminuyendo el costo del proyecto.

Se consideran algunos equipos por sus características y su estado actual. En el caso de las estaciones de trabajo se reutilizará todas, esto es debido a que se encuentran en perfecto estado para realizar las diferentes tareas de acuerdo al tipo de usuario al que pertenezcan.

4.1.1 EQUIPOS DE NETWORKING

4.1.1.1 Switches de Acceso

Algunos de estos equipos serán reutilizados en los laboratorios. Cabe indicar que no cumplen con las características de los switches de acceso requeridos. Sin

embargo debido al alto costo se pueden seguir utilizando hasta adquirir los nuevos switch.

Finalmente, es importante mencionar que los equipos de networking que se reutilizaran serán utilizados solo para conectar las estaciones de trabajo por lo que no se conectará cámaras o teléfonos IP ya requieren de mejores características de los switches.

Los equipos reutilizados se detallan en la tabla 4.1

EQUIPO	CARACTERISTICAS
D-Link Des 1024 R	24 puertos de 10/100Mbps Auto negociación entre 100BASE-TX y 10BASE-T Modo de comunicación full y half-duplex. 2 puertos para fibra óptica (opcional) Control de flujo Apilable hasta 2 switches Soporta los siguientes estándares - IEEE 802.3 10BASE-T Ethernet - IEEE 802.3u 100BASE-TX Fast Ethernet - IEEE 802.3u 100BASE-FX Fast Ethernet - ANSI/IEEE 802.3 NWay auto-negotiation - IEEE 802.3x Flow Control Protocolo: CSMA/CD
	

Tabla 4. 1 Características de los Switches de acceso. [1]

4.1.1.2 Router

Se reutilizará el router inalámbrico 3COM® WIRELESS 11N CABLE/DSL FIREWALL como uno de los Access Point y firewall en el proyecto ya que cumple con las características que se requiere.

Las características técnicas del equipo están detalladas en la tabla 4.2

EQUIPO	3COM® WIRELESS 11N CABLE/DSL FIREWALL	
	CARACTERÍSTICAS	
	Mínimos Requerimiento del sistema	Interfaces Ethernet 10/100BASE Soporta IEEE 802.11n 802.11g y 802.11b
Número de Usuarios simultaneos	32 usuarios inalámbricos, la administración de los usuarios inalámbricos la realiza por filtrado MAC	
Wireless Networking	Wireless distribution system (WDS); WDS con WEP y WPA/WPA2 Soporta canales de 20 Mhz y 40 Mhz Soporta WMM (IEEE 802.11e) Filtrado de direcciones MAC	
Banda de Operación	2.4 GHz	
Modulación	OFDM CCK	
Técnica de acceso al medio	CSMA/CA	
Pila de protocolos	Direccionamiento IP estático y dinámico DHCP server IP to MAC address binding NAT/PAT (with TCP and UDP), PPPoE, PPTP, IP, PAP, CHAP, MS CHAP, IPCP, SNTP, L2TP	
Routing y Networking	RIP 1 y 2 Ruteo estático IGMP snooping Puertos basados en VLANs	
Calidad de Servicio (QoS)	WMM Diferenciación de servicio (DiffServ); mark/remark up para 16 regles de mapeo	
Seguridad	Utiliza 128-bit WPA/WPA2 con TKIP/AES 40-/64-bit y 128-bit WEP para encriptación Soporta servidor virtual Soporta ACL Proxy ARP Virtual DMZ support (up to 8 servers) SSID Broadcast Disable MAC address filtering NAT/PAT/NAT off Traffic metering Full stateful packet inspection (SPI) firewall with DoS/DDoS protection NAT-T draft 2.0 SIP ALG	
VPN	IPSec, PPTP y L2TP/IPSec Encryption: DES, 3DES, AES-128, AES-256 Key management: IKE (main and aggressive modes) IKE keep-alive FQDN support y PFS	
Administración	Browser-based administration Administración remota via HTTP E-mail alerts y SNMP v1/2c (MIBII)	

Tabla 4. 2 Características del Router inalámbrico. [2]

4.1.2 SERVIDORES

Se reutilizará los dos servidores, para ello se deben adquirir 2 HD (discos duros) de 500 GB, 2 memorias RAM de 1 GB a más de una fuente de poder, las características técnicas están detalladas en la tabla 4.3.

Marca	**HP**
Modelo	ProLiant ML350G5
RAM	512 MB
Velocidad de la RAM	667 MHz
HD	Tres discos de 146 GB
Procesador	Intel Xeon 5160 de doble núcleo, 3.00 GHz
Cache	4 MB
Ranuras de Expansión	3 PCI Express x8 (velocidad x4) 1 PCI-X 133 MHz de 64 bits 2 PCI-X 100 MHz de 64 bits
Sistema Operativo	Microsoft® Windows® Server 2003/R2 y Centos 4.5

Tabla 4. 3 Características de los servidores. [3]

4.1.3 CLOSET DE TELECOMUNICACIONES

El closet de telecomunicaciones que se va a reutilizar es el que está ubicado en el laboratorio de secundaria es de 19", este elemento cumple con las característica requeridas para instalar los equipos de networking en el laboratorio.

4.2 SISTEMA DE CABLEADO ESTRUCTURADO

Para cableado estructurado en el mercado existe una gran variedad de elementos que se diferencian por el costo dependiendo de la marca y el modelo, generalmente algunos de estos elementos son baratos porque son genéricos. Razón por la cual se acudió a un proveedor mayorista para solicitar una proforma y obtener el costo de los elementos requeridos. En la tabla 4.4 se detalla el costo de forma individual de cada elemento.

ELEMENTO	DESCRIPCIÓN	CANTIDAD (U)	COSTO	
			INDIVIDUAL	TOTAL
Jacks	Cat 5 E	159	5.120	814.08
	Cat 6	30	7.650	229.50
Face Plate	Dobles	79	2.20	173.80
	Simples	8	1.830	14.64
Canaleta Plástica	32X12	18	2.250	40.50
	40X25	16	4.990	79.84
	40X40	12	5.990	71.88
	60X40	6	7.830	46.98
Codo Interno	32X12	6	0.450	2.70
	40X25	16	0.840	13.44
	40X40	16	1.50	24
	60X40	6	2.040	12.24
Codo Externo	32X12	6	0.450	2.70
	40X25	13	0.840	10.92
	40X40	11	1.50	16.5
	60X40	5	2.040	10.20
Codo Plano	32X12	5	0.450	2.25
	40X25	3	0.840	2.52
	40X40	2	1.50	3
	60X40	2	2.040	4.08
Derivación en T	40X25	1	0.840	0.84
	40X40	2	0.80	1.6
	60X40	4	2.190	8.76
Terminación	32X12	18	0.330	5.94
Cable UTP CAT 5E	Bobina de 305 m	9	166.02	1494.18
Cable UTP CAT 6	Bobina de 305 m	2	219.6	439.20
Conduit Metálico 3 m	¾	39	4.990	194.61
	1	13	7.410	96.33
	1 1/4	10	11.850	118.50
Codos Metálicos	¾	39	1.250	48.15
	1	11	2	22

ELEMENTO	DESCRIPCIÓN	CANTIDAD (U)	COSTO	
			INDIVIDUAL	TOTAL
Codos Metálicos	1 1/4	3	2.750	8.25
Cajetines	De paso 20x20	9	9.730	87.57
Patch Cord de 3m	Cat 5E	158	3.36	530.88
Patch Cord de 3m	Cat 6	30	9.91	297.30
Patch Pannel	Cat 6, 24 p	12	30	360
Organizador	Horizontal	13	12.040	156.52
Organizador	Vertical	10	43.450	434.50
Panel de Alimentación	AC	5	31.670	158.35
Closet de Telecomunicaciones	12 U	1	251.50	251.50
	18 U	1	321.460	321.460
Rack abierto	24 U	1	120.740	120.740
SUBTOTAL			**6732.95**	
DESCUENTO 15%			**1009.94**	
I.V.A. 12%			**686.76**	
TOTAL			**6409.77**	

Tabla 4. 4 Costo de los elementos para Cableado Estructurado. [4]

La proforma fue solicitada a la empresa ELECTRO COMERCIAL MEJÍA la cual proporcionó la información de los elementos de las siguientes marcas: DEXON, PANDUIT y FUJI. Los detalles de la misma se encuentran en el **ANEXO G**.

Cabe indicar que la empresa realiza un descuento del 15% en todos sus productos esto es solo para ventas en efectivo.

4.3 EQUIPOS DE NETWORKING

El costo de los equipos de networking es determinante en el diseño de cualquier proyecto esto se debe a que varía de acuerdo a las características técnicas, robustez y marca que tenga el equipo.

Cabe indicar, que en el mercado se tiene una gran variedad de equipos de networking que se diferencian por su funcionalidad y robustez. A más del soporte y garantía que ofrecen los proveedores.

Para la red de datos de la UESMDM se considera equipos pertenecientes a tres fabricantes que son: D-Link, Cisco y HP. D-link debido a que en la red actual se tiene solo dispositivos de esta marca, HP y Cisco porque son marcas que ofrecen confiabilidad, robustez, garantía, entre otras, en sus equipos. Además en el caso de Cisco cuenta con una Academia que instruye a los profesionales para configurar y administrar dichos equipos logrando de ellos un desempeño óptimo.

De acuerdo a lo requerido para los switches de acceso y de core en el numeral 3.12.2 del capítulo 3, se detallan en las tablas 4.5 y 4.6 las 3 opciones con sus respectivas características y costos de cada uno de ellos.

SWITCHES DE ACCESO	
EQUIPO	SF300-24P
MARCA	**CISCO**
IMAGEN	
CARACTERÍSTICAS	
Switching de capa 2	• Protocolo de árbol de expansión (STP) • Agrupación de puertos • VLAN • VLAN de voz • Protocolo genérico del registro de la VLAN (GVRP)/Protocolo genérico del registro de atributos (GARP) • Retransmisor de DHCP (Protocolo de configuración dinámica de host) en capa 2 • Detección del Protocolo de administración de grupos de Internet (IGMP) versiones 1, 2 y 3 • Función de consulta de IGMP • Bloqueo en la cabecera de la línea (HOL)

Capa 3	• Routing IPv4 • Routing entre dominios sin clase (CIDR) • Retransmisor DHCP en la capa 3 • Retransmisor de UDP (Protocolo de datagramas de usuario) • Protocolo Secure Shell (SSH) • Capa de sockets seguros (SSL) • IEEE 802.1X (función de Autenticador) • Perímetro de VLAN privada (PVE) con aislamiento de capa 2 y comunidad VLAN
Seguridad de los puertos	• RADIUS/TACACS+ • Control de tormentas • Prevención de Denegación de servicios (DoS) • Prevención de congestión • ACL • Calidad de servicio (QoS) • Niveles de prioridad • Programación • Clase de servicio • Limitación de tráfico
Estándares	• IEEE 802.3 10BASE-T Ethernet • IEEE 802.3u 100BASE-TX Fast Ethernet • IEEE 802.3ab 1000BASE-T Gigabit Ethernet • IEEE 802.3ad LACP • IEEE 802.3z Gigabit Ethernet • IEEE 802.3x Control de flujo • IEEE 802.1D (STP, GARP y GVRP) • IEEE 802.1Q/p VLAN • IEEE 802.1w RSTP • IEEE 802.1s STP múltiple • IEEE 802.1X Autenticación de acceso a puertos • IEEE 802.3af • IEEE 802.3at
IPv6	• ACL IPv6 • Calidad de servicio de IPv6 • Detección de Multicast Listener Discovery (MLD) • Aplicaciones IPv6 • Web/SSL • servidor Telnet/SSH • Ping • Traceroute • Protocolo simple de tiempo de red (SNTP) • Protocolo trivial de transferencia de archivos (TFTP) • SNMP • RADIUS • Syslog • Cliente DNS • VLAN basadas en protocolos
Administración	• Interfaz de usuario web • SNMP v 1,2,3 • MIB SNMP • Supervisión remota (RMON) • Alimentación por Ethernet (PoE)

GARANTÍA	1 Año
COSTO	***696,93***
EQUIPO	**DES-3526**
MARCA	**D-Link**
IMAGEN	
CARACTERISTICAS	
Interfaces	• 24 puertas 10/100Mbps – Autosensing • 2 puertas 1000Mbps Autosensing tipo Combo • 1 RS-232, Consola
Perfomance	• Velocidad de Backplane 8,8 Gbps • Velocidad de conmutación de paquetes 6.6 Mbps
PoE	• 802.3af and 802.3at
Estándares	• IEEE 802.3u • IEEE 802.3x, Flow Control • IEEE 802.3ab • IEEE 802.3z • ANSI/IEEE 802.3 Nway auto-negotiation
VLAN	• IEEE 802.1Q Tagged VLAN • GARP/GVRP • Asymmetric VLAN • Número de VLANs: 255 (max.) • Port VLAN
QoS	• IEEE 802.1p • 4 colas de prioridades en modo Stack
CLASIFICACIÓN DEL TRÁFICO (COS)	• TOS • Diffserv (DSCP) • Port-based • MAC address • IP address • TCP/UDP port numbe
Access Control List (ACL)	• Port Number • TOS • DiffServ (DSCP) • MAC address • Packet protocol type • TCP/UDP port number (definibles por el usuario) • TCP/UDP payload (definibles por el usuario) • Defición de ACL por puerta
Administración	• SNMP v2c y v3 • RMON monitoring • Telnet server. Máximo 8 sesiones • TACACS+ • RADIUS
GARANTÍA	1 Año
COSTO	***350.00***
EQUIPO	**HP 2520-24**
MARCA	**HP**

IMAGEN	
CARACTERISTICAS	
Interfaces	• 24 RJ-45 autosensing 10/100 PoE ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3af PoE); Media Type: Auto-MDIX; Duplex: half or full • 2 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Media Type: Auto-MDIX; Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only • 2 dual-personality ports; each port can be used as either an RJ-45 10/100/1000 port (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-TX; IEEE 802.3ab 1000Base-T Gigabit Ethernet) or as a SFP slot (for use with SFP transceivers) 1 RJ-45 serial console port
Switching capacity	12.8 Gbps
Standard	• IEEE 802.1D MAC Bridges • IEEE 802.1p Priority • IEEE 802.1Q VLANs • IEEE 802.1s Multiple Spanning Trees • IEEE 802.1w Rapid Reconfiguration of Spanning Tree • IEEE 802.3 Type 10BASE-T • IEEE 802.3ab 1000BASE-T • IEEE 802.3ad Link Aggregation Control Protocol (LACP) • IEEE 802.3af Power over Ethernet • IEEE 802.3x Flow Control
Network management	• IEEE 802.1AB Link Layer Discovery Protocol (LLDP) • RFC 1098 A Simple Network Management Protocol (SNMP) RMON: 1 (statistics), 2 (history), 3 (alarm) and 9 (events) • LLDP Media Endpoint Discovery (LLDP-MED) • SNMPv1/v2c/v3
QoS/CoS	• DiffServ precedence, with 4 queues per port • DiffServ Architecture • DiffServ Assured Forwarding (AF) • DiffServ Expedited Forwarding (EF)
Security	• IEEE 802.1X Port Based Network Access Control • TACACS+ • RADIUS Authentication • RADIUS Accounting • Secure Sockets Layer (SSL)
GARANTÍA	*1 Año*
COSTO	***1.249***

