ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

REDISEÑO DE RED MULTISERVICIOS PARA EL COLEGIO "FERNANDO DAQUILEMA" DE LA CIUDAD DE RIOBAMBA

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

JARAMILLO PINOS EDUARDO SEBASTIÁN
eduardojp2307@gmail.com

DIRECTOR: Ing. Mónica Vinueza
mvinueza@mailfie.epn.edu.ec

Quito, Agosto 2013

DECLARACIÓN

Yo, Eduardo Sebastián Jaramillo Pinos, 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.

Eduardo Jaramillo P.

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Eduardo Sebastián Jaramillo Pinos, bajo mi supervisión.

Ing. Mónica Vinueza
DIRECTORA DE PROYECTO

DEDICATORIA

Dedico el presente trabajo a mis Padres quienes me han apoyado en todo momento de mi vida y que me han inculcado los valores éticos y morales que me permitieron dar este gran paso en mi vida profesional.

A mis hermanas María Fernanda e Ibeth que siempre han estado pendientes de mí, alentándome para que sea alguien mejor.

Eduardo

CONTENIDO

CAPÍTULO I

FUNDAMENTOS TEÓRICOS

ÍNDICE DE TABLAS

CAPÍTULO I: FUNDAMENTOS TEÓRICOS

CAPÍTULO II: ANÁLISIS DE LA RED Y DETERMINACIÓN DE REQUERIMIENTOS

CAPÍTULO III: REDISEÑO DE LA INFRAESTRUCTURA DE RED

ÍNDICE DE FIGURAS

CAPÍTULO I: FUNDAMENTOS TEÓRICOS

CAPÍTULO II: ANÁLISIS DE LA RED Y DETERMINACIÓN DE REQUERIMIENTOS

CAPÍTULO III: REDISEÑO DE LA INFRAESTRUCTURA DE RED

CAPÍTULO IV: IMPLEMENTACIÓN Y PRUEBAS EN LA INFRAESTRUCTURA DE RED

RESUMEN

En el presente trabajo se muestra el rediseño de una red convergente de voz, video y datos para el Colegio Fernando Daquilema (CFD) de la ciudad de Riobamba, que permita el mejoramiento de la infraestructura y servicios de red con los que dispone en la actualidad. El trabajo incluye el análisis sobre las necesidades actuales de la institución, el rediseño de la red, se presenta un presupuesto referencial para la red rediseñada, y se realiza la implementación de los servicios de red y pruebas de los mismos.

En el Capítulo I, se presenta un análisis teórico sobre las diferentes tecnologías y protocolos usados para la transmisión de voz, datos y video sobre una red de datos basada en la arquitectura TCP/IP; además, se revisan las normas y componentes de los sistemas de cableado estructurado; y por último, se presenta una explicación sobre el software libre.

En el Capítulo II, se realiza un análisis del número de usuarios, tipo de servicios y cantidad de tráfico que cursa por la red; se analiza la infraestructura física y tecnológica presente en la institución; y se determinan los requerimientos en base a los resultados de este análisis y de las encuestas aplicadas a los usuarios de la red.

En el Capítulo III, se realiza el rediseño de la red convergente, para lo cual se dimensiona el crecimiento del número de usuarios a 5 años y la correspondiente cantidad de tráfico que se va a generar. En este trabajo se incluye el diseño del Sistema de Cableado Estructurado, LAN, WLAN y los sistemas de Telefonía IP y Video Seguridad; además, se realiza una comparación entre los sistemas de software libre existentes para su instalación en el servidor de comunicaciones.

En el Capítulo IV, se realiza la implementación y pruebas de los servicios de red que se van a instalar sobre el servidor que posee el CFD en la actualidad. Además, se realiza la implementación de un prototipo de red en el que se verifican el funcionamiento de los servicios de video, voz y datos.

En el Capítulo V, se incluyen las conclusiones y recomendaciones obtenidas en la ejecución del proyecto.

La parte de Anexos contiene: las características técnicas de los equipos activos que posee el CFD, el análisis detallado del tráfico actual de la red, el cálculo y los costos de los materiales usados en el rediseño del sistema de cableado estructurado, y los archivos de configuración utilizados en los servicios de red que se instalaron dentro del servidor que posee actualmente el CFD.

PRESENTACIÓN

El avance de la tecnología ha permitido el funcionamiento de varios servicios como el video, la voz y los datos sobre una misma infraestructura de red, lo que permite bajar los costos de instalación y ha facilitado la configuración y administración de estos servicios.

El Colegio Fernando Daquilema, es una institución educativa que ha crecido sostenidamente durante los últimos años y se ha convertido en uno de los centros académicos más concurridos en la ciudad de Riobamba, pero que, lamentablemente no posee una planificación establecida para mejorar su infraestructura de comunicaciones.

El presente trabajo, tiene como objetivo ser una guía que podrá usar la institución en el futuro para el mejoramiento de su infraestructura de red y la prestación de nuevos servicios como la entrega de información sobre la institución en Internet, dinamizar el intercambio de información administrativa, mejorar el sistema de telefonía y la seguridad física del colegio. A su vez, también se identificarán las necesidades de conectividad de los profesores y estudiantes para permitir el acceso a los recursos en Internet.

Al ser el CFD una institución pública se debe impulsar el uso de tecnologías de software libre en todas las soluciones y servicios que se presten en su red, es por ello, que en el presente trabajo todos los servicios de red que se utilizarán, serán escogidos entre las herramientas de software libre que ofrece el mercado.

CAPÍTULO I

FUNDAMENTOS TEÓRICOS

1.1 REDES DE INFORMACIÓN

Las Redes de Información son el conjunto de tres o más computadoras conectadas entre sí, que comparten recursos e información utilizando protocolos de red. Los protocolos de red utilizados en las redes de información son estandarizados por organismos internacionales.

1.1.1 MODELO DE REFERENCIA OSI[L1, L2, F1]

Este modelo fue desarrollado por la Organización Internacional de Normas (ISO en sus siglas en inglés). Su nombre es Open Systems Interconection (*OSI*) pues se ocupa de garantizar la conexión de sistemas heterogéneos por medio de la definición de lo que cada capa de red deberá hacer.

El modelo OSI se divide en siete capas, cada una diseñada para que cumpla funciones concretas, pensando en la definición de protocolos estandarizados internacionalmente.

En la Figura 1.1 se muestra el modelo de referencia OSI con sus siete capas: Física, Enlace de Datos, Red, Transporte, Sesión, Presentación y Aplicación.

1.1.2 MODELO DE REFERENCIA TCP/IP

El modelo de referencia TCP/IP, consiste en un conjunto de protocolos que se han elegido como estándares en Internet, por lo que, oficialmente no es un modelo de referencia, aunque en base a los protocolos estándar desarrollados se puede organizar todas las tareas de comunicación en cuatro capas independientes: Aplicación, Transporte, Internet y Acceso a la Red.

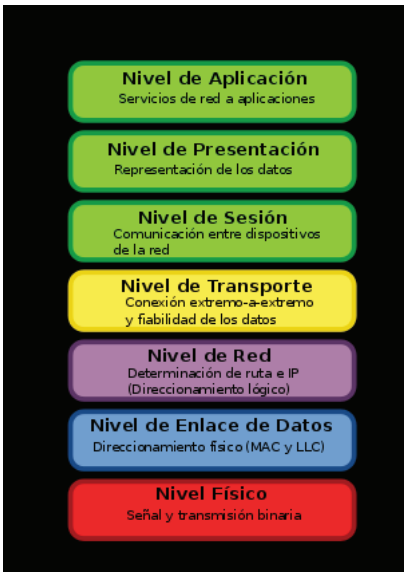


Figura 1.1: Modelo de referencia OSI[PW1]

1.1.2.1 Capa Aplicación

En la capa Aplicación se manejan protocolos de alto nivel que permiten la interacción entre las aplicaciones y el usuario. Para cada tipo de aplicación se necesita un protocolo con funciones específicas; algunos de los protocolos más comunes son FTP[1*] (*File Transfer Protocol*), HTTP[2] (*Hyper Text Transfer Protocol*), DNS[3] (*Domain Name System*), TELNET (*TELecommunication NETwork*), etc.

1.1.2.2 Capa de Transporte

La capa Transporte se encuentra debajo de la capa Aplicación. Esta capa permite a las aplicaciones pares en los nodos[4] de origen y destino llevar a cabo una conversación, para lo cual, se definieron dos protocolos extremo a extremo, el protocolo TCP (*Transmission Control Protocol*) y el protocolo UDP (*User Datagram Protocol*).

TCP es un protocolo confiable orientado a conexión que garantiza la entrega de la información sin errores, por ello, es utilizado por aplicaciones cuya prioridad es que toda la información enviada llegue sin ningún error a su destino.

---

* La definición de todas las palabras marcadas con un superíndice se encuentran en la sección de Glosario.

UDP es un protocolo no confiable, no orientado a conexión, pues, no asegura que los datos lleguen a su destino o que estos lleguen correctamente. Es utilizado por aplicaciones en tiempo real (video y voz) que desean principalmente la pronta entrega de su información sin tomar en cuenta los errores que contenga esa información.

Cada protocolo añade a la carga útil (*PDU*, *Payload Data Unit*) información de control, misma que es retirada al ser recibida. La PDU con toda la información de control añadida en la capa de Transporte se llama “segmento”.

En la Figura 1.2 se muestra como en el proceso de encapsulación cada capa añade información de control a los datos, esta información también es llamada “cabecera”.

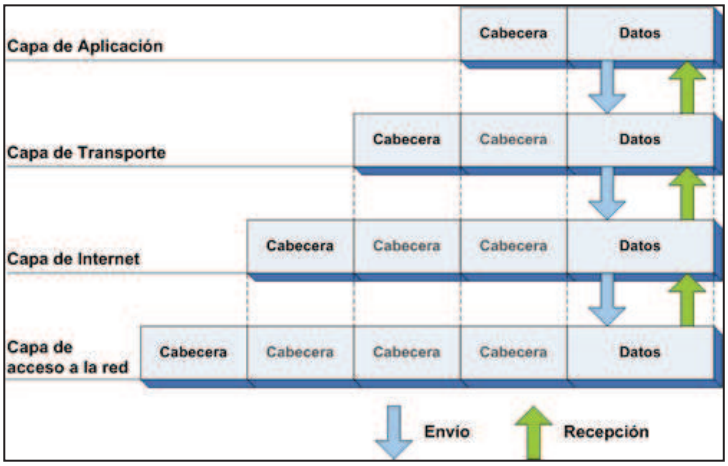


Figura 1.2: Proceso de encapsulación TCP/IP[PW2]

1.1.2.3 Capa de Internet

Esta capa tiene como objetivo el enviar información entre cualquier red de forma transparente para las capas superiores, para lo cual se añade información de control a los datos que provienen de la capa de Transporte, donde se especifican las direcciones del host origen y destino para su posterior enrutamiento por la red.

El protocolo más importante en esta capa es IP (*Internet Protocol*) pues, es el que cumplirá con las funciones básicas para la transmisión de los datos. IP es un protocolo no confiable, no orientado a conexión, ya que, no ofrece mecanismos para asegurar que un paquete ha llegado a su destino, dejando el control de

errores y control de flujo para los protocolos de capas superiores. Entre sus funciones están: definir el datagrama o paquete (unidad de datos de la capa Internet), definir el esquema de direccionamiento de la red, realizar fragmentación y re-ensamblaje de los paquetes, encauzar los paquetes hacia su red destino por medio de las direcciones IP origen y destino de cada paquete.

1.1.2.4 Capa Acceso a la Red

La capa Acceso a la Red es la encargada de interactuar con el hardware y el encaminamiento de la información a través de la red local. El modelo de referencia TCP/IP no define un protocolo a usar, por lo que, esto dependerá de la plataforma de comunicación.

1.1.3 REDES DE ÁREA LOCAL[F2]

Las Redes de Área Local (LAN, *Local Area Networks*) son aquellas que conectan estaciones de trabajo, periféricos, terminales y otros dispositivos de red dentro de una oficina, edificio o campus. Los medios de transmisión comúnmente utilizados en las LAN son el cable UTP (*Unshielded Twisted Pair*), la fibra óptica y los medios inalámbricos.

1.1.3.1 Arquitecturas de Red de Área Local

La arquitectura de las redes LAN está normalizada en los estándares IEEE[5] 802. Los diferentes estándares en este grupo se diferencian en la capa física y en la subcapa MAC (*Medium Access Control*), pero todos son compatibles en la subcapa LLC (*Logical Link Control*).

En la Figura 1.3 se muestran los estándares IEEE 802, y su ubicación dentro de las capas modelo de referencia OSI. En el modelo de IEEE se considera que la capa enlace de datos se divide en las subcapas LLC y MAC.

La subcapa LLC es aquella que proporciona una interfaz independiente de la tecnología usada en el medio de transmisión. Las funciones principales que realiza esta subcapa son el control del flujo y el control de errores.

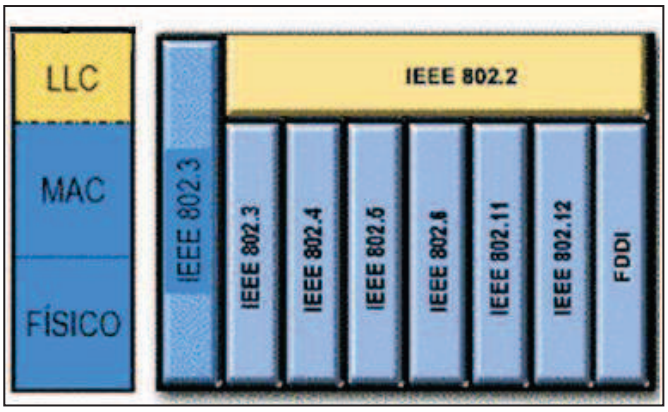


Figura 1.3: Arquitecturas LAN [PW3]

La subcapa MAC cumple con las funciones de agregar direcciones MAC de nodos fuente y destino, controlar el acceso al medio de transmisión compartido, enviar y recibir tramas hacia y desde la capa física.

1.1.3.2 Tecnología de Redes de Área Local

Una gran cantidad de LAN a nivel mundial utilizan tecnologías que han sido definidas en el estándar IEEE 802.3 llamado comúnmente "Ethernet". Esta tecnología tiene ventajas como:

- Fácil implementación, mantenimiento y administración.
- Gran flexibilidad en la topología para satisfacer las necesidades de redes grandes y medianas.
- Compatibilidad entre los dispositivos de varios fabricantes.
- Precios bajos de los equipos.

El estándar IEEE 802.3 abarca una familia de tecnologías LAN que ofrecen diferentes velocidades de transmisión por cable. Entre estas tecnologías se destacan Ethernet, Fast Ethernet y Gigabit Ethernet.

1.1.3.2.1 Ethernet

El estándar 10BaseT utiliza cable UTP con topología física tipo estrella y topología lógica tipo bus, para lo cual, se utilizó un concentrador de cableado (HUB) al que se conectan todas las estaciones con cable UTP categoría 3 aunque se puede utilizar categorías superiores.

En esta tecnología el medio de transmisión era compartido entre todas las estaciones, por lo que se utilizó el mecanismo de Acceso Múltiple por Escucha de Portadora y Detección de Colisiones (CSMA/CD por sus siglas en inglés) con el objetivo de minimizar el número de colisiones entre los paquetes que viajan por la red y aumentar el rendimiento de la misma.

Aunque con el mecanismo CSMA/CD el rendimiento de las redes aumentó con respecto a mecanismos de acceso al medio de transmisión anteriores como: Aloha, Aloha ranurado y CSMA; pero al incrementarse el número de estaciones conectadas el medio de transmisión este se satura y el rendimiento de la red baja rápidamente; es por ello que se pasó al uso de redes conmutadas reemplazando al HUB por el switch[6]. El switch al recibir un paquete no lo retransmite por todos sus puertos sino que lee las direcciones origen y destino de la trama, y con ello reenvía la trama por el puerto de salida en donde esté conectada la estación destino.

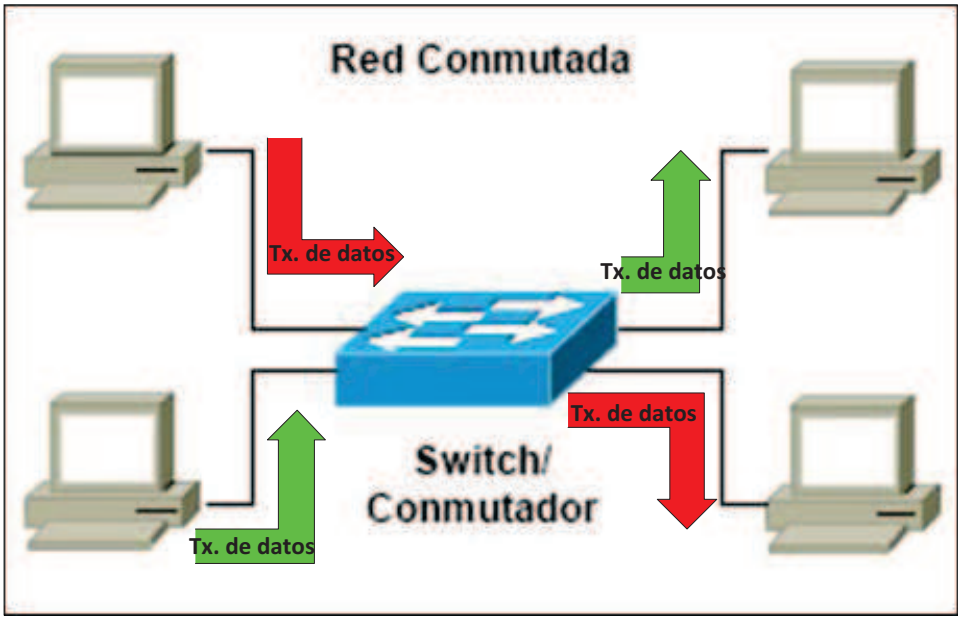


Figura 1.4: LAN conmutada

Las conexiones entre una estación y un switch pueden funcionar en modo half-duplex[7] y fullduplex[8], la diferencia entre los dos modos consiste en que en el modo fullduplex la estación puede enviar y recibir información simultáneamente mientras que en el modo half-duplex solo puede recibir o transmitir información pero no los dos a la vez.

1.1.3.2.2 Fast Ethernet

Fast Ethernet tiene como objetivo el incrementar la velocidad de transmisión que se tiene con el estándar 100BaseT, pero conservando el tipo de cableado y el formato de trama.

En función al medio de transmisión usado se tiene dos estándares en Fast Ethernet, cada uno con su propio tipo de codificación: 100Base-X que utiliza cable STP (*Shielded Twisted Pair*), UTP categoría 5 o superior, o fibra óptica; 100Base-T4 utiliza cable de voz categoría 3.

El estándar 100Base-X incluye dos especificaciones: 100Base-TX que utiliza par trenzado STP o UTP categoría 5 o superior, y 100Base-FX que utiliza fibra óptica.

En la Tabla 1.1 se muestran las características principales de cada estándar en Fast Ethernet y sus respectivas especificaciones.

Estándar		**Tipo Cable**	**Tipo Codificación**	**Longitud máxima de enlace [m]**
100Base-X	100Base-FX	STP y UTP cat. 5	MLT-3	100
	100Base-FX	Fibra óptica multimodo	4B5B-NRZI	400
100Base-T4		UTP cat. 3 o superior	8B6T	100

Tabla 1.1: Características principales de los estándares Fast Ethernet[F2]

1.1.3.2.3 Gigabit Ethernet

Gigabit Ethernet aumenta la velocidad de transmisión de los datos a 1000 Mbps[9]. En operación Half-duplex utiliza el mismo formato de trama y método de acceso al medio que los estándares IEEE 802.3 de velocidades de 10 y 100 Mbps. Para la operación Full-duplex se necesita tener una red conmutada.

En el estándar 802.3z se definen las especificaciones: 1000Base-LX, 1000Base-SX, 1000Base-CX. En este estándar se ofrece la posibilidad de usar ráfagas de

tramas, que consisten en enviar varias tramas como una sola, con un límite de tamaño máximo de ráfaga de 8192 Bytes.

1000Base-SX utiliza como medio de transmisión fibra óptica multimodo de 62.5µm o 50µm en la ventana de 850nm para cubrir distancias de 220 a 550 metros por enlace, según el diámetro de la fibra óptica utilizada.

1000Base-LX utiliza fibra óptica multimodo de 50 y 65.5 µm y fibra monomodo de 9µm en la ventana de 1300nm. Con esta especificación se puede alcanzar distancias de enlace de 550 a 5000 metros según la fibra óptica utilizada.

1000Base-CX utiliza dos pares del cable STP y cubre una distancia máxima de 25 metros, por lo que suele ser utilizado en conexiones entre equipos de red que están dentro del cuarto de telecomunicaciones.

Otro estándar desarrollado para redes Gigabit Ethernet es el 802.3ab, también conocido como 1000Base-T. Éste estándar usa un cable UTP cat. 5 de 4 pares y cubre una distancia máxima de enlace de 100 metros.

En la Tabla 1.2 se muestra las características principales de los estándares 802.3z y 802.3ab.

Estándar		**Tipo de cable**	**Distancia máxima del enlace [m]**
IEEE 802.3z	1000Base-LX	Fibra óptica monomodo, de 9µm de diámetro de núcleo	5000
		Fibra óptica multimodo, de 50µm de diámetro de núcleo	550
		Fibra óptica multimodo, de 62,5µm de diámetro de núcleo	440
	1000Base-SX	Fibra óptica multimodo, de 50µm de diámetro de núcleo	550
		Fibra óptica multimodo, de 62,5µm de diámetro de núcleo	220
	1000Base-CX	Dos pares de cable STP	25
IEEE 802.3ab	1000Base-T	Cable UTP de 4 pares cat. 5	100

Tabla 1.2: Características de las especificaciones 1000Base-LX y 1000Base-SX[F2]

1.1.4 REDES DE ÁREA LOCAL INALÁMBRICA[F5]

Las Redes de Área Local Inalámbrica o WLAN (*Wireless Local Area Network*) usan tecnologías de radiofrecuencia para la comunicación de los datos y conectar dispositivos a la red.

Las aplicaciones de las redes WLAN son: extender la cobertura de una red LAN, interconectar edificios y dar acceso a la red a usuarios móviles.

Las ventajas que ofrecen las redes WLAN son:

- Rápida instalación
- Acceso a la red desde lugares a los que la red cableada no puede llegar
- Fácil incorporación de nuevos usuarios a la red
- Brindan movilidad a los usuarios
- Permiten la interconexión de redes de edificios no contiguos
- Ofrecen una red de comunicación de datos escalable

1.1.4.1 Estándar IEEE 802.11[F3]

El estándar IEEE 802.11 define la capa Física, la subcapa de Acceso al Medio (MAC) y la capa de Administración de Estación que es la que coordinará las interacciones entre la capa Física y la subcapa MAC.

El método de acceso al medio se basa en la detección de portadora evitando las colisiones (CSMA/CA). Debido a que las estaciones no pueden transmitir y receptar datos al mismo tiempo, se definió las tramas de RTS (*Request To Send*), CTS (*Clear To Send*) y ACK (*Acknowledgment*), y con el uso de éstas evitar las colisiones.

En la Figura 1.5 se muestra la arquitectura que se define en el estándar 802.11, misma que está formada de la siguiente manera: en la capa Física, por la subcapa PMD (*Physical Medium Dependent*, Dependiente del Medio Físico) que define la características de funcionamiento, métodos de modulación y codificación para la comunicación de datos por medios inalámbricos; y por la subcapa PLCP (*Physical Layer Convergence Procedure*, Procedimiento de Convergencia de la

Capa Física) que es la encargada de convertir la PDU MAC a un formato adecuado para su transmisión y recepción por un medio de transmisión dado; la subcapa MAC (*Medium Access Control*) es la que se ocupa de la fragmentación y re ensamblaje de las tramas, además, de los mecanismos de acceso; la capa de Administración de Estación está formada por la subcapa PLME (*Physical Layer Management Entity*, Entidad de Administración de Capa Física) que selecciona la frecuencia o canal a la que trabajará la comunicación; y por la subcapa MLME (*MAC Layer Management Entity*, Entidad de Administración MAC) que es responsable de la administración de potencia, y de los procesos de asociación, desasociación y reasociación que se dan en el registro de una estación inalámbrica en la red WLAN.

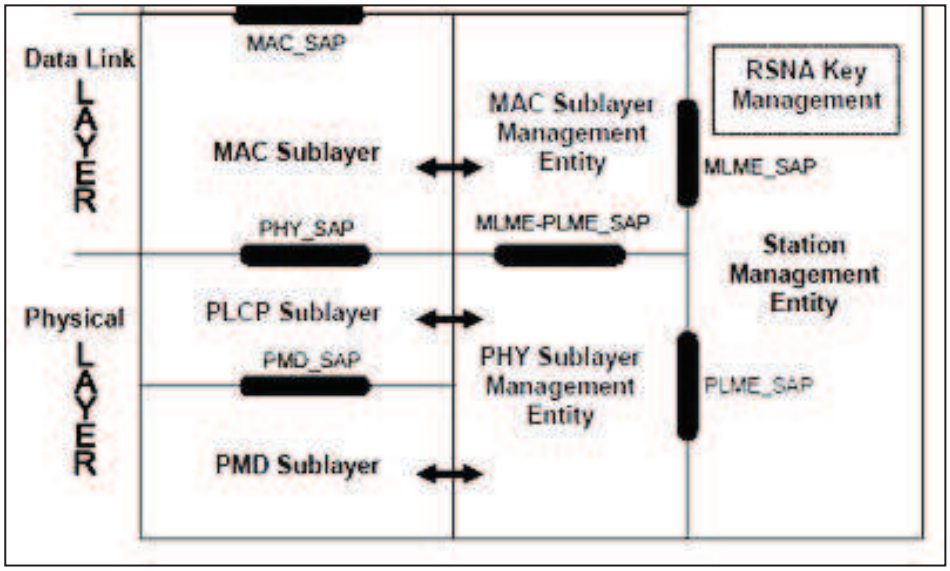


Figura 1.5: Arquitectura IEEE 802.11[PW4]

En la Figura 1.6 se muestra los bloques principales que forman una red WLAN de infraestructura, que está formada por un conjunto de estaciones que están asociadas a un punto de acceso (AP, *Access Point*[10]), este conjunto es llamado BSS (*Basic Service Set*, Conjunto de Servicios Básicos), y su área de cobertura es llamada BSA (*Basic Service Area*, Área de Servicios Básicos). Para interconectar varios BSS's se utiliza un sistema de distribución (DS),y esta agrupación toma el nombre de ESS (*Extended Service Set*, Conjunto de Servicios Extendidos), por la cual se puede acceder a la red cableada por medio de dispositivos llamados "portales".

El estándar 802.11 posee varias especificaciones para su capa física, que se diferencian entre sí por la velocidad de transmisión, modulación, área de cobertura y frecuencia de funcionamiento.