Tabla 4. 5 Características y costo de los Switches de Acceso. [5]

SWITCHES DE CORE	
EQUIPO	Catalyst 3560X 24 Port Data IP Base
MARCA	**CISCO**
IMAGEN	

	
CARACTERÍSTICAS	
Estándares	• IEEE 802.1s • IEEE 802.1w • IEEE 802.1x • IEEE 802.1x-Rev • IEEE 802.3ad • IEEE 802.1ae • IEEE 802.3af • IEEE 802.3at • IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and • 1000BASE-T ports • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS Prioritization • IEEE 802.1Q VLAN • IEEE 802.3 10BASE-T specification • IEEE 802.3u 100BASE-TX specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3z 1000BASE-X specification • RMON I and II standards • SNMPv1, SNMPv2c, and SNMPv3
Capacidad de Switching	160 Gbit/s
Seguridad	• Private VLANs • Private VLAN Edge • Unicast Reverse Path Forwarding (RPF) • Multidomain Authentication • Cisco security VLAN ACLs • Cisco standard and extended IP security router ACLs • Port-based ACLs • Secure Shell (SSH) Protocol, Kerberos, and Simple Network Management Protocol Version 3 • (SNMPv3) • TACACS+ and RADIUS authentication • MAC Address Notification • Multilevel security on console access • Bridge protocol data unit (BPDU) Guard • Spanning Tree Root Guard (STRG) • IGMP filtering • Dynamic VLAN assignment
Disponibilidad	• High availability • High-performance IP routing • Superior QoS • Location awareness and mobility
Switching	160 Gbps
Número de VLANs	1005
GARANTÍA	1 Año
COSTO	***3.475,48***

EQUIPO	DGS-362720 giga, 4 puertos combo,3 uplink 10G
MARCA	D-Link
IMAGEN	
CARACTERISTICAS	
Performance	☐ Velocidad de backplane mínima de 108 Gbps
Características Capa 2	• IGMP Snooping v1, v2, v3 • 1K IGMP Snooping Groups • 64 Static Multicast Address • Spanning Tree • 802.1D STP - 802.1w RSTP • 802.1s MSTP - Loopback Detection v 4.0 • BPDU Filtering per Port and per Device • Trunking Across Stack • RSPAN • 64 Static Multicast Addresses • 802.3ad Link Aggregation • Up to 32 Groups per Device • Up to 8 Gigabit Ports or 2 10-Gigabit Ports per Group • Port Mirroring • Per Flow (ACL) Mode
VLAN	• 802.1Q • Total 4K VLAN Groups • Maximum 255 Dynamic VLAN Groups • GVRP • 802.1v • Maximum 4K Static VLAN Groups • Configurable VLAN ID from 1 to 4094 • Selective Q-in-Q
Características Capa 3	• **L3 Routing** Up to 12K entries (all route entries combined) Up to 256 IPv4 static route entries Up to 128 IPv6 static route entries Up to 12K IPv4 dynamic route entries Up to 6K IPv6 dynamic route entries • **Floating Static Route** IPv4 Floating Static Route IPv6 Floating Static Route • Policy Based Route • RIPng (IPv6)2 • Multiple IP Interfaces per VLAN (Up to 5) • Multi Path Routing Supporting Equal Cost (EC) and Weighted Cost (WC) • VRRP • IPv6 Ready Phase 1 • IGMP v1, v2, v3 • DVMRP v3 • Per Port Limit IP Multicast Address Range for Control Packet • **L3 Forwarding** Up to 8K IPv4 Forwarding Entries

	Up to 4K IPv6 Forwarding Entries Up to 8K Entries (all L3 Hardware Forwarding Entries Combined) • OSPF v2 OSPF Passive Interface OSPF NSSA (Not So Stubby Area) OSPF Equal Cost Route • RIP v1, v2 • Up to 64 IP Interfaces • Multicast Up to 64 Static Multicast Groups Up to 1K Dynamic Multicast Groups Up to 1K Multicast Groups (Static and Dynamic D-Link® Safeguard Engine™ Multicast Groups Combined) • Multicast Duplication (Up to 32 VLAN per Port) • PIM-DM/SM/SDM for IPv4 IPv6 Tunneling
QoS (Quality of Service)	☐ Per Port Bandwidth Control (Granularity of 64Kbits per Second) • Per Flow Bandwidth Control (Granularity of 64Kbits per Second) • 802.1p Priority Queues (8 Queues) Queue Handling Mode Support: WRR and Strict Modes • **CoS Based On:** Switch Port VLAN ID 802.1p Priority Queues MAC Address IPv4/v6 Address DSCP Protocol Type IPv6 Traffic Class IPv6 Flow Label TCP/UDP Port User-Defined Packet Content
ACL (Access Control List)	• Up to 8 Profiles • Up to 1792 Global Rules, Each Rule Can Set Its Own Port Range • **ACL Based On:** Switch Port VLAN ID 802.1p Priority Queues MAC Address IPv4/v6 Address DSCP Protocol Type IPv6 Traffic Class IPv6 Flow Label TCP/UDP Port User Defined Packet Content Time (Time-based ACL)
Security	• RADIUS Authentication for Management Access (RFC 2138, 2139) • SSH v2 • SSL v3 • Web-based Access Control

	• MAC-based Access Control • Traffic Segmentation • D-Link Safeguard Engine • Support Microsoft® Network Access Protection • TACACS+ Authentication for Management Access (RFC 1492) • Port Security (Up to 16 MAC Addresses per Port) • 802.1x Port-based/MAC-based Access Control • Guest VLAN • Broadcast Storm Control (Minimum Granularity of 1 PPS) • IP-MAC-Port Binding (Up to 500 Entries per Device) • Supporting ARP/ACL/DHCP Snooping Modes • DHCP Server Screening
Administración	• Single IP Management v1.6 • CLI • Telnet Server • Telnet Client2 • SNMP v1, v2c, v3 • SNMP Trap on MAC Notification • BootP/DHCP Client • System Log • Trap/Alarm/Log Severity Control • Flash File System • CPU Monitoring via Web, CLI, SNMP • Virtual Interface2 • Web-based GUI • Web GUI Traffic Monitoring • TFTP Client • RMON v1, v2 • sFlow • DHCP Auto-Configuration • DHCP Relay Option 82 • DHCP Server • Dual Image • Dual Configuration LLDP
GARANTÍA	1 Año
COSTO	***4.360***
EQUIPO	***HP E3500-24G***
MARCA	
IMAGEN	
CARACTERISTICAS	
Interfaces	• 20 autosensing 10/100/1000 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T); Media Type: • Auto-MDIX; Duplex: 10Base-T/100Base-TX: half or full; 1000Base-T: full only. • 1 RJ-45 serial console port • 4 dual-personality ports; each port can be used as either an RJ-45 10/100/1000 port (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-TX; IEEE 802.3ab 1000Base-T Gigabit Ethernet) with PoE or an open mini-GBIC slot (for use with mini-GBIC transceivers)

	• Supports a maximum of 4 10-GbE ports
Estándares y protocolos	• IEEE 802.1ad Q-in-Q • IEEE 802.1AX-2008 Link Aggregation • IEEE 802.1D MAC Bridges • IEEE 802.1p Priority • IEEE 802.1Q VLANs • IEEE 802.1s Multiple Spanning Trees • IEEE 802.1v VLAN classification by Protocol andPort • IEEE 802.1w Rapid Reconfiguration of SpanningTree • IEEE 802.3ad Link Aggregation Control Protocol (LACP) • IEEE 802.3af Power over Ethernet • IEEE 802.3x Flow Control • UDP, TFTP Protocol (revision 2), ICMP, TCP, ARP, TELNET, Time Protocol, BOOTP, RIPv1, TFTP Protocol (revision 2), CIDR, BOOTP Extensions (SNTP) v4, DHCP, RIPv2, (MS-RAS-Vendor only), DHCP Relay Agent Information Option, RADIUS (CoA only), VRRP, RADIUS VLAN & Priority y UDLD (Uni-directional Link Detection)
IP multicast	• Draft 2 PIM Dense Mode, Draft 10 PIM Sparse Mode • IGMPv3 (host joins only)
IPv6	• IPv6 Path MTU Discovery, IPv6 Multicast Address Assignments, IPv6 Specification, Transmission of IPv6 over Ethernet Networks, Multicast Listener Discovery (MLD) for IPv6, Definitions of Managed Objects for, Remote Ping, Traceroute, and Lookup Operations (Ping only), MLDv1 MIB, DHCPv6 (client and relay), Default Address Selection for IPv6, IPv6 Global Unicast Address Format, DNS Extension for IPv6, MLDv2 (host joins only), MIB for TCP, MIB for UDP, SSHv6 Architecture, SSHv6 Authentication, SSHv6 Transport Layer, SSHv6 Connection, IP Version 6 Addressing Architecture, MIB for IP, IPv6 Node Requirements, Key Exchange for SSH, ICMPv6, IGMP & MLD Snooping Switch, IPv6 Neighbor Discovery y OSPFv3 for IPv6
MIBs	• MIB II, Bridge MIB, RIPv2 MIB, OSPFv2 MIB, RMONv2 MIB, IP Forwarding Table MIB, SMON MIB, RADIUS Client MIB, RADIUS Accounting MIB, Ethernet-Like-MIB, 802.3 MAU MIB, 802.1p and IEEE 802.1Q Bridge MIB, Entity MIB (Version 2), VRRP MIB y Ping MIB
Network management	• sFlow • IEEE 802.1AB Link Layer Discovery Protocol (LLDP) Four groups of RMON: 1 (statistics), 2 (history), 3 (alarm) and 9 (events) • LLDP Media Endpoint Discovery (LLDP-MED) • SNMPv1/v2c/v3
QoS/CoS	• DiffServ Precedence, including 8 queues/port • DiffServ Assured Forwarding (AF) • DiffServ Expedited Forwarding (EF)
Security	• IEEE 802.1X Port Based Network Access Control • TACACS+ • RADIUS (client only) • RADIUS Accounting • Secure Sockets Layer (SSL) • SSHv1/SSHv2 Secure Shell
GARANTÍA	1 Año
COSTO	***2.699***

Tabla 4. 6 Características y costo de los Switches de Core. [6]

Las marcas de equipos para Access Point que se consideraron son Cisco, D-Link y HP, en la tabla 4.7 se detalla las características de cada equipo con su respectivo costo.

ACCESS POINT	
EQUIPO	**802.11g/n Fixed Auto AP; Int Ant; A Reg Domain**
MARCA	**CISCO**
IMAGEN	
CARACTERÍSTICAS	
Performance con protección inversa	• M-Drive tecnología optimizada RF • Six times faster than 802.11a/g networks • Backward-compatible con clients 802.11a/b/g
Fácil Instalación	• 802.11n performance with switches con PoE • Sleek design blends into a variety of indoor environments
Draft 802.11n Version 2.0 (and Related) Capabilities	• 2x3 multiple-input multiple-output (MIMO) with two spatial streams • Maximal ratio combining (MRC) • Legacy beamforming (hardware supports this capability; not yet enabled in software) • 20- and 40-MHz channels • PHY data rates up to 300 Mbps • Paquetes de agregación: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx) • 802.11 dynamic frequency selection (DFS) (Bin 5) • Cyclic shift diversity (CSD) support
Tasa de datos soportada	802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps 802.11n data rates (2.4 GHz and 5 GHz)
Frecuencia y número de canales	• 2.412 to 2.462 GHz; 11 canales • 5.180 to 5.320 GHz; 8 canales • 5.500 to 5.700 GHz, 8 canales (excludes 5.600 to 5.640 GHz)
Integrated Antenna	• 2.4 GHz, Gain 4.0 dBi, horizontal beamwidth 360° • 5 GHz, Gain 3 dBi, horizontal beamwidth 360°
Interfaces	• 2 puertos 10/100/1000BASE-T autosensing (RJ-45)
IEEE Standard:	• IEEE 802.11a/b/g • IEEE 802.11n draft 2.0 • IEEE 802.11h • IEEE 802.11d
Seguridad	• Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP) • 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA • 802.1X
Protocolos	• DHCP • DNS
EAP Type(s)	• Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) • EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake

	Authentication Protocol Version 2 (MSCHAPv2) • Protected EAP (PEAP) v0 or EAP-MSCHAPv2 • Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) • PEAPv1 or EAP-Generic Token Card (GTC) • EAP-Subscriber Identity Module (SIM)
Multimedia	• Wi-Fi Multimedia (WMM™)
GARANTÍA	1 Año
COSTO	***378,20***
EQUIPO	**DAP-2360**
MARCA	**D-LINK**
IMAGEN	
CARACTERISTICAS	
Estándares	• IEEE 802.11n • IEEE 802.11g • IEEE 802.3ab • IEEE 802.3af • IEEE 802.3u • IEEE 802.3
Administración de Red	• Telnet - Secure (SSH) Telnet • Web Browser interface • HTTP y HTTPS • VLAN • SNMP $v_{1,2,3}$ • D-View Module - Private MIB • AP Administración II • AP Array
Seguridad	• WPA™-Personal • 64/128-bit WEP • WPA-Enterprise • SSID Broadcast Disable • WPA2™-Personal • MAC Address Access Control • WPA2-Enterprise • Rogue AP Detection
VLAN/SSID	802.1q/Multiple SSID support up to 8
Frecuencia	2.4GHz to 2.4835GHz
QoS	4 Priority Queues y WMM Wireless Priority
Modos de operación	• Access Point (AP) • WDS/Bridge • WDS with AP • Wireless Client
GARANTÍA	1 Año
COSTO	***256***
EQUIPO	***HP MSM313 Access Point (WW)***

MARCA	*HP*
IMAGEN	
CARACTERISTICAS	
Interfaces	• 2 RJ-45 auto-sensing 10/100 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX); Duplex: half or full • 1 RJ-11 serial console port
AP operation modes	Autonomous
Wi-Fi Alliance Certification	a/b/g Wi-Fi Certified
Soporta	• 25 simultaneous Guest Access users • Included Services WLAN Management Guest Access Captive Portal • PCI - DSS compliant for wireless PoS traffic • IEEE 802.3af PoE compliant
Frecuencia	2.4GHz to 2.4835GHz
Quality of Service (QoS)	IEEE 802.1p prioritization SpectraLink voice priority (SVP) support
Wireless:	• L2/L3/L4 classification: IEEE 802.1p VLAN priority, SpectraLink SVP, DiffServ, VTP/TCP, and Post • Wi-Fi MultiMedia (WMM), IEEE 802.11e EDCF, and Service-Aware priority assigned by VSC • Maximum VoIP call capacity: 12 active calls on • IEEE 802.11a/b/g
Network management:	• Fully manageable using HP PCM 3.0 AU1 and HP Mobility Manager 3.0 AU2 • SNMP v2c, SNMP v3, MIB-II with Traps, and • RADIUS Authentication Client MIB • Embedded HTML management tool with secure access (SSL and VPN) • Scheduled configuration and firmware upgrades from central server
Rock-solid security:	• IEEE 802.1X/EAP) • Hardware identifiers (MAC address and WEP key), • IEEE 802.11i, WPA/RC4, and/or WEP.
High-performance, multiservice networking:	• Quality of Service (QoS), • Authentication, encryption, bandwidth allocation, • VLANs based on user, device, or application identity. • TOS/DiffServ • IEEE 802.1p, and TCP/UDP port. IEEE 802.11e • Wireless MultiMedia (WMM) and SpectraLink • Voice Priority (SVP) provide voice performance.
GARANTÍA	**1 Año**
COSTO	***999***

Tabla 4. 7 Características y costo de los AP. [7]

4.4 EQUIPOS PARA LA RED DE TELEFONÍA IP

4.4.1 CENTRAL TELEFÓNICA IP

De acuerdo al análisis realizado en el literal 3.6.3.2.6 del capítulo 3 donde se sugirió en el caso de que se decida utilizar una central telefónica comercial basada en Asterisk el equipo Appliance ELX-025 que ofrece la empresa Palosanto Solutions.

En la tabla 4.8 se detalla las características y costos de la central telefónica Appliance ELX-025 de Palosanto Solution.

CENTRALES TELEFONICAS	
EQUIPO	**APPLIANCE ELX -025**
MARCA	***ELASTIX***
IMAGEN	
CARACTERISTICAS	
VoIP PBX	• Grabación de llamadas • Voicemail • IVR configurable y flexible • Soporte para sintetización de voz • Herramienta para crear extensiones por lotes • Cancelador de eco integrado • Provisionador de teléfonos vía Web • Soporte para Video-teléfonos • Interfaz de detección de hardware • Servidor DHCP para asignación dinámica de IPs • Panel de operador basado en Web • Parqueo de llamadas • Reporte de detalle de llamadas (CDRs) • Tarifación con reporte de consumo por destino • Reporte de uso de canales • Soporte para colas de llamadas • Centro de conferencias con salas virtuales • Soporte para protocolos SIP e IAX, entre otros • Codecs soportados: ADPCM, G.711 (A-Law & µ-Law), G.722, • G.723.1 (pass through), G.726, G.729, GSM, entre otros • Soporte para interfaces análogas FXS/FXO • Soporte para interfaces digitales E1/T1/J1 a través de los • protocolos PRI/BRI/R2 • Identificación de llamadas (Caller ID)

	• Troncalización • Rutas entrantes y salientes con configuración • por coincidencia de patrones de marcado • Soporte para follow-me • Soporte para grupos de timbrado
Fax	• Servidor de fax administrable desde Web • Visor de faxes integrado, pudiendo descargarse los • faxes desde el Web en formato PDF • Aplicación fax-a-email • Personalización de faxes-a-email • Control de acceso para clientes de fax • Puede ser integrado con Winprint Hylafax
General	• Ayuda en línea embebida • Disponible en 22 idiomas • Monitor de recursos del sistema • Configurador de parámetros de red • Control de apagado/re-encendido de la • central vía Web • Manejo centralizado de usuarios y perfiles gracias al • soporte de ACLs • Administración centralizada de actualizaciones • Soporte para backup/restore a través del • Web • Soporte para temas o skins • Interfaz para configurar fecha, hora y uso horario de la • central
Email	• Servidor de Email con soporte multidominio • Administración centralizada vía Web • Interfaz de configuración de Relay • Cliente de Email basado en Web • Soporte para cuotas • Soporte Antispam
Mensajería instantánea	• Servidor de mensajería instantánea basado en OpenFire • Cliente de mensajería instantánea Spark • Inicio de llamadas desde Spark • Servidor de mensajería es configurable desde Web • Soporta grupos de usuarios • Soporta conexión a otras redes de mensajería como MSN, • Yahoo Messenger, GTalk, ICQ • Reporte de sesiones de usuarios • Soporta Jabber • Soporta plugins • Soporta LDAP • Soporta conexiones server-to-server para compartir usuarios
	• 8 puertos Analógicos FXO
GARANTÍA	1 Año
COSTO	***1,704.00***

Tabla 4. 8 Características de las centrales telefónicas. [8]

La otra opción fue utilizar un servidor para instalar una IP PBX basada en Asterisk ya que este software no requiere de mayores exigencias de hardware. El software que se sugirió fue Trixbox CE por su fácil instalación y configuración.

Se sugiere en este proyecto utilizar servidores de tipo Rack de las marcas IBM y HP, esto se debe a la gran experiencia que tienen estas dos marcas en soluciones de tipo servidor. Las características de los servidores de acuerdo a lo requerido en el numeral 3.6.3.1.2 del capítulo 3 se detallan en la tabla 4.9.

EQUIPO	IBM	HP
MODELO	**Servidor IBM System x3550**	**HP DL160 G6 E5620 Hot Plug 4LFF 8GB US Svr**
IMAGEN		
CARACTERÍSTICAS	• 1 x Intel Xeon X5680 3.33 GHz - 7944N2U • Supported: 2 Number • Processors Installed: 1 Processor Manufacturer: Intel • Cache: 12 MB 64-bit Processing: Yes Hyper-Threading • Memory: 12 GB Maximum Memory: 192 GB Memory Technology: DDR3 SDRAM Memory Standard: DDR3-1333/PC3-10600 • Number of Total Memory Slots: 18 **Controllers** Controller Type: Serial Attached SCSI (SAS) **I/O Expansions** Expansion Bays: 4 x 2.5" Drive Bay Total Hot-swappable Expansion Slots: • 4 port sGigabit Ethernet • Rack 1U	• Intel Xeon E5620 (2.40 GHz) • 12MB L3 Cache • 8GB (2 x 4GB) RDIMM • HP NC362i Integrated Dual Port Gigabit Server Adapter • HP Smart Array P410 Controller (RAID 0/1/1+0) • 4 LFF Hot Plug drives / 500W high efficiency multi-output supply • Rack (1U) • HP 500GB 3G SATA 7.2K 3.5in MDL HDD • Memoria: 4 MB, 8 MB or 12 MB • Slots de expansión: 2 PCI-Express
GARANTÍA	3 Año	3 años en Piezas
COSTO	**7.999**	***2.110***

Tabla 4. 9 Características de los servidores. [9]

4.4.2 TELÉFONOS IP

Para la elección de los teléfonos IP se tomará en cuenta las especificaciones requeridas en el numeral 3.12.2 del capítulo 3. Además, se considerará 3 tipos de marcas las cuales son: Cisco Panasonic y YeaLink esto es debido a la gran difusión que existe en el mercado y a su experiencia tecnológica que tienen estas marcas.

En la tabla 4.10 se detallan las características de los teléfonos IP considerados como una alternativa para este proyecto.

TELÉFONOS IP	
EQUIPO	**SPA504G Cisco**
MARCA	**CISCO**
IMAGEN	
CARACTERÍSTICAS	
Principales	• 4 interfaces 10/100 Mbps • Soporta PoE y puerto PC • Speakerphone • Call hold • Call waiting • ID de llamada con nombre y número • Transferencia de llamadas • Video conferencia de llamada de tres formas con mezcla local • On-hook dialing • Call blocking: anonymous and selective • Directorio personal • Multiples ring tones • NAT • DNS SRV • 802.3af-compliant PoE • HTTPS with factory-installed client certificate • Secure Real-Time Transport Protocol (SRTP) • DHCP • Soporta QoS • Algoritmos de voz • G.711 (A-law and μ -law) • G.726 (16/24/32/40 kbps) • G.729 A • G.722

	• Real-Time Transport Protocol (RTP) • HTTP digest: encrypted authentication via MD5 (RFC 1321) • Up to 256-bit Advanced Encryption Standard (AES) encryption • SIP over Transport Layer Security (TLS) • VLAN tagging 802.1p/Q
GARANTÍA	1 Año
COSTO	***201,25***
EQUIPO	**KX-NT321**
MARCA	**PANASONIC**
IMAGEN	
CARACTERISTICAS	
	• Automatic Rerouting to Secondary PBX • Voice Encryption • 1-Line LCD Display • NAVI Key Operation • 8 Programmable Keys • Speakerphone • 2 Ethernet Ports (100Base-T) • SIP v2 • Power Over Ethernet (PoE) • Headset Jack • Available in White or Black • Conecciones per-to-per • VLAN • QoS • Cliente DHCP • CODEC(G.722) • TDA Compatibility • Seguridad VoIP • Programación Local
CODEC	G.729A,G.711 y G.722
GARANTÍA	1 año
COSTO	***145***
EQUIPO	***SIP-T22P***
MARCA	***YEALINK***
IMAGEN	
CARACTERISTICAS	
	3 lineas,PoE, BLF, HD, 132x64 LCD, 2 LAN y 3 keys
Códecs y Voz	• Wideband codec: G.722 • Narrowband codec: G.711µ/A, G.723.1 • G.726, G.729AB • VAD, CNG, AEC, PLC, AJB, AGC • Full-duplex speakerphone with AEC
Network	• SIP v1 (RFC2543), v2

	• DNS SRV • Redundant server support • NAT Traversal: STUN mode • DTMF: In-Band, RFC2833, SIP Info • Proxy mode and peer-to-peer SIP link mode • IP Assignment: Static/DHCP/PPPoE • Bridge/router mode for PC port • TFTP/DHCP/PPPoE client • Telnet/HTTP/HTTPS server • DNS client, NAT/DHCP server • Logout
Administración	• Auto-provision via FTP/TFTP/HTTP/HTTPS • Auto-provision with PnP • SNMP V1/2 optional, TR069 optional • Configuration: browser/phone/auto-provision • Factory configuration customized • Trace package and system log export
Seguridad	• 802.1x, VLAN QoS (802.1pq) • Transport Layer Security (TLS) • HTTPS (server/client), SRTP (RFC3711) • Digest authentication using MD5/MD5-sess • Secure configuration file via AES encryption • Phone lock for personal privacy protection • Admin/VAR/User 3-level configuration mode
GARANTÍA	***1 Año***
COSTO	***172.50***

Tabla 4. 10 Características de los teléfonos IP. [10]

4.5 EQUIPOS PARA VIDEO VIGILANCIA IP

Para la elección de las cámaras IP se tomará en cuenta las especificaciones requeridas en el numeral 3.12.2 del capítulo 3. Además, se considerará 3 tipos de marcas las cuales son: KD, D-Link y Panasonic esto es debido a la gran difusión que existe en el mercado y a su experiencia tecnológica que tienen estas marcas.

CAMARAS IP	
EQUIPO	**KD-DD61RC30-PT-W**
MARCA	**KD**
IMAGEN	
CARACTERISTICAS	
Soporta	802.11b/g Frecuencia 2.4GHZ

	Distancia maxíma 100 metros WEP,WPA y WPA2
Network Interface	Self-adaption 10/100Mbps RJ45 port
Iluminación	0.4Lux
Sensor de imagen	1/4 OV CMOS
Compresión	H.264 y MJPEG
PAN/ TILT	Ángulo Horizontal de0º---355º Angulo vertical de 0º—90º
Definición de Video	VGA:640*480,1-30f/s QVGA:320*240,1-30f/s QQVGA:160*128,1-30f/s
Video Frame Rate	PAL: 1-25fps NTSC:1-30fps
Video Bit rate	32Kbps--16Mbps
Compresión de Audio	G.726 , 32K bits
Interfaz	Self-adaption 10/100Mbps RJ45 port 1 channel RS485
Protocolos de Red	TCP/IP, UDP, RTP, RTSP, RTCP, HTTP, DNS, DDNS, DHCP, FTP, NTP PPPOE, FTP, SMTP y UPNP
Funcionalidad	Dia / Noche, res. 704 x 480
GARANTÍA	1 Año
COSTO	***372.00***
EQUIPO	**DCS-5610**
MARCA	**D-LINK**
IMAGEN	
CARACTERISTICAS	
Principales	• Sony VGA Progressive ¼" CCD Sensor • 2.6x Optical Zoom • 4x Digital Zoom • Power over Ethernet (PoE) • Lux Sensitivity for Low-Light Recording • SIP 2-Way Audio • Motion Detection Recording • Samba Client Built-in for Network Attached Storage (NAS) Devices • 3GPP Mobile Surveillance1 • Real-time MPEG-4 and Motion JPEG (MJPEG) Compression with VGA/QVGA/QQVGA Resolution
Algoritmos de Video	• JPEG for Still Image • MPEG-4/MJPEG Simultaneous Dual Format Compression • 3G Video Support1
Resolución	• Up to 30fps at 640x480 • Up to 30fps at 320x240 • Up to 30fps at 176x144
Administración Remota	• Vía Web browser • D-ViewCam™ 2.0
Conectividad	10/100BASE-T
Protocolos	• 802.3af PoE • IPv4, ARP, TCP, UDP, ICMP

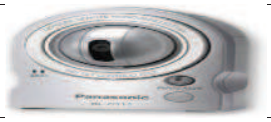
	• DHCP Client • NTP Client • DNS Client • DDNS Client • SMTP Client • FTP Client • HTTP Server • Samba Client • PPPoE • UPnP Port Forwarding • RTP • RTSP • RTCP • IP Filtering • 3GPP
GARANTÍA	1 Año
COSTO	***795***
EQUIPO	***BL-C111A Network Camera Wired***
MARCA	**PANASONIC**
IMAGEN	
CARACTERISTICAS	
Compresión	JPEG (Motion JPEG), MPEG-4
Resolución	640 x 480, 320 x 240 (default), 192 x 144
Calidad de imagen	JPEG (favor clarity, standard, favor motion), MPEG4
Frame rate	Max. 30 frames/sec (640 x 480*3, 320 x 240 or 192 x 144)
Seguridad	User ID/password
Protocolos que soporta	• IPv4 / IPv6 Dual-Stack • TCP, UDP, IP, HTTP, FTP, SMTP, DHCP, DNS, ARP, ICMP, POP3, NTP, UPnPTM, SMTP Authentication, RTP, RTSP, RTCP, IPv6: TCP, UDP, IP, HTTP, FTP, SMTP, DNS, ICMPv6, POP3, NDP, NTP, RTP, RTSP, RTCP
Buffered images	• Approx. 250 images (320 x 240) • Standard image quality •with time display
Zoom	10x digital zoom (by area)
Viewing angle	• 49° horizontal(total 149°) • 37° vertical(total 87°)
Sensor type	1/6 inch CMOS sensor, approx. 320,000 pixels
Network interface	10Base-T/100Base-TX
GARANTÍA	1 Año
COSTO	***279***

Tabla 4. 11 Características de las cámaras IP. [11]

4.6 EQUIPOS SELECCIONADOS

El objetivo de este literal es comparar los equipos ofertados por los diferentes distribuidores y seleccionar la mejor alternativa de acuerdo a sus características técnicas y el costo.