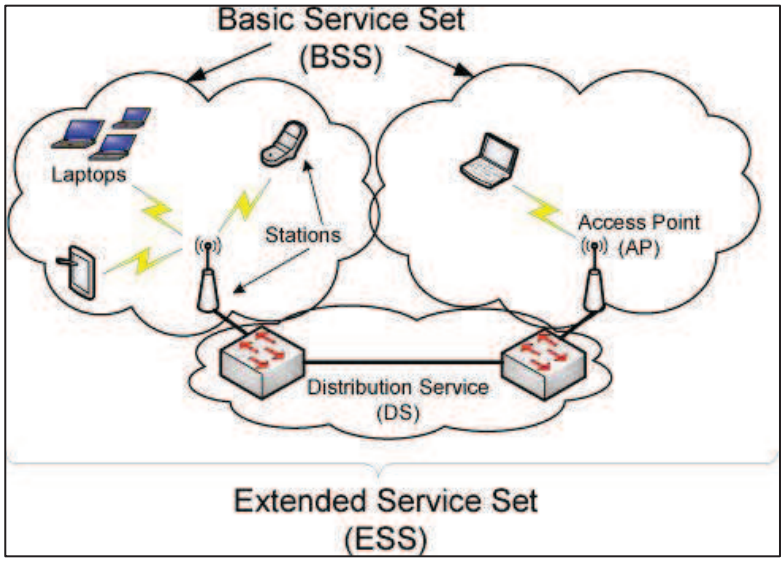


Figura 1.6: Conjunto de Servicios Extendidos (ESS)[PW5]

a) IEEE 802.11a.-

Utiliza modulación OFDM (*Orthogonal Frequency Division Multiplexing*, Multiplexación por División de Frecuencia Ortogonal) con velocidades de transmisión mandatorias de 6, 12, 24 y 54 Mbps. Opera en la bandas de frecuencia U-NII[11]: 5.15-5.25GHz, 5.25-5.35GHz, y 5.725-5.825GHz. Su espectro de frecuencia se divide en 12 canales de 20 MHz de ancho de banda no sobrelapados entre sí, de los cuales 8 canales son para utilización en ambientes indoor[12] y 4 para ambientes outdoor[13].

b) IEEE 802.11b.-

La frecuencia de operación de este estándar es la banda de los 2.4GHz. El tipo de modulación depende de la velocidad a la que está trabajando, pues a velocidades de 1 a 2 Mbps utiliza modulación DSSS, para velocidades de 5.5 a 11 Mbps modulación CCK. En la Figura 1.7 se muestra como el espectro de frecuencias se encuentra dividido en 11 canales de 22MHz de ancho de banda sobrelapados entre sí, dejando 1 grupo de 3 canales que no se sobrelapan entre ellos.

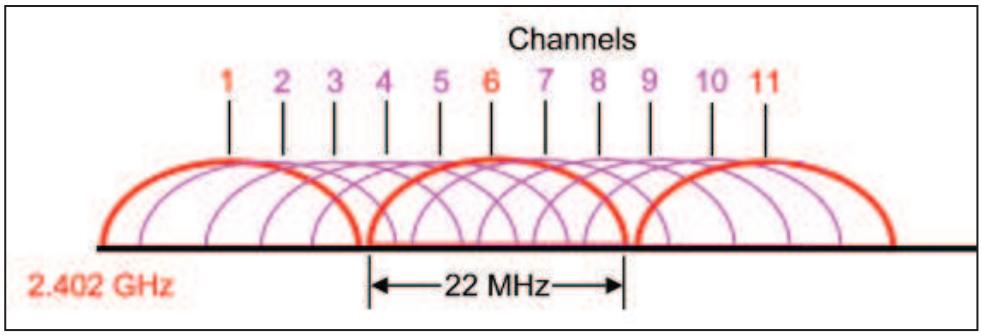


Figura 1.7: Canales de 802.11b USA[PW6]

c) IEEE 802.11g.-

Este estándar opera en la frecuencia de 2.4GHz, manteniendo compatibilidad con los estándares anteriores, por lo que, para velocidades de hasta 11 Mbps funciona de igual manera como lo hace 802.11b y para velocidades de hasta 54 Mbps utiliza la modulación OFDM. Los canales de frecuencia que utiliza son iguales que los de 802.11b.

d) IEEE 802.11n.-

802.11n utiliza los mismos tipos de modulación que 802.11a y 802.11g, operando en las bandas de frecuencia de 2.4GHz y 5GHz. Para mejorar la velocidad de transmisión utiliza la técnica de multiplexación espacial utilizando MIMO, que consiste en utilizar varias antenas para la transmisión y recepción de datos de forma simultánea. Las velocidades que se soporta están en el rango de entre 6.5 Mbps a 300 Mbps.

1.1.4.2 Seguridad en 802.11[F3]

Para obtener una seguridad robusta es necesario que la red inalámbrica brinde los servicios de Autenticación, Confidencialidad, Integridad, Disponibilidad.

Se entiende como Autenticación a la verificación de la identidad de los usuarios mediante claves o credenciales que el usuario presenta; en caso de las redes inalámbricas es necesario que la autenticación sea en los dos sentidos, pues se debe poder verificar tanto autenticidad de usuario como de la red a la cual se está asociando éste.

La Confidencialidad en las redes inalámbricas es de suma importancia, pues, siendo el medio de transmisión ondas de radiofrecuencia, cualquier estación en el rango de cobertura puede escuchar los datos que están siendo enviados, por lo que, se debe garantizar que la información que circula por la red sea visible solo por los usuarios autorizados; para ello, se utilizan mecanismos de cifrado robustos.

El servicio de Integridad ayudará a prevenir que usuarios no autorizados alteren la información que circule por red al usar mecanismos como comprobación de CRC (*Cyclic Redundancy Check*) o a través de un código de integridad del mensaje.

La Disponibilidad tiene como objetivo otorgar a la red inalámbrica mayor resistencia y capacidad de recuperación ante los ataques, o accidentes que puedan sufrir los equipos, esto se logra por medio del uso de políticas de seguridad, claves robustas para el acceso a la consola de administración de los AP's, y la protección de los equipos ante la manipulación o daño físico.

Los principales métodos para dar seguridad a una red inalámbrica son:

WEP (*Wired Equivalent Privacy*): es un sistema de cifrado basado en el algoritmo RC-4 con claves de 64 y 128 bits. Este sistema provee a la red inalámbrica de autenticación, confidencialidad e integridad. Utiliza la misma clave para autenticación y cifrado. Debido a debilidades en los métodos de autenticación, cifrado e integridad no se recomienda su uso.

IEEE 802.1x y EAP: 802.1x es el protocolo de control de acceso basado en una arquitectura cliente-servidor. Su funcionamiento se basa en la utilización del protocolo EAP (*Extensible Authentication Protocol*) para el envío y recepción de mensajes de autenticación entre la estación y el servidor de autenticación RADIUS (*Remote Authentication Dial-In User Service*).

WPA (Wifi Protected Access): WPA puede funcionar de dos modos: empresarial y residencial. En el modo empresarial utiliza como mecanismo de autenticación 802.1x y EAP; el modo residencial es utilizado para evitar el uso obligatorio de un servidor de autenticación, por lo que, trabaja con pre compartición de claves (PSK). El cifrado se realiza con TKIP (*Temporal Key Integrity Protocol*) que tiene

una longitud de clave de 128 bits, cifra cada sesión y paquete con una clave diferente, refuerza el vector de inicialización y mejora la integridad de los paquetes cifrados al implementar un código de integridad. En WPA2 se cambia el algoritmo de cifrado por AES (*Advanced Encryption Standard*).

1.1.5 DIRECCIONAMIENTO EN REDES [PW7]

La dirección IP es un identificador único de cada host[14] dentro de su red. Cada host que está conectado a una red debe tener una dirección IP, asignada distinta de todas las demás direcciones que sean visibles por el host.

Las direcciones IP están compuestas de 4 bytes (32 bits) y se representan de la forma “a.b.c.d”, cada letra representa un número decimal entre 0 y 255.

La dirección IP conceptualmente se divide en dos partes: el *identificador de red* y el *identificador de host*; cada una de las partes utiliza un determinado número de bits con los que se calcula el número de hosts en cada red.

Según este criterio las redes se clasificaron en cinco clases: Las clases A, B y C son llamadas primarias y son aquellas en las que cada dirección IP representa a un solo dispositivo en la red; la clase D es llamada de multicast[15] pues cada dirección IP representa a un grupo de dispositivos de la red; y, la clase E es aquella que no puede utilizarse, ya que, sus direcciones han sido reservadas. En la Tabla 1.3 se muestra detalladamente el número de redes, número de host por red y el rango de direcciones de cada clase de red.

Clase	Formato de dirección (n = red, s= host)	Número de redes	Número de hosts	Rango de direcciones de red
A	n.s.s.s	128	1677214	1.0.0.0 - 127.255.255.255
B	n.n.s.s	16384	65534	128.0.0.0 - 191.255.255.255
C	n.n.n.s	2097152	254	192.0.0.0 - 223.255.255.255
D	IP grupal	-	-	224.0.0.0 - 239.255.255.255
E	No válida	-	-	240.0.0.0 - 255.255.255.255

Tabla 1.3: Clasificación de las redes IP [PW7]

Las direcciones IP se clasifican en:

Direcciones IP públicas: Son aquellas direcciones que son visibles desde Internet. El organismo internacional que asigna direcciones IP públicas en América Latina es LACNIC (*Latin American and Caribbean Internet Addresses Registry*).

Direcciones IP privadas: Son aquellas que son visibles solo por los hosts de su propia red u otras redes privadas interconectadas con routers. Estas direcciones son asignadas a las estaciones de trabajo dentro de las empresas. Los ordenadores con IP privadas pueden salir a Internet por medio de un router o proxy que tenga una IP pública, pero desde Internet los ordenadores no son alcanzables. Las direcciones IP privadas son:

- Clase A: 10.0.0.0 a 10.255.255.255
- Clase B: 172.16.0.0 a 172.31.255.255
- Clase C: 192.168.0.0 a 192.168.255.255

Hay direcciones IP que son utilizadas para funciones especiales como:

- La dirección IP 0.0.0.0 está reservada para identificación local.
- La red 127.0.0.0 está reservada para las direcciones de loopback[16].
- La dirección IP cuyos bits de host tengan el valor 1, está reservada para direccionar a todos los hosts dentro de una red IP específica, es por eso que toma el nombre de broadcast dirigido.
- La dirección IP cuyos bits de red y de host tengan el valor 1, está reservada para cumplir funciones de broadcast[17].

Al trabajar con redes basadas en clases, la distribución de direcciones IP es ineficiente, ya que, muchas direcciones se desperdiciaban, por lo que, surgió VLSM (V*ariable Length Subnet Mask*) y CIDR (*Classless Inter Domain Routing*) como solución a este problema.

1.1.5.1 VLSM

VLSM se emplea para la segmentación de una red en subredes de tamaño variable, que se ajusten mejor al número de hosts que se quieren abarcar, por

esta misma variabilidad la máscara de cada subred también tendrá un tamaño variable.

1.1.5.2 CIDR

CIDR permite el agregar o sumarizar un grupo rutas para representarlas mediante una sola dirección IP con su respectiva máscara, reduciendo de esta manera el tamaño de la tabla de enrutamiento y la cantidad de recursos necesarios en el router para procesarla.

1.2 SISTEMA DE CABLEADO ESTRUCTURADO[F4, P1]

El Sistema de Cableado Estructurado permite brindar una solución única para conectar dispositivos de voz, datos y video, así como también equipos de conectividad.

El Sistema de Cableado Estructurado está basado en estándares que garantizan independencia de equipos y productos utilizados, flexibilidad, modularidad en crecimiento, uniformidad en diseño, y soporte de cualquier servicio de transmisión actual o futuro.

1.2.1 ESTÁNDARES DEL SISTEMA DE CABLEADO ESTRUCTURADO

Los estándares más comúnmente usados en el mundo para los Sistemas de Cableado Estructurado son aquellos propuestos por la TIA (*Telecomunications Industry Association*), y reconocidos por ANSI (Instituto Nacional Americano de Normalización). Las normas más utilizadas son:

1.2.1.1 TIA-568-C

Este estándar reemplaza al estándar EIA/TIA-568-B desde el año 2009. El mayor avance que se dio en este documento es el permitir que todas las adendas se compilen en un solo documento y señalen otros avances que vale la pena tener en cuenta. En este nuevo estándar se incluyen los estándares EIA/TIA 568-B.1, 568-B.2 y 568-B.3.

En el estándar TIA-568-C fue desarrollado una serie específica con el objetivo de ser un documento genérico para usarse cuando un estándar específico no estuviera disponible, por ejemplo, para el diseño del cableado en un aeropuerto, esta serie es la TIA-568-C.0.

1.2.1.1.1 TIA-568-C.0

Este estándar tiene como fundamento el convertirse en la base de otros estándares presentes o futuros, que pueden enfocar su contenido en aspectos que se permitan dentro del estándar 568-C.0, lo que causará que los nuevos documentos sean más cortos y especializados, de manera que, se puedan desarrollar más rápido.

La nomenclatura de esta norma también es nueva, para que se ajuste a los casos genéricos. En la Figura 1.8 se muestra la nueva nomenclatura que toman los elementos funcionales de un sistema de cableado estructurado, donde a los segmentos de cableado se los llama “Subsistemas de Cableado”, “Distribuidor” a los puntos de conexión, y “Salida de Equipos” al distribuidor del final.

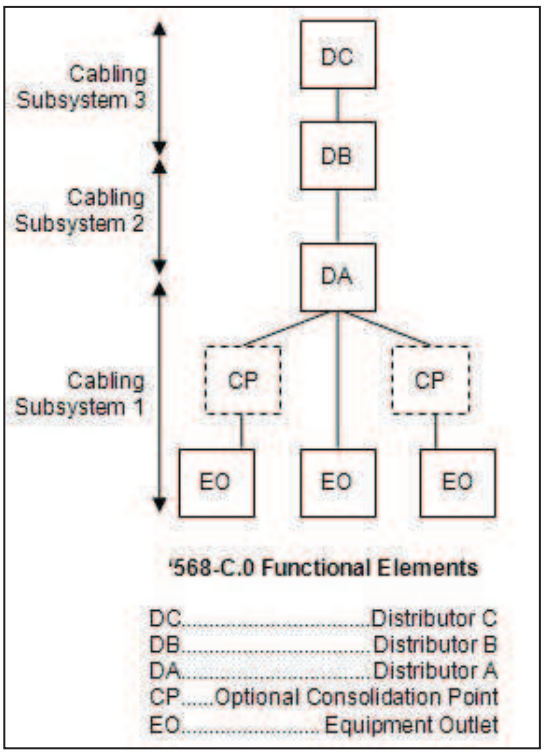


Figura 1.8: Elementos funcionales del estándar TIA-568-C.0[PW8]

Otras novedades de este documento son:

- Reconocimiento del cable UTP categoría 6A.
- Requisitos para las pruebas de enlace y rendimiento de fibra óptica se trasladaron a este documento.
- El radio mínimo de curvatura del cable de par entorchado durante su instalación ha sido modificado a 4xOD (*Out Diameter*) tanto para el cable UTP como para el STP.

1.2.1.1.2 TIA-568-C.1

El estándar TIA-568-C.1 es una revisión del estándar 568-B.1, con la diferencia de que este estándar ya no es independiente como lo es el 568-B.1, pues, el cableado para edificios comerciales ahora es cubierto por el estándar 568-C.1 y complementado por el 568-C.0.

Algunos cambios técnicos que se hicieron en este estándar son:

- La información común fue trasferida a la 568-C.0.
- Se recomienda seleccionar la fibra óptica 50/125um @ 850nm, como la fibra multimodo para edificios comerciales.
- El cableado STP de 150 ohmios, UTP categoría 5 y cable coaxial de 50 y 75 ohmios ya no son medios reconocidos.
- Los requisitos de prueba y desempeño de los sistemas de cobre fueron transferidos para ser incluidos en la 568-C.2.

La nomenclatura usada en la norma 568-B.1 sigue vigente, y los nombres de los subsistemas son los mismos: Entrada de Servicios, Cuarto de Equipos, Cuarto de Telecomunicaciones, Cableado Vertical, Cableado Horizontal y Área de Trabajo.

1.2.1.1.3 TIA-568-C.2

En este estándar se especifican el cable y componentes para los cables de par trenzado balanceado de cobre categoría 3, categoría 5E, categoría 6 y categoría 6A.

Los principales cambios que se hicieron en esta norma son:

- Se ha introducido atenuación de acoplamiento como un parámetro que está en estudio para la caracterización de potencia máxima radiada, generados por las corrientes de modo común para cables apantallados.
- Uno de los métodos de ensayo de laboratorio se definió para todas las categorías de hardware de conexión.
- Se recomienda cableado de categoría 5e para el apoyo de aplicaciones de 100 MHz.

1.2.1.1.4 TIA-568-C.3

Este estándar especifica las pruebas de rendimiento para el medio de transmisión y sus componentes para un Sistema de Cableado Estructurado de fibra óptica.

Los principales cambios que se hizo en esta norma son:

- Aumento del ancho de banda OFL mínimo para fibra de 62,5μm (200/500 MHz*km)
- Especificaciones para fibra óptica multimodo optimizada para láser de 850 nm, 50/125μm.
- Especificaciones para cableado en interior/exterior.
- Especificaciones para conectores multifibra (MTP).

En la Tabla 1.4 se muestran los parámetros de rendimiento y la nueva nomenclatura de fibra óptica, donde la fibra multimodo es representada por “OM” y la fibra monomodo es representada con “OS”.

1.2.1.2 EIA/TIA-606-A

Especifica criterios de administración para la infraestructura de telecomunicaciones en edificios comerciales, proporcionando lineamientos para el etiquetado, el código de colores y la documentación básica a presentar para realizar modificaciones, ampliaciones, así como también la detección y resolución de problemas en todo el sistema de cableado estructurado.

Fibra óptica y tipo de cable[2]	Longitud de onda (nm)	Atenuación máxima (dB/km)	Ancho de banda modal overfilled mínimo del producto (MHz•km)[1]	Ancho de banda modal efectiva mínimo del produc (MHz•km)[1]
62,5/125 µm Multimodo TIA 492AAAA (OM1)	850 1300	3,5 1,5	200 500	No requerido No requerido
50/125 µm Multimodo TIA 492AAAB (OM2)	850 1300	3,5 1,5	500 500	No requerido No requerido
850 nm Optimizado para láser 50/125 µm Multimodo TIA 492AAAC (OM3)	850 1300	3,5 1,5	1500 500	2000 No requerido
850 nm Optimizado para láser 50/125 µm Multimodo TIA 492AAAD (OM4)	850 1300	3,5 1,5	3500 500	4700 No requerido
Monomodo Interior-Exterior TIA 492CAAA (OS1) TIA 492CAAB (OS2)[3]	1310 1550	0,5 0,5	N/D N/D	N/D N/D
Monomodo Planta interna TIA 492CAAA (OS1) TIA 492CAAB (OS2)[3]	1310 1550	1,0 1,0	N/D N/D	N/D N/D
Monomodo Planta externa TIA 492CAAA (OS1) TIA 492CAAB (OS2)[3]	1310 1550	0,5 0,5	N/D N/D	N/D N/D

Tabla 1.4: Parámetros de rendimiento de fibra óptica[PW9]

1.2.1.3 EIA/TIA-607

Especifica la interconectividad a los sistemas de tierra del edificio para evitar poner en peligro a los equipos y al personal frente a posibles voltajes peligrosos que puedan surgir por subidas de voltaje repentinas en la red eléctrica o por rayos que impacten cerca del cableado eléctrico o telefónico.

1.2.2 SUBSISTEMAS DEL CABLEADO ESTRUCTURADO[F4]

El Sistema de Cableado Estructurado se divide en varios subsistemas: Entrada de Servicios, Cuarto de Equipos, Cuarto de Telecomunicaciones, Cableado Vertical, Cableado Horizontal y Área de Trabajo.

1.2.2.1 Entrada de Servicios

Consiste en el punto por donde van a ser recibidas las conexiones provenientes de las empresas proveedoras de servicios, también puede contener rutas de cableado vertical a otros edificios en situaciones de campus.

Los métodos de ingreso al edificio son mediante medios subterráneos, aéreos y enterrados.

1.2.2.2 Cuarto de Equipos

El cuarto de equipo es un espacio centralizado de uso específico para equipos de conectividad que van a ser compartidos por todos los usuarios de la red. En este espacio se encuentran el campo de distribución principal (MDF), centrales telefónicas, servidores de red, consolas de monitoreo del sistema de seguridad.

Esta área debe proporcionar seguridad, iluminación, protecciones para el equipo y el personal, energía eléctrica, banco de baterías; y no debe tener una extensión menor a los 14 m^2 con opción a expandirse.

1.2.2.3 Cuarto de Telecomunicaciones

Es un área dentro del edificio exclusiva para equipos de telecomunicaciones, cuya función es la distribución del cableado horizontal en un piso o área del edificio. En este cuarto se termina el cableado horizontal y el vertical en equipos de conectividad compatibles con los medios de transmisión utilizados.

La ubicación del cuarto de telecomunicaciones debe ser lo más cerca posible al centro del área a la que se sirve.

1.2.2.4 Cableado Vertical

El subsistema de Cableado Vertical es aquel que conecta cuartos de telecomunicaciones, cuartos de equipos y entradas de servicios de la LAN, incluyendo también la interconexión entre edificios.

La topología física que se usa para la implementación del Cableado Vertical dentro de edificios es la topología tipo estrella jerárquica. En la Figura 1.9 se muestran los elementos del subsistema de Cableado Vertical, como la Conexión Cruzada Principal (MC) que representa al Cuarto de Equipos, la Conexión Cruzada Intermedia (IC) que representa a los cuartos de distribución del cableado

del edificio, la Conexión Cruzada Horizontal (HC) que representa a los cuartos de Telecomunicaciones, y la Entrada de Servicios (ER).

Los tipos de medios de transmisión que se utilizan son:

- Cableado multipar UTP y STP de 100 ohmios (categoría 3, 5E, 6 y 6A).
- Fibra óptica multimodo de 62.5/125µm y 50/125µm.
- Fibra óptica monomodo.

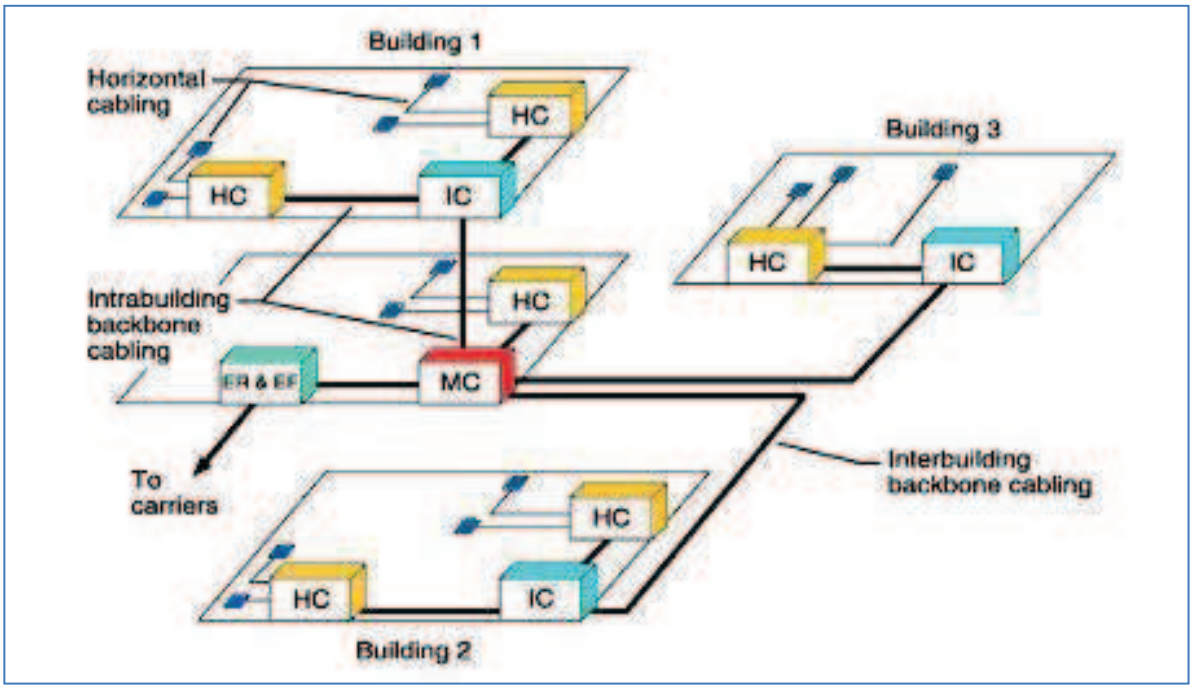


Figura 1.9: Topología Subsistema de Cableado Vertical[PW10]

1.2.2.5 Cableado Horizontal

El subsistema de Cableado Horizontal está formado por el medio de transmisión o cableado horizontal, el conector de salida de telecomunicaciones, los patch panels, patch cords[18] y racks de los cuartos de Telecomunicaciones y de Equipos. La topología física que se sigue es de tipo estrella.

Las salidas de telecomunicaciones para los cables de cuatro pares deben terminar en una interfaz de 8 posiciones, cuya distribución de pines viene dada por las normas T568A o T568B, tal como se muestra en la Figura 1.10.

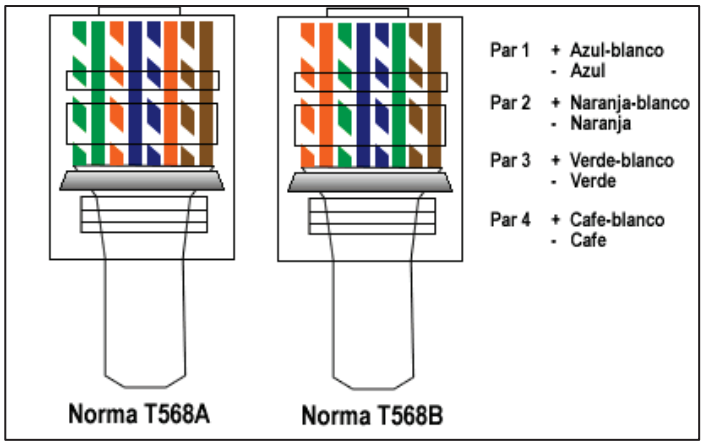


Figura 1.10: Normas T568A y T568B[PW11]

Al usar cable trenzado de cuatro pares, la distancia entre la Conexión Cruzada Horizontal que se encuentra en el Cuarto de Telecomunicaciones y la estación de trabajo no debe superar los 100 metros. En la Figura 1.11 se muestran las distancias máximas que pueden llegar a tener los patch cords del rack, equipo y el cableado fijo.

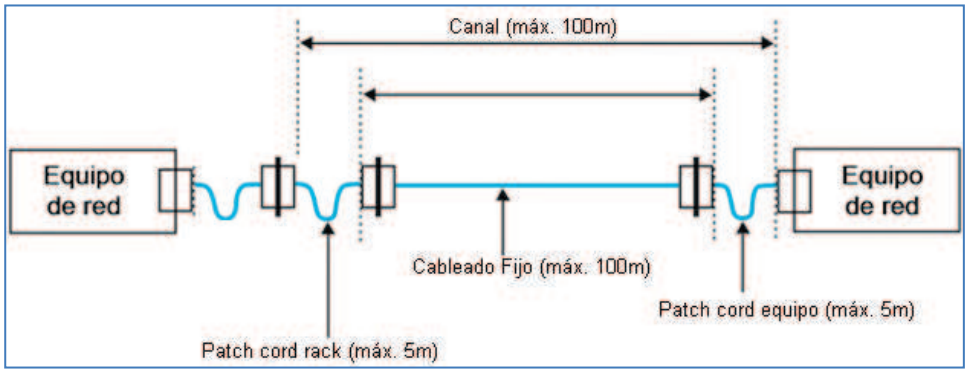


Figura 1.11: Distancias de Cableado Horizontal[PW12]

Los medios de transmisión aceptados para usar en este subsistema son:

- Cable UTP y STP de cuatro pares de 100 ohmios (categoría 3, 5E, 6 y 6A).
- Fibra óptica multimodo de 62.5/125µm y 50/125µm.
- Fibra óptica monomodo.