4.6.1 COMPARACIÓN DE LOS SWITCHES DE ACCESO

En la tabla 4.12 se compara los Switches de Acceso de acuerdo a los requerimientos básicos que deben cumplir los equipos.

MARCA	CISCO	D-LINK	HP
MODELO CARACTERISTICAS REQUERIDAS	SF300-24P 24-port 10/100 PoE Managed Switch w/Gig Uplinks	DES-3526	HP 2520-24-PoE Switch
24 puertos *de* 10/100 Mbps full dúplex	✓	✓	✓
2 puertos Uplink *de* 10/100 /1000 Mbps full dúplex	✓	✓	✓
Auto negociación de la velocidad de los puertos	✓	✓	✓
Apilable	✓	✓	✓
Administrable mediante consola o vía interfaz Web	✓	✓	✓
Conmutación a nivel de capa 2	✓	✓	✓
Debe soportar el protocolos IP, STP, DHCP, Telnet y SNMP V1, V2 y V3 (opcional)	✓	✓	✓
Soporte de VLANs IEEE 802.1q	✓	✓	✓
Debe soportar el estándar de seguridad IEEE 802.1X, listas de control de acceso (ACL), prevención mediante (DoS) y filtrado basado en MAC.	✓	✓	✓
Soportar calidad de servicio (QoS) en base a IEEE 802.1p e IEEE802.1q.	✓	✓	✓
Velocidad de backplane mínima de 8.8 Gbps	✓	✓	✓
IP versión 4 y 6	✓	✓	✓

Soporte de 8000 direcciones MAC	✓	✓	✓
Soporte de paquetes de telefonía IP (VoIP)	✓	✓	✓
Garantía	1 Año	1 Año	1 Año
Costo	***696.93***	***350.00***	***1.249***

Tabla 4. 12 Comparación de los Switches de Acceso. [12]

Los switches de acceso a utilizar en la Institución son los de D-linl por su precio con relación a las otras marcas con las que se comparo y porque cumple con todas las caracteristicas requeridas.

4.6.2 COMPARACIÓN DE LOS SWITCHES DE CORE

En la tabla 4.13 se compara los Switches de Core de acuerdo a los requerimientos básicos que deben cumplir los equipos.

MARCA	**CISCO**	**D-LINK**	**HP**
MODELO **CARACTERISTICAS REQUERIDAS**	**SCatalyst 3560X 24 Port Data IP Base**	**DGS-3120-24PC20 giga 4puerto combo**	**E3500-24G**
24 puertos de 10/100/1000 Mbps full dúplex	✓	✓	✓
Auto negociación de la velocidad de los puertos	✓	✓	✓
Apilable	✓	✓	✓
Administrable mediante consola o vía interfaz Web	✓	✓	✓
Conmutación a nivel de capa 2,3 y 4	✓	✓	✓
Debe soportar el protocolos IP, STP, RSTP, RIPv1 y 2, DHCP, Telnet y SNMPV (1, 2 y 3), OSPFV (2 y 3), RMONV (2 y 3) entre Otros.	✓	✓	✓
Manejo y Administración de VLANs IEEE 802.1q	✓	✓	✓
Debe soportar el estándar de seguridad IEEE 802.1X, listas de control de acceso (ACL) a nivel 2,3 y 4, prevención mediante (DoS) y filtrado basado en MAC.	✓	✓	✓
Soportar calidad de servicio (QoS) en base a IEEE 802.1p e IEEE802.1q.	✓	✓	✓
Velocidad de backplane mínima de 88	✓	✓	✓

Gbps			
IP versión 4 y 6	✓	✓	✓
Manejo, priorización y clasificación de tráfico VoIP	✓	✓	✓
Garantía	1 Año	1 Año	1 Año
Costo	***3.475,48***	***4.360***	***2.699***

Tabla 4. 13 Comparación de los Switches de Core. [13]

Los 3 tipos de switches seleccionados cumplen con las características básicas requeridas en el capítulo 3: sin embargo se opto por la línea de Cisco por su robustez, soporte técnico ofrecido, tiempo de respuesta en caso de falla durante la garantía y porque la mayoría de profesionales están instruidos sobre esta marca lo que garantiza una buena configuración de los equipos, lo que es importante para optimizar el rendimiento de los mismos.

4.6.3 COMPARACIÓN DE LOS ACCESS POINT

En la tabla 4.14 se compara los AP de acuerdo a los requerimientos básicos que deben cumplir los equipos.

MARCA	**CISCO**	**D-LINK**	**HP**
MODELO **CARACTERISTICAS REQUERIDAS**	**802.11g/n Fixed Auto AP; Int Ant; A Reg Domain**	**DAP-2360**	**MSM313 Access Point (WW)**
Tasa de transmisión de 54 Mbps	✓	✓	✓
Protocolo de gestión: SNMP (v1, v2, v3) (Opcional)	✓	✓	✓
IEEE 802.3af	✓	✓	✓
Algoritmo de cifrado DES y AES	✓	✓	✓
Filtrado MAC	✓	✓	✓
Soporte estándares: IEEE 802.11g, IEEE 802.11e, IEEE 802.11q y IEEE 802.11x	✓	✓	✓
1 interfaz Fast Ethernet	✓	✓	✓
Configuración de SSID	✓	✓	✓
Soporte de VLANs	✓	✓	✓
Certificación Wi-Fi	✓	✓	✓
Garantía	1 Año	1 Año	1 Año
Costo	***378.20***	***256***	***999***

Tabla 4. 14 Comparación de los AP. [14]

Los 3 equipos comparados cumplen con las características requeridas por la Institución: sin embargo, el equipo seleccionado es el ofrecido por D-Link por su precio.

4.6.4 COMPARACIÓN DE LOS TELÉFONOS IP

En la tabla 4.15 se realiza la comparación de los equipos seleccionados para telefonía IP de acuerdo a los requerimientos básicos en el diseño de la red.

MARCA	CISCO	PANASONIC	YEALINK
MODELO	SPA504G Cisco	KX-NT321	*SIP-T22P*
CARACTERISTICAS REQUERIDAS			
2 Interfaces RJ45	✓	✓	✓
PoE support (802.3af)	✓	✓	✓
Soportar el protocolo SIP	✓	✓	✓
Soporte de códecs G.729	✓	✓	✓
Soporte DHCP	✓	✓	✓
QoS (802.1p)	✓	✓	✓
Compatibilidad con protocolos de administración	✓	✓	✓
Soporte de VLANs	✓	✓	✓
Calidad de voz	✓	✓	✓
Identificador de llamadas	✓	✓	✓
Llamada en espera	✓	✓	✓
Transferencia de llamadas	✓	✓	✓
Seguridad	✓	✓	✓
Garantía	1 Año	1 Año	1 Año
Costo	***201,25***	***145***	***172.50***

Tabla 4. 15 Comparación de los Teléfonos IP. [15]

Los tres equipos cumplen con lo requerido en la tabla 3.10.2 del capítulo 3: sin embargo los equipos de ofrece Cisco y YeaLink tienen mejores características.

En este diseño se utilizará los equipos que de Palosanto Solution que son de marca YeaLink por razones tales como:

- Son equipos diseñados especialmente para trabajar con centrales telefónicas basadas en Asterisk.
- Son administrables mediante el protocolo SNMP $v_{1,2}$
- Cuentan con un teléfono IP diseñado para que trabaje como operador que es el YEALINK-T28P
- Tiene excelentes características y es de menor costo que los de Cisco
- Ofrecen seguridad mediante autenticación y encripción

4.6.5 COMPARACIÓN DE LAS CÁMARAS IP

En la tabla 4.16 se comparan las cámaras IP de acuerdo a los requerimientos básicos que deben cumplir estos equipos.

MARCA	KD	D-LINK	PANASONIC
MODELO CARACTERISTICAS REQUERIDAS	KD-DD61RC30-PT-W	DCS-5610	BL-C111A Network Camera Wired
Un puerto 10/100 Fast Ethernet	✓	✓	✓
Protocolos TCP/IP, ARP, ICMP, HTTP, TELNET, SNMP Y DHCP	✓	✓	✓
Movimiento horizontal de cobertura 90°	✓	✓	✓
Detección de movimiento tanto de día como de noche (VMD)	✓	✓	✓
Formato de compresión MPEG-4 ó H.264	✓	✓	✓
Resolución de 640X480 pixeles ó superior	✓	✓	✓
Autenticación de usuario.	✓	✓	✓
Deberán soportar PoE norma IEEE 802.3af	✓	✓	✓
Administrables	✓	✓	✓
Garantía	1 Año	1 Año	1 Año
Costo	***372***	***795***	***279***

Tabla 4. 16 Comparación de las cámaras IP. [16]

Los 3 equipos cumplen con las características requeridas: sin embargo por tener la capacidad de grabar en la noche se selecciona la cámara **KD-DD61RC30-PT-W**

4.6.6 FIREWALL PARA SEGURIDAD PERIMETRAL

Los UTM considerados son: DFL-1660 y Astaro 320, sus características se detallan en la tabla 4.17.

MODELO	**DFL-860E-NB**
MARCA	**D-LINK**
IMAGEN	
CARACTERISTICAS	• Firewall Throughput: 150Mbps • VPN Performance: 50Mbps (3DES/AES) • 2 10/100 Ethernet WAN Ports • 7 10/100 Ethernet LAN Ports • 1 10/100 Ethernet DMZ Port
Integrated Firewall/VPN Appliance	• Powerful Firewall Engine • Virtual Private Network (VPN) Security • Granular Bandwidth Management • 802.1Q VLAN Tagging • 3 Proactive End-Point Security With D-Link ZoneDefense
Advanced Firewall Functions	• Stateful Packet Inspection (SPI) • Detect/Drop Intruding Packets • Server Load Balancing • Policy-Based Routing • Robust Application Security for ALGs
Unified Threat Management	• Intrusion Prevention System (IPS) • Anti-Virus (AV) Protection • Web Content Filtering (WCF) • Optional Service Subscriptions
Virtual Private Network (VPN)	• IPSec NAT Traversal • VPN Hub and Spoke • IPSec, PPTP, L2TP • DES, 3DES, AES, Twofish, Blowfish, CAST-128 Encryption • Automated Key Management via IKE/ISAKMP • Aggressive/Main/Quick Negotiation
Performance Optimization	• Hardware-Based UTM Acceleration • 2 Multiple WAN Interfaces for Traffic Load Sharing
Enhanced Network Services	• DHCP Server/Client/Relay • IGMP V3 • H.323 NAT Traversal

	• SIP ALG • OSPF Dynamic Routing Protocol • Run-Time Web-Based Authentication
Certificaciones	• ICSA Labs Certified IPSec y Firewall Corporate • VPNC Certified AES y Basic Interop
Garantía	1 Año
Costo	***1.015***
MODELO	**Astaro ASG 320 Full Guard Bundle**
MARCA	***ASTARO***
IMAGEN	
CARACTERISITCAS	
Aplicaciones de seguridad	• Essential Firewall • Network Security • Mail Security • Web Security • Web Application Security • Wireless Security
Capacidad	
	• Número máximo de usuarios con licencia **sin restricciones** • Número máximo de usuarios recomendados (FW/UTM) **800/200** • Rendimiento del cortafuegos **3.4 Gbps** • Rendimiento del IPS **1000 Mbps** • Rendimiento de la VPN **560 Mbps** • Rendimiento del UTM **165 Mbps** • Rendimiento de RED **120 Mbps** • Rendimiento del correo electrónico (analizado/observado) **78.000/600.000 correos electrónicos/h** • Conexiones simultáneas **600.000** • Unidad de disco duro para archivos de registro y de cuarentena locales **160 GB**
Interfaces físicas	• Interfaces Ethernet 8 x Gigabit Ethernet • Puertos de E/S 2 x USB, 1 x COM (RJ45), 1 x VGA
Certificaciones	• CE, FCC Clase A, CB, VCCI, C-Tick, UL • ICSA Labs probó y renovó la Certificación de Firewall Certification para la versión actual de Astaro Security Gateway.
Garantía	1 Año
Costo Total	**3.345**

Tabla 4. 17 Equipos Appliance UTM. [17]

Para equipo perimetral se utilizará un UTM DFL-860E-NB por sus características técnicas y por su precio.

La suscripción de los servicios deben ser pagados anualmente por la Institución para mantener la defensa completa durante todo el tiempo: sin embargo se deja a criterio del administrador de la red si, continúa pagando dichas suscripciones o utiliza otros métodos para mantener estos servicios.

4.6.7 EQUIPOS SELECIONADOS

Los equipos seleccionados se detallan en la tabla 4.18 y sus características técnicas se especifican en el **ANEXO H**.

EQUIPO	MARCA	MODELO
Switch de Core	Cisco	Catalyst 3560X 24 Port Data IP Base
Switch de Acceso	D-Link	DES-3526
Access Point (AP)	D-Link	DAP-2360
Servidor	HP	DL160 G6 E5620 Hot Plug 4LFF 8GB US Svr
Central Telefónica	Elastix	Appliance ELX-025
Teléfonos IP	YEALINK	SIP-T22P
Cámaras IP	KD	KD-DD61RC30-PT-W
Firewall	D-Link	DFL -1660

Tabla 4. 18 Equipos Seleccionado. [18]

4.7 ANTIVIRUS

Kaspersky es una solución de seguridad TI de clase mundial que ofrece un nuevo nivel de protección contra malware y otras amenazas. Manteniendo la información intacta, e incremente su productividad con menos esfuerzo y tiempo administrativo. Su diseño por capas permite cubrir cualquier tipo de dispositivo de red de una forma flexible a los requerimientos del cliente. Todo el tráfico entrante y saliente de estaciones de trabajo, teléfonos inteligentes, servidores y gateways, puede ser revisado contra contenido malicioso. Las soluciones de Kaspersky proveen lo último en rendimiento confiable y efectivo, con implementación sencilla, interfaz amigable y herramientas administrativas eficientes, para que las

instituciones educativas puedan obtener los mejores resultados en protección antimalware.

ANTIVIRUS	No. DE LICENCIAS	SERVICIOS INCLUIDOS	COSTO UNITARIO	COSTO TOTAL
Kaspersky Enterprise Space Security.	140	• Exploración de Antivirus para contenido del disco • Protección por ataques desde la red • Protección proactiva sobre las aplicaciones de Microsoft Office • Antihacker • Antispam para cada máquina • Antispyware • Intercepción de virus de escritura • Actualización permanente y automática de firmas de virus (hasta 3 veces al día) • 1 Consola de administración centralizada para equipos dentro de la red • Soporte técnico 24x7x365	19.75	***2.765***

Tabla 4. 19 Características del Antivirus Kaspersky. [19]

4.8 COSTO DE OPERACIÓN

Para un correcto funcionamiento de la red se debe considerar los costos de operación y de mantenimiento que se estiman en la tabla 4.20

SERVICIO	DESCRIPCION	COSTO (USD)
Internet	***Paquete Office Pack 2000*** • Compartición 2:1 • Velocidad Kbps Down = 2048 Up = 2048 • 15 cuentas de correo electrónico de 250 MB • 1 dirección IP pública dinámica (default) • Disponibilidad del servicio 99,5%	199,00 Mensuales
Administrador	Sueldo estimado por recursos humanos de la Institución para ocupar el cargo de administrador de la red trabajando 8 horas con todos los beneficios de ley	600
TOTAL MENSUAL		***799.00***

Tabla 4. 20 Costos de Operación (Mensual). [20]

4.9 COSTO TOTAL DEL PROYECTO REUTILIZANDO EQUIPOS

Si se desea reutilizar equipos en la nueva red, los únicos que cumplirían con los requerimientos mínimos son:

- 2 switches de acceso
- 1 router Inalámbrico
- 2 Servidores
- 2 closet de telecomunicaciones

A continuación se presenta el costo total para la implementación de la red en la parte activa y pasiva.

ITEM	COSTO (USD)
Cableado Estructurado	5.640,56
Equipos de Conectividad	6.275,48
Firewall	1.015
Telefonía IP	4.291.50
Video Vigilancia IP	2.976
Red Inalámbrica	512
Antivirus	2.765
SUB TOTAL	23.475,56
IVA 12%	2.817,06
TOTAL	26.292,60

Tabla 4. 21 Costo Total de la red UESMDM reutilizando equipos. [21]

4.10 COSTO TOTAL DEL PROYECTO SIN REUTILIZAR EQUIPOS EXISTENTES

Costo total adquiriendo todos los equipos, lo que es lo recomendado para un óptimo desempeño de la red de la UESMDM.

ITEM	COSTO (USD)
Cableado Estructurado	5.640,56
Equipos de Conectividad	6.975,48
Firewall	1.015
Servidores	4.220
Telefonía IP	4.291.50
Video Vigilancia IP	2.976
Red Inalámbrica	768
Antivirus	2.765
SUB TOTAL	28.651,54
IVA 12%	3.438,18
TOTAL	32.089.72

Tabla 4. 22 Costo Total de la red UESMDM sin reutilizar equipos. [22]

Los precios de los equipos de Networking Antivirus y Firewall se encuentran en las proformas que se detallan en el **ANEXO I**

CAPÍTULO 5

CONCLUSIONES

Y

RECOMENDACIONES

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

El análisis realizado a la red actual de la UESMDM, permitió conocer el desempeño y debilidades que tiene. Con el objetivo de optimizar e incrementar los servicios y recursos que esta provee. Dichas debilidades son falta de: políticas de seguridad, administración e infraestructura de cableado estructutado.

El rediseño establecido provee redundancia a nivel de cableado vertical, esto evitará que los recursos de red se vean afectados si un enlace se daña.

En lo concerniente a redes privadas que es caso de la red de la Institución, cuentan con dos infraestructuras: Una para voz y otra para datos. La nueva perspectiva apunta a que converjan en una sola disminuyendo costos y operación.

Actualmente la migración a telefonía IP se basa a lo económico, por la disminución de costos en llamadas internacionales, menor gasto en líneas telefónicas, flexibilidad de instalar nuevas extensiones sin necesidad de realizar una nueva instalación de cableado y adquirir nuevos teléfonos, debido a que se puede ínstalar un teléfono basado en software utilizando la misma infraestructura de red.

Acceder a los servicios que brinda la red de la Institución de forma inalámbrica brinda la posibilidad de que los profesores, estudiantes y personal administrativo puedan utilizar equipos personales para realizar normalmente sus actividades. Además, permite el acceso en lugares que no justifican la implementación de una red cableada o son de difícil acceso.

Implementar los servicios básicos de la red tales como correo, impresión, DNS, DHCP, Proxy entre otros, da la posibilidad de tener una plataforma adecuada para una implementación de servicios integrados en el futuro. Para el caso en particular de una Institución educativa los nuevos servicios pueden ser aulas virtuales, consultas en línea entre otros, permitiéndole a la Institución aprovechar al máximo el desarrollo tecnológico en el proceso educativo.

Contar con políticas de seguridad que permitan un buen desempeño y administración de la red de la Institución es uno de los objetivos de este proyecto, por ende se han creado políticas que restrinjan el acceso físico al personal no autorizado llevando un registro de ingreso a la sala de equipos, dicho registro debe contener hora, motivo de ingreso y firma de autorización. Para restringir el acceso de forma lógica a la red de los diferentes departamentso se crarán redes virtuales.

Debido a la inseguridad informática que existe es necesario utilizar equipos UTM que brinden seguridad perimetral para mantener la red segura de ataques internos y externos.

La nueva red contará con el servicio de video vigilancia IP para monitorear algunos sitios críticos donde se tiene equipos de alto costo a más de información crítica de la UESMDM. Además, la administración se la realizará de forma

centralizada en la cual solo el personal autorizado podrá acceder, modificar y eliminar las grabaciones guardadas en el servidor de video.

La tecnología seleccionada para este proyecto fue la propuesta por Cisco (nivel de core) por su robustez y alto desempeño que tienen los equipos y D-Link a nivel de acceso porque fue la propuesta más viable desde el punto de vista técnico y económico.

La configuración de un servidor DNS es fácil sin embargo se debe ser cauteloso al incrementar código en los archivos de configuración porque conforme puede ser muy útil para repartir dominios también puede convertirse en un caos para la red.

Las soluciones de software libre utilizadas como centrales telefónicas, en este caso en concreto Trixbox, son cada vez más populares y más usadas por su fácil configuración y gran variedad de servicios que ofrecen.

5.2 RECOMENDACIONES

Dadas las nuevas características de la red se recomienda contratar un profesional para el área de sistemas, el cual estará encargado de realizar la implementación, mantenimiento, gestión y administración de la red.

Dicho profesional debe capacitar a los usuarios sobre las políticas de seguridad que se van a implementar en la institución para un correcto uso de los recursos y aplicaciones optimizando el funcionamiento de la red. Además, debe indicar a los trabajadores que ellos son los encargados de los equipos que la institución les proporciona y que deben considerar que la implementación de esta nueva tecnología e infraestructura existe un gran gasto económico por lo que tienen la responsabilidad del buen uso de los equipo.

Es importante que la persona encargada de administrar la central telefónica IP tenga conocimientos sobre el software libre, de telefonía IP. También, de tener un buen nivel de conocimiento del sistema operativo Linux para que realice el mantenimiento a los servidores.

Para este proyecto se recomienda adquirir una central telefónica IP basada en Asterisk como por ejemplo Elastix o Trixbox CE porque no necesitan licencia además, son fáciles de configurar y prestan los mismos o mejores servicios que una central propietaria.

Se recomienda llevar un registro con hora, fecha y el motivo de ingreso al personal que accede al cuarto de equipos, esto es necesario para saber las modificaciones que se realizan en la red.

Se recomienda que todos los puertos de red que no están siendo utilizados sean bloqueados y si un usuario requiere utilizar dicho puerto debe presentar un documento firmado por la rectora de la institución indicando el motivo por el cual requiere conectarse a dicho puerto.

Se recomienda realizar un mantenimiento anual tanto de hardware como de software de los siguientes equipos: servidores, estaciones de trabajo, teléfonos IP, cámaras IP y equipos de Networking, dicho mantenimiento estará a cargo del personal de sistemas. Esto es necesario para aumentar el tiempo de vida útil de los dispositivos y así recuperar la inversión que tiene este proyecto.

Tomando en cuenta que Elastix tiene incorporado una opción para realizar el monitoreo de llamadas, el personal encargado debe realizar un informe mensual de todas las llamadas realizadas y recibidas, esto es necesario para determinar los usuarios que generan mayor tráfico y ver cuál es la hora pico.

Para la red inalámbrica, se recomienda realizar pruebas con los equipos activos para una mejor cobertura y recepción de la señal en los principales sitios donde se requiere el servicio. Además, considerar la ubicación adecuada de los dispositivos donde cuenten con seguridad física.

Se recomienda adquirir un UPS para los closets de telecomunicaciones y la sala de equipos debido a que en estos sitios se encuentran los equipos más sensibles y caros de la red.

REFERENCIAS BIBILIOGRÁFICAS

LIBROS

[LB1] **STALLINGS**, William, "Comunicaciones y Redes de Computadores", 6ª edición, Prentice Hall, 2000.

[LB2] **TANEMBAUM**, Andrew, "Comunicaciones y Redes de Computadoras", Tercera edición. Prentice Hall, 1998.

[LB3] **MEGGELEN**, Jim Van, **SMITH**, Jared, "Asterisk, The future of telephony", o'Reilly. 2005.

FOLLETOS

[FT1] **HIDALGO**, Pablo, "Redes de Área Local", ESCUELA POLITÉCNICA NACIONAL, Marzo 2008

[FT2] **HIDALGO**, Pablo, "Redes TCP/IP", ESCUELA POLITÉCNICA NACIONAL, Marzo 2008

[FT3] **SINCHE**, Soraya, "Cableado Estructurado", ESCUELA POLITÉCNICA NACIONAL 2008

[FT4] **GONZALEZ**, Fabio, "Sistema de Cableado Estructurado", ESCUELA POLITÉCNICA NACIONAL, 2009

[FT5] **BERNAL,** Iván, "Comunicaciones Inalámbricas", ESCUELA POLITÉCNICA NACIONAL, 2009

[FT6] **JIMÉNEZ**, Soledad, "Teoría de Comunicaciones", ESCUELA POLITÉCNICA NACIONAL, 2009

[FT7] Agenda de la Unidad Educativa Santa María Mazzarello, 2011

[FT8] Informe 2010, sobre los equipos que están en red, 2010

[FT9] **FREEMAN**, Roger, "Ingeniería de sistemas de Telecomunicaciones"

DIRECIONES WEB

[PW1] “Red de Computadoras”

URL: http://es.wikipedia.org/wiki/Red_de_computadoras

[PW2] “Modelo de Referencia OSI y TCP/IP”

URL: http://www.ie.itcr.ac.cr/marin/mpc/redes/Modelo_osi_tcp_ip(oficial).pdf

[PW3] “Introducción IP v4”

URL: http://www.albertnogues.com/attachments/014_IntroIp.pdf

[PW4] “IPv4”

URL:http://www.ie.itcr.ac.cr/marin/telematica/.../Direccionamiento%20IP2.pdf

[PW5] “Tecnología 1000BASE-T”

URL: http://es.wikipedia.org/wiki/1000BASE-T

[PW6] “Tecnología 1000BASE-X”

URL: http://es.wikipedia.org/wiki/1000BASE-X

[PW7] “Seguridad en Redes Inalámbricas”

URL: http://www.seguridadwireless.net/hwagm/wpa.html

[PW8] “Protocolos de señalización”

URL: http://www.it.uc3m.es/~jmoreno/articulos/protocolssenalizacion.pdf

[PW9] “Protocolos VoIP”

URL:http://www.idris.com.ar/pdf/ART0002%20%20Protocolos%20en%20VoIP.pdf

[PW10] “Protocolo H.323”

URL: ftp://neutron.ing.ucv.ve/pub/Seminarios/.../H.323.ppt

[PW11] “Protocolo H.323 vs SIP”

URL:http://www.grc.upv.es/docencia/.../Abel_H.323%20vs%20SIP%20(1).pdf

[PW12] “Ntop”

URL: http://es.wikipedia.org/wiki/Ntop

[PW13] “Servidores”

URL: http://es.wikipedia.org/wiki/Servidor

[PW14] “Wireshark”

URL: http://casidiablo.net/wireshark-introduccion-instalacion/

[PW15] “D-link”

URL:http://www.dlink.es/cs/Satellite?c=Guide_P&childpagename=DLinkEurope-ES/DLGeneric&cid=1197380409000&p=1197318960420&packedargs=locale=1195806681347&pagename=DLinkEurope-ES/DLWrapper

[PW16] “Redes Inalámbricas”

URL:http://multingles.net/docs/Manual%20%20Redes%20WiFi%20inalambricas.pdf

[PW17] “Seguridad en Redes”

URL:http://www.cantv.com.ve/Portales/Cantv/Data/Eventos/SemanaSeguridad_2k8/Mendillo_SEMANADELA_SEGURIDAD_Cantv.pdf

[PW18] “Seguridad en redes WIFI”

URL:http://trajano.us.es/~fornes/RSR/2005/SeguridadWIFI/Trabajo%20WIFI.pdf

[PW19] “Medios de Transmisión”

URL: http://es.wikipedia.org/wiki/Medio_de_transmisi%C3%B3n

[PW20] “Fibra Óptica”

URL: http://es.wikipedia.org/wiki/Fibra_%C3%B3ptica

[PW21] “Cableado Estructurado”

URL: http://materias.fi.uba.ar/6679/apuntes/CABLEADO_ESTRUC.pdf

[PW22] “Cableado Estructurado”

URL:http://www.uazuay.edu.ec/estudios/electronica/proyectos/cableado_estructurado.pdf

[PW23] “Nmap”

URL: http://nmap.org/

[PW24] “Nagios”

URL: http://www.nagios.org/documentation

[PW25] “Manual de Wireshark”

URL: http://www.ftp.ucv.ve/Documentos/Wireshark/Manual.doc

[PW26] “Servidores HP”

URL:http://h18006.www1.hp.com/products/quickspecs/13247_div/13247_div.HTML

[PW27] “Estándares IEEE”

URL: http://standards.ieee.org/resources/glance.html

[PW28] “Tecnología 10 G”

URL: http://www.10gea.org

[PW29] “Tecnología 10 G y 40 G”

URL: www.ethernetalliance.org

[PW30] “Redes Inalámbricas”

URL:http://senet.wikispaces.com/file/view/REDES_INALAMBRICAS_UCC.pdf

[PW31] “Switch D-Link”

URL:http://www.dlink.es/cs/Satellite?c=Guide_P&childpagename=DLinkEuropeES/DLGeneric&cid=1197380409000&p=1197318960420&packedargs=locale=1195806681347&pagename=DLinkEurope-ES/DLWrapper

[PW32] “Herramientas para seguridad informática”

URL:http://insecure.org/tools/tools-es.html

[PW33] “IPTraf”

URL:http://es.wikipedia.org/wiki/IPTraf

[PW34] “Ntop”

URL: http://www.ntop.org/OpenSourceConf_Athens2008.pdf

[PW35] “Router 3 Com”

URL: www.3com.com

[PW36] “Modem CNt”

URL: www.cnetusa.com

[PW37] “Servidores HP Proliant 350”

URL: www.hp.com/servers/proliantml350.