1.2.2.6 Área de Trabajo

El Área de Trabajo es el sitio donde el usuario se conecta a los servicios de comunicación. Está compuesto por las salidas de Telecomunicaciones, los cables

de conexión (patch cord) para los equipos de trabajo (Computadores, terminales de datos, teléfonos, etc.) y por los adaptadores, baluns, filtros, etc.

1.3 TELEFONÍA IP[P2, P3, P4]

La Telefonía IP es un servicio basado en la tecnología VoIP, que permite realizar llamadas desde redes IP, es decir, permite comunicar computadores o teléfonos a otros computadores o teléfonos de todo el mundo.

Además, la Telefonía IP tiene la ventaja de tener los servicios de la telefonía analógica, como la identificación de llamadas, servicio en espera, buzón de voz, transferencia de llamadas y filtros de llamadas; algunos de los cuales debían ser contratados a la compañía telefónica para poder utilizarlos, y que ahora son totalmente gratuitos.

Una de las características de la telefonía IP es que permite que la información de video codificada viaje junto con la información de audio dentro de los paquetes RTP, lo que le permite realizar video llamadas.

1.3.1 VOZ SOBRE IP

La Voz sobre IP (VoIP) es el conjunto de protocolos usados para enviar a través de Internet señales de voz, de manera digital dentro de paquetes de datos.

Entre las ventajas que ofrece el uso de VoIP están: el funcionar sobre las redes IP existentes, su fácil administración y mantenimiento, el uso de estándares internacionales abiertos, el uso de técnicas avanzadas de digitalización de voz que usan menos ancho de banda, y el uso de protocolos de control y priorización de tráfico.

1.3.2 FUNCIONAMIENTO DE LA TELEFONÍA IP

Para explicar el funcionamiento de la Telefonía IP se va a tomar como escenario a una conversación entre dos usuarios, mismos que se conectan a un servidor VoIP por medio de sus terminales IP.

La terminal que desea comenzar la comunicación pregunta al servidor sobre la terminal receptora por medio de un protocolo de control (SIP, H.323, etc.), el servidor devuelve como respuesta al emisor los datos de contacto del receptor (dirección IP del receptor).

Los dos terminales establecen una conexión y acuerdan el tipo de codificación a usar (G.711, G.729, GSM, H.261, H.263, etc.) para digitalizar y comprimir información analógica. La voz y el video digitalizado se encapsulan dentro de un protocolo de transporte (RTP) para ser enviados. El receptor recibe los datos y los decodifica para reproducir la información de voz y video.

1.3.3 PROTOCOLOS MULTIMEDIA

Los protocolos utilizados para la transmisión de datos multimedia sobre redes IP se dividen según las funciones que desempeñan, por lo que, se tiene protocolos de transporte y protocolos de señalización.

1.3.3.1 Protocolos de Señalización

Los protocolos de señalización son los encargados de establecer, modificar y terminar las sesiones creadas. Entre los protocolos más comúnmente usados están:

1.3.3.1.1 H.323

El estándar H.323 es una tecnología utilizada para la transmisión de audio, video y datos en redes basadas en paquetes como lo son las redes LAN, MAN, WAN e Internet.

H.323 proporciona una gran variedad de servicios, lo que, permite que sea utilizado en gran variedad de aplicaciones multimedia, destinadas a consumidores ó a negocios.

El estándar H.323 especifica cuatro tipos de componentes, que trabajando juntos proporcionan los servicios de comunicación punto a punto o punto multipunto. En la Figura 1.12 se muestran estos componentes.

Terminales.- Son los dispositivos que digitalizan y comprimen la información analógica, como la voz y el video. Los terminales pueden estar representados en hardware (teléfono IP o videoteléfono IP) o en software (softphone[19]). El objetivo principal del estándar H.323 es que exista interoperabilidad entre todos los terminales multimedia.

Figura 1.12: Estructura de red H.323[PW13]

Gatekeepers.- Su función principal es el control de llamadas y gestión del sistema de direccionamiento.

Aunque los terminales por sí solos pueden conectarse directamente, éste tipo de funcionamiento es muy limitado y difícil para los usuarios.

Todos los terminales antes de comenzar una llamada primero deben consultar con el Gatekeeper, éste otorga el permiso para que se lleve a cabo la llamada dependiendo de la cantidad de tráfico de voz que esté circulando por la red, para así evitar la saturación del sistema; además el Gatekeeper es quien realiza la traslación entre el identificador de usuario destino y su dirección IP.

Gateway.- Permite interconectar una red H.323 con una red que no lo sea. Un Gateway permitiría por ejemplo la comunicación entre un terminal H.323 y una red de circuitos conmutados como la PSTN[20].

Unidad de Control Multipunto (*MCU*).- El MCU proporciona el soporte de conferencias entre tres o más terminales H.323. El MCU administra los recursos de conferencia, negocia la codificación a usar entre los terminales para el audio y video, y además mantiene el flujo de multimedia.

Los Gatekeepers, Gateways y MCUs son componentes separados de estándar H.323 pero pueden ser implementados en un solo dispositivo.

1.3.3.1.2 SIP (Protocolo de Inicio de Señalización)

SIP es un protocolo desarrollado por la IETF (*Internet Engineering Task Force, Grupo Especial en Ingeniería de Internet*) que principalmente define la iniciación, modificación y terminación de sesiones interactivas de comunicación multimedia entre usuarios.

El Gatekeeper utilizado en H.323 es reemplazado por el SIP-Server, que tiene mejores aspectos de escalabilidad para grandes redes.

SIP es muy similar a HTTP (*Hiper Text Transfer Protocol, Protocolo de Transferencia de Hiper Texto*), y al igual que éste tiene una arquitectura cliente-servidor, en la que los procesos se basan en un intercambio de mensajes en forma de peticiones y repuestas entre el cliente y el servidor.

En la Figura 1.13 se muestran los componentes de una red que utiliza el protocolo de señalización SIP. A continuación se va a describir cuál es la función de cada uno de los componentes del protocolo SIP.

UserAgent.- Se refiere a los videoteléfonos, teléfonos, softphones y cualquier otro dispositivo que se utilice para establecer una sesión. Los agentes de usuario se comportan como clientes (UAC, *User Agent Clients*) y como servidores (UAS, *User Agent Servers*). Son UAC cuando realizan peticiones y son UAS cuando las reciben.

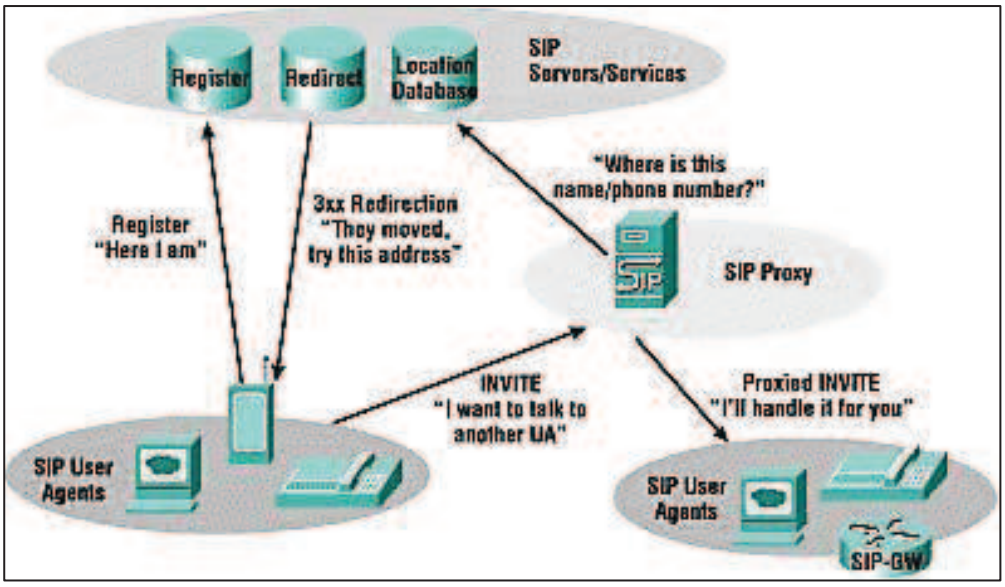


Figura 1.13: Estructura de red SIP[PW14]

Servidor Proxy.- Es el responsable del encaminamiento de los mensajes entre equipos finales. Se encarga de interpretar y modificar si es que fuera necesario, la petición que recibe para reenviarla hacia su destino.

Servidor de Redirección.- Es aquel que responde a peticiones de un UAC con la dirección del destino o de otro servidor que lo acerque al destino.

Servidor de Localización.- Suministra la información sobre la posible localización del destinatario de la llamada.

Servidor de Registro.- Aquí se realiza la asociación entre la dirección física que tiene una terminal con su dirección lógica de usuario SIP. Una dirección lógica del protocolo SIP es de la forma *usuario@dominio*. La dirección física (denominada "dirección de contacto") es dependiente del lugar en donde el usuario está conectado (de su dirección IP).

Cuando el terminal inicia su funcionamiento el agente de usuario SIP que reside en dicho terminal envía una petición registro hacia el Servidor de Registro, informando a qué dirección física debe asociarse la dirección lógica del usuario, entonces, el servidor realiza dicha asociación. Esta asociación tiene un período de vigencia y si no es renovada, caduca. También puede terminarse mediante el proceso de borrado del registro.

1.3.3.2 Protocolos de Transporte

1.3.3.2.1 RTP (Real Transfer Protocol)

Es un protocolo de la capa sesión desarrollado por la IETF encargado de transmitir la información de audio y video en tiempo real a través de Internet. La función básica de RTP es multiplexar varios flujos de datos en tiempo real en un solo flujo de paquetes UDP, pudiéndose enviar tanto a un solo destino (unicast[21]) o múltiples destinos (multicast).

Los paquetes RTP tienen un número de secuencia que será útil para que la aplicación conozca si ha fallado algún paquete o no en la transmisión, si es que ha fallado alguno, la mejor opción es la interpolación de los datos.

El protocolo RTP no tiene un control de flujo o de errores, paquetes de confirmación ni de solicitud de transmisión. RTP está formado conjuntamente con el protocolo RTCP (*RTP Control Protocol*), cuya función principal es proporcionar mecanismos de realimentación para informar sobre la calidad en la distribución de los datos.

1.3.3.2.2 RTCP (Real Transfer Control Protocol)

El protocolo RTCP es complementario a RTP y le brinda a éste un mecanismo de control. RTCP utiliza el protocolo UDP en la capa de transporte, con el número de puerto adyacente al que ocupa RTP.

El protocolo RTCP se basa en la periódica transmisión de paquetes de control a todos los participantes en sesión, ofreciéndole al emisor información sobre la calidad de los datos distribuidos.

1.3.4 CODECS[P2, P3]

Los estándares de codificación o también llamados Codecs (*codificador / decodificador*), son los que especifican la manera en que transformarán las señales de audio y video para que sean transmitidas sobre redes basadas en paquetes. Los codecs utilizados para en aplicaciones de voz son llamados también “vocoders”.

Para la utilización de algunos de los codecs es necesaria la adquisición de una licencia para su uso comercial ya que están protegidos por derechos de autor; mientras que otros como el códec G.711 son de libre uso. En la Tabla 1.5 se muestra los parámetros de Bit rate[22], tamaño de trama y paquetes de voz por trama de los códecs de voz más utilizados.

Códec	**Bit rate**	**Sample Size**	**Frame Size** [Bytes]	**Sample/Frame**	**MOS (***Mean Opinion Score***)/5**	**Requiere Licencia**
G.711	64 Kbps	20 ms	160	1	4.1	No
G.723.1	5.3/6.3 Kbps	30 ms	24	1	3.9	Sí
G.726	32 Kbps	20 ms	80	1	3.85	No
G.728	16 Kbps	10 ms	10	4	3.61	Sí
G.729A	8 Kbps	10 ms	10	2	3.92	Sí

Tabla 1.5: Códecs de voz más utilizados en la telefonía IP[PW15]

1.3.4.1 G.711

G.711 es un estándar de codificación de alta tasa de bit (64 Kbps) desarrollado por la ITU-T. El usar el codec G.711 para voz sobre IP otorga la mejor calidad de voz, ya que no utiliza compresión, por lo que, es el mismo codec utilizado para la PSTN, además, no tiene latencia, pues no necesita de un procesamiento para descomprimir la información. Sin embargo, ésta forma de funcionamiento aumenta el consumo de ancho de banda.

1.3.4.2 G.723.1

El codec G.723.1 es un codec que requiere de la compra de una licencia para su uso. El nombre oficial del codec es *Codificador de voz de doble velocidad para Transmisiones en Comunicaciones Multimedia,* pues puede funcionar a un bit rate de 5.3 y 6.3 Kbps y es por esto que este codec es especialmente utilizado para aplicaciones de VoIP donde el ancho de banda es limitado. El tiempo de procesamiento de codificación puede llegar a los 37.5ms, y los tonos DMTF no pueden ser transmitidos usando este codec.

1.3.4.3 G.726

G.726 es un estándar desarrollado por ITU-T para la transmisión de voz codificada a velocidades de 16, 24, 32 y 40 Kbps usando ADPCM (*Modulación Adaptiva Diferencial por Impulso Codificado*).

1.3.4.4 G.728

Este codec puede funcionar a un bit rate 16 Kbps, y con un tiempo de demora de codificación corto de entre 0.62 ms a 2.5 ms, y si se lo compara con G.726 se puede ver que otorga la misma calidad de voz pero con un bit rate igual a la mitad. Este codec no puede usarse para la transmisión de melodías o música debido a que su algoritmo de codificación usa modelos de predicción de formas de onda específicas solo para la voz.

1.3.4.5 G.729A

Estándar desarrollado por la ITU-T que posee un algoritmo de codificación de voz de 8 Kbps usando CS-ACELP (*Predicción Lineal de Código Algebraico Activado en Estructura Conjugada*).

G.729 es un codec muy utilizado para sistemas de transmisión de voz sobre IP debido a su gran tasa de compresión que disminuye el ancho de banda ocupado, mientras mantiene una buena calidad de voz. Una limitación de este codec es que solo puede transmitir voz y no puede transmitir de forma confiable los tonos DMTF.

1.4 VIDEO SOBRE IP[P5]

El Video sobre IP consiste en la transmisión de imágenes y video en tiempo real a través de redes IP como por ejemplo Internet. Las aplicaciones que tienen el Video sobre IP son videoconferencias, televisión sobre IP y video vigilancia.

1.4.1 FUNCIONAMIENTO DEL VIDEO SOBRE IP

Las diferentes aplicaciones de video sobre IP funcionan de manera distinta, por

ejemplo la transmisión de televisión sobre IP utiliza el Broadcast de Video, mientras que la videoconferencia es un intercambio entre dos partes que envían su propia señal de video.

El Broadcast de video consiste en la transmisión de un archivo de video a todos los usuarios de la red, los mismos que solo pueden mostrar el video más no pueden interactuar con él o enviar su propia señal de video. La transmisión de video broadcast puede ser de forma Unicast o Multicast. En la transmisión Unicast el servidor de video transmite un archivo de video para cada terminal cliente, lo que puede sobrecargar la red; mientras que en la transmisión Multicast un solo archivo de video se emite y un grupo de usuarios clientes pueden mirarlo simultáneamente.

Los protocolos multimedia que se utilizan para la trasmisión de video sobre IP son los mismos que se utilizan para el transporte de la voz sobre IP, pero además existen los protocolos RSVP (*Resource Reservation Protocol*) y RTSP (*Real Time Streaming Protocol*) usados también para la transmisión de flujos de datos multimedia.

1.4.1.1 RSVP (*Resource Reservation Protocol*)

Protocolo usado para la reservación de recursos de red (Ancho de Banda) con el objetivo de dar calidad de servicio a la transmisión de los datos multimedia. Para identificar a un flujo de datos multimedia RSVP utiliza la dirección destino, el protocolo de identificación y, opcionalmente, el puerto de destino.

1.4.1.2 RTSP (*Real Time Streaming Protocol*)

RTSP es un protocolo usado para establecer y controlar sesiones de streaming multimedia. Entre las características de RTSP están: controlar los dispositivos (cámara IP: zoom, inclinación, etc.), sincronizar la presentación entre varios servidores multimedia y soporta cualquier descriptor de sesión.

Las funcionalidades principales de RSTP son:

- **Petición de medios:** para ello primero pide al servidor multimedia una descripción de presentación, luego verifica si es una sesión Unicast o Multicast, en caso de ser Multicast permite escoger una dirección IP.
- **Participación en conferencias:** Se invita a un servidor a ser parte de una conferencia o solo a grabar parte de la misma.
- **Streaming en vivo:** puede agregar contenido multimedia dentro de una misma sesión.
- **Control por cada streaming:** Permite tener control sobre cada tipo de contenedor multimedia o por cada servidor multimedia.

1.4.2 VIDEO VIGILANCIA IP[T1]

Los sistemas de video vigilancia IP poseen las ventajas de ser flexibles, escalables, rápidos de implementar, fáciles de configurar y de administrar; esto se debe a varios factores como el que las cámaras IP que se utilizan en este tipo de sistemas pueden utilizar la infraestructura de la red de datos existente lo que agiliza el proceso de la instalación física; además estas cámaras son fácilmente configurables por medio de sus interfaces Web y los videos capturados por ellas se almacenan digitalmente lo que ayuda en la administración de los recursos necesarios para el almacenamiento de los mismos.

1.4.2.1 Cámaras IP

La cámara IP es un dispositivo que captura imágenes y video en formato análogo, los digitaliza y los comprime para luego transmitirlos por medio de una red IP. Las cámaras IP pueden estar conectadas de manera cableada o inalámbricamente, y pueden capturar video en condiciones de luz diurna o nocturna.

Las cámaras IP vienen con un servidor Web al cual se puede acceder localmente o de forma remota para realizar configuraciones o visualizar el video que la cámara está capturando en ese instante.

1.4.2.2 Codecs

Los codecs que las cámaras IP utilizan permiten ajustar el tamaño de los archivos que van a ser transmitidos por medio de la red o que van a ser almacenados;

dependiendo del códec utilizado será el ancho de banda y la calidad que el video tendrá después de la compresión.

1.4.2.2.1 H.261

H.261 es un estándar de codificación de video diseñado para la transmisión sobre la Red Digital de Servicios Integrados (*ISDN*) a velocidades múltiplos de 64 Kbps. El algoritmo de codificación fue creado para ser capaz de operar a velocidades entre los 40 Kbps a los 2 Mbps.

H.261 fue el primer estándar de codificación de video digital, en su diseño se basaron los demás codificadores de video posteriores.

1.4.2.2.2 H.263

H.263 es un codec de video diseñado por la ITU-T como una solución de codificación de baja tasa de bits (bajo 64 Kbps) para videoconferencias. Fue diseñado para ser utilizado en sistemas basados en el estándar H.324[23], pero ha sido usado en sistemas como H.323, H.320[24], RSTP[25] y SIP.

H.263 es una mejora del protocolo H.261 y los estándares MPEG-1 y MPEG-2. La última versión de este codec es la número 3 o H.263++.

1.4.2.2.3 MJPEG

El protocolo Motion JPEG o MJPEG que funciona comprimiendo cada cuadro de video como si fuera una imagen JPEG independiente, lo que causa que su tasa de compresión sea baja en comparación con otros codecs, por esta razón para mantener bajas la tasa de bits de transmisión y el tamaño del video resultante se puede configurar dentro de la cámara IP una tasa de captura de 15 a 20 cuadros por segundo y un tamaño de imagen máximo de 640x480 pixeles. Este tipo de transmisión de datos es el más soportado por las cámaras IP debido a su sencillez.

1.4.2.2.4 MPEG-4

Método de compresión para audio y video definido como un estándar por la ISO/ IEC MPEG (*Moving Picture Experts Group*). MPEG-4 está formado por varios

estándares llamados *Partes*, el estándar al cual se le llama comúnmente MPEG-4 corresponde al estándar MPEG-4 parte 2.

La norma MPEG-4 define un conjunto de Perfiles y Niveles que van a especificar los subconjuntos de herramientas apropiadas para cada tipo de aplicación, como por ejemplo transmisiones de películas o trasmisiones para teléfonos móviles.

En el mercado se usan principalmente dos Perfiles MPEG-4:

- El Perfil Simple que es usado para tener un menor tiempo de procesamiento y menor compresión, usado para software de codificación en tiempo real, redes móviles y video telefonía. Posee una tasa de bits desde 10 Kbps.
- El Perfil Avanzado que proporciona un gran nivel de compresión. Este perfil es usado en ambientes de Broadcast, Unicast y Streaming de video. Soporta una gran cantidad de tasas de bits, en 56 Kbps para ancho de banda limitado, 300 Kbps – 750 Kbps para transmisión en banda ancha y 1 Mbps -8 Mbps para transmisión de video en alta definición.

1.5 SOFTWARE LIBRE Y LICENCIAS GPL[PW16, PW17]

El término Software Libre según la FSF (*Free Software Foundation*) se refiere a la libertad que tienen los usuarios que han adquirido un software de ejecutar éste código, copiarlo, distribuirlo, estudiarlo, modificarlo y distribuirlo modificado, sin tener que pagar o pedir permiso al programador del software para ello.

Estas libertades están totalmente prohibidas en el software con licencias propietarias o cerradas, pues en esos casos el costo del producto solo permite el uso del software, más no la modificación y distribución del mismo.

1.5.1 LICENCIAS GPL

La licencia GPL (*General Public License*) fue desarrollada por la Free Software Foundation. Esta licencia permite la instalación y uso de un programa GPL en un ordenador o tantos como se desee, además, se permite la modificación del mismo

para adaptarlo a las necesidades del usuario y distribuirlo de forma original o ya modificado.

La distribución puede ser por medio de su venta o gratuitamente, con la única obligación de entregar siempre el código fuente[26] junto al código binario[27] del software, para permitir que los usuarios que lo adquieran puedan estudiar el programa.

Utilizando este tipo de licencias se pueden encontrar a sistemas operativos tan confiables como RedHat, CentOS y Ubuntu; mismos que son utilizados principalmente para la instalación de servidores de aplicaciones que también cuentan con la licencia GPL, y que han demostrado proveer la robustez y desarrollo necesario para ser utilizados en ambientes empresariales de manera sobresaliente.

Es por esta confiabilidad y robustez que la utilización de software libre para soluciones en redes corporativas y gubernamentales ha ido creciendo rápidamente en el país. Por estas razones se ha optado en la utilización de programas de software libre para la implementación de los servicios de red que se plantean en este proyecto.

1.5.2 LICENCIAS BSD

La licencia BSD es un tipo de licencia extremadamente simple que fue creada por la Universidad de California en Berkley, Estados Unidos, y fue usada por primera vez para el sistema operativo UNIX BSD que era una versión mejorada del sistema operativo original UNIX.

Las licencias BSD (*Berkeley Software Distribution*) son licencias de software libre muy similar a las licencias GPL pero con la diferencia de que los programas bajo esta licencia pueden ser utilizados dentro de programas propietarios.

La licencia BSD solo posee dos restricciones: la primera se refiere a que solo se puede pretender que el software es propio si es que se modificó de alguna manera el software original; y la segunda restricción es que el desarrollador del

software no es responsable si éste no funciona de la manera adecuada o deseada.

CAPÍTULO II

ANÁLISIS DE LA RED Y DETERMINACIÓN DE REQUERIMIENTOS

2.1 ANTECEDENTES

El Colegio Fernando Daquilema (CFD), es una institución educativa fiscal de la ciudad de Riobamba provincia de Chimborazo. El CFD cuenta con 1022 alumnos, 56 docentes y 9 administrativos. Su instalación física posee 27 aulas de clase, 2 salas de computación, 1 salón de profesores, 1 salón de actos, 1 biblioteca, 1 Salón de Reuniones, 7 oficinas administrativas, 1 Lab. de Física, 1 Lab. de Química, 1 Lab. de Biología, 1 consultorio de Enfermería y 1 consultorio de Odontología.

La infraestructura de comunicaciones actual del CFD está formada por 54 computadoras, 3 switches no administrables, 2 Access Points y un servidor marca Hewlett-Packard. El principal servicio que se brinda en la red es el acceso a Internet, para lo cual, se utiliza el Access Point D-Link DIR-655 como gateway permitiendo a todas las computadoras en red tener acceso a Internet.

Al ser una institución pública, su infraestructura de comunicaciones debe seguir un lineamiento de Software Libre según lo establecido en el Decreto Ejecutivo 1014 que prioriza el uso de Software Libre sobre las soluciones propietarias, por lo que, es necesario buscar soluciones basadas en Software Libre que otorguen las mismas o mejores prestaciones que las soluciones con licencias privadas.

El servicio de Internet es provisto por la Corporación Nacional de Telecomunicaciones (CNT) mediante una conexión por fibra óptica con una capacidad de 2 Mbps.

2.2 ESTRUCTURA ORGANIZACIONAL

En la Figura 2.1 se muestra la estructura organizacional del CFD, que se sustenta en el Reglamento de la Ley de Educación Intercultural.

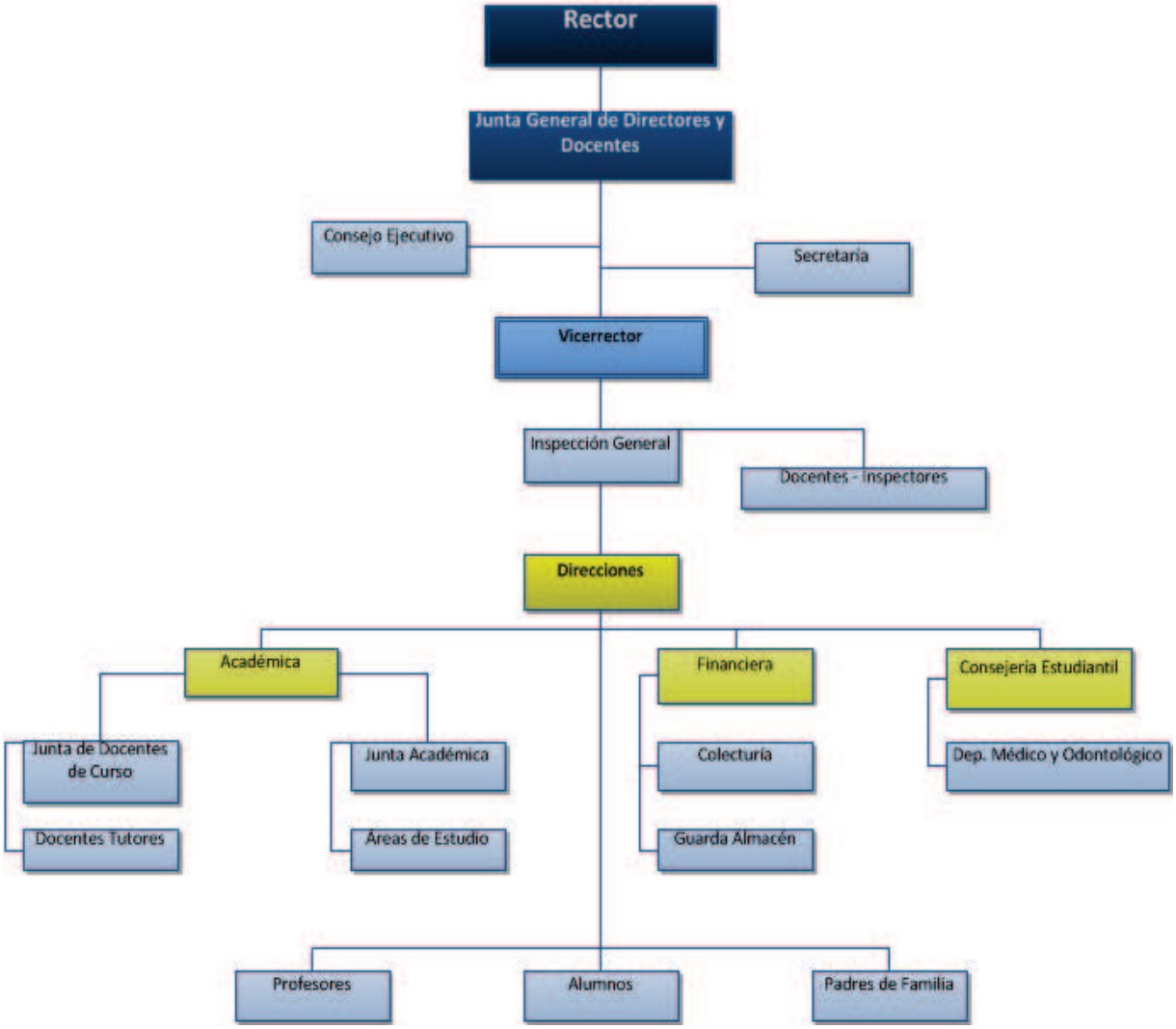


Figura 2.1: Estructura Orgánico-Funcional del Colegio Fernando Daquilema

El CFD al ser una institución educativa, su objetivo principal es el desarrollo académico y personal de sus estudiantes, para lo cual, posee una estructura organizacional que permite realizar la planificación, seguimiento y apoyo a los estudiantes, mediante sus direcciones Académica, Financiera y Consejería Estudiantil.