[PW38] “Cámaras IP”

URL:http://www.axis.com/files/brochure/bc_techguide_33337_es_0902_lo.pdf

[PW39] “Códecs VoIP”

URL: http://www.ozvoip.com/codecs.php

[PW40] “Páginas web”

URL: http://technet.microsoft.com/es-es/library/cc745931.aspx

[PW41] “Tamaño de una página web”

URL:http://www.maxglaser.net/el-tamano-de-las-paginas-web-se-ha-triplicado-desde-el-2003/

[PW42] “Peso promedio de un mensaje”

URL:http://www.movistar.com.ve/particulares/Internet/soporte_preguntas_frecuentes.asp

[PW43] “Telefonía IP”

URL:http://store.palosanto.com/index.php/catalog/product_compare/index/

[PW44] “Tarjetas PCI”

URL: http://www.digium.com/switchvox

[PW45] “WhatsUP”

URL: http://www.ipswitch.com/international/spanish/whatsupgold.asp

[PW46] “SoftPhone”

URL: http://www.3cx.es

[PW47] “IEEE 802”

URL: http://www.ieee802.org/11

URL: http://grouper.ieee.org/groups/802/11/

[PW48] “Tecnología Inalámbrica”

URL:http://www.josechu.com/tecnologia_inalambrica/faq.htm

[PW49] “Herramientas para buscar redes inalámbricas”

URL: http://www.wirelessethernet.org

URL: http://www.extremenetworks.com

URL: http://www.lairent.com.ar/

URL: http://www.wilac.net/tricalcar

URL: http://www.ampnetconnect.com/

[PW50] “VoIP”

URL: http://www.packetizer.com/voip/h323/standards.html

URL: http://www.packetizer.com/voip/h323_vs_sip/

[PW51] “Video Vigilancia IP”

URL: http://www.videovigilanciadlink.es/

[PW52] “Infraestructura de Telecomunicaciones para Data Center”

URL:http://tesis.pucp.edu.pe/files/PUCP000000001081/DISE%D1O%20DE%20INFRAESTRUCTURA%20DE%20TELECOMUNICACIONES%20PARA%20UN%20DATA%20CENTER.pdf

[PW53] “VoIP para Novatos”

URL: http://www.voipnovatos.es/

[PW54] “Central IP basadas en software”

URL: http://www.trixbox.org/

URL: http://www.elastix.org/

URL: http://www.freepbx.org/

URL: http://www.3cx.es/voip-sip/codecs.php

[PW55] “Antivirus Kaspersky”

- http://www.kaspersky.es/

[PW56] http://www.configurarequipos.com/doc835.html

PROYECTOS DE TITULACIÓN

[T1] **QUELAL**, Josué, “*Rediseño de la Red de Comunicaciones de la empresa metropolitana de obras públicas (EMOP-Q) para soportar aplicaciones de voz sobre IP (VoIP)*”, Tesis E.P.N., Marzo 2010

[T2] **BOLAÑOS**, Emilio, "*Diseño de la Red Inalámbrica de área local para los edificios la tribuna y villafuerte de Petroproducción bajo el Estándar IEEE 802.11g y su Interconectividad"*, Tesis E.P.N, Septiembre 2008

[T3] **LOVATO**, Diana, **CADENA**, Luis, "*Diseño de la Red de Telefonía IP y su integración con la red de datos para la comunicación de la matriz con las sucursales de Importadora Vega S.A*", Tesis E.P.N., Septiembre 2010

[T4] **CORTEZ**, Darwin, **LÓPEZ**, Jaime, *"Rediseño de la red de comunicaciones para la Universidad Estatal de Bolívar que soporte aplicaciones de voz, datos y videoconferencia*", Tesis E.P.N., 2004

[T5] **POZO,** Diego*, "Estudio y Diseño de una Red de Voz y Datos para la Unidad Educativa Municipal Quitumbe utilizando la tecnología Gigabit Ethernet para soportar servicios en tiempo real de VoIP, Video seguridad y Videoconferencia*", Tesis E.P.N., Junio 2009

[T6] **HERRERA,** Myriam, *"Ingeniería de detalle para el diseño de una Intranet con conexión a Internet para aplicaciones de voz, Datos y Video utilizando la arquitectura TCP/IP"*, Tesis E.P.N., Octubre 2004

[T7] **MUÑOZ**, Andrea, **LEIVA**, Williams, "*Ingeniería de detalle para el diseño de la red para voz y datos, acceso remoto e intranet para la empresa Acurio & Asociados*", Tesis E.P.N., Mayo 2011.

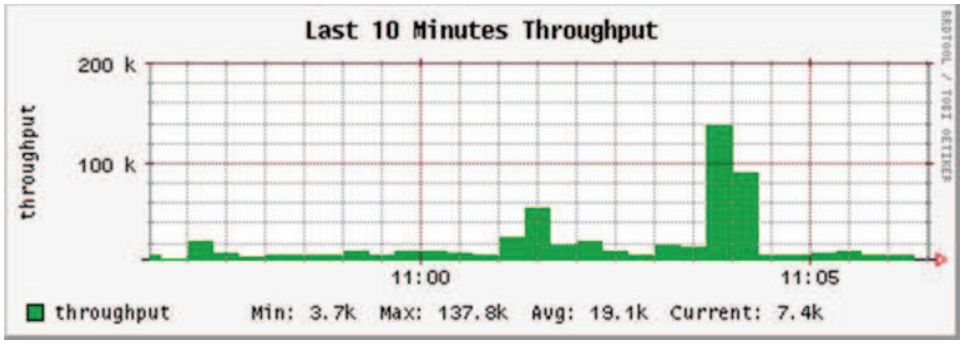
[T8] GOMEZ Fernando, "Diseño, estudio y análisis de costos de una red inalambrica para el sistema de comunicaciones interno de PETROECUADOR ", Tesis ESPE, 2006

ANEXOS

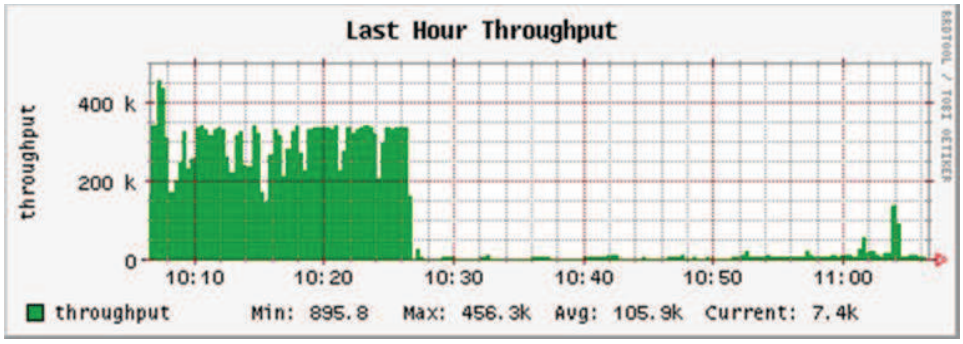
ANEXOS

ANEXO A

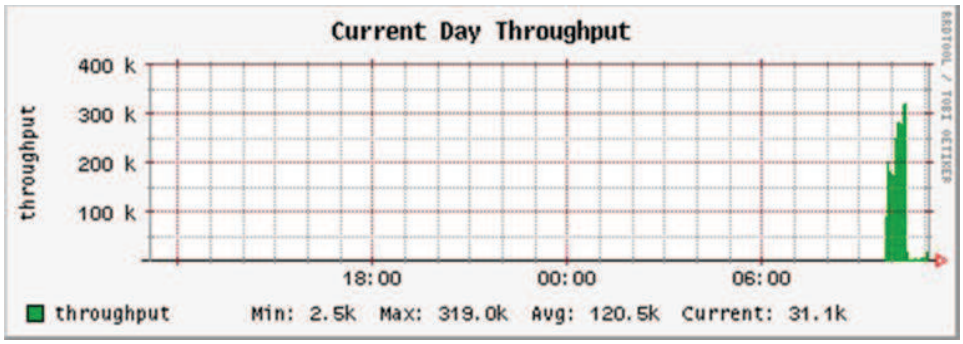
Estadísticas de carga de la red



Time [Thu May 26 10:55:58 2011 through now]

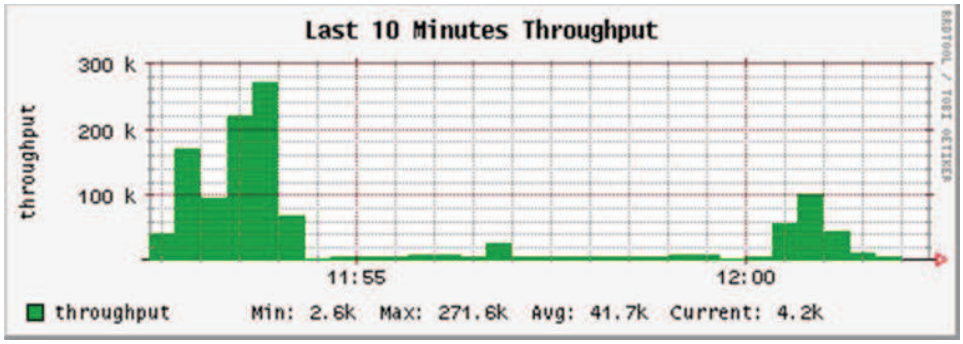


Time [Thu May 26 10:05:58 2011 through now]

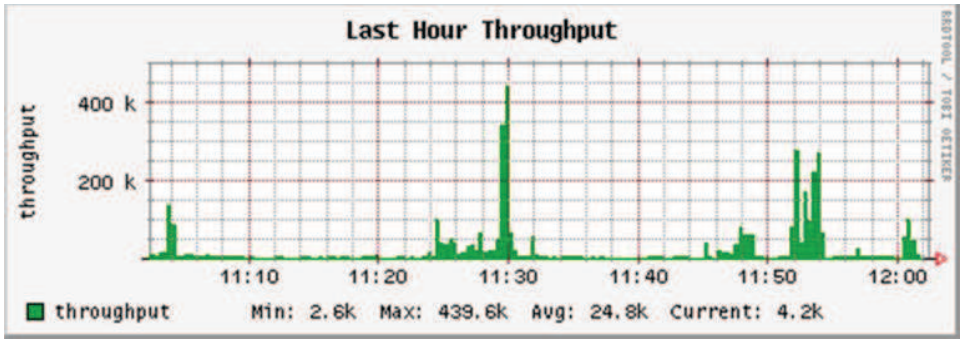


Time [Wed May 25 11:05:58 2011 through now]

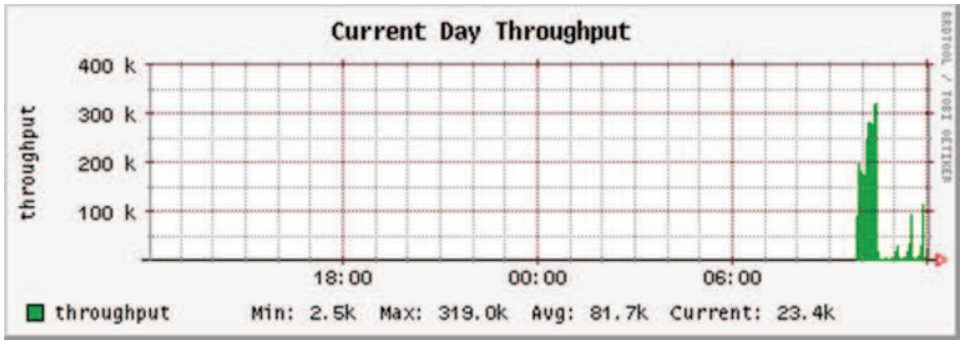
ANEXO A



Time [Thu May 26 11:51:59 2011 through now]



Time [Thu May 26 11:01:59 2011 through now]