2.3 ANÁLISIS DE LA INFRAESTRUCTURA DE COMUNICACIONES

El análisis abarcará la realidad interna de los servicios de voz y datos del CFD, sin profundizar en las configuraciones y funcionamiento de los equipos dejados por la empresa CNT para la conexión de Internet.

2.3.1 DETERMINACIÓN DEL NÚMERO DE USUARIOS

El personal administrativo del CFD para cumplir con su trabajo, está dotado con un computador con acceso a Internet y un teléfono analógico. La institución también brinda el acceso inalámbrico a Internet para los docentes y administrativos dentro de las áreas de Biblioteca, Salón de Reuniones, Rectorado, Vicerrectorado, Secretaría y Colecturía, además para éstas oficinas administrativas excepto para Rectorado las computadoras de escritorio usan cableado UTP cat. 5E para su conexión a la red. La conexión de uno de laboratorios de computación y el laboratorio de Física también se realiza mediante cableado UTP cat. 5E; estas dos áreas también tienen acceso a Internet.

El segundo laboratorio de computación, los laboratorios de Química, Biología, el Salón de Actos, las aulas y, los consultorios de Enfermería y Odontología no están conectados a la red por ningún medio.

En la Tabla 2.1 se muestra el número de usuarios que se conectan por cable UTP a la red del colegio.

USUARIOS DE RED	
DEPARTAMENTO	**No. USUARIOS**
Vicerrectorado	1
Secretaría	2
Colecturía	1
Inspección General	1
Orientación Vocacional	1
Bodega	1
Laboratorio Computación 2	22
Laboratorio Física	1
Biblioteca	4
Total	34

Tabla 2.1: Total de usuarios actuales de la infraestructura de red del CFD

2.3.2 CABLEADO ESTRUCTURADO Y EQUIPOS DE CONECTIVIDAD

2.3.2.1 Descripción de la Distribución Física de la Red de Datos

En la Figura 2.2 se muestra la red conmutada del CFD y la manera en que están conectadas las computadoras a la red de la institución.

En el Bloque A se encuentra el Cuarto de Telecomunicaciones de la Institución, en el que se hallan un servidor HP Proliant DL160, un router inalámbrico D-Link DIR-655 y los equipos del proveedor de servicio de Internet (ISP). El servidor HP Proliant no es utilizado para ningún servicio de red ni tampoco está conectado a la LAN del colegio, pues el sistema operativo Windows 2008 Server que tiene instalado es de una versión de prueba que tiene restricciones en el número de estaciones de trabajo a las que se puede ofrecer los servicios de red como DHCP, DNS y directorio, haciendo que éste equipo no pueda ser de utilidad; como una solución temporal se utiliza el router inalámbrico D-Link DIR-655 para conectar la red entera, proporcionando el servicio de DHCP, DNS y traducción de direcciones de red (NAT) a todos los clientes en la red del colegio, y así todos ellos puedan acceder a Internet por medio este equipo. En este edificio también se encuentran: las oficinas de Rectorado, Vicerrectorado, Secretaría y Colecturía que cuentan con 4 computadores; la Biblioteca que posee 4 computadores y el Salón de Reuniones que no posee ninguna estación de trabajo.

El router inalámbrico D-Link DIR-655, los 4 computadores administrativos y los 4 computadores de la Biblioteca se encuentran conectados al switch NEXXT No.1 (24 puertos 100 Mbps) por medio de cableado tendido en el Bloque A de manera artesanal.

En el Bloque B se encuentran dos laboratorios de computación con 20 y 22 computadoras en cada uno respectivamente y 1 switch NEXXT No. 2 (24 puertos 100 Mbps) no administrable ubicado en el Laboratorio No. 2. Las computadoras dentro del laboratorio de computación No.1 del Bloque B no poseen ninguna clase de conexión en red; y solo en el laboratorio No. 2 existe el cableado horizontal para conectar sus computadoras con el switch NEXXT No. 2. Además, también existe un Access Point (AP D-Link DWL - 2100) que se conecta al switch NEXXT

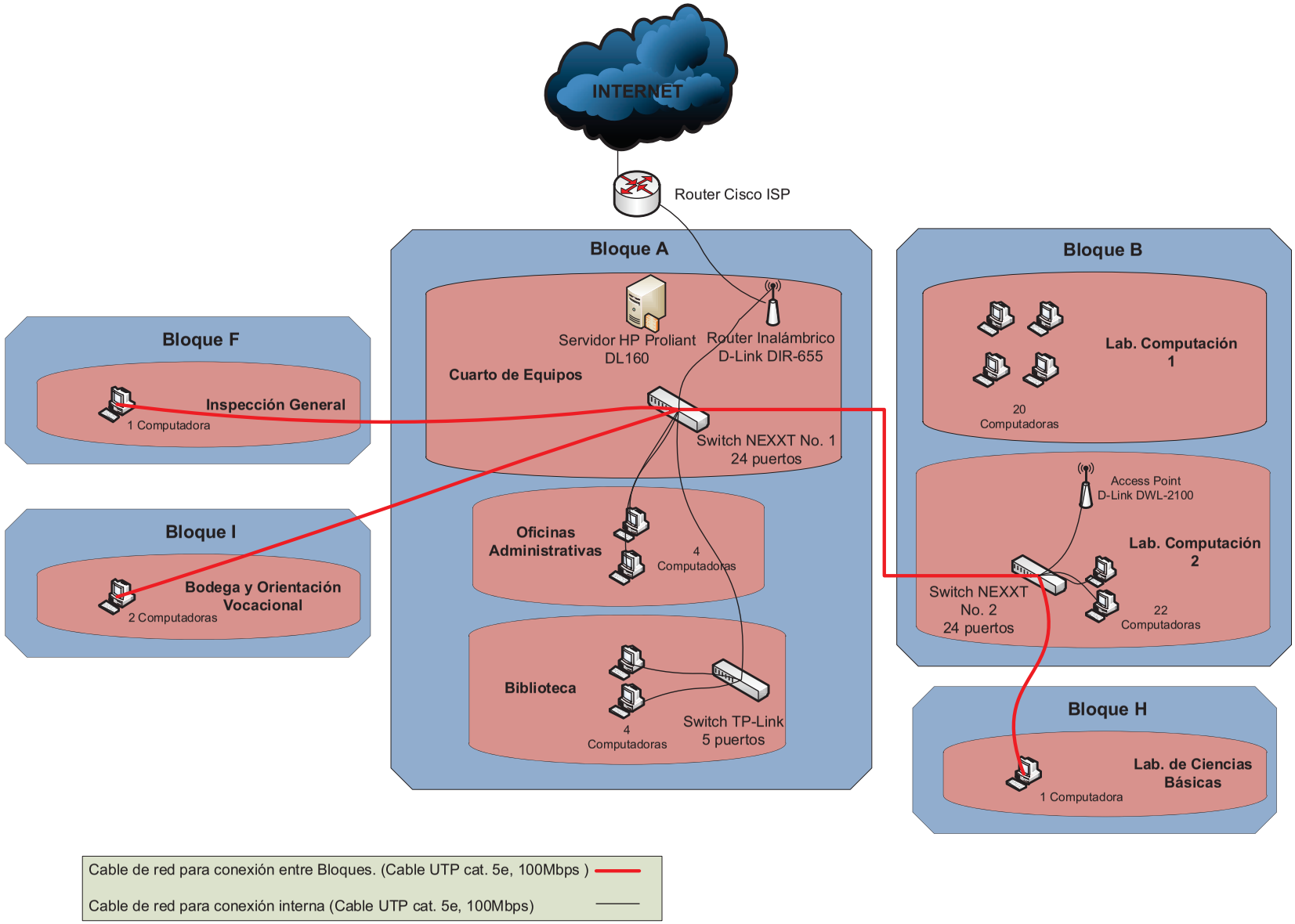


Figura 2.2: Esquema de red actual del CFD

No. 2 para brindar Internet inalámbrico a docentes y administrativos en las áreas de Rectorado, Vicerrectorado, Salón de Reuniones, Secretaría, Colecturía, y Biblioteca.

En el laboratorio de Física ubicado en el Bloque H existe una computadora que está conectada con el switch No. 2 que se encuentra en el Bloque B, mediante cableado UTP cat. 5E que se extiende a la intemperie.

Para la conexión de la computadora de Inspección General que se encuentra dentro del Bloque F se usa un cable UTP cat. 5E que se enlaza al switch NEXXT No. 1; este cable se extiende sin ninguna protección sobre la parte exterior del Bloque A.

Para el Bloque I se extiende cableado UTP cat. 5E para la conexión a la red de las 2 computadoras de Orientación Vocacional y Bodega que se encuentran. Los consultorios de Enfermería y Odontología que también se encuentran dentro de este Bloque no están conectados a la red ni de manera inalámbrica ni cableada.

2.3.2.1 Análisis del Cableado Estructurado

Una vez hecha una descripción general sobre la situación actual de la red del CFD se procederá a realizar un análisis más detallado sobre el estado del cableado estructurado en las zonas en las que actualmente se tiene tendido cableado de red, zonas tales como: el laboratorio de computación No. 2, las oficinas administrativas, el cuarto de equipos y los puntos de red de los Bloques F, H e I.

2.3.2.1.1 Cuarto de Equipos

El Cuarto de Equipos está ubicado junto a la oficina de Colecturía dentro del Bloque A. Este cuarto cuenta con múltiples ventanas, algunas de las cuales permanecen permanentemente abiertas; además esta área sirve como depósito de documentos y archivos antiguos del colegio, es por ello que existe mucho polvo en el ambiente que afectará a los dispositivos de red que funcionen en este espacio.

Para la canalización del cableado de backbone, cableado horizontal o el cableado de acometida de los servicios de telecomunicaciones no se utilizan canaletas, tuberías o bandejas de cable, sino que se utilizan las aberturas de las ventanas para que por el exterior de la edificación el cableado UTP se extienda hasta llegar a las estaciones de trabajo que necesitan conexión a la red.

En cuanto al montaje de los equipos de red y de las conexiones a los mismos, se debe aclarar que no se posee los racks, patch panels, ni bandejas de cable que son un requisito para tener un Cuarto de Equipos que cumpla con las normas de cableado estructurado. El CFD en su Cuarto de Equipos solo posee un rack abierto que fue instalado por el ISP al momento de la contratación del servicio de Internet y que es aprovechado por el colegio para el montaje del switch NEXXT No 1, mientras que el servidor HP se encuentra ubicado y sin funcionar sobre un escritorio pues no es posible instalarlo en el rack abierto, ya que el largo del servidor es mucho mayor al espacio que existe entre el rack abierto y la pared que se encuentra tras él.

Las conexiones del cableado a los dispositivos de red activos se realizan de manera directa, es decir el cableado horizontal y vertical se conectan directamente al switch NEXXT No.1 pues no existen patch panels para tener conexiones cruzadas; también se debe especificar que el cableado no se encuentra organizado ni etiquetado por lo que es muy difícil distinguir a un punto de red de otro. En la Figura 2.3 se puede observar la forma en que se encuentran las conexiones del cableado horizontal en los switches utilizados en la red del colegio.

Figura 2.3: Conexión de cableado al Switch de Acceso NEXXT

Las condiciones de seguridad del Cuarto de Equipos son deficientes pues no existe ninguna medida para contrarrestar incendios, su seguridad física solo está protegida mediante una puerta de madera, la instalación eléctrica de este cuarto es artesanal y en épocas lluviosas existen goteras, por lo que es posible que puedan ocasionarse cortocircuitos.

2.3.2.1.2 Oficinas y Biblioteca

Las oficinas de Vicerrectorado, Secretaría y Colecturía, y, el área de Biblioteca se encuentran en el primer piso del Bloque A y sus puntos de red están conectados al switch NEXXT No.1 que está dentro del Cuarto de Equipos siguiendo una topología física en estrella. Todo el cableado utilizado de esta zona es UTP cat. 5E que fue ponchado de manera artesanal por el administrador de la red de la institución. La velocidad de todas las conexiones es de 100 Mbps.

El tendido del cable en esta edificación no sigue ninguna norma de cableado estructurado, pues no se utiliza ningún tipo de canalización para el cable, no se tiene cajas de revisión, no se etiqueta el cable y no posee faceplates[28] para las salidas de telecomunicaciones. En la Figura 2.4 se puede observar cómo el cableado horizontal se conecta directamente con las estaciones de trabajo obviando completamente el uso de faceplates y etiquetado de los puntos de red.

Figura 2.4: Conexión de cableado horizontal a las estaciones de trabajo

2.3.2.1.3 Laboratorios de Computación

De los dos laboratorios de computación que posee el colegio solo el laboratorio No. 2 tiene cableado de red tendido para la conexión de las computadoras presentes en esta aula; el laboratorio de computación No. 1 no posee conectividad pues no tiene cableado de red tendido ni ninguna otra forma para que sus computadores se conecten a la red.

La manera en que se encuentra tendido el cableado en el laboratorio de computación No. 2 no cumple con ninguna de las condiciones que exigen las normas de cableado estructurado, lo que causa dificultades al momento de identificar las conexiones de cada una de las computadoras del laboratorio, pues no existe un etiquetamiento apropiado, ni se utilizan faceplates para la salida de telecomunicaciones de cada punto de red. En la Figura 2.5 se puede observar cómo el cableado horizontal se extiende por medio de canaletas plásticas que no se encuentran sujetas al suelo y también se nota la ausencia de faceplates para las salidas de telecomunicaciones de los puntos de red.

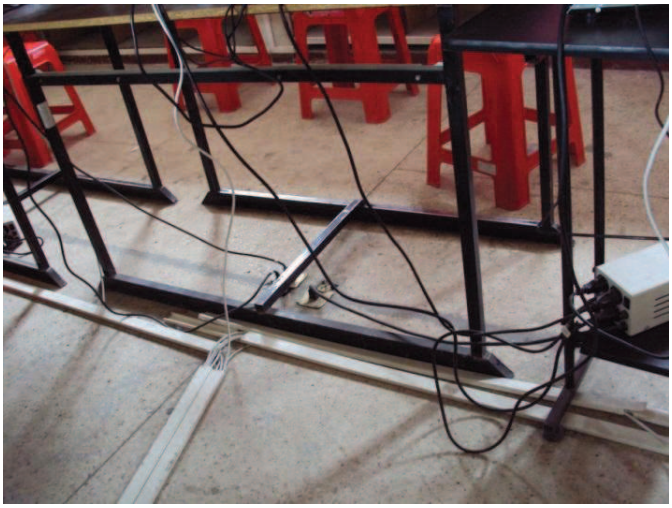


Figura 2.5: Tendido de cableado horizontal por medio de canaletas

Además en el laboratorio No. 2 se encuentra funcionando el switch NEXXT No.2, al cual se conectan todos los puntos de red de este laboratorio; este switch se encuentra funcionando sobre un escritorio de esta aula ya que no existe un rack para su instalación apropiada, esto junto con la forma en la que está tendido el cableado causa problemas de funcionamiento en la red debido a tropiezos con el cableado, desconexión del cable de red en el switch y en las computadoras, lazos

de conmutación por errores de conexión del cableado por falta etiquetas de identificación, y avería de los cables de red.

Figura 2.6: Tendido de cableado horizontal sin canaletas

En la Figura 2.6 se muestra el conjunto de cables de red que se extienden directamente por el suelo de forma desprolija, sin etiquetas de identificación, sin ninguna clase de organizadores y con las conexiones al switch expuestas a ser manipuladas por personas no autorizadas.

El cableado de Backbone también se encuentra tendido de forma artesanal, usando canaletas para cruzar una distancia de 15m entre las edificaciones A y B de la institución, tal como se muestra en la Figura 2.7. Todo el cableado utilizado en la red LAN es de tipo UTP categoría 5E.

Figura 2.7: Tendido del cableado por encima del techo del Bloque A

2.3.2.1.4 Puntos de red de los Bloques F e I

Los puntos de red de los Bloques F e I son utilizados por personal administrativo de la institución y están conectados al switch NEXXT No.1 que se encuentra en Cuarto de Equipos en el Bloque A. Para el tendido del cableado de red hasta estos otros bloques se sale por medio de las ventanas del Cuarto de Equipos y se extienden el cable sobre el techo del Bloque A.

Al llegar a las oficinas de los distintos bloques se ingresa el cable por medio de las ventanas de las mismas. En la Figura 2.8 se puede ver como ingresa el cable a la oficina de Inspección General en el Bloque F, y en la Figura 2.9 se observa como de la misma manera el cable ingresa a la oficina de Orientación Vocacional y a la Bodega que están ubicadas en el Bloque I.

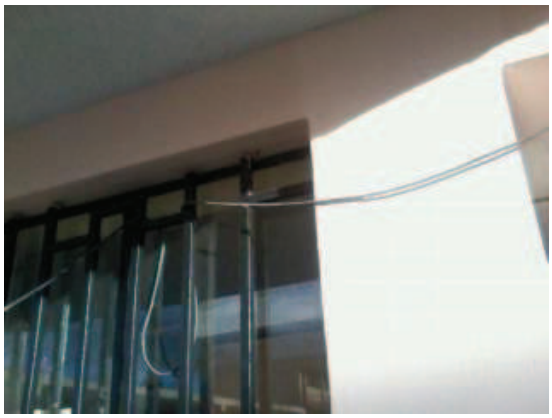


Figura 2.8: Ingreso del cable de red a la oficina de Inspección General

Figura 2.9: Ingreso del cable de red a las oficinas O. Vocacional (1er piso) y Bodega (2do piso)

2.3.2.1.5 Laboratorio de Física - Bloque H

En el laboratorio de Física en el Bloque H, existe una computadora que es utilizada por los profesores de Física y Matemáticas del CFD. Para dar conectividad a esta computadora está tendido un cable de red UTP cat. 5E desde el switch NEXXT No. 2 que está ubicado en el laboratorio de computación No.2, éste cable se extiende de forma aérea utilizando como punto de fijación a un poste ubicado en el patio de la institución permitiendo al cable de red llegar hasta el laboratorio de Ciencias Básicas ubicado al otro extremo del patio. En la Figura 2.10 se observa como el cable de red se sujeta al poste ubicado en el patio del colegio.

Figura 2.10: Tendido de cable de red de manera aérea

La forma en la que sale de una aula a otra el cable de red, es a través de las ventanas de cada aula debido a que no existe los ductos o canalizaciones adecuadas para ello; además por la forma en la que el cable está tendido se somete al cable UTP a soportar estrés físico para el que no fue diseñado. Los laboratorios de Química, Biología y el Salón de Profesores que también se ubican dentro del Bloque H, no poseen conexión con la LAN por ningún medio.

2.3.2.2 Análisis de los Equipos Activos de la red del CFD

2.3.2.2.1 Estaciones de Trabajo y Periféricos

Las estaciones de trabajo que existen en el CFD son de diferentes modelos y capacidades, pues, se han ido adquiriendo de manera paulatina durante varios

años, y muchos de ellos cumplen con las características apropiadas para el desarrollo de las actividades de los estudiantes y el personal administrativo.

Las estaciones de trabajo ubicadas en el área de la Biblioteca son de menores características y deberían ser reemplazadas por modelos de mejores capacidades ya que actualmente estas máquinas no permiten funcionar de manera fluida los programas como el editor de texto o el navegador web y peor aún si se utilizan las dos aplicaciones a la vez.

El equipamiento tecnológico con el que cuenta el CFD es:

- 42 computadoras con procesadores Intel Pentium Dual-Core usadas por los 2 laboratorios de computación.
- 7 computadoras utilizadas por personal administrativo con procesadores Intel Core 2 Duo.
- 4 computadores utilizados en la Biblioteca y en el laboratorio de Ciencias Básicas con procesadores Intel Celeron.
- Se cuenta con 2 proyectores (EPSON H309A) utilizados principalmente por los docentes para aquellas clases que lo requieran.
- En secretaría existen 1 copiadora-impresora a Blanco-Negro (Canon ImageRunner 1025) y 1 impresora a Blanco y Negro/Color(HP- P2015), ninguna de estas impresoras tiene la funcionalidad para conectarse en red.
- En el Laboratorio No. 1 existe una impresora a Blanco-Negro/Color (Samsung CLP-325W) utilizada para las impresiones ocasionales de docentes y exámenes de la asignatura de computación; esta impresora no posee puerto para su conexión en red.
- Todas las computadoras excepto aquellas ubicadas en Biblioteca se encuentran conectadas a reguladores de voltaje (ALTEK AVR-1600D y KLIP K-VR1200).

La información detallada sobre las características técnicas de los equipos anteriormente mencionados se encuentra en el Anexo 1.

2.3.2.2.2 Equipos de Red Activos

Los equipos de conectividad con los que cuenta el CFD son de características básicas y de diferentes fabricantes, pues para su adquisición solo se pensó en la necesidad de brindar servicio de Internet a las oficinas y laboratorios de computación, sin prever que en el futuro se puedan ofrecer más servicios como la telefonía IP y video sobre IP.

Para la conexión de la LAN de la institución educativa hacia Internet la Corporación Nacional de Telecomunicaciones (CNT) instaló un Router Cisco y un conversor de Fibra Óptica a Fast Ethernet, por lo que, no fue necesaria la compra de equipos extras por parte de CFD para esta conexión.

Los equipos de conectividad con que cuenta el CFD son:

- Switches NEXXT NW223NXT54 de 24 puertos no administrables
- 1 Access Point (D-Link DWL-2100AP)
- 1 router inalámbrico (D-Link DIR-655)
- 1 switch TP Link de 5 puertos no administrable
- 1 Servidor Hewlett-Packard Proliant DL160 G6, con el sistema operativo Windows Server 2008 versión de prueba

A continuación se hace un análisis de cada uno de los equipos mencionados haciendo énfasis en su estado de funcionamiento actual y sus características técnicas.

a) Switch NEXXT NW223NXT54

Este es un switch de 24 puertos de 100 Mbps con ajuste de velocidad de puerto automático, que no tiene puerto de Uplink[30], además no es administrable. No es posible la configuración de VLAN's para separar el tráfico de voz, datos o video en diferentes redes, tampoco permite la configuración de puertos troncales, y aún menos brindar un trato diferenciado a los diferentes tipos de tráfico que pueden cursar por la red.

b) 1 Access Point (D-Link DWL-2100AP)

Este Access Point tiene las siguientes características técnicas:

- 1 puerto Fast Ethernet
- Soporte de 802.11 b/g
- Modos de Autenticación: Open, Shared Key, WPA/WPA2-PSK/WPA-EAP, 802.1x
- Modos de operación: Access Point, AP Repetidor, AP Cliente
- Potencia de transmisión: 15 dBm
- Antena dipolo: 1dBm
- Administración por servicio web

Este Access Point se encuentra brindando conexión inalámbrica a los profesores y personal administrativo en la zona de las oficinas del Bloque A utilizando el modo de autenticación WPA2-PSK.

c) 1 router inalámbrico (D-Link DIR-655)

Este router inalámbrico es utilizado como servidor DHCP, DNS y como salida predeterminada para brindar el servicio Internet a toda la red del CFD. Las características técnicas de este equipo son:

- 4 puertos Gigabit Ethernet
- 1 puerto WAN Gigabit Ethernet
- Soporte de 802.11 b/g/n
- Modos de Autenticación: Open, Shared Key, WEP, WPA/WPA2-PSK
- Servicios de: DHCP, NAT, Filtro MAC/IP
- 3 Antenas Dipolo de 2dBi
- Administración por servicio web

d) 1 switch TP Link

Es un switch de 5 puertos Fast Ethernet MDI/MDI-X auto sensible, que no posee puerto de Uplink. Al ser no administrable, tampoco tiene funcionalidades de

separación de tráfico por VLAN's, ni clasificación de tráfico por dirección IP, MAC o número de puerto.

e) Servidor HP Proliant DL160 G6

El servidor HP Proliant DL160 en éste momento tiene instalado el sistema operativo Microsoft Windows Server 2008 que viene por defecto grabado en su disco duro pero que al ser solo una versión de prueba tiene limitaciones de funcionamiento que no permiten realizar ciertas acciones como por ejemplo el poder funcionar como puerta de enlace y servidor DHCP para más de 10 usuarios en la red a la vez. Estas limitaciones podrían solucionarse si el CFD adquiere una licencia que haga que este sistema operativo funcione con todas sus características. Es por estas limitaciones que el servidor no está siendo usado en la actualidad.

A nivel de hardware el servidor HP posee las siguientes características técnicas:

- Servidor para montaje en rack de 19". Sus dimensiones son 17.6" x 26.9" y factor de forma de 1U[29].
- Tiene un procesador Intel Xenon de 4 núcleos 64 bits 2 GHz; con capacidad de instalar un procesador adicional de las mismas características.
- Disco duro SATA de 120 GB, con posibilidad de ampliar el espacio en disco hasta 4 TB (4x 1TB) al añadir discos SATA o SSD.
- Memoria RAM DDR4 de 4 GB con posibilidad de expandir la memoria hasta 24 GB
- Posee 2 interfaces de red Gigabit Ethernet.
- Un lector de disco DVD
- 2 puertos USB 2.0

Como se puede observar las capacidades actuales del servidor son suficientes para funcionar como servidor DHCP, servidor DNS y como puerta de enlace para la salida a Internet de todos clientes presentes en la red del CFD; además se debe notar que si se necesita instalar servicios de red que necesiten de mayor

procesamiento, más memoria RAM o más almacenamiento se puede repotenciar este mismo servidor ahorrando así la compra de un nuevo equipo.

Más detalles de las características técnicas de los equipos de conectividad con los que cuenta el CFD están en el Anexo 2.