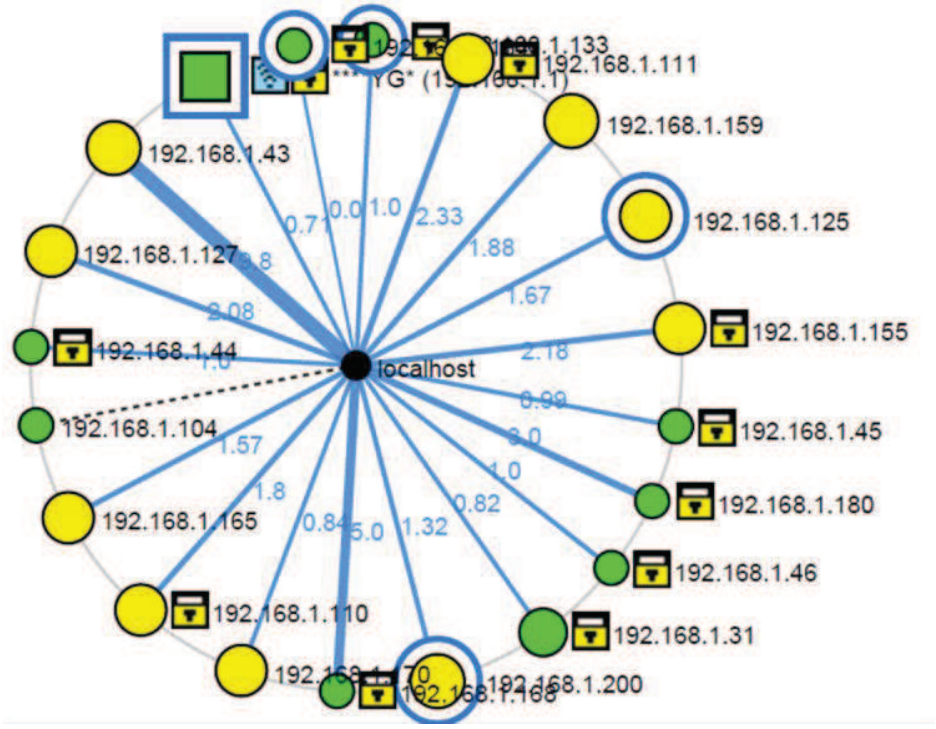


Time [Wed May 25 12:01:59 2011 through now]

ANEXO A.1

Comando	nmap -v sn 192.168.1.0/24
Estaciones de trabajo no encontradas	**Estaciones de trabajo encontradas**
Starting Nmap 5.51 (http://nmap.org) at 2011-05-19 10:59 ECT	Discovered open port 80/tcp on 192.168.1.1
Failed to resolve given hostname/IP: sn. Note that you can't use '/mask' AND '1-4,7,100-' style IP ranges	Discovered open port 445/tcp on 192.168.1.104
Initiating Ping Scan at 10:59	Discovered open port 80/tcp on 192.168.1.104
Scanning 256 hosts [2 ports/host]	Discovered open port 80/tcp on 192.168.1.159
Completed Ping Scan at 10:59, 2.22s elapsed (256 total hosts)	Discovered open port 135/tcp on 192.168.1.104
Initiating Parallel DNS resolution of 256 hosts. at 10:59	Discovered open port 21/tcp on 192.168.1.159
Completed Parallel DNS resolution of 256 hosts. at 10:59, 0.04s elapsed	Discovered open port 139/tcp on 192.168.1.104
Nmap scan report for 192.168.1.0 [host down]	Discovered open port 443/tcp on 192.168.1.104
Nmap scan report for 192.168.1.2 [host down]	Discovered open port 1025/tcp on 192.168.1.104
Nmap scan report for 192.168.1.3 [host down]	Discovered open port 139/tcp on 192.168.1.159
Nmap scan report for 192.168.1.4 [host down]	Completed Connect Scan against 192.168.1.255 in 1.52s (3 hosts left)
Nmap scan report for 192.168.1.5 [host down]	Discovered open port 912/tcp on 192.168.1.104
Nmap scan report for 192.168.1.6 [host down]	Discovered open port 1031/tcp on 192.168.1.104
Nmap scan report for 192.168.1.7 [host down]	Completed Connect Scan against 192.168.1.1 in 7.55s (2 hosts left)
Nmap scan report for 192.168.1.8 [host down]	Increasing send delay for 192.168.1.1 from 0 to 5 due to 11 out of 17 dropped probes since last increase.
Nmap scan report for 192.168.1.9 [host down]	Increasing send delay for 192.168.1.104 from 0 to 5 due to 11 out of 22 dropped probes since last increase.
Nmap scan report for 192.168.1.10 [host down]	Increasing send delay for 192.168.1.159 from 0 to 5 due to 11 out of 18 dropped probes since last increase.
Nmap scan report for 192.168.1.11 [host down]	Completed Connect Scan against 192.168.1.159 in 49.86s (1 host left)
Nmap scan report for 192.168.1.12 [host down]	Completed Connect Scan at 11:00, 51.02s elapsed (4000 total ports)
Nmap scan report for 192.168.1.13 [host down]	Nmap scan report for (192.168.1.1)
Nmap scan report for 192.168.1.14 [host down]	Host is up (0.0029s latency).
Nmap scan report for 192.168.1.15 [host down]	Not shown: 999 filtered ports
Nmap scan report for 192.168.1.16 [host down]	PORT STATE SERVICE
Nmap scan report for 192.168.1.17 [host down]	80/tcp open http
Nmap scan report for 192.168.1.18 [host down]	
Nmap scan report for 192.168.1.19 [host down]	Nmap scan report for 192.168.1.104
Nmap scan report for 192.168.1.20 [host down]	Host is up (0.0034s latency).
Nmap scan report for 192.168.1.21 [host down]	Not shown: 992 filtered ports
Nmap scan report for 192.168.1.22 [host down]	PORT STATE SERVICE
Nmap scan report for 192.168.1.23 [host down]	80/tcp open http
Nmap scan report for 192.168.1.24 [host down]	135/tcp open msrpc
Nmap scan report for 192.168.1.25 [host down]	139/tcp open netbios-ssn
Nmap scan report for 192.168.1.26 [host down]	443/tcp open https
Nmap scan report for 192.168.1.27 [host down]	445/tcp open microsoft-ds
Nmap scan report for 192.168.1.28 [host down]	912/tcp open apex-mesh
Nmap scan report for 192.168.1.29 [host down]	1025/tcp open NFS-or-IIS
Nmap scan report for 192.168.1.30 [host down]	1031/tcp open iad2
Nmap scan report for 192.168.1.31 [host down]	
Nmap scan report for 192.168.1.32 [host down]	Nmap scan report for 192.168.1.159
Nmap scan report for 192.168.1.33 [host down]	Host is up (0.0093s latency).
Nmap scan report for 192.168.1.34 [host down]	Not shown: 997 filtered ports
Nmap scan report for 192.168.1.35 [host down]	PORT STATE SERVICE
Nmap scan report for 192.168.1.36 [host down]	21/tcp open ftp
Nmap scan report for 192.168.1.37 [host down]	80/tcp open http
Nmap scan report for 192.168.1.38 [host down]	139/tcp open netbios-ssn
Nmap scan report for 192.168.1.39 [host down]	
Nmap scan report for 192.168.1.40 [host down]	Nmap scan report for 192.168.1.255
Nmap scan report for 192.168.1.41 [host down]	Host is up (0.011s latency).
Nmap scan report for 192.168.1.42 [host down]	Not shown: 999 closed ports
Nmap scan report for 192.168.1.43 [host down]	PORT STATE SERVICE
Nmap scan report for 192.168.1.44 [host down]	514/tcp filtered shell
Nmap scan report for 192.168.1.45 [host down]	
Nmap scan report for 192.168.1.46 [host down]	[oscar@localhost ~]$ nmap 192.168.1.1-255
Nmap scan report for 192.168.1.47 [host down]	Starting Nmap 5.51 (http://nmap.org) at 2011-05-18 11:25 ECT
Nmap scan report for 192.168.1.48 [host down]	
Nmap scan report for 192.168.1.49 [host down]	
Nmap scan report for 192.168.1.50 [host down]	
Nmap scan report for 192.168.1.51 [host down]	

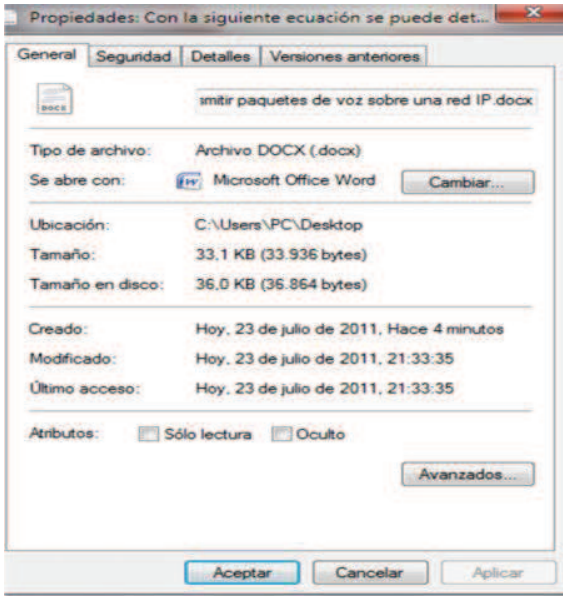
Nmap scan report for 192.168.1.52 [host down]	Nmap scan report for (192.168.1.1)
Nmap scan report for 192.168.1.53 [host down]	Host is up (0.0016s latency).
Nmap scan report for 192.168.1.54 [host down]	Not shown: 998 filtered ports
Nmap scan report for 192.168.1.55 [host down]	PORT STATE SERVICE
Nmap scan report for 192.168.1.56 [host down]	80/tcp open http
Nmap scan report for 192.168.1.57 [host down]	8085/tcp open unknown
Nmap scan report for 192.168.1.58 [host down]	
Nmap scan report for 192.168.1.59 [host down]	Nmap scan report for 192.168.1.66
Nmap scan report for 192.168.1.60 [host down]	Host is up (0.0049s latency).
Nmap scan report for 192.168.1.61 [host down]	Not shown: 999 filtered ports
Nmap scan report for 192.168.1.62 [host down]	PORT STATE SERVICE
Nmap scan report for 192.168.1.63 [host down]	443/tcp open https
Nmap scan report for 192.168.1.64 [host down]	
Nmap scan report for 192.168.1.65 [host down]	Nmap scan report for 192.168.1.159
Nmap scan report for 192.168.1.66 [host down]	Host is up (0.0072s latency).
Nmap scan report for 192.168.1.67 [host down]	Not shown: 995 filtered ports
Nmap scan report for 192.168.1.68 [host down]	PORT STATE SERVICE
Nmap scan report for 192.168.1.69 [host down]	21/tcp open ftp
Nmap scan report for 192.168.1.70 [host down]	80/tcp open http
Nmap scan report for 192.168.1.71 [host down]	139/tcp open netbios-ssn
Nmap scan report for 192.168.1.72 [host down]	515/tcp open printer
Nmap scan report for 192.168.1.73 [host down]	9100/tcp open jetdirect
Nmap scan report for 192.168.1.74 [host down]	
Nmap scan report for 192.168.1.75 [host down]	Nmap scan report for 192.168.1.170
Nmap scan report for 192.168.1.76 [host down]	Host is up (0.11s latency).
Nmap scan report for 192.168.1.77 [host down]	Not shown: 987 filtered ports
Nmap scan report for 192.168.1.78 [host down]	PORT STATE SERVICE
Nmap scan report for 192.168.1.79 [host down]	80/tcp open http
Nmap scan report for 192.168.1.80 [host down]	135/tcp open msrpc
Nmap scan report for 192.168.1.81 [host down]	139/tcp open netbios-ssn
Nmap scan report for 192.168.1.82 [host down]	443/tcp open https
Nmap scan report for 192.168.1.83 [host down]	445/tcp open microsoft-ds
Nmap scan report for 192.168.1.84 [host down]	912/tcp open apex-mesh
Nmap scan report for 192.168.1.85 [host down]	1025/tcp open NFS-or-IIS
Nmap scan report for 192.168.1.86 [host down]	1026/tcp open LSA-or-nterm
Nmap scan report for 192.168.1.87 [host down]	1027/tcp open IIS
Nmap scan report for 192.168.1.88 [host down]	1028/tcp open unknown
Nmap scan report for 192.168.1.89 [host down]	1031/tcp open iad2
Nmap scan report for 192.168.1.90 [host down]	2869/tcp open icslap
Nmap scan report for 192.168.1.91 [host down]	3000/tcp open ppp
Nmap scan report for 192.168.1.92 [host down]	
Nmap scan report for 192.168.1.93 [host down]	Nmap scan report for 192.168.1.200
Nmap scan report for 192.168.1.94 [host down]	Host is up (0.43s latency).
Nmap scan report for 192.168.1.95 [host down]	Not shown: 995 filtered ports
Nmap scan report for 192.168.1.96 [host down]	PORT STATE SERVICE
Nmap scan report for 192.168.1.97 [host down]	21/tcp open ftp
Nmap scan report for 192.168.1.98 [host down]	80/tcp open http
Nmap scan report for 192.168.1.99 [host down]	139/tcp open netbios-ssn
Nmap scan report for 192.168.1.100 [host down]	515/tcp open printer
Nmap scan report for 192.168.1.101 [host down]	9100/tcp open jetdirect
Nmap scan report for 192.168.1.102 [host down]	
Nmap scan report for 192.168.1.103 [host down]	Nmap scan report for 192.168.1.255
Nmap scan report for 192.168.1.105 [host down]	Host is up (0.10s latency).
	Not shown: 999 closed ports
	PORT STATE SERVICE
	514/tcp filtered shell

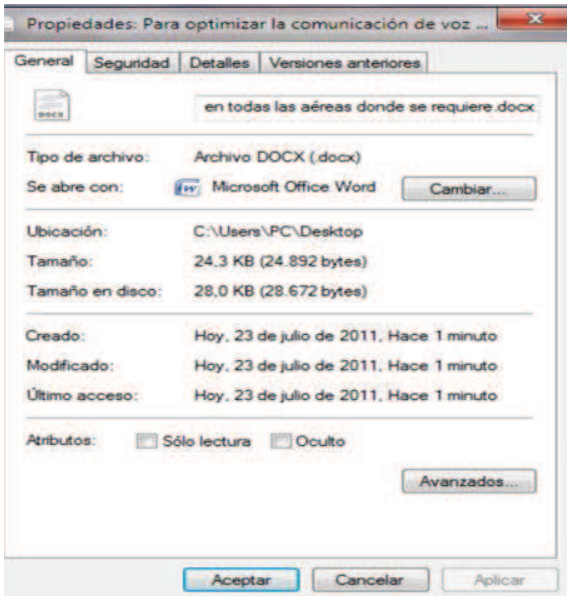


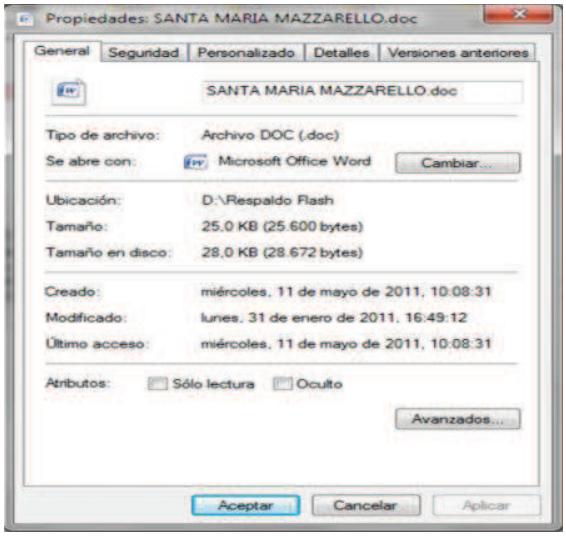
En el gráfico anterior se puede observar las estaciones de trabajo encontradas durante el escaneó utilizando Nmap

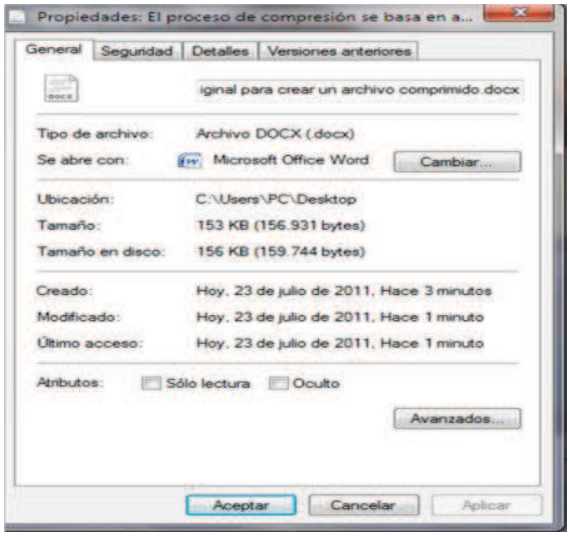
ANEXO B

Para encontrar un peso promedio que tiene una hoja se realizó el análisis de algunas hojas de Word que contienen diferente contenido como: solo texto, solo imágenes, texto e imágenes y demás combinaciones obteniendo los siguientes resultados los cuales se detallan a continuación.









El Promedio es: ***47.08***

ANEXO C

PLANOS ARQUITECTONICOS

ANEXO D

Para mejor administración y segmentación de tráfico se va a utilizar un patch pannel solo para puertos de voz y para puertos de video vigilancia.

Departamento	Puerto de datos	Puerto de Voz	Puerto de Video
Dobe 1	DOB1-R1B-PD01	DOB1-R1C-PV01	-
Dobe 2	DOB2-R1B-PD02	DOB2-R1C-PV02	-
Bodega	BO-R1B-PD03	DO-R1C-PV03	-
Coordinación E. Básica	CEB-R1B-PD04	CEB-R1C-PV04	-
Vicerrectorado	VR-R1B-PD05	VR-R1C-PV05	-
Rectorado	RE-R1B-PD06	RE-R1C-PV06	-
Secretaria	SE-R1B-PD07	SE-R1C-PV07	-
Almacén	AL-R1B-PD08	AL-R1C-PV08	-
Colecturía	CO-R1B-PD09	CO-R1C-PV09	-
Recepción	RC-R1B-PD10	RC-R1C-PV10	-
Médico	ME-R1B-PD11	ME-R1C-PV11	-
Sala de profesores	SP-R1B-PD12	SP-R1C-PV12	-
	SP-R1B-PD13		-
	SP-R1B-PD14		-
	SP-R1B-PD15		-
Cámaras	-	-	CAM1-R1C-PVV13
	-	-	CAM2-R1C-PVV14
	-	-	CAM3-R1C-PVV15
	-	-	CAM4-R1C-PVV16
			CAM5-R1C-PVV17

Tabla Departamento Administrativo

- Para el Laboratorio de Secundaria el armario de telecomunicaciones se le asigna el identificador ATS.

	Patch Pannel A de 24 p	Patch Pannel B de 24 p
Lab. Secundaria	LS-ATSA-PD01	LS-ATSB-PD01
	LS-ATSA-PD02	LS-ATSB-PD02
	LS-ATSA-PD03	LS-ATSB-PD03
	LS-ATSA-PD04	LS-ATSB-PD04
	LS-ATSA-PD05	LS-ATSB-PD05
	LS-ATSA-PD06	LS-ATSB-PD06
	LS-ATSA-PD07	LS-ATSB-PD07
	LS-ATSA-PD08	LS-ATSB-PD08
	LS-ATSA-PD09	LS-ATSB-PD09
	LS-ATSA-PD10	LS-ATSB-PD10
	LS-ATSA-PD11	LS-ATSB-PD11
	LS-ATSA-PD12	LS-ATSB-PD12
	LS-ATSA-PD13	LS-ATSB-PD13
	LS-ATSA-PD14	LS-ATSB-PD14
	LS-ATSA-PD15	LS-ATSB-PD15
	LS-ATSA-PD16	LS-ATSB-PD16
	LS-ATSA-PD17	LS-ATSB-PD17
	LS-ATSA-PD18	LS-ATSB-PD18
	LS-ATSA-PD19	CAM6-ATSB-PD19
	LS-ATSA-PD20	P20 No asignado
	LS-ATSA-PD21	P21 No asignado
	LS-ATSA-PD22	P22 No asignado
	LS-ATSA-PD23	P23 No asignado
	LS-ATSA-PD24	P24 No asignado

Tabla Lab. Secundaria

- Para el Laboratorio de Básica el armario de telecomunicaciones se le asigna el identificador ATB.

	Patch Pannel A de 24 p	Patch Pannel B de 24 p	Patch Pannel C de 12 p
Lab. Básica	LB-ATBA-PD01	LB-ATBB-PD01	CAM7-ATBC-PD01
	LB-ATBA-PD02	LB-ATBB-PD02	P02 No asignado
	LB-ATBA-PD03	LB-ATBB-PD03	P03 No asignado
	LB-ATBA-PD04	LB-ATBB-PD04	P04 No asignado
	LB-ATBA-PD05	LB-ATBB-PD05	P05 No asignado
	LB-ATBA-PD06	LB-ATBB-PD06	P06 No asignado
	LB-ATBA-PD07	LB-ATBB-PD07	P07 No asignado
	LB-ATBA-PD08	LB-ATBB-PD08	P08 No asignado
	LB-ATBA-PD09	LB-ATBB-PD09	P09 No asignado
	LB-ATBA-PD10	LB-ATBB-PD10	P10 No asignado
	LB-ATBA-PD11	LB-ATBB-PD11	P11 No asignado
	LB-ATBA-PD12	LB-ATBB-PD12	P12 No asignado
	LB-ATBA-PD13	LB-ATBB-PD13	
	LB-ATBA-PD14	LB-ATBB-PD14	

	LB-ATBA-PD15	LB-ATBB-PD15	
	LB-ATBA-PD16	LB-ATBB-PD16	
	LB-ATBA-PD17	LB-ATBB-PD17	
	LB-ATBA-PD18	LB-ATBB-PD18	
	LB-ATBA-PD19	LB-ATBB-PD19	
	LB-ATBA-PD20	LB-ATBB-PD20	
	LB-ATBA-PD21	LB-ATBB-PD21	
	LB-ATBA-PD22	LB-ATBB-PD22	
	LB-ATBA-PD23	SA-ATBB-PD23	
	LB-ATBA-PD24	SA-ATBB-PD24	

Tabla Lab. Básica

- Para el Nuevo Laboratorio el armario de telecomunicaciones se le asigna el identificador ATN.

	Patch Pannel A de 24 p	**Patch Pannel B de 24 p**
Lab. Nuevo	LN-ATNA-PD01	TS-ATNB-PD01
	LN-ATNA-PD02	IN-ATNB-PD02
	LN-ATNA-PD03	EP-ATNB-PD03
	LN-ATNA-PD04	CAM8-ATNB-PD04
	LN-ATNA-PD05	P05 No asignado
	LN-ATNA-PD06	P06No asignado
	LN-ATNA-PD07	TS-ATNB-PV07
	LN-ATNA-PD08	IN-ATNB-PV08
	LN-ATNA-PD09	EP-ATNB-PV09
	LN-ATNA-PD10	P10 No asignado
	LN-ATNA-PD11	P11 No asignado
	LN-ATNA-PD12	P12 No asignado
	LN-ATNA-PD13	
	LN-ATNA-PD14	
	LN-ATNA-PD15	
	LN-ATNA-PD16	
	LN-ATNA-PD17	
	LN-ATNA-PD18	
	LN-ATNA-PD19	
	LN-ATNA-PD20	
	LN- ATNA -PD21	
	LN- ATNA -PD22	
	P23 No asignado	
	P24 No asignado	

Tabla 3.5.1.7.4 Lab. Nuevo

- Para la Biblioteca el armario de telecomunicaciones se le asigna el identificador ATL.

	Patch Pannel A de 24 p
Biblioteca	BI-ATLA-PD01
	BI-ATLA-PD02
	BI-ATLA-PD03
	BI-ATLA-PD04
	BI-ATLA-PD05
	BI-ATLA-PD06
	BI-ATLA-PD07
	BI-ATLA-PD08
	BI-ATLA-PD09
	BI-ATLA-PV10
	EN-ATLA-PD11
	EN-ATLA-PD12
	CA-ATLA-PD13
	CA-ATLA-PD14
	P15 No asignado
	P16 No asignado
	P17 No asignado
	P18 No asignado
	P19 No asignado
	P20 No asignado
	P21 No asignado
	P22 No asignado
	P23 No asignado
	P24 No asignado

Tabla 3.5.1.7.5 Biblioteca

ANEXO E

Software para Administra redes de datos		
Características Principales	**WhatsUp Gold**	**Axence NetTools Pro 4.8**
	Monitorización de la 2 y 3 capa de red	Monitorización de la disponibilidad de hosts.
	Monitorización completa de todos los equipos conectados a la red	Visualización de todos los paquetes entrantes y salientes de la red
	Trabaja con el protocolo SNMP (V1, V2 y V3) para cualquier dispositivo que lo soporte	
	Reportes Predefinidos Sobre el Rendimiento del Sistema, Utilizando Contadores de WMI (Para redes Windows)	Escaneo de la red para descubrir todos los nodos que tiene la red
	Monitores y Reportes de Rendimiento Personalizados, Utilizando Cualquier Contador WMI	Crea una lista exhaustiva de información del sistema de computadoras con el sistema operativo Windows: detallando todos los procesos y servicios que se encuentran ejecutando, registro, eventos, discos, memoria ,etc.
	Adicione MIBs con simples “Drag-and-Drop”	Despliegue de la información local de un determinado host.
	Monitoreo de Contenido Web (HTTPS/HTTP)	TCP/IP WorkShop
	Monitoreo de ancho de banda de routers y análisis de tendencias	Escáner excautivo de la red
	Gestión de recursos /Reportes de buscador de direcciones MAC	Tiene alertas para indicar si un host no está trabajando adecuadamente
	Suite integrada de herramientas para la base de datos del WhatsUp	
	Asignación de recursos mediante priorización.	SNMP Browser y otras herramientas para lanzar Trazas, Pings, entre otros
	Solución de problemas en base a gráficos en tiempo real	

Tabla Comparación de herramientas de administración de red

ANEXO F

Antivirus Empresarial			
			
Versión	**Panda Security For Business**	**Kaspersky Enterprise Space Security.**	**Symantec™ Protection Suite Small Business Edition**
Características	Máximo nivel de protección frente amenazas sobre virus, gusanos, troyanos, Spyware, adware, rootkits, y phishing, incluyendo protección para ficheros y correo electrónico, descargas HTTP/FTP y mensajería instantánea. Protección optimizada para todos los EndPoints de la empresa. Provee bloque preventivo. Gestión centralizada y sencilla mediante la utilización de la herramienta AdminSecure. Optimización de recursos Reportes en tiempo real. Auditoría bajo demanda.	Protección anti-virus para nodos clave de la red: estaciones de trabajo, laptops, servidores de archivo y smartphones Un nuevo motor anti-virus que asegura el uso óptimo de los recursos Protección proactiva mejorada para estaciones de trabajo y servidores de archivo contra nuevos programas maliciosos Escaneo “sobre la marcha” de correos electrónicos y de tráfico de Internet Firewall personal para protección en cualquier tipo de red, incluyendo WiFi Protección local contra correos electrónicos no deseados y contra phishing Previene filtro de información de smartphones extraviados Protección para servidores de archivo que ejecutan Windows, Linux y Novell NetWare Protección exhaustiva para servidores de terminales y para grupos de servidores Balanceo de carga de procesamientos del servidor Protección anti-virus para servidores de correo electrónico Sendmail, qmail, Postfix y Exim	Efectiva Protección contra virus, malware, apyware, spam y nuevas amenazas. Protección de estaciones de trabajo, mail, servidores y sistema de recuperación. Protección integrada. Seguridad Centralizada Seguridad más acelerada y efectiva recomendada para pequeñas y medianas empresas. Bloquea el 99% de Spam y protege el correo electrónico en Exchange Fácil administración optimizando optimizados. Además, Identificación y control del flujo de información

		Escaneo de mensajes, bases de datos y otros objetos en servidores Lotus Notes/Domino Escaneo de todos los mensajes en servidores Microsoft Exchange, incluyendo carpetas públicas Bloquea envíos masivos de correos y epidemias de malware Soporte completo para sistemas de 64-bit	
Componentes	Panda AdminSecure Panda security for desktops Panda security For File Servers Panda security ComandLine	Exploración de Antivirus para contenido del disco Protección por ataques desde la red Protección proactiva sobre las aplicaciones de Microsoft Office Antihacker Antispam para cada máquina Antispyware Intercepción de virus de escritura Actualización permanente y automática de firmas de virus (hasta 3 veces al día) 1 Consola de administración centralizada para equipos dentro de la red Soporte técnico 24x7x365	Servidores y estaciones de trabajo. Servidor de administración de Endpoint Protection Small Business Edition. Mail Security para Exchange. Backup Exec System Recovery Desktop

Tabla Comparación de Antivirus empresariales

ANEXO G

PROFORMA PARA LA RED PASIVA

CABLEADO ESTRUCTURADO

ANEXO H

DATA SHEET DE LOS EQUIPOS SELECIONADOS

ANEXO I

PROFORMA PARA LA RED ACTIVA