2.3.2.3 Direccionamiento IP

El direccionamiento IP se lo hace por medio del servicio DHCP que brinda el router inalámbrico D-Link DIR-655, que es también usado como puerta de enlace de la red LAN del CFD para el acceso hacia Internet. La dirección de red utilizada en el servicio DHCP es la 192.168.1.0/24, siendo la IP del router inalámbrico la 192.168.1.1/24.

La empresa CNT otorgó al CFD la subred de direcciones IP públicas 186.46.249.153/29 para que puedan ser utilizadas para las conexiones hacia Internet. La dirección IP pública utilizada por el router inalámbrico para acceder a Internet es la 186.46.249.154/29.

Las direcciones IP de DNS primaria y secundaria que se utilizan son 200.107.10.52 y 200.107.60.58, estas direcciones fueron dadas por CNT como parte su servicio de Internet.

2.3.3 SERVICIOS DE RED

Los únicos servicios de red que se ofrecen dentro del colegio en la actualidad son los siguientes:

- DHCP
- DNS
- Internet

Los servicios de DHCP y DNS son proporcionados por medio del uso del router D-Link DIR-655, que actúa además como la puerta de enlace de Internet para las computadoras de las oficinas administrativas, biblioteca, laboratorio de

computación No. 2 y para los usuarios que de manera inalámbrica se conecten a la red usando el Access Point D-Link DWL-2100AP.

2.3.3.1 Análisis del enlace de Internet

El enlace de Internet que tiene contratado el CFD con la empresa CNT es de una velocidad de 2 Mbps simétrico, que llega por medio de fibra óptica tendida por postes y al llegar a las instalaciones del colegio entra a un convertidor óptico – eléctrico para luego conectarse con un patch cord a una velocidad de 100 Mbps a un router Cisco ISP al cual debe conectarse el router D-Link DIR-655 que se usa como servidor DHCP, DNS y como puerta de enlace para toda la red del colegio, tal como se muestra en la Figura 2.2. El convertidor óptico – eléctrico y el router Cisco pertenecen a CNT y no se tiene acceso a sus configuraciones.

El servicio de Internet tiene una gran importancia dentro del desarrollo normal de las actividades educativas, pues permite a los estudiantes y personal docente acceder a videos educativos, documentación sobre investigaciones, simulaciones de experimentos y otros recursos académicos que facilitan el aprendizaje.

Para el área administrativa de la institución el servicio de Internet tiene una importancia aún más crítica, ya que, constantemente deben intercambiar información con algunos sistemas de las entidades gubernamentales que se encuentran en línea, además de la revisión de las páginas oficiales de los Ministerios de Educación y Economía para revisar nuevas notificaciones y documentación oficial relevante.

Para los docentes, además de los recursos educativos, el servicio de Internet les permite ingresar al sistema gubernamental SIProfe en el que pueden consultar, inscribirse, retirarse y revisar sus calificaciones de los cursos de capacitación y seminarios que este sistema ofrece.

2.3.3.1.1 Sistemas de Entidades Gubernamentales

Los sistemas de entidades gubernamentales constantemente deben ser revisados por el personal administrativo debido a que en estos sistemas se realizan actividades como la carga de datos, la revisión de disposiciones y reglamentos, y,

la administración de los recursos humanos y financieros de la institución; todos estos sistemas se encuentran dentro de los diferentes servidores web publicados en Internet por los ministerios de Educación y Finanzas del Ecuador. A continuación se detallan los sistemas informáticos a los que usualmente el personal administrativo tiene acceso.

- **SIME (*Sistema de Información del Ministerio de Educación*):**

Sistema informático que permite la automatización de los procesos del Ministerio de Educación, facilitando los trámites, evitando información duplicada, mejorando los tiempos de respuesta, generando reportes detallados e integrando ésta información con la de otros ministerios u otras instituciones públicas, con el objetivo de brindar una atención oportuna y eficiente.

Dentro de este sistema el personal administrativo debe subir archivos con información detallada y resumida sobre el desempeño de los estudiantes y docentes de la institución educativa.

- **SIPROFE (*Sistema de Desarrollo Profesional Educativo*):**

Sistema informático orientado al desarrollo profesional de los educadores del sistema educativo fiscal, para lograr el mejoramiento de sus conocimientos, habilidades y competencias, lo que permitirá ascensos dentro de las categorías del escalafón o la promoción de una función a otra dentro de la carrera docente.

A este sistema ingresan el rector, vicerrector y docentes del colegio para registrar a directivos y docentes, consultar sobre cursos y otros servicios, etc.

2.3.3.1.2 Análisis del Tráfico intercambiado con Internet

Para analizar el tráfico generado por la navegación en Internet, se utilizarán los datos obtenidos por medio del software de monitoreo de tráfico MRTG (*Multi Router Traffic Grapher*), por medio del servicio SNMP (*Simple Network Management Protocol*) durante un período de tiempo de 5 semanas, en los meses de Marzo y Abril del 2013.

Debido a que el router D-Link DIR-655 que está funcionando como puerta de enlace para la red CFD no tiene la funcionalidad de agente SNMP, se procedió a

conectar el servidor HP Proliant DL160 G6 para que actúe como enlace entre el router Cisco del ISP y el router D-Link DIR-655 tal como se muestra en la Figura 2.11; este enlace se hizo con el objetivo de instalar el agente SNMP dentro del servidor HP y con ello monitorear el tráfico que pasa por sus interfaces de red; éste tráfico corresponde al flujo de datos que los usuarios de la red del colegio intercambian con Internet.

También se debe señalar que en el servidor HP se instaló un Firewall para realizar las traducciones NAT de IP's privadas a la IP pública del ISP haciendo que el AP D-Link DIR-655 solo sea utilizado como servidor DHCP. También se instaló en el equipo HP Proliant DL 160 un servidor Proxy Web con el que se bloqueó las direcciones web que no eran necesarias para los usuarios del colegio, como por ejemplo las redes sociales, las páginas de juegos en línea, las páginas de descarga de música-videos, y las páginas pornográficas; con estas restricciones en el tráfico web se puede establecer que el ancho de banda que se va a medir con MRTG corresponderá en su mayoría a tráfico web que se utiliza en las actividades académicas y administrativas del CFD.

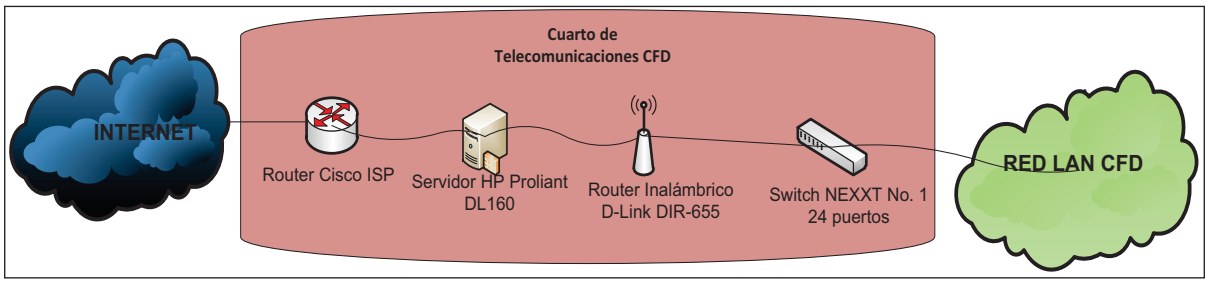


Figura 2.11: Enlace de servidor HP con router Cisco (ISP) y router D-Link DIR-655

En las Figuras 2.12 y 2.13 se muestra con más detalle la cantidad de tráfico que se está descargando y que se envía a Internet por la interfaz del servidor, estos datos corresponden a la semana con mayor cantidad de tráfico registrada por monitor MRTG; para observar con más detalle la gráficas de tráfico de navegación en Internet mirar el Anexo 3.

Por lo que se puede observar en la Figura 2.13 se puede concluir que la velocidad de subida a Internet contratada es más que suficiente, pues la cantidad de ancho de banda consumido por picos esporádicos llegan a un máximo de 1.4 Mbps de un total 2 Mbps disponibles; pero también se muestra que la velocidad de bajada

desde Internet es insuficiente pues se observan varios picos consecutivos con velocidades máximas de 2.5 Mbps, lo cual implica que el enlace de Internet está saturando, es decir la velocidad de descarga del enlace de Internet que tiene la institución no abastece la demanda en los horarios críticos en los que los usuarios de la red desean acceder a Internet. En el Anexo 3 se explican con más detalle los resultados que se obtiene del monitoreo de MRTG.

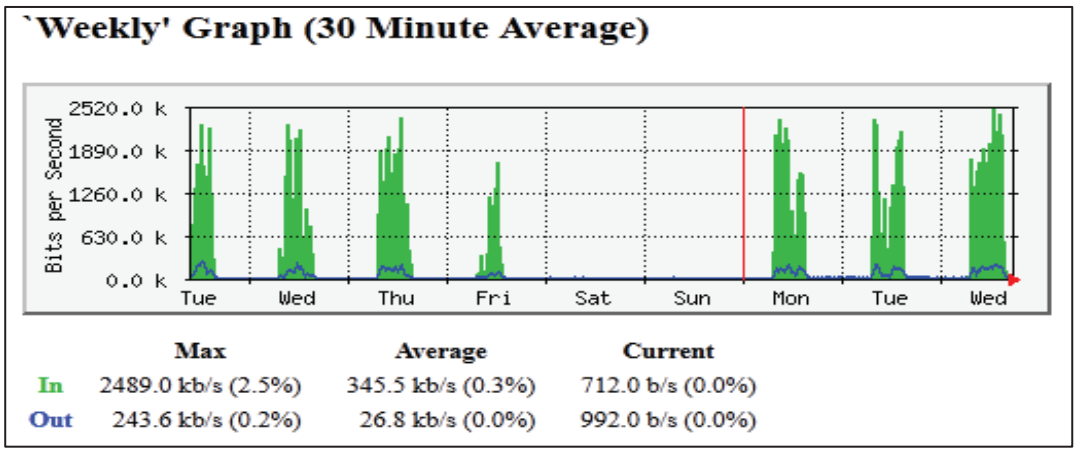


Figura 2.12: Datos de MRTG sobre la navegación en Internet

2.3.4 ANÁLISIS DEL TRÁFICO EN LA RED DEL CFD

Para determinar el tráfico actual que existe en la red del CFD se va a diferenciar entre dos tipos de usuarios: estudiantes y personal administrativo, ya que ellos son los que utilizan más frecuentemente los servicios de red que tiene el colegio, que en la actualidad solo es el servicio de Internet.

De la misma manera en que se midió el tráfico en el servidor HP Proliant DL160 G6 se realizaron las medidas para 2 computadores del personal administrativo y para 2 computadores del laboratorio de computación No. 2, para medir el tráfico generado por los estudiantes; a partir de estas medidas se obtuvieron los siguientes resultados:

El tráfico que es generado por el personal administrativo en la red del CFD en el caso más crítico llega a tener una velocidad de bajada y de subida 2.3 Mbps; estos datos son los más altos que han sido registrados mediante el monitoreo de las interfaces de red de los 2 computadores del personal administrativo.

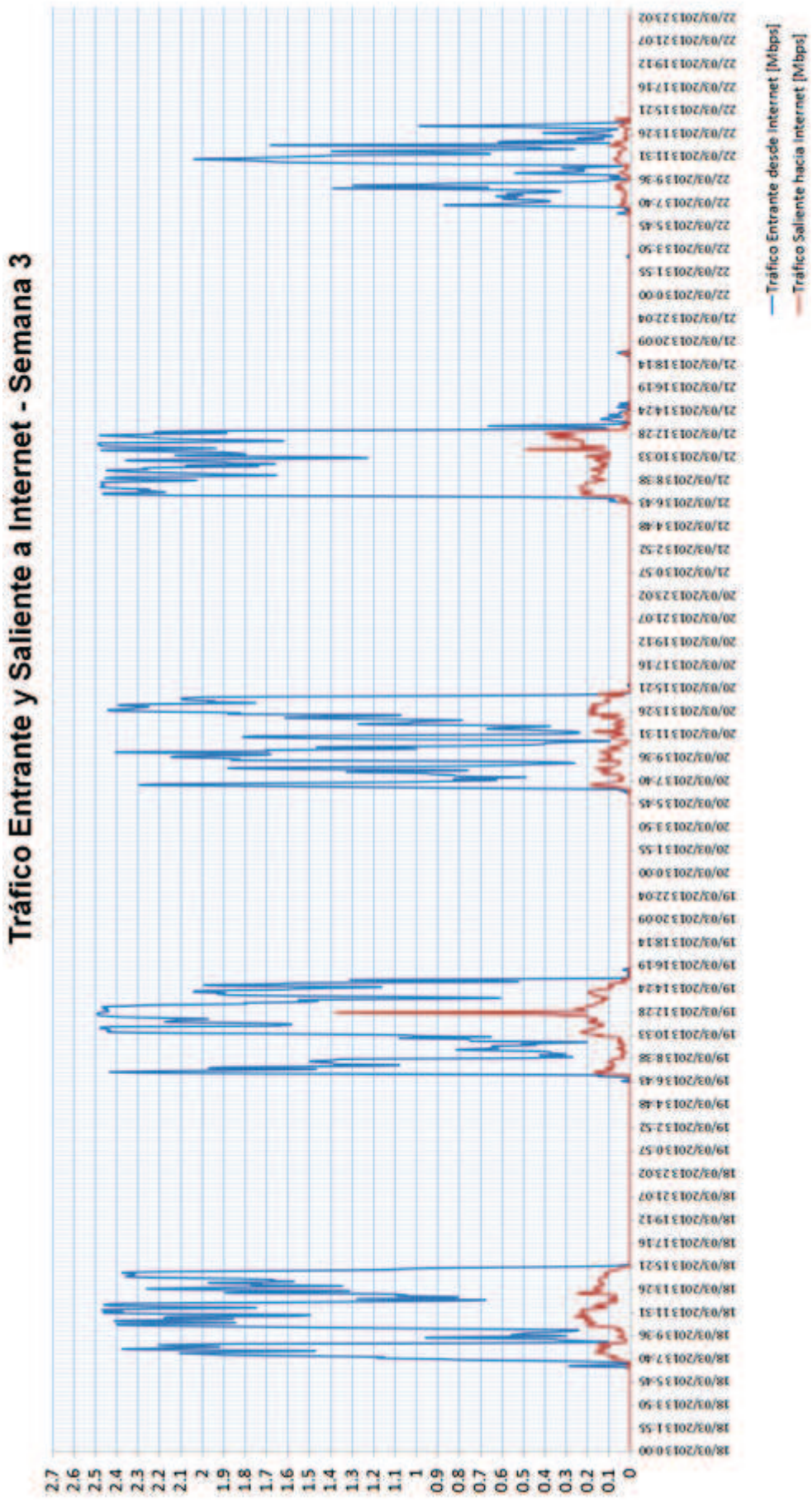


Figura 2.13: Gráfico de la semana con mayor tráfico registrado entre la LAN del CFD e Internet

Las velocidades máximas registradas en las computadoras de los estudiantes fueron de 1.85 Mbps de bajada y 222 Kbps de subida; también se notó que las horas en que los estudiantes generan tráfico en la red es en los horarios de 7h00 a 9h00 y luego de 12h00 a 14h00, mientras que el personal administrativo genera tráfico en las horas de 9h00 a 11h00 y 13h00 a 15h00. En el Anexo 4 se muestran en detalle las gráficas del tráfico de todas las 5 semanas monitoreadas a las computadoras de los estudiantes y del personal administrativo.

Como se puede observar en la Tabla 2.2 el máximo tráfico registrado por un usuario de la red es de 2.36 Mbps de bajada y 2.35 Mbps de subida. Sabiendo que todas las conexiones de red tienen una velocidad de 100 Mbps se concluye que los enlaces a nivel de acceso entre los Switches NEXXT y las estaciones de trabajo conectadas a ellos no se encuentran saturados.

MÁX. TRÁFICO DENTRO DE LA RED LAN DEL CFD		
USUARIO	**Vel. Bajada [Mbps]**	**Vel. Subida [Mbps]**
Estudiantes	1.85	0.222
Personal Administrativo	2.36	2.35
Vel. Máxima	**2.36**	**2.35**

Tabla 2.2: Máximo tráfico por tipo de usuario en la red LAN del CFD

Como se observó en la Figura 2.2 existe también un enlace de distribución entre el switch NEXXT No.1 y el switch NEXXT No.2, éste último switch tiene 22 estaciones de trabajo conectadas que son pertenecientes al laboratorio de computación No.2 del colegio; para determinar con total seguridad si este enlace de distribución podría estar saturando se realizó el siguiente cálculo tomando en cuenta la velocidad máxima de la Tabla 2.2, aun cuando estas velocidades corresponden al tráfico del personal administrativo. Para el cálculo también se considera que un 35% de los usuarios están generando tráfico en la red simultáneamente, y también se debe aclarar que los servicios a los que se acceden por parte de los estudiantes en estas computadoras se limita al acceso a Internet para realizar búsquedas e ingresar a páginas con herramientas para el desarrollo de Blogs entre otras, estos datos se obtuvieron luego de observar una clase de dentro del laboratorio de computación No.2.

$$Tráfico\ por\ el\ Enlace\ de\ Distribución = 22\ Computadores * 35\% * Vel.Máx.$$

$$Tráf.Enlace\ de\ Distribibución = 22\ Comp.* 35\% * 2.36\ Mbps = 18.7\ Mbps$$

Las velocidad resultante es de 18.7 Mbps, es decir aun cuando el tráfico de estas 22 computadoras sea igual al máximo registrado no existe ningún tipo de dificultad al usar un enlace de 100 Mbps para la conexión de distribución entre los switches NEXXT, aunque se recomienda que estos switches solo se utilicen con computadoras que solo intercambien tráfico de datos debido a que no poseen ningún tipo de mecanismo para el trato diferenciado de tráfico.

2.3.5 ANÁLISIS DE LA INFRAESTRUCTURA DE TELEFONÍA

El CFD posee una infraestructura de voz basada en la telefonía analógica, mediante una central telefónica Panasonic de más de diez años de antigüedad y que tiene problemas de funcionamiento, debido a que una descarga eléctrica lo quemó hace más de un año y no fue posible repararlo de manera adecuada lo que causó que en algunas de las líneas internas las funcionalidades de llamada en espera y transferencia de llamada no funcionen correctamente.

Esta infraestructura de telefonía es usada principalmente para comunicar al personal administrativo con otras instituciones como los ministerios de Finanzas y de Educación, la Dirección de Educación Provincial de Chimborazo o la Dirección Regional de Educación en Tungurahua.

En la Figura 2.14 se muestra la central telefónica que se encuentra ubicada en el segundo piso del Bloque A, dentro de la oficina de secretaría; esta central telefónica tiene capacidad para 3 líneas troncales y 8 líneas internas de las cuales se utilizan 5 de ellas para comunicar las oficinas administrativas de la institución (rectorado, vicerrectorado, secretaría, colecturía e inspección general) y una extensión interna se utiliza para el uso particular del conserje del colegio, pues él y su familia viven dentro de la institución, y mediante esta extensión se les provee el servicio de telefonía.

Figura 2.14: Central Telefónica Panasonic EASA-Phone KX-T30830

Las oficinas administrativas poseen teléfonos analógicos de diferentes marcas y modelos, pero todos con las funciones de transferencia de llamada y llamada en espera; todas estas oficinas pueden realizar y recibir llamadas desde y hacia la red telefónica de CNT utilizando las 3 líneas telefónicas troncales que el colegio tiene contratado con esta empresa. Las oficinas de orientación vocacional y bodega no poseen extensión.

Al igual que el cableado de la red datos el cableado de telefonía tampoco está tendido dentro de canalizaciones apropiadas, sino que se extiende directamente por el suelo de las oficinas hasta conectarse con los teléfonos analógicos de cada una de ellas, lo que puede causar daños al cable por estar expuesto para su manipulación.

En cuanto al funcionamiento a la central telefónica se debe indicar que al llegar llamadas al colegio éstas son directamente enviadas hacia la extensión de secretaría ya que no existe un menú de voz interactivo que indique y reenvíe automáticamente las llamadas a las diferentes oficinas con las que se puede comunicar un usuario externo.

Los servicios que ofrece esta central telefónica son: llamada en espera, transferencia de llamada y conferencia entre 3 extensiones; pero como se indicó anteriormente algunas de esas funciones no pueden utilizarse en ciertas

extensiones como por ejemplo en la extensión de rectorado en ocasiones no se pueden transferir llamadas desde ese teléfono.

2.3.5.1 Análisis del Tráfico de Telefonía

Para analizar el tráfico del sistema de telefonía se utilizará la información proporcionada por CNT sobre el consumo de las 3 líneas telefónicas que posee el colegio. No se pudo acceder a los datos de monitorización de la central telefónica Panasonic.

Las facturas de consumo de las líneas telefónicas proporcionaron información sobre el número de llamadas hechas diariamente, la duración de cada llamada, y la hora en la que se realizó.

Para el análisis se consideró solo aquellas llamadas realizadas dentro de los días laborables en la jornada laboral de 7h00 a 16h00, sin tomar en cuenta las llamadas que se encuentran fuera de este rango, ya que se consideran como llamadas particulares realizadas por el conserje del colegio, pues como ya se explicó en la sección anterior en la habitación del conserje existe una extensión para brindarle servicio telefónico a él y su familia.

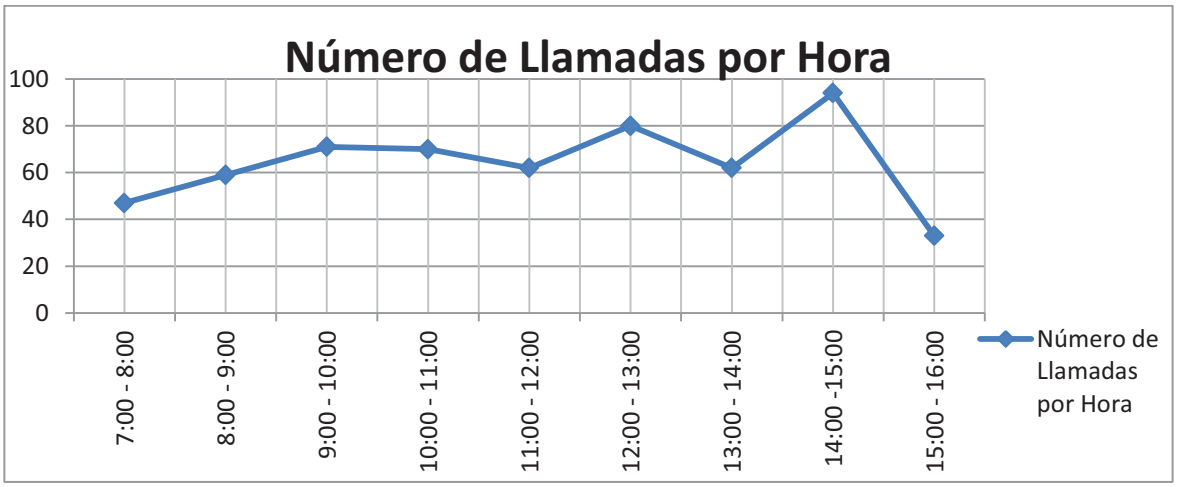


Figura 2.15: Número de llamadas por hora en las 3 líneas telefónicas troncales

Con estas observaciones se encontró que se generan un máximo de 39 llamadas diarias, cada una con una duración de entre 1 y 2 minutos, y con un tiempo

promedio de 114.8 segundos. El análisis detallado del tráfico de voz se muestra en el Anexo 5.

Para identificar la hora pico y el número de llamadas en ese período de tiempo se realizó un análisis sobre la cantidad de llamadas llevadas a cabo en cada hora; de este análisis se obtuvo la gráfica que se muestran en la Figura 2.15 en la que se observa como el tráfico de voz tiene un diferente comportamiento en el transcurso del día, observándose un patrón que se repite en las tres líneas troncales; con estos resultados se determinó que el tiempo de la jornada laboral, se debe dividir en cinco horarios: 7h00 – 9h00, 9h00 – 11h00, 11h00 – 13h00, 13h00 – 15h00 y de 15h00 - 16h00. En la Tabla 2.3 se muestra una estimación del número de llamadas diarias realizadas en cada horario y su porcentaje respecto al número total de llamadas que se realizaron durante los dos meses que se analizaron.

DISTRIBUCIÓN DE LLAMADAS EN CADA HORARIO						
Horario	**7:00-9:00**	**9:00-11:00**	**11:00-13:00**	**13:00-15:00**	**15:00-16:00**	**Total Llamadas**
Número de llamadas	106	141	142	156	33	578
Porcentaje	18.34%	24.39%	24.57%	26.99%	5.71%	100%

Tabla 2.3: Distribución de llamadas realizadas en cada rango de horarios

Con estos datos se procede a calcular el volumen y la intensidad de tráfico que presenta el sistema de telefonía. El volumen de tráfico viene dado en unidades de tiempo, por ejemplo segundos; y la intensidad del tráfico tiene como unidad al Erlang que equivale a tener una llamada de una hora de duración. Las fórmulas para calcular estos dos parámetros son las siguientes:

$$V_t = n * d$$

V_t = Volumen de tráfico

n = número de llamadas

d = duración promedio de cada llamada

$$I_t = V_t/\mathrm{T}$$

I_t = Intensidad de tráfico

T = Período de tiempo de observación

En la Tabla 2.4 se muestra el volumen e intensidad de tráfico para los rangos de tiempo que se muestran en la Tabla 2.3. El cálculo para obtener el volumen de tráfico se realizó de la siguiente manera: con los porcentajes de llamadas por horario que se tiene en la Tabla 2.3 y sabiendo que se tiene en promedio 39 llamadas diarias se obtuvo el número de llamadas que se realizan en cada rango de tiempo (7:00-9:00, 9:00-11:00, etc.); con este dato y la duración promedio de la una llamada (114.8s) ya se puede calcular el volumen y la intensidad de tráfico. Según estos resultados se puede concluir que el rango de tiempo con mayor intensidad de tráfico de voz es aquel comprendido entre las 13h00 y las 15h00.

VOLUMEN E INTENSIDAD DEL TRÁFICO DE VOZ						
Duración promedio de llamada [seg]	114.8					
Rangos de Tiempo	7:00-9:00	9:00-11:00	11:00-13:00	13:00-15:00	15:00-16:00	Total
Número de llamadas	7	9	10	11	2	39
Volumen de tráfico [seg]	803.6	1033.2	1148	1262.8	229.6	4477.2
Tiempo Obser. [horas]	2	2	2	2	1	9
Int. de tráfico [Erlangs]	0.11	0.14	0.16	0.18	0.06	0.14

Tabla 2.4: Volumen e Intensidad del tráfico de voz

2.3.6 SEGURIDAD

La seguridad informática presente en la institución la provee software antivirus de licencia gratuita, instalado en cada una de las computadoras del personal administrativo en conjunto con el firewall presente en el sistema operativo; también se debe mencionar que cada computadora tiene su usuario y clave de acceso. Las computadoras de los laboratorios y de Biblioteca no poseen un software antivirus instalado, y su única medida ante el contagio de software malicioso es el uso de software de congelamiento del disco duro, para de esa manera eliminar cualquier programa malicioso que se pudo instalar o copiar durante el día; estas computadoras no poseen usuarios y passwords de inicio de sesión.

La seguridad física de los equipos de red como los switches NEXXT y el servidor HP es brindada por una puerta de madera con un candado que cierra al Cuarto de Equipos de la institución.

Para la seguridad lógica de los equipos de red se tiene dos escenarios, los equipos que permiten ser configurados tales como el servidor HP, el router D-Link DIR-655 y el Access Point D-Link DWL-2100AP poseen claves de acceso, mientras que los switches NEXXT no poseen ningún tipo de seguridad lógica pues estos equipos no son administrables.

En cuanto a la seguridad física de los espacios y áreas del colegio se tiene varios escenarios; como por ejemplo, las oficinas y laboratorios se encuentran protegidos por medio de rejas metálicas en puertas y ventanas; mientras que para las demás aulas de la institución solo se cuenta con puertas de madera y cerraduras con candado. Sobre la seguridad del perímetro del colegio se puede decir que es muy pobre, pues no se encuentra protegido por alambrado ni ningún otro tipo de medida disuasoria; además, algunas secciones de los muros y mallas metálicas no son lo suficientemente altas como para detener la entrada de intrusos.

Además se debe señalar que no existe ninguna política, normativa o reglamento con respecto a la utilización responsable de los recursos tecnológicos que ofrece la institución.

2.3.7 ANÁLISIS DE LAS NECESIDADES PERCIBIDAS POR LOS USUARIOS DEL CFD [PW18]

Para el análisis de las necesidades que son percibidas por los usuarios que integran el CFD se aplicarán encuestas que estarán enfocadas por estratos, dividiendo a la población total de la institución educativa en dos grupos: el primero formado por docentes y personal administrativo, y el segundo por los estudiantes. Esta estratificación se debe a que los estudiantes solo tendrán acceso al servicio de Internet; y solo el personal administrativo y docente tienen acceso a los servicios de red especiales como el correo electrónico institucional, intercambio de archivos, etc.

Según los informes oficiales que el CFD envía anualmente al Ministerio de Educación, son 1087 el número total de personas que conforman esta institución educativa (período 2011-2012), total que esta integrado por el personal docente, administrativo y estudiantil, distribuidos de la siguiente manera:

- 56 Docentes
- 9 Administrativos
- 1022 Estudiantes

Para lograr un alto nivel de exactitud en los resultados que obtendrán al aplicar las encuestas se trabajará con un margen de error del 5%, para obtener un 95% de confianza en los resultados (ver Anexo 6 para más detalles).

A continuación se muestra la fórmula utilizada para obtener el tamaño de la muestra, y el cálculo de cuántas encuestas se debe hacer a cada grupo de usuarios. Los cálculos detallados del tamaño de la muestra y distribución proporcional por estratos de usuarios, las muestras de las encuestas y los resultados tabulados obtenidos de las mismas se detallan en el Anexo 6.

La fórmula para encontrar el tamaño de la muestra en una población finita con un 95% de grado de confianza es:

$$n = \frac{m}{e^2\ m - 1\ + 1}$$

n = tamaño de la muestra
m = población total (1087 personas)
e = error admisible (5% de error)

$$n = \frac{(56\ +\ 9 + 1022)}{0{,}05^2\ (59 + 9 + 1022) - 1\ + 1} = \frac{1087}{3{,}715} = 292{,}59$$

$$n = \mathbf{293}$$

Con el tamaño de la muestra se debe calcular la fracción muestral, la misma que representa la proporción que constituyen las 293 encuestas en relación al número

total de personas que forman el CFD. Con ese dato se puede calcular el número de encuestas que se deberá aplicar a cada grupo de usuarios (docentes-administrativos y estudiantes).

$$f = \frac{n}{m} = \frac{293}{1087} = 0{,}2695$$

La fórmula para calcular el número de encuestas que deberá aplicarse a cada grupo de usuarios es:

$$\#\ de\ Usuarios\ de\ un\ Grupo * Fracción\ Muestral = \#\ de\ Encuestas\ para\ este\ Grupo$$

- Número de encuestas dirigidas a docentes y personal administrativo:

  65 x 0,2695 = 17,52 = **18**

- Número de encuestas dirigidas a estudiantes:

  1022 x 0,2695 = 275,43 = **275**

Al tener dos grupos diferenciados de usuarios se deberán tener dos modelos de encuestas, cada uno dirigido a un grupo. Las preguntas dirigidas a tópicos como: la cantidad de tiempo y la frecuencia con que los usuarios acceden a Internet dentro de la institución, y la calidad percibida por los usuarios sobre el servicio de Internet del colegio; estarán presentes en las encuestas para los dos grupos ya que el servicio de Internet estará disponible para todos los usuarios de la red. Para las encuestas dirigidas a docentes y personal administrativo se añadirán los siguientes tópicos: la posibilidad de uso de laptops para conectarse inalámbricamente a la red, la calidad percibida sobre el sistema de telefonía de la institución, el interés de cambiar el sistema de telefonía actual por otro que les permita tener más funcionalidades, el interés de tener servicios de red adicionales (correo institucional, transferencia de archivos por red, página web, y aulas virtuales, etc.), y la opinión de los usuarios sobre la necesidad de mejorar la seguridad de oficinas y laboratorios para resguardar materiales e información valiosa por medio del uso de video vigilancia.

Luego de haber encuestado a docentes, personal administrativo y docentes del CFD se obtuvieron los siguientes resultados (para ver los resultados de cada pregunta de la encuesta mirar el Anexo 6):

- Sobre la frecuencia y tiempo total al que acceden los usuarios del CFD a Internet se pudo observar que los estudiantes son el grupo que accede en mayor porcentaje a Internet con un nivel de acceso del 75%; aunque su tiempo de uso oscila entre ½ hora y 2 horas diarias.

  Para los docentes y personal administrativo se obtuvo que el 53% de estos usuarios no utilizan Internet, pero el 47% restante de ellos utiliza este servicio entre 1 y 2 horas diarias.

  Con estos resultados se puede observar que tanto para los estudiantes como para el personal docente y administrativo el servicio de Internet es de gran relevancia.

	½ hora	1 hora	2 horas	3 horas	Más de 3 horas	No utiliza
Personal Docente y Administrativo	0%	11%	26%	5%	5%	53%
Estudiantes	24%	39%	12%	0%	0%	25%

Tabla 2.5: Porcentaje de tiempo de uso de Internet

- Para el personal docente y administrativo se consultó sobre la posibilidad de que se utilizaran laptops personales para la conexión a la red del colegio, y con ello facilitar y extender el uso de los servicios de red que ofrece el CFD. El resultado obtenido fue de un 100% de interés por parte de los usuarios para acceder inalámbricamente a los servicios de red que se ofrecen en el colegio.

- También se consultó sobre el porcentaje de docentes y personal administrativo que poseen laptops propias, de lo que se obtuvo que un 32% de ellos poseen un computador portátil para su uso personal, mientras que el 64% que no posee una laptop indicó que en el próximo año también utilizarán un computador portátil.

- En cuanto a la calidad percibida sobre el servicio de telefonía con respecto a parámetros como número de extensiones adicionales que se pueden añadir, funcionalidades adicionales que puedan agregarse, seguridad de cuenta de usuario por cada extensión, y aspectos como confiabilidad y estabilidad de la central telefónica; se obtuvo que la mayoría de usuarios consideran que el sistema de telefonía con el que cuenta el colegio es Bueno debido a que, aunque funciona de manera estable, la posibilidad de añadir más funcionalidades y un mayor número de extensiones se encuentra limitada por las características de la central telefónica y por la antigüedad que tiene la misma.

	Malo	Regular	Bueno	Muy Bueno	Excelente
Personal Docente y Administrativo	0%	0%	79%	21%	0%

Tabla 2.6: Calidad percibida sobre el servicio de telefonía

- Sobre el cambio del sistema de telefonía se obtuvo el resultado de que el 100% de los usuarios consultados creen que el sistema de telefonía actual debería ser cambiado por otro que ofrezca mayores funcionalidades como un menú de bienvenida interactivo, un buzón de voz, identificador de llamada, seguridad en las cuentas de usuario, y la posibilidad de crear un mayor número de extensiones telefónicas de las que en este momento se pueden crear; también otra razón por la cual los usuarios del colegio desean el cambio de central telefónica es debido a que aunque se pueden realizar llamadas de forma normal la transferencia de llamadas entre algunas de las extensiones actuales ya no funciona correctamente y esto causa molestias pues los usuarios deben ser contactados personalmente para que se acerquen a la oficina donde se tomó la llamada.

- La consulta sobre los servicios de red que se considera se deberían brindar a la comunidad educativa del CFD mostró que el 100% de usuarios piensan que a más del servicio de Internet, el colegio debería implementar los servicios de correo electrónico institucional, aulas virtuales, página web y el servicio para la transferencia de archivos en red.

- La pregunta relacionada con la implementación de un sistema de video vigilancia en las instalaciones del CFD obtuvo un resultado que indica que el 100% de los docentes y personal administrativo creen que es necesario contar con video vigilancia para aumentar la seguridad del colegio.

NECESIDAD DE IMPLEMENTAR UN SISTEMA DE VIDEO VIGILANCIA EN EL CFD	
Sí	100%
No	0%

Tabla 2.7: Necesidad de implementar un sistema de video vigilancia en el CFD

2.4 ANÁLISIS FINAL DEL ESTADO ACTUAL DE LA RED

2.4.1 SISTEMA DE CABLEADO ESTRUCTURADO DEL CFD

Luego de haber hecho un análisis del estado del Sistema de Cableado Estructurado del CFD se nota claramente que no se cumplen con las normas TIA 568-C, TIA/EIA 606-A y TIA/EIA 607. Entre los problemas encontrados están los siguientes:

- En el CFD no existen áreas destinadas para los Cuartos de Equipos y Telecomunicaciones ni racks cerrados que cumplan con esa función en los lugares donde los equipos de conectividad se encuentra funcionando como por ejemplo en laboratorio de computación No. 2.

- El Cuarto de Equipos tiene los siguientes problemas:
  - ✓ No posee medidas de seguridad física.
  - ✓ No posee un control de acceso.
  - ✓ La puerta de ingreso a este cuarto no posee las dimensiones mínimas según la norma TIA 568 -C.
  - ✓ No posee medidas mínimas contra incendios.
  - ✓ Existe demasiado polvo en el ambiente.
  - ✓ Existen goteras.

- ✓ No posee canalizaciones para la organización del cableado dentro de esta área.
- ✓ No posee racks para el montaje de los dispositivos de conectividad como el servidor y el switch NEXXT No.1.
- ✓ No posee los ductos apropiados para la canalización del cableado Vertical y Horizontal.
- ✓ No existe identificaciones para los puntos de red.
- ✓ La instalación eléctrica a la que se conecta los dispositivos de conectividad no es la adecuada ya que es artesanal y los cables eléctricos se encuentran sobre el suelo.
- ✓ No posee ningún tipo de aterramiento pues no se cuenta con un Sistema de Puesta a Tierra.

- El Cableado Horizontal tiene los siguientes problemas:
  - ✓ No se utilizan faceplates para las salidas de telecomunicaciones.
  - ✓ No se etiquetan el cableado en el Cuarto de Telecomunicaciones ni en el lado de la estación de trabajo.
  - ✓ La canalización del cableado horizontal no se encuentra sujeto a una superficie fija como el suelo por lo que todo el cableado dentro de la canaleta se estira y se mueve, y esto puede causar daños en los cables de red.
  - ✓ En todas las oficinas administrativas y en la biblioteca no existe ningún tipo de canalizaciones para el tendido del cableado.
  - ✓ No existen cajas de revisión, ni ductos para el paso del cableado por medio de una pared, como por ejemplo para la salida o entrada del cableado horizontal del Cuarto de Telecomunicaciones hacia las oficinas de Secretaría, Vicerrectorado, etc. por lo que se utilizan las ventanas de las oficinas y aulas para el ingreso del cableado.

- El Cableado Vertical tiene los siguiente problemas:
  - ✓ El tendido del Cableado Vertical que se extiende desde el Cuarto de Telecomunicaciones en el Bloque A hacia otras oficinas en otras

edificaciones del CFD se realiza de manera improvisada al tender el cable en ocasiones dentro de canaletas plásticas que no están sujetas a ninguna superficie fija y en otras ocasiones sin ningún tipo de canalización.

- ✓ Se extiende vía aérea cableado UTP que no está diseñado para ese tipo de instalaciones.

- Las Áreas de Trabajo tienen los siguientes problemas:
  - ✓ No se utilizan patch cords para la conexión entre la estación de trabajo y la salida de telecomunicaciones, sino que se conecta directamente el cableado horizontal con la estación de trabajo.
  - ✓ No se utilizan faceplates para la salida de telecomunicaciones de cada punto de red.
  - ✓ No se etiquetan los puntos de red en el área de trabajo.

- La Entrada de Servicios posee el siguiente problema:
  - ✓ El CFD no posee ductos adecuados para la entrada del cableado de los servicios de telecomunicaciones contratados, por lo que el cableado de estos servicios entran al Cuarto de Equipos por medio de una ventana que se encuentra abierta en este cuarto.

2.4.2 EQUIPOS ACTIVOS DEL CFD

Luego de analizar los equipos activos de la red del CFD se detectaron algunas falencias:

- Para las estaciones de trabajo de la Biblioteca se recomienda su reemplazo por computadores de mejores características pues debido a su antigüedad su hardware no puede ser actualizado pues sus repuestos ya no existen en el mercado y por estas razones los equipos continuamente se quedan congelados y deben ser reiniciados para que funcionen de nuevo.

- El problema que se detectó en el servidor HP Proliant DL160 G es su sistema operativo Windows Server 2008 que no posee activadas todas sus funcionalidades, por lo que ha hecho que no se utilice el servidor y se tenga

que usar un router inalámbrico D-Link DIR-655 como servidor DHCP, DNS y como puerta de enlace para la red del colegio.

- En el switch NEXXT NW223NXT54 se detectaron los siguientes problemas:
  - ✓ No posee un puerto de Uplink de mayor capacidad para que el tráfico que se dirija hacia el servidor pueda transmitirse; esto puede ocasionar un cuello de botella en esa conexión.
  - ✓ No posee ningún tipo de mecanismo para su configuración y por lo tanto no posee ninguna clase de funcionalidad extra que permita por ejemplo el uso de VLAN's, enlaces troncales, listas de acceso, medidas de seguridad por puerto, controlar los lazos de conmutación, tener políticas de calidad de servicio, etc.; es por ello que este switch solo puede usarse en redes que no necesiten separación en subredes a nivel de switch, y que no necesiten un trato diferenciado para el tráfico que cursa por él.

2.5 ANÁLISIS DE REQUERIMIENTOS

La red del CFD va a ser una red multiservicios, es decir tendrá integrado en ella los servicios de voz, datos y video. Tomando en cuenta lo anterior y de acuerdo con los resultados obtenidos mediante las encuestas realizadas, y, al análisis de la infraestructura de red existente, se pudo determinar que la red del CFD tiene los siguientes requerimientos:

2.5.1 REQUERIMIENTOS DEL SISTEMA DE CABLEADO ESTRUCTURADO

El Sistema de Cableado Estructurado del CFD presenta un sin número de falencias que no le permiten cumplir con las normas de cableado TIA, es por ello que a continuación se listan los requerimientos que deben ser cumplidos por la red del CFD para ésta funcione según las normativas de los estándares de cableado estructurado.

- El Cuarto Equipos y Cuartos de Telecomunicaciones tienen los siguientes requerimientos:

  - ✓ Se deben crear espacios para el funcionamiento de los Cuartos de Telecomunicaciones dentro del área del colegio.
  - ✓ Ubicar los Cuartos de Telecomunicaciones de manera que estén los más central posible del área a la que dan servicio.
  - ✓ El Cuarto de Equipos aunque tiene un espacio suficiente (5.6m x 3m) destinado para su funcionamiento, el área ocupada para los equipos de conectividad y el cableado estructurado en éste cuarto es muy reducido porque se lo comparte con documentos y archivos antiguos de la institución. Es por esto que se debe reubicar todo este material para que éste cuarto sea ocupado exclusivamente por los dispositivos de conectividad que pertenecen a la red del colegio. Otra necesidad específica de éste cuarto es la reparación de las goteras y la refacción de las ventanas para que permanezcan cerradas.
  - ✓ Se deben instalar y organizar los equipos de conectividad sobre racks adecuados.
  - ✓ Se debe colocar medidas de seguridad física más disuasivas como por ejemplo puertas de metal con las dimensiones mínimas que establece la norma TIA 568-C para el acceso a los cuartos de Telecomunicaciones y de Equipos.
  - ✓ Implementar métodos de monitoreo del acceso a los Cuartos de Telecomunicaciones y de Equipos, como por ejemplo cámaras de video.
  - ✓ Los Cuartos de Telecomunicaciones y de Equipos deben poseer medidas anti incendios como pintura anti fuego, detectores de humo y extintores.
  - ✓ Se debe cuidar que los espacios de los cuartos de Telecomunicaciones y de Equipos sean ambientes libres de polvo que pueda dañar a los equipos de conectividad.

- ✓ Instalación de canalizaciones y ductos adecuados para la organización y tendido del cableado horizontal y vertical que llega hasta los cuartos de Equipos y Telecomunicaciones.
- ✓ Instalación de un sistema eléctrico dentro de los cuartos de Telecomunicaciones y de Equipos que proporcione alimentación a los dispositivos de conectividad de forma segura.
- ✓ Instalar un sistema de puesta a Tierra dentro de cada cuarto de Telecomunicaciones y de Equipos.

- El Cableado Horizontal debe cumplir con los siguientes requerimientos:
  - ✓ Etiquetar el cableado en los cuartos de Telecomunicaciones y de Equipos.
  - ✓ Se debe implementar un método para la canalización del cableado horizontal que cumpla con la norma EIA/TIA 569-A para todos los puntos de red que se tenga en la institución.
  - ✓ Todas las canalizaciones y ductos deben estar llenos hasta máximo un 60% de su capacidad para permitir el tendido de cableado adicional en el futuro.
  - ✓ Utilizar un medio de trasmisión que permita tener un ancho de banda a nivel de acceso que soporte el tráfico generado por las aplicaciones de red presentes y futuras; siempre tomando en cuenta la posibilidad de la reutilización del cableado actual si es que éste cumple con las características deseadas de ancho de banda.
  - ✓ Utilización de cajas de revisión de tamaño y con la frecuencia que se especifica en la norma EIA/TIA 569-A, para poder tener acceso fácil al cableado durante su recorrido hasta la salida de telecomunicaciones.
  - ✓ Utilización de ductos y canalizaciones para el tendido de cableado que tenga que ingresar a oficinas o aulas y así evitar el ingreso del mismo por medio de ventanas o puertas.

- El Cableado Vertical debe cumplir con los siguientes requerimientos:

- ✓ El tendido del Cableado Vertical debe hacerse dentro de canalizaciones y ductos que permitan cumplir con las normas establecidas en el estándar EIA/TIA 569-A.
- ✓ Todas las canalizaciones y ductos deben estar llenos hasta máximo un 40% de su capacidad para permitir el tendido de cableado adicional en el futuro.
- ✓ Se debe etiquetar el cableado vertical en los Cuartos de Telecomunicaciones y de Equipos.
- ✓ Se debe usar medios de transmisión permitan tener un ancho de banda que evite el aparecimiento de cuellos de botella en la red.
- ✓ Se deben respetar las distancias máximas permitidas para las conexiones de cableado vertical según el tipo de medio de transmisión utilizado.
- ✓ El cableado vertical debe poseer enlaces de respaldo por si es que alguno de sus enlaces sufre un corte.

- Las Áreas de Trabajo tienen los siguientes requerimientos:

  - ✓ Todos los puntos de red destinados a dar servicio a estaciones de trabajo deberán terminar en conectores instalados en faceplates con su debida identificación.
  - ✓ Se deberán utilizar patch cords terminados en fábrica para las conexiones entre la estación de trabajo y el punto de red ubicado de un faceplate.

- La Entrada de Servicios posee el siguiente requerimiento:

  - ✓ Instalación de ductos adecuados para el ingreso del cableado de los servicios de telecomunicaciones como Internet y telefonía analógica hasta el interior del Cuarto de Equipos del colegio.

- El Sistema de Puesta a Tierra a diseñar tiene los siguientes requerimientos:

- ✓ Se debe implementar un sistema de puesta a tierra dentro de los cuartos de Telecomunicaciones y de Equipos de la institución que cumpla con la norma EIA/TIA 607.
- ✓ El diámetro de cable a utilizar para la unión entre las barras de puesta a tierra y las varillas de tierra debe ser proporcional a la distancia que separe a cada uno de estos elementos.
- ✓ El cableado que une las barras de puesta a tierra y las varillas deberá tenderse dentro de ductos o canalizaciones exclusivas para este propósito.
- ✓ Se deberá conectar todo el sistema de puesta a tierra a una malla de tierra compuesta por varillas de tierra y un terreno tratado para tener una resistividad menor o igual a 5 Ω.

2.5.2 RED ACTIVA DEL CFD

La red activa del CFD está compuesta por las estaciones de trabajo, los equipos de conectividad y los servicios de red; de los cuales se ha determinado un conjunto de requerimientos que se detallan a continuación.

2.5.2.1 Estaciones de Trabajo y Equipos de Conectividad del CFD

En las estaciones de trabajo y los equipos de conectividad se requiere:

- Los equipos que se encuentran dentro de la Biblioteca de la institución deben ser reemplazados por otros de mejores condiciones para que se pueda brindar un servicio de calidad a los usuarios que requieran consultas en línea.
- La instalación de un sistema operativo basado en software libre en el servidor Hewlett-Packard DL160 G6 es una necesidad urgente, que debe solventarse con prontitud, ya que, este dispositivo puede ser utilizado para brindar los servicios de red que necesita la institución educativa.
- El servidor HP DL160 G6 debe ser repotenciado en caso de que se necesiten mayores capacidades para el funcionamiento de los servicios de red que se instalen dentro del mismo.

- Los switches NEXXT deberán ser utilizados por los usuarios que solo requieran de los servicios sin calidad de servicio como la navegación web.
- Se requiere de equipos de conectividad que brinden calidad de servicio al tráfico de una red convergente de voz, datos y video, debido a que el sistema de telefonía y de video seguridad va a utilizar el cableado de red para trasmitir sus datos.
- Las características mínimas que deben tener los equipos de conectividad a utilizar en la red deben ser: permitir el uso de VLANS, capacidades para trato diferenciado del tráfico de video, voz y datos, uso de protocolos que eviten lazos de conmutación, capacidad para brindar una seguridad de acceso por puerto, soporte para la actualización de su software de ser necesario, soporte para protocolos de administración como por ejemplo SNMP y permitir la administración remota de los equipos utilizando protocolos de encriptación de la información que se intercambia con los equipos. También se debe analizar si los dispositivos de red que posee la institución pueden ser reutilizados.
- La administración del servidor y de los dispositivos de conectividad en lo posible debe hacerse físicamente junto a estos equipos, pero de no ser posible se debe habilitar consolas de administración remota que permitan la encriptación de la información que se intercambie.
- Monitorear los dispositivos de conectividad mediante el uso del protocolo SNMP.

2.5.2.2 Servicios de red del CFD

Los servicios de red del CFD requieren:

- Redimensionar el enlace de Internet que el CFD tiene contratado con CNT debido a que en la actualidad este enlace se encuentra saturado con el tráfico de la navegación en Internet aun cuando este tráfico está controlado por medio del servidor proxy web para evitar el ingreso a páginas web que no tienen relación con las actividades académicas y administrativas del CFD. Como se observa en la Figura 2.13 la velocidad de bajada máxima

registrada en el enlace a Internet supera a la velocidad contratada de 2 Mbps y es por ello que este enlace debe ser redimensionado.

- Instalación de los servicios de red de DHCP y DNS en el servidor HP del colegio, para reemplazar y evitar los inconvenientes que se presentan al utilizar al router D-Link DIR-655 debido a fallas en su funcionamiento que producía fallas en el servicio de Internet y el servicio DHCP.
- Implementar un servicio de Proxy Web dentro del servidor HP para permitir el acceso diferenciado a Internet de los usuarios del CFD, junto con la aplicación de reglas con respecto a permisos sobre páginas web y horarios para los que la navegación en Internet están permitidos.
- Para facilitar el control sobre el cumplimiento de las restricciones sobre las páginas web permitidas para la navegación, se requiere instalar un generador de reportes del servidor Proxy.
- Por las necesidades indicadas en la sección 2.3.7 de este capítulo, que se obtuvieron mediante aplicación de encuestas al personal administrativo, docente y estudiantes de la institución; se concluyó la necesidad de implementar los servicios de correo electrónico institucional, intercambio de archivos, página web y aula virtual en la red del CFD.
- La vigilancia de los servicios de red de la institución se los hará de manera automática por medio de la implementación de un software de monitorización que también permita administrar mediante el protocolo SNMP a los equipos de conectividad.
- Instalación de un servidor SSH para permitir la administración remota de los servicios de red instalados en el servidor.
- Instalar un servidor de directorio que permitirá tener un control centralizado sobre los permisos que los usuarios tendrán sobre los recursos de la red.
- Implementación de un sistema de telefonía IP que permita tener mayores funcionalidades. Un mayor detalle sobre los requerimientos que debe tener este servicio se verán más adelante.
- Instalar un servicio de firewall dentro del servidor HP para que actúe como una protección para los usuarios de la red CFD frente a Internet, debido a

que en la actualidad las estaciones de trabajo de la institución solo están protegidas por el firewall de su sistema operativo.

2.5.2.3 Requerimientos de los Equipos de Conectividad del CFD

La red LAN del CFD va a soportar el tráfico de voz, video y datos, por lo que los requerimientos detectados sobre el tráfico dentro de la red LAN son:

- Se deberá cambiar el modo en que están distribuidos los equipos de conectividad del CFD para que sigan un sistema jerárquico de tres capas (Acceso, Distribución y Núcleo) pues este modo de organización ofrece ventajas como facilidad en la administración, implementación, crecimiento, y detección de fallas.
- Las capacidades de los switches y los enlaces de Uplink con los que se cuenta en la actualidad no abastecerán a una red con los servicios de voz, video y datos, por lo que se debe usar un sistema jerárquico en el que las características de velocidad de transmisión y capacidad para manejar flujos de datos vayan aumentando según el nivel en el que se encuentre funcionando el dispositivo de red.
- Analizar si la velocidad de acceso de 100 Mbps es adecuada para la transmisión de los servicios de datos, telefonía de manera simultánea.
- Calcular la velocidad de los enlaces de Uplink para evitar cuellos de botella en las conexiones hacia los dispositivos de conectividad de capas superiores.
- Los switches deberá tener capacidades para brindar una calidad de servicio mediante un trato diferenciado al tráfico de voz, datos y video.

2.5.2.4 Sistema de Telefonía

Por las falencias detectadas en el sistema de telefonía actual del CFD se recomienda ser reemplazado. Las funcionalidades con las que debe cumplir este sistema serán los siguientes:

- Capacidad para un crecimiento futuro de forma fácil y organizada.

- Integración con el servicio de directorio por medio del servicio de directorio LDAP.
- Capacidad para utilizar bases de datos para almacenar los datos de cuentas de usuario y registros de llamadas.
- Capacidad para la conexión con la PSTN y redes de datos externas.
- Funcionalidades para asignar permisos para llamadas locales, nacionales, internacionales y hacia celulares con la utilización de perfiles de usuario.
- Cuentas de usuario móviles y seguras con la utilización de passwords individuales para cada usuario.
- Capacidad para conferencias entre varias terminales telefónicas a la vez.
- Utilización de codecs de voz de licencia gratuita.
- Utilización de licencias privadas que tengan un menor bit rate para que si en futuro se requiera realizar una llamada entre centrales telefónicas IP ubicadas en diferentes lugares geográficos el ancho de banda que ocupen estas llamadas sea limitado y el costo del enlace VPN por el que realizará esta comunicación sea menor.
- Capacidad para la implementación de un menú de bienvenida interactivo (IVR, *Interactive Voice Response*) para las llamadas que recibe el colegio.
- Terminales telefónicos que permitan tener funciones como: transferencia, parqueo, reenvío, historial de llamadas y llamada en espera.
- Función de contestadora automática en caso de que el usuario no conteste o se encuentre ausente; y almacenamiento de los mensajes de voz en cuentas individuales.
- Acceso mediante menús interactivos a la cuenta de usuario personal, mensajes de voz y directorio telefónico.
- Encriptación para el tráfico de voz y de control que se intercambia por la red.
- Para tener una mejor administración y ayudar en la gestión diferenciada del tráfico de voz, los terminales telefónicas IP deberán pertenecer a una VLAN independiente.

- Los terminales telefónicos deberán poder seguir funcionando aun cuando el suministro eléctrico falle, para ello se deberá recibir energía de un UPS por el cable de red (PoE 802.3af) por medio el equipo de conectividad (switch) al que esté conectado.

2.5.2.5 Seguridad

Luego del análisis de la seguridad informática y física del colegio se determinaron lo siguientes requerimientos:

- Definición de políticas de seguridad generales que deberán ser conocidos y respetados por todos los usuarios que utilicen los servicios y recursos tecnológicos del CFD.
- Implementación de un sistema de video seguridad que garantice la integridad de las oficinas y objetos de valor que sean de propiedad de la institución.
- Se deberá poder configurar diferentes tipos de perfiles de vigilancia que permita tener diferentes comportamientos en el modo en que funciona el sistema video vigilancia dependiendo de la hora de día.
- El sistema de video seguridad deberá permitir usar a las cámaras IP como sensores de movimiento que disparen una alarma para evitar el robo de los objetos valiosos del colegio.
- Los videos del sistema de vigilancia se podrán ver por medio de un monitor web que permita observar tanto los videos tomados en vivo, como también los eventos pasados en los que se haya detectado movimiento por medio de las mismas cámaras.
- Todo el tráfico que se intercambie con el monitor de video seguridad deberá estar encriptado para proteger la información de videos y cuentas de usuario de esta interfaz.
- El sistema de seguridad deberá estar conectado a un sistema de respaldo de energía para que pueda seguir funcionando en caso de una falla en el servicio eléctrico.

- Debido a que la ubicación de las cámaras IP van a estar en lugares de difícil acceso y sin posibilidad de alimentación por la red eléctrica, éstos dispositivos deberán contar con la posibilidad de tomar energía eléctrica mediante el cable de red.
- Se deberán poner cámaras en exteriores para vigilar la entrada al colegio, y los patios del mismo con el fin de detectar de manera temprana a personas que hayan invadido las instalaciones del colegio, principalmente en las noches.
- Las cámaras deberán poseer la capacidad de grabación diurna y nocturna, por medio del uso de iluminación infrarroja que la misma cámara debe emitir.

CAPÍTULO III

REDISEÑO DE LA INFRAESTRUCTURA DE RED

3.1 INTRODUCCIÓN

La infraestructura de red convergente del CFD brindará a los usuarios un sistema completo de comunicaciones flexible, escalable y confiable que permita el desarrollo de sus actividades de manera apropiada.

En el rediseño de la infraestructura de red se contemplará la implementación de todos los servicios de red que necesita el CFD, tomando en cuenta que ésta solución debe estar dimensionada para soportar un crecimiento futuro en número de usuarios y cantidad de tráfico de datos, voz y video.

3.2 DIMENSIONAMIENTO DE TRÁFICO

El dimensionamiento del tráfico de la red permitirá evitar cuellos de botella que puedan entorpecer las comunicaciones, especialmente, en el tráfico de voz y video que son susceptibles a retrasos.

Debido a que los equipos que actualmente posee el CFD no tienen las capacidades necesarias para el correcto funcionamiento de la página web institucional, se instalará dentro de un servidor (hosting) fuera de la institución, pero para el diseño se incluirá el tráfico que generen las peticiones a este servicio.

Para dimensionar la necesidad actual de la capacidad del enlace para la navegación en Internet, se usarán los datos obtenidos en la sección 2.3.3.1 sobre la cantidad de tráfico de navegación en Internet por parte de alumnos y personal administrativo, mediante el uso del software de monitoreo de tráfico MRTG.

3.2.1 TRÁFICO GENERADO POR LOS SERVICIOS DE RED DEL CFD

Con el objetivo de obtener una proyección los más cercana a la realidad se realizó una estimación sobre el crecimiento en el número de usuarios de red del CFD a 5 años, por medio del análisis de los datos oficiales del Ministerio de Educación del Ecuador sobre el número de docentes, alumnos y personal administrativo que posee el CFD desde el año 2008 hasta el año 2012.

En la Tabla 3.2 se puede observar la estimación de crecimiento del personal administrativo y docente para los próximos 5 años, obtenidos por medio de la observación de las tendencias que muestran los datos.

Según esta estimación se tendrán 71 usuarios entre docentes y personal administrativo para el año 2017. En cuanto al número de alumnos se realiza el mismo procedimiento y los resultados se muestran en la Tabla 3.3.

En la Tabla 3.1 se muestra que el porcentaje de crecimiento esperado en los próximos 5 años. El número de usuarios administrativos y docentes crecerá en el 9.23%, y el crecimiento en el número de estudiantes será del 4.69% (para más detalles del cálculo de estos porcentajes ver Anexo 7).

Usuario	% Crecimiento usuarios en 10 años
Administrativos y Docentes	9.23
Estudiantes	4.69

Tabla 3.1: Porcentaje de crecimiento en 5 años del número de estudiantes, docentes y personal administrativo

Con los porcentajes de crecimiento que se muestran en la Tabla 3.1 se determinó el número de docentes, personal administrativo y estudiantes que se espera tener en 5 años en el CFD; estos datos se muestra en la Tabla 3.4. Además se debe indicar que todos los cálculos realizados en este rediseño de red se harán tomando en cuenta el número de usuarios esperados para el año 2017.

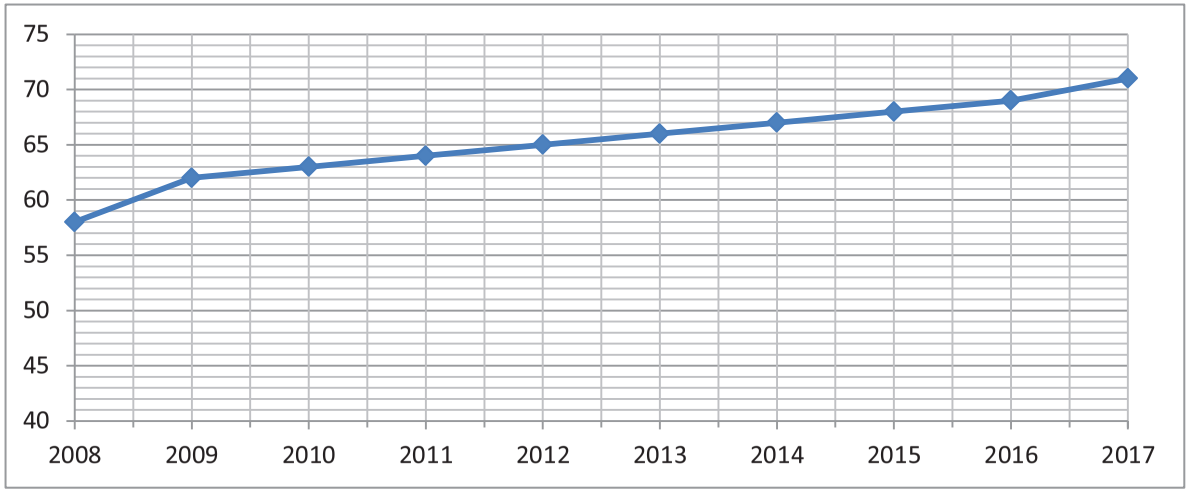
Año	Número de Usuarios	Gráfico
2008	58	
2009	62	
2010	63	
2011	64	
2012	65	
2013	66	
2014	67	
2015	68	
2016	69	
2017	71	

Tabla 3.2: Estimación de crecimiento del número de docentes y personal administrativo

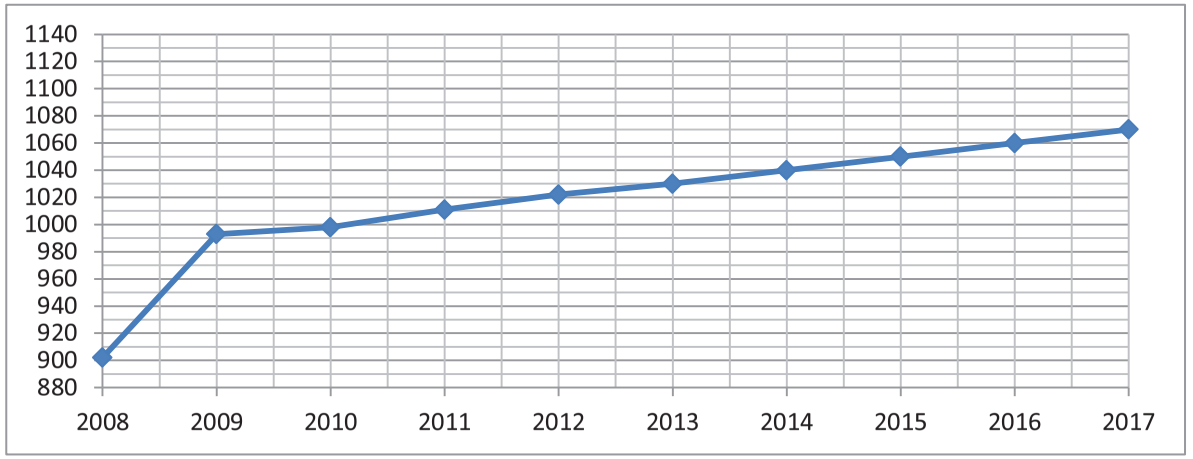
Año	Número de Usuarios	Gráfico
2008	902	
2009	993	
2010	998	
2011	1011	
2012	1022	
2013	1030	
2014	1040	
2015	1050	
2016	1060	
2017	1070	

Tabla 3.3: Estimación de crecimiento del número de estudiantes

Usuario	Número de Usuarios 2012	% Crecimiento usuarios en 5 años	Número de Usuarios 2017
Administrativos	9	9.23	10
Docentes	56	9.23	61
Estudiantes	1022	4.69	1070

Tabla 3.4: Número de usuarios esperado en 5 años para el CFD

3.2.1.1 Correo Electrónico

El servicio de correo electrónico lo utilizarán los usuarios administrativos y profesores del colegio por lo que se tendrán un máximo de 71 cuentas de correo electrónico (10 administrativos y 61 profesores). Este servicio se ocupará solo para la comunicación y envío de documentación relacionada directamente con el CFD; se considera una velocidad de 100 Kbps para el envío y recepción de los emails pues el correo electrónico no es en tiempo real y los archivos que se podrán adjuntar no superarán los 5 MB pues estos serán en su mayoría documentos y comunicaciones editados en una herramienta ofimática como Microsoft Word u Open Office. Para determinar el índice de simultaneidad para los usuarios de administrativos se habló con las personas que mayor número de correos envían y reciben, y se observó que al menos 4 personas administrativas pueden estar ocupando el servicio a la vez lo que resulta en una simultaneidad del 40%, y para los docentes se realizó un procedimiento similar con lo que se encontró que se tendrá un 10% de simultaneidad de uso de este servicio dentro de la hora mayor tráfico registrada en las monitorizaciones (7h00 – 9h00). El cálculo del ancho de banda consumido por este servicio sería:

$$Correo\ Electr. = 100\ Kbps\ x\ 11\ usuarios\ x\ 40\% = 440\ Kbps$$

Según el resultado de la Tabla 3.5 el ancho de banda necesario para el funcionamiento del servicio de correo electrónico es de 1050 Kbps aproximadamente.

Tipo Usuario	# Usuarios en 5 años	Índice de Simultaneidad	A.B. Consumido [Kbps]
P. Administrativo	10	40%	440
Profesores	61	10%	610
Total Ancho de Banda consumido			1050

Tabla 3.5: Velocidad consumida por el Correo Electrónico

3.2.1.2 Intercambio de Archivos

El servicio de intercambio de archivos o FTP (*File Transfer Protocol*) se utilizará para la transmisión de documentos o archivos que tengan un tamaño superior los 5 MB, pues en la actualidad se hace uso de memorias USB para realizar este intercambio. Al igual que con el correo electrónico se tendrán un máximo de 71 usuarios (profesores y administrativos) y se estima que el índice de simultaneidad no superará el 10% para todos los usuarios pues la compartición de archivos entre oficinas y de profesores no se realiza de manera frecuente. Este servicio fue pensado para compartir de manera automática con los profesores y personal administrativo archivos de interés común como documentos de Word, Excel y Pdf, es por ello que se considera que el tamaño máximo de un documento o un archivo será de 10MB y que éste deberá descargarse en 5 minutos lo que representa una velocidad de 250 Kbps.

La ancho de banda necesario para solventar el funcionamiento del servicio de intercambio de archivos en la red del colegio es de 1.9 Mbps.

$$Int.Archivos = 250Kbps\ x\ 71\ usuarios\ x\ 10\% = 1775\ Kbps$$

Tipo Usuario	# Usuarios en 5 años	Índice de Simultaneidad	A.B. Consumido [Kbps]
P. Administrativo y Profesores	71	10%	1775
Total Ancho de Banda consumido			1775

Tabla 3.6: Velocidad consumida por el Intercambio de Archivos

3.2.1.3 Aula Virtual[PW19]

Para el acceso desde Internet al Aula Virtual se debe considerar el estatus económico de los alumnos de la institución ya que la mayoría de ellos no poseen computadores en sus hogares, y aún menos alumnos poseen servicio de Internet; es por esto que se considera que en un principio solo el 20% del total de alumnos del colegio accederán a las aulas virtuales (214 usuarios) y se espera un 30% de simultaneidad, estas consideraciones se basan en que los contenidos de las aulas virtuales serán más de carácter complementario a las clases presenciales del colegio por lo que tendrán información adicional, textos de lectura y enlaces a otras páginas para acceder a otros contenidos en línea.

El contenido que se mostrará en el aula virtual será en su mayoría texto, imágenes ilustrativas, alertas de tareas, indicaciones para proyectos y enlaces hacia otros sitios web; es por ello que se proyecta que cada página de un aula virtual tendrá un tamaño máximo de 400 KB, y que debería descargarse en máximo 40 segundos para ofrecer una navegación fluida a través del aula virtual, lo que da una velocidad de acceso por usuario de 218.45 Kbps.

$$Aula\ Virt. = \frac{400\ KB/pag.web}{40\ seg.}\ x\ 1070\ usuarios\ x\ 20\%\ acces.serv.x\ 30\%\ simult. = 5259.3Kbps$$

Con esto se muestra que el ancho de banda del enlace necesario para el funcionamiento del aula virtual dentro de la red LAN del CFD es de 5259.3 Kbps.

Tipo Usuario	# Usuarios	% de los usuarios que acceden al Aula Virtual	Índice de Simultaneidad	A.B. Consumido [Kbps]
Estudiantes	1070	20%	30%	5259.3
Total Ancho de Banda consumido				5259.3

Tabla 3.7: Ancho de Banda consumido por el Aula Virtual

Para el caso del acceso a las aulas virtuales desde los laboratorios de computación se tendrá un máximo de 40 usuarios, pues este es el número de computadoras que los laboratorios poseen, y el índice de simultaneidad esperado es de un 35%, que es el índice de simultaneidad encontrado luego de haber presenciado el desarrollo de una clase en la que los alumnos tenían que acceder a información en Internet. El ancho de banda que consumiría este servicio dentro de la LAN será:

$$Aula\ Virt.LAN = \frac{400\ KB/pag.web}{15\ seg.}\ x\ 40\ usuarios\ x\ 35\%\ simult. = 3058.34Kbps$$

Se debe señalar que a las aulas virtuales se accederá principalmente desde Internet y que el acceso desde la LAN será esporádico por lo que el ancho de banda que se consume dentro de la red local no afectará a otros servicios.

3.2.1.4 Página Web

Como se mencionó anteriormente el servicio de página web de la institución será implementado dentro de un hosting contratado, debido a que en estos momentos el CFD no cuenta con los recursos para montar un servidor web dedicado para esta tarea, pero en el futuro se prevé migrar este servicio para que funcione dentro las instalaciones del colegio, es por ello que se incluirá el tráfico que se genere por este servicio dentro del dimensionamiento del enlace de Internet.

La página web institucional tendrá una función informativa para docentes, alumnos, padres de familia y público en general, se considera que se atenderán 1 petición cada 15 segundos en el instante de mayor demanda, estos datos se obtuvieron de las estadísticas que el hosting proporciona sobre el número de visitas que se tiene actualmente en la página web del CFD, para observar estos datos ver el Anexo 8. El tamaño máximo estimado de la página web es de 800 KB, ya que se espera que ésta página muestre contenido multimedia como fotografías y animaciones referentes al CFD que hacen que la página web tenga un tamaño elevado.

Con estos datos se calcula el ancho de banda que el enlace de Internet del CFD deberá tener para el funcionamiento de la página web desde la red interna de la institución:

$$A.B.\,Página\ Web = 800\ \text{KB}\ x\frac{2^{10}B}{1\ KB}x\frac{8\ bits}{1\ B}x\frac{1\ Kbit}{1000\ bits}x\ \frac{1\ petición}{15\ s} = 436.9\ Kbps$$

Del cálculo se obtuvo que se necesita 436.9 Kbps para poder solventar 1 petición cada 15 segundos, pero se espera que el número de peticiones simultáneas y de visitas a la página web del colegio vayan creciendo con el tiempo mientras los estudiantes, padres de familia y público en general se entere de que el CFD cuenta su página web, es por esto que se debería dimensionar al menos un ancho de banda de 1.2 Mbps para este servicio, con lo que se podrá solventar hasta 3 peticiones simultáneas cada 15 segundos o lo que es lo mismo 1 petición cada 5 segundos.

ANCHO DE BANDA CONSUMIDO POR PÁGINA WEB	
Tamaño promedio página web [KB]	**A.B [Kbps]**
800	1200

Tabla 3.8: Ancho de Banda necesario para funcionamiento de página web del CFD

3.2.1.5 Navegación en Internet [PW23]

Como se pudo observar en la sección 2.3.3.1 del capítulo 2, el enlace bajada de Internet del CFD se encuentra saturando, ya que el tráfico que se consume supera por 500 Kbps a la velocidad máxima (2 Mbps) que el colegio tiene contratado en el enlace de Internet; es por ello que se debe definir como una necesidad el aumento del ancho de banda en el enlace de Internet.

Además considerando los resultados que se muestran en la sección 2.3.7 del capítulo 2 sobre la inconformidad de los usuarios de la red en relación con la calidad del servicio de Internet en el CFD, se calculó el ancho de banda consumido por un usuario a partir del tamaño promedio de la páginas web más

visitadas en la institución; para realizar estos cálculos se utilizó los datos que son presentados en los reportes del servidor proxy web.

Según los resultados obtenidos de las páginas web más visitadas, el tamaño promedio de estas páginas es de 1276 KB (para más detalles ver Anexo 9), que deberá descargarse en un tiempo medio de 50 segundos, lo que resulta en una velocidad de descarga aproximada de 210 Kbps por usuario de red.

Los usuarios que tienen acceso a Internet son el personal administrativo (10 computadores) y a los estudiantes que como parte de las asignaturas de informática acceden a Internet por medio de los computadores presentes en los dos laboratorios de computación del colegio (42 computadores), para estos dos tipos de usuarios se prevé un índice de simultaneidad del 35% pues para sus actividades académicas y administrativas es necesario el uso de los navegadores web. Los profesores de la institución según los resultados de las encuestas realizadas sobre el uso de Internet este grupo de personas no accede habitualmente a este servicio debido a que la mayoría no poseen computadores portátiles personales para poder utilizar este servicio desde las aulas, pero se considera que en un futuro al menos la mitad de ellos ya cuenten con este equipo; además por esto se estima que el índice simultaneidad de estos usuarios no superará el 20%, de la misma manera se los considerará a los usuarios invitados.

*A.B. de Entrada Navegación en Internet = 210 Kbps * # Total Usuarios (10 administrativos, 30 docentes, 42 estudiantes y 10 invitados) * %Uso simultáneo*

Tipo de Usuario	Número de Usuarios	Índice de simultaneidad	Vel. de navegación [Kbps]	A.B. de Navegación/clase de usuario [Kbps]
Administrativos	10	35%	210	735
Estudiantes	42	35%		3087
Docentes	30	20%		1260
Invitados	10	20%		420
Total Ancho de Banda [Kbps]				5502

Tabla 3.9: Cálculo del ancho de banda necesario para la navegación en el CFD

Con el número de usuarios, el índice de simultaneidad y la velocidad de descarga, se procederá al cálculo del ancho de banda necesario para la navegación en el enlace de Internet del CFD. En la Tabla 3.9 se muestran los resultados de los cálculos y según esto se necesita 5.5 Mbps de ancho de banda para la navegación en Internet.

3.2.1.6 Cálculo de la capacidad del enlace del Internet del CFD

En el enlace de Internet se recomienda que tenga una capacidad suficiente para solventar todo el tráfico que fluye desde y hacia Internet, es decir, servirá para la navegación en Internet de todos los usuarios de la institución, para la página web y el aula virtual; se tomó esta decisión debido a que esos servicios serán los más utilizados, mientras que los servicios de correo electrónico e intercambio de archivos al no ser servicios en tiempo real y al tener un menor uso por parte de los usuarios del colegio no se los tomará en cuenta en este cálculo.

Otra consideración que se debe hacer para cálculo del enlace de Internet es el modo en que los servicios ocupan el ancho de banda de este enlace, por ejemplo el Aula Virtual y la Página Web utilizan el enlace de subida pues principalmente envían información hacia el Internet, mientras que la navegación web de los usuarios del colegio utiliza el enlace de bajada desde Internet; es por ello que se debe hacer una diferencia entre el enlace de bajada y el enlace de subida de la conexión hacia Internet.

Al calcular la capacidad del enlace que necesita cada servicio solo se calculó el ancho de banda más relevante en cada uno de ellos, es decir solo el ancho de bajada (navegación web) o subida (aula virtual, pagina web) según cada caso; estos cálculos se realizaron de esa manera sabiendo que el ancho de banda no calculado no cambiará la capacidad del enlace de Internet total, pues representa una pequeña parte de la capacidad de ese enlace en comparación con los datos que si se calcularon de cada servicio y que son los que realmente van a dimensionar de manera correcta el enlace a Internet; además al ser un enlace de tipo corporativo y que funcionará por medio de un enlace físico como fibra óptica el enlace tendrá una relación 1:1 en el ancho de banda por lo que para su

dimensionamiento solo se necesitan los anchos de banda más relevantes de cada uno de los servicios que van a salir a Internet.

En la Tabla 3.10 se muestra el dimensionamiento del enlace de Internet, y solo aparecen los valores de ancho de banda que son más relevantes de cada servicio, mientras que los valores no calculados no se encuentran especificados en la tabla.

Enlace de Internet		
Tipo de Usuario	**A.B. Entrada [Kbps]**	**A.B. Salida [Kbps]**
Aula Virtual	-	5259.3
Página Web	-	1200
Navegación en Internet	5502	-
Total	5502	6459.3

Tabla 3.10: Cálculo de la capacidad del enlace de Internet del CFD

Según los datos obtenidos con los cálculos de la Tabla 3.10 se recomienda tener un enlace primario de una capacidad de 7 Mbps.

Para el caso en que el enlace de Internet primario falle es necesario que las computadoras de secretaria, colecturía y vicerrectorado se mantengan conectados a Internet, por lo que se propone el uso de 3 módems celulares para que a través de éstos las estaciones antes mencionadas puedan estar siempre conectadas con los sistemas web de los ministerios de Educación y Finanzas del Ecuador, pues sus actividades laborales están fuertemente ligadas a la interacción con estos sistemas. La capacidad de enlace según Movistar de estos modems pueden estar entre los 7.2 Mbps a 21.6 Mbps dependiendo de la red celular a la que estén conectados; con estos datos se observa que estas velocidades son suficientes para dar un servicio de navegación en Internet óptimo.

3.2.1.7 Características del Enlace de Internet

El enlace a Internet debe cumplir con ciertas características mínimas para garantizar la calidad y confiabilidad del mismo. Entre las características que debe tener están:

- Para el enlace principal debe proporcionar un enlace de relación 1:1 sin compartir el ancho de banda.
- La capacidad de ancho de banda del enlace primario debe poder expandirse previa notificación.
- El proveedor debe garantizar una disponibilidad mínima del 99.6%, debido a que con este nivel de disponibilidad se asegura que el servicio de Internet estaría fuera de línea como máximo 5 minutos diarios durante un año, lo que aseguraría el acceso al personal administrativo a los sistemas informáticos en línea de los ministerios de Educación y de Finanzas a cualquier hora del día.
- El proveedor de servicio debe permitir la resolución de dominios y subdominios en los servidores de su red. La disponibilidad del servicio DNS debe estar en concordancia con el nivel de disponibilidad del enlace de Internet.
- El proveedor de servicio debe realizar la instalación de su cableado de acuerdo con las normas de cableado estructurado para la canalización de la acometida.
- El proveedor de servicio debe mantener acuerdos de Peering[31] Internacional y al menos dos rutas de salida para acceso internacional, garantizando con ello que la salida hacia servidores internacionales siempre estará disponible.
- El proveedor de servicio debe tener al menos dos enlaces hacia la red NAP[32] (*Network Access Point*) Ecuador, para el intercambio de tráfico nacional con otros proveedores de Internet locales.
- Para los módems celulares se debe asegurar la compatibilidad de los mismos con el sistema operativo de las computadoras donde va ser utilizados (vicerrectorado, secretaría y colecturía) para poder evitar errores de funcionamiento y poder hacer uso de los mismo de manera inmediata de ser necesario.

3.2.2 SISTEMA DE TELEFONÍA

3.2.2.1 Tráfico generado por la Telefonía IP

Para calcular el tráfico generado por la telefonía IP dentro de la LAN del colegio se deberá primero establecer el tipo de códec que se utilizará; para ello se analizará la calidad de voz percibida, la capacidad de compresión y si el códec es de libre utilización o si se debe pagar una licencia para ello.

3.2.2.1.1 Selección de Codec de Voz

Para la selección del códec de voz se analizarán a los códecs con mejor calidad de voz percibida, es decir el códec G.711 y el códec G.729A que tienen calificaciones de 4.1 y 3.92 respectivamente sobre una calificación máxima de 5 puntos (para más detalles ver Tabla 1.5).

De estos dos codecs el que menor ancho de banda ocupa para la transmisión de la voz es el códec G.729A que tiene un bit rate de 8 Kbps, mientras que el códec G.711 tiene un bit rate de 64 Kbps.

Por último se tomó en cuenta que el códec G.711 es de libre utilización y está ampliamente soportado por los terminales telefónicos IP, mientras que para utilizar el códec G.729A se debe comprar una licencia por cada canal a utilizar.

Luego de revisar estos tres aspectos se recomienda el uso del códec G.711 debido a que provee una alta calidad de voz, es de libre utilización y está ampliamente soportada por los terminales y centrales telefónicas IP.

3.2.2.1.2 Ancho de Banda consumido en llamada IP

Para calcular el ancho de banda consumido en la telefonía IP es necesario establecer el tamaño de cada paquete, número de paquetes por segundo, la sobrecarga debido a cabeceras de los protocolos de capa de enlace, red, transporte y aplicación.

El número de paquetes de voz por segundo generado por un teléfono IP utilizando el códec G.711 es de 1 paquete por cada trama, y el tamaño de cada paquete de

voz es de 160 Bytes; a este dato se debe añadir la información que se adiciona con las cabeceras de las capas de sesión, transporte, red y enlace.

Para saber cuántos bytes por trama pertenecen a sobrecarga de los protocolos de las capas de enlace, red, transporte y aplicación, se debe tomar en cuenta el tamaño de cabecera y cola de cada uno de estos protocolos.

Capa	Protocolo	Longitud Cabecera y Cola [Bytes]
Sesión	RTP	12 (variable)
Transporte	UDP	8
Red	IP	20 – 60
Enlace	Ethernet	22
Total		62

Tabla 3.11: Tamaño de las cabeceras de los protocolos utilizados en VoIP

La información de la voz digital que entrega el códec se encapsula primero dentro del protocolo RTP en la capa de sesión, éste a su vez en la capa de transporte se encapsula dentro del protocolo UDP, y en la capa de red los paquetes UDP se encapsulan dentro de un paquete IP. En la capa de enlace éste paquete IP se encapsula dentro de una trama. Las cabeceras y colas de cada uno de estos protocolos se muestran en la Tabla 3.11.

Con estos valores y los datos sobre los codecs presentados de la Tabla 1.5 se calcula el ancho de banda que utiliza una llamada de telefonía IP utilizando la siguiente fórmula [P3]:

$$A.B = \frac{Tamaño\ de\ Paq.de\ Voz * \#\ Paq.por\ Trama\ de\ Voz\ \ + Tamaño\ de\ Cabeceras\ \ B}{Tiempo\ entre\ Paq.de\ Voz *\ \#\ de\ Paq.por\ Trama\ de\ Voz\ [s]} x\ 8\ bits$$

El Ancho de banda que el códec G.711 ocuparía en una llamada sería:

$$A.B.códec\ G.711 = \frac{160\ Bytes * 1\ paq./trama\ +62\ Bytes}{0.02\ s * 1\ paq./Trama} x\ 8\ bits = 88.8\ Kbps$$

De los cálculos se obtiene que una llamada telefónica ocupa 88.8 Kbps de ancho de banda.

Los usuarios administrativos tendrán un terminal telefónico en cada oficina (rectorado, vicerrectorado, secretaría, colecturía, inspección general, orientación vocacional y bodega) excepto en secretaría en la que se dejarán dos terminales telefónicos; además se dejará 1 extensión para los consultorios de enfermería y odontología, es decir se tendrán 9 extensiones en total en estas áreas. En cuanto a los profesores se debe aclarar que ellos no poseen oficinas, sino que se reúnen dentro de la sala de profesores, este es un espacio que tiene un área de $38m^2$ y que puede albergar aproximadamente 20 personas, es por ello que se colocará dentro de ésta área una extensión telefónica por cada $10m^2$ con lo que se tendría 4 extensiones, una por cada 5 profesores lo que se considera un número suficiente de extensiones para los docentes del colegio tomando en cuenta de que este el servicio de telefonía solo deberá ser usado para llamadas que están asociadas con las actividades del colegio. En total se calcula que se tendrán 13 extensiones telefónicas funcionando dentro del colegio.

3.2.2.1.3 Cálculo de número de líneas telefónicas [PW24, PW25]

Para el cálculo del número de líneas telefónicas necesarias para las llamadas que se dirijan hacia la PSTN se utilizarán los datos contenidos en la Tabla 2.4, mismos que fueron el resultado del análisis sobre la intensidad de tráfico de telefonía en colegio; todo el análisis se encuentra detallado en la sección 2.3.5 del capítulo 2.

Intensidad de Tráfico [Erlang]	0.5
Probabilidad de bloqueo	1%
Número de canales	3

Tabla 3.12: Número de líneas telefónicas analógicas para la central telefónica IP

La intensidad de tráfico registrada durante la hora de mayor ocupación en el sistema de telefonía del colegio es de 0.18 Erlangs y se considera una probabilidad de bloqueo de llamadas hechas o recibidas del 1%. Con la intensidad de tráfico y la probabilidad de bloqueo se obtiene el número de canales necesarios según los datos de la tabla de Erlang B del Anexo 10. Con estos

datos se obtuvo que se necesitan 3 líneas telefónicas analógicas para permitir la conexión de la red telefónica IP interna con la PSTN.

3.2.3 VIDEO SEGURIDAD

El sistema de video seguridad consistirá en la utilización de cámaras IP ubicadas en lugares estratégicos de la institución para salvaguardar los bienes e información valiosa del colegio. Todos los videos de seguridad serán monitoreados mediante una aplicación web en un monitor.

Al igual que el tráfico de voz, el tráfico de video dependerá del códec a utilizar, del número de cámaras IP, del número de cuadros por segundo y del tamaño en bytes de la imagen a capturar.

La función principal del tráfico de video en el CFD es el proporcionar video seguridad a las oficinas e instalaciones donde se guarden objetos de valor que puedan ser substraídos; por lo que, se deben tener grabaciones continuas de largos períodos de tiempo como las noches y días no laborables.

3.2.3.1 Selección de Codec de Video

La mayoría de las cámaras IP soportan los codecs de video M-JPEG y MPEG-4. Para escoger entre dos codecs se analizará la calidad de video, la cantidad de datos que se envían por la red, la compresión de cada códec y el soporte de cada códec en las cámaras IP actuales.

La calidad del video y el tamaño del cuadro de la imagen con que ambos codecs pueden trabajar poseen valores similares, por lo que en este punto se puede decir que estos dos codecs son equivalentes.

Sobre la cantidad de ancho de banda utilizado y la compresión de datos, el códec MPEG-4 tiene una gran ventaja, pues utiliza un algoritmo de compresión de video que reduce el número de datos que deben enviarse por la red; mientras que el codec MJPEG utiliza un algoritmo de compresión de imágenes, las mismas que después de su compresión deben ser enviadas por la red, por lo que este códec utiliza un mayor ancho de banda para el envío de datos.

Por último se analizó cuál de los dos codecs es soportado por la mayoría de las cámaras IP, y se observó que las cámaras IP para la mediana y pequeña empresa tienen un soporte más difundido para el códec MJPEG.

Luego de analizar los puntos anteriores y de considerar que el sistema de video vigilancia no necesita gran fidelidad de imagen, ni un tamaño de cuadro demasiado grande, y que el ancho de banda consumido para el envío de los datos no es una limitante ya que el sistema trabaja dentro de una LAN; se ha llegado a la conclusión que se debería utilizar el codec MJPEG en el sistema de video vigilancia de la institución, ya que presenta todas las ventajas del códec MPEG-4 y además la mayoría de las cámaras IP soportan este tipo de códec.

3.2.3.2 Ancho de Banda Consumido por una Cámara IP

El ancho de banda consumido por una transmisión de video en MJPEG depende del tamaño del cuadro, la resolución de video y del número de cuadros por segundo (*IPS*) que se capturen. En la Tabla 3.10 se muestran las velocidades de transmisión para cada una de las variantes anteriormente mencionadas; los valores que se presentan en esa tabla fueron obtenidos mediante la medición manual del ancho de banda consumido por una cámara IP funcionando con el códec MJPEG en las condiciones de tamaño de cuadro, calidad de imagen y cuadros por segundo especificadas.

Tamaño de Cuadro	Calidad de Imagen	Velocidad de Transmisión [Mbps]	
		15 IPS	30 IPS
640 x 480	Alta	5.2	4.4
320 x 240		2	3.5
640 x 480	Media	3.1	3.7
320 x 240		1.6	3.3

Tabla 3.13: Velocidad de transmisión de video vigilancia utilizando MJPEG

Como ya se dijo anteriormente en el sistema de video vigilancia no es necesario tener una alta calidad de imagen sino que se requiere un tamaño de cuadro y una calidad de imagen moderados en los que se puedan apreciar de manera clara a las personas y objetos de las zonas vigiladas; por estas razones se recomienda la

utilización de la siguiente configuración para el video de las cámara IP: 320 x 240@15 IPS en calidad media. Con esta configuración se tendría una velocidad de transmisión de video aproximadamente de 1.6 Mbps según los datos expuestos en la Tabla 3.13.

3.2.3.3 Determinación de lugares para las Cámaras IP

Los lugares más importantes para ubicar las cámaras IP serán dentro de las áreas donde se encuentran los objetos de valor como computadores, y equipamiento; es por ello que se recomienda que las cámaras estén instaladas dentro de las oficinas administrativas, laboratorios de computación, Química, Física, Biología, en la biblioteca y en bodega; todas estas cámaras deberán poseer detección de movimiento y capacidad para filmar en modo nocturno.

Para proteger el perímetro del colegio ante intrusiones se decidió ubicar cámaras en la zona alta de los Bloques A, esta cámara estará apuntando hacia la entrada principal del colegio, y hacia los muros Norte y Este de la institución que colindan con la Av. Leopoldo Freire y la calle Luxemburgo respectivamente. Para vigilar el lado Sur del colegio se decidió ubicar una cámara en la parte alta del Bloque I.

Una vez determinado que se necesitan cámaras para vigilar tanto el exterior como el interior de las instalaciones del colegio, se define la ubicación de cada una de las cámaras. En la en la Tabla 3.14 se muestra la descripción de los lugares donde se colocarán las cámaras IP.

Según las distribución de cámaras de la Tabla 3.14 se necesitan 17 cámaras IP dentro de las instalaciones de la institución por lo que el ancho de banda ocupado por las transmisiones de video sería aproximadamente 27.2 Mbps. La ubicación aproximada de las cámaras IP puede observarse en los planos del Anexo 11.

3.2.4 ANCHO DE BANDA UTILIZADO SEGÚN EL SERVICIO, NÚMERO DE USUARIOS E ÍNDICE DE SIMULTANEIDAD

Se proyectará el tráfico que surcará por la red del CFD en los próximos 5 años para lo cual se calculará el ancho de banda tomando en cuenta el tráfico genera -

TIPO DE CÁMARA IP, CANTIDAD Y UBICACIÓN		
Tipo	**Cantidad**	**Ubicación**
Externa	1	Techo Bloque A – Cámara Móvil. Vigila hacia los Bloques C, D, F, la sección de patio entre estos bloques, la entrada del colegio y los parqueaderos.
	1	Techo Bloque I – Cámara Móvil. Vigila los Bloques B, H y la sección de patio comprendida entre estos bloques.
Interna	1	Cámara Fija - Vigila la Biblioteca
	1	Cámara Fija – Vigila la entrada a Colecturía y Cuarto de Telecomunicaciones
	1	Cámara Fija – Vigila entrada a Secretaría y a Rectorado
	1	Cámara Fija – Vigila entrada a la Sala de Reuniones y al Vicerrectorado
	1	Cámara Fija - Vigila Corredor de la planta alta del Bloque A
	1	Cámara Fija – Vigila oficina de Inspección General.
	1	Cámara Fija – Vigila entrada al Enfermería y Odontología
	1	Cámara Fija – Vigila entrada a la Consejería Estudiantil
	1	Cámara Fija – Vigila entrada de la Bodega General
	1	Cámara Fija – Vigila la entrada al Laboratorio de Computación No. 1
	1	Cámara Fija – Vigila la entrada al Laboratorio de Computación No. 2 y al Cuarto de Equipos del B
	1	Cámara Fija – Vigila la entrada al segundo Cuarto de Equipos ubicado en el Bloque G
	1	Cámara Fija – Vigila la entrada al Laboratorio de Física
	1	Cámara Fija – Vigila la entrada al Laboratorio de Química
	1	Cámara Fija – Vigila la entrada al Laboratorio de Biología
No. Total de cámaras	17	

Tabla 3.14: Ubicación y tipo de Cámaras IP

do por un servicio de red, por el número de usuarios que acceden al servicio y el índice de simultaneidad esperado para cada uno.

Estos cálculos ayudarán a dar una idea de la velocidad de acceso que deberán tener los enlaces hacia las estaciones de trabajo y también la velocidad que necesitan tener los enlaces de cableado vertical para intercomunicar los dispositivos de conectividad (switches).

3.2.4.1 Velocidad de Acceso por usuario

Para los cálculos se tomará en cuenta la mayoría de los servicios de red que van

a ser ocupados por el personal administrativo y docente de la institución, excepto por el acceso a las aulas virtuales y la página web a las cuales principalmente se accederán desde Internet, es por ello que se realizará una diferenciación en los cálculos.

Otra consideración que se hará para los cálculos de la velocidad de acceso es la simultaneidad en el uso de uno o varios de los servicios de red por un usuario; para lograr tener un resultado que refleje este escenario se realizarán los cálculos para el switch de la LAN que soportará mayor cantidad de tráfico; este es un switch de 24 puertos que estará ubicado en el Cuarto de Equipos y tendrá conectado a la mayoría de las cámaras IP, y el cableado horizontal para los datos y telefonía de los usuarios administrativos.

Servicio de Red	V. de acceso x usuario [Kbps]	# Total de Usuarios conectados x servicio	Usuarios simultáneos x servicio	V. de acceso x servicio [Kbps]
Telefonía IP	88.8	8	2	177.6
Navegación en Internet	210	11	4	840
Correo Electrónico	100	11	3	300
Intercambio de archivos	250	11	1	250

Tabla 3.15: Velocidad por cada servicio del CFD en el switch con más tráfico en la LAN

Los índices de simultaneidad ocupados en la Tabla 3.15 en cada servicio de red corresponden con los usados en las secciones 3.2.1 y 3.2.2 de este capítulo.

Como se puede notar en la Tabla 3.15 una de las columnas muestra el número total de usuarios conectados al switch y que tienen acceso a cada uno de los servicios de red, en este caso se trata de 8 usuarios administrativos que poseen el servicio de telefonía y servicio de datos ocupando un mismo punto de red, y los otros 3 usuarios conectados al switch son docentes que tienen acceso solo a los servicios de datos, con esto se tendrían ya 11 puntos de red de los 24 del switch; los otros 13 puntos de red no se los tomó en cuenta en los cálculos pues solo son ocupados por las cámaras IP y estas siempre van a utilizar el mismo ancho de banda en los puertos de acceso.

Al sumar todos los usuarios simultáneos se obtiene que son 10, lo que indica que cada uno de estos usuarios se encuentra utilizando un solo servicio a la vez, mientras que 1 de los usuarios que también está conectado a este switch no se encuentra ocupando ningún servicio de red; con esta observación se puede concluir que la velocidad de acceso necesaria corresponde al ancho de banda más alto de entre los servicios de red que un usuario administrativo y docente tienen acceso en la red, que en este caso es la velocidad del servicio de intercambio de archivos (250 Kbps); pero el caso más crítico que se debería tener la capacidad de afrontar es que el usuario utilice los 3 servicios de mayor ancho de banda al mismo tiempo (Telefonía, Internet, Intercambio de Archivos) que daría una velocidad de 549 Kbps.

Con estos resultados se puede determinar que la tecnología a usar en la LAN del CFD debe ser Fast Ethernet, pues brinda una velocidad de 100 Mbps por cada enlace lo que es muy superior al ancho de banda máximo que un usuario consumiría en la red, y además ésta es la capacidad de enlace mínima que usan los switches presentes actualmente en el mercado.

3.2.4.2 Velocidad de Backbone

Al igual que para determinar la velocidad de acceso, para la velocidad de backbone se usará el mismo método y los mismos cálculos pues se requiere saber cuál será el tráfico máximo transmitido desde un switch de acceso hacia las capas superiores de la red.

Una vez determinado la velocidad de acceso por cada servicio de red en el switch de mayor tráfico, se sumarán estos valores para estimar la velocidad mínima que se debería tener en los enlaces backbone en la LAN del colegio. Además de los servicios de red mostrados en la Tabla 3.15 se tiene añadir el tráfico que las cámaras IP van a transmitir hacia el servidor de video seguridad que se encuentra en una capa superior de la red.

Según el resultado de la Tabla 3.16 la velocidad de backbone es de 28.8 Mbps, en la que se toman en cuenta las llamadas telefónicas IP, un monitor de video

seguridad y el tráfico generado por los servicios de red en el switch con mayor tráfico en la red.

Servicio de Red	V. x servicio [Kbps]
Telefonía IP	177.6
Navegación en Internet	840
Correo Electrónico	300
Intercambio de archivos	250
Video seguridad	27200
TOTAL	28767.6

Tabla 3.16: Velocidad de Backbone en la red del CFD

3.3 INFRAESTRUCTURA DE COMUNICACIONES DE SERVICIOS INTEGRADOS

La tecnología de red que usará para el cableado estructurado debe ser capaz de soportar tráfico de voz, datos, video, y soportar el crecimiento en número de usuarios y el aparecimiento de nuevos servicios y aplicaciones dentro de los próximos 10 años.

El esquema de red usará la tecnología de transmisión de datos Ethernet con topología física en estrella. El modelo de red lógico sigue el esquema núcleo – distribución – acceso, pero por el tamaño de la red del CFD se ha decidido fusionar la capa de núcleo con la capa de distribución.

3.3.1 SISTEMA DE CABLEADO ESTRUCTURADO

El Sistema de Cableado Estructurado(SCE) brindará conectividad entre los equipos de red basándose en estándares internacionales que garanticen la escalabilidad, disponibilidad, confiabilidad, seguridad, y permita soportar cualquier nuevo servicio o aplicación que aparezca durante los próximos 10 años; además, se considerará un diseño que permita tener flexibilidad en la ubicación de estaciones de trabajo dentro de oficinas de la institución, para con ello evitar ampliaciones o remodelaciones en el SCE.

El SCE proporcionará enlaces de Backbone con cableado cat. 6, y en la capa de acceso cable UTP cat. 5E, siendo todos los enlaces de una distancia máxima de 100 metros.

El SCE presentará una topología en estrella, la misma que tendrá su centro en el Cuarto de Equipos, ubicado en el segundo piso del Bloque A, desde el cual saldrá el cableado vertical hacia los Cuartos de Telecomunicaciones.

Los estándares con los que se trabajará son: ANSI/TIA 568-C.1 que especifica el cableado de telecomunicaciones en Edificios Comerciales, ANSI/TIA 568-C.2 de requerimientos que debe cumplir el cableado UTP cat. 5E y 6, ANSI/TIA/EIA 606-A estándar que especifica los criterios de administración para la infraestructura de telecomunicaciones, ANSI/TIA/EIA 607 especifica la conexión del sistema de puesta a tierra de la infraestructura de telecomunicaciones.

Los Subsistemas del SCE según la norma ANSI/TIA 568-C.1 son:

- Área de Trabajo
- Cableado Horizontal
- Cableado Vertical (Backbone)
- Entrada de Servicios
- Cuarto de Equipos
- Cuarto de Telecomunicaciones

El número de puntos que se tendrá en SCE dependerá del número de usuarios, dispositivos de red y uso que tenga el área específica de la instalación. Para las estaciones de trabajo de oficinas se utilizará un solo punto de red para conectar un teléfono IP y una conexión de datos. La ubicación de los puntos de red dependerá de la división física de oficinas y aulas, ubicación de los escritorios, pizarras, tarimas y ubicación de dispositivos de red.

El Subsistema de Cableado Horizontal estará tendido por medio de canaletas decorativas, debido al menor costo de instalación comparado a realizar un cableado por la pared internamente. Para la ubicación de los Cuartos de Telecomunicaciones se tomó en cuenta la cantidad de usuarios que debe servir en esa zona, distancia entre el último punto de red y el Cuarto de Equipos, medidas de seguridad existentes en las edificaciones dentro de las cuales se van

ubicar los cuartos de telecomunicaciones y la existencia de áreas libres de dimensiones adecuadas para la instalación de los mismos.

Debido a que en un futuro un mayor número de docentes van a poseer computadores portátiles personales y a que en el colegio se aumentarán el número de computadoras en la biblioteca y en los laboratorios de computación, se dejarán puntos adicionales en la áreas de biblioteca, sala de reuniones, salón de actos y las aulas de los laboratorios de computación.

En las siguientes figuras se muestra a distribución de los puntos de red dentro de cada área de la institución, en el que se puede observar el número de puntos por cada Bloque y se puede observar también la ubicación de los Cuartos de Telecomunicaciones y del Cuarto de Equipos; pero si se desea observar en detalle la ubicación de los cuartos de equipos, cuarto de telecomunicaciones, puntos de red, cajas de revisión y canalizaciones del cableado mirar el Anexo 11.

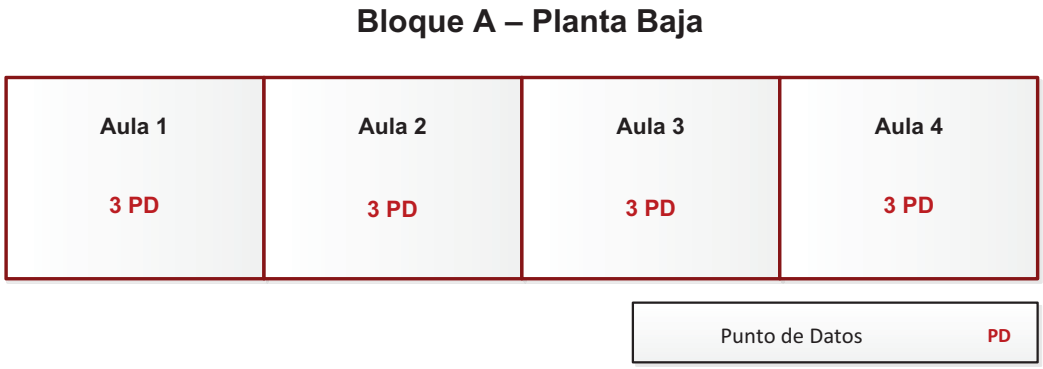


Figura 3.1: Esquema de distribución de los puntos de red en el Bloque A–Planta Baja

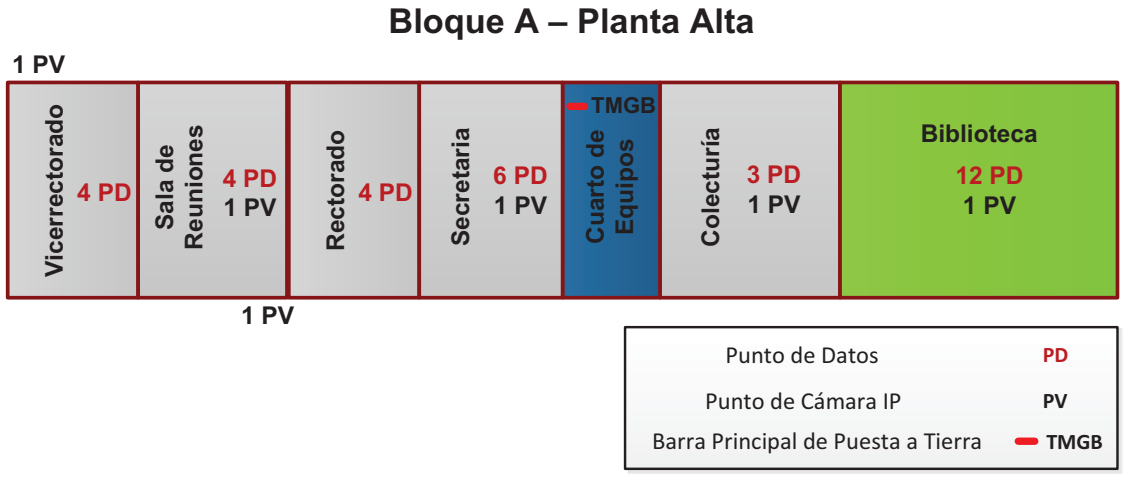


Figura 3.2: Esquema de distribución de los puntos de red en el Bloque A–Planta Alta

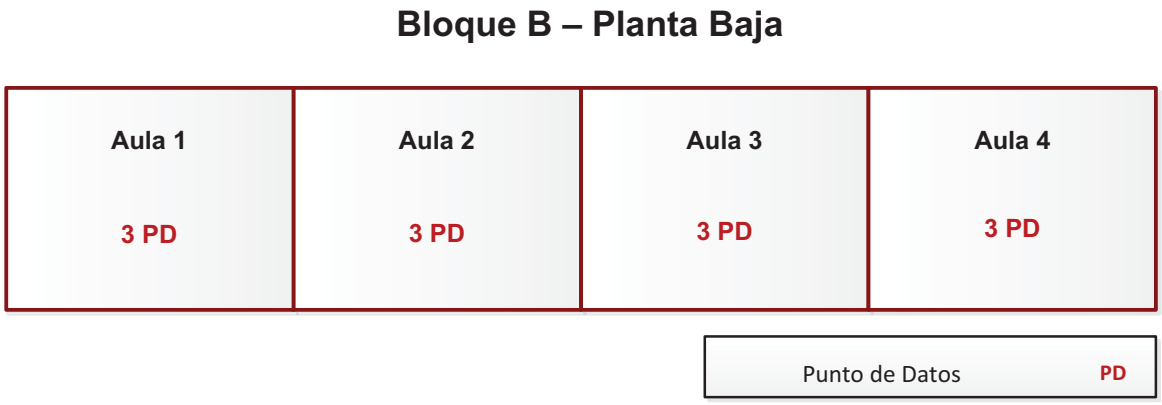


Figura 3.3: Esquema de distribución de los puntos de red en el Bloque B–Planta Baja

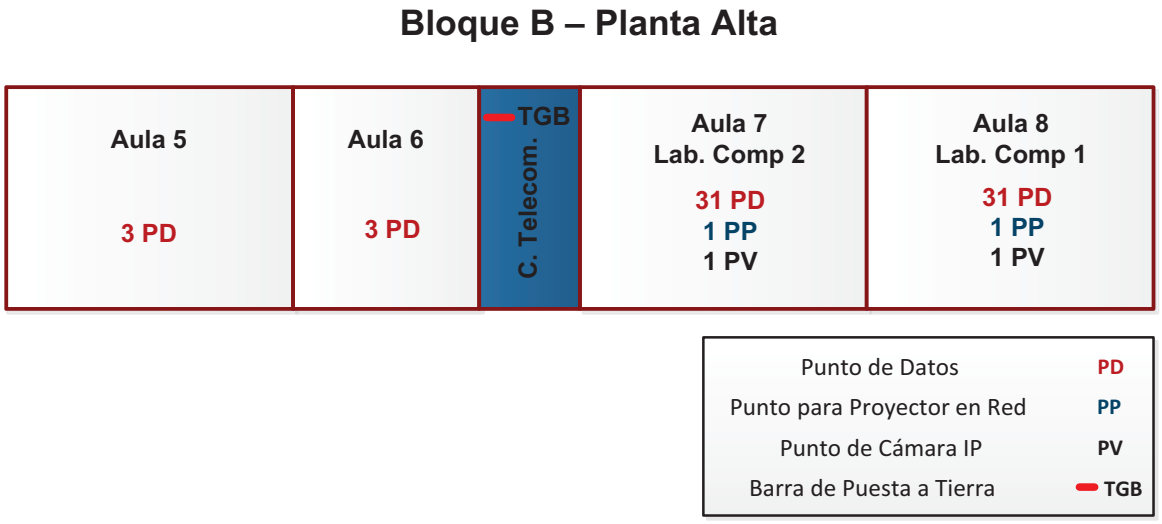


Figura 3.4: Esquema de distribución de los puntos de red en el Bloque B–Planta Alta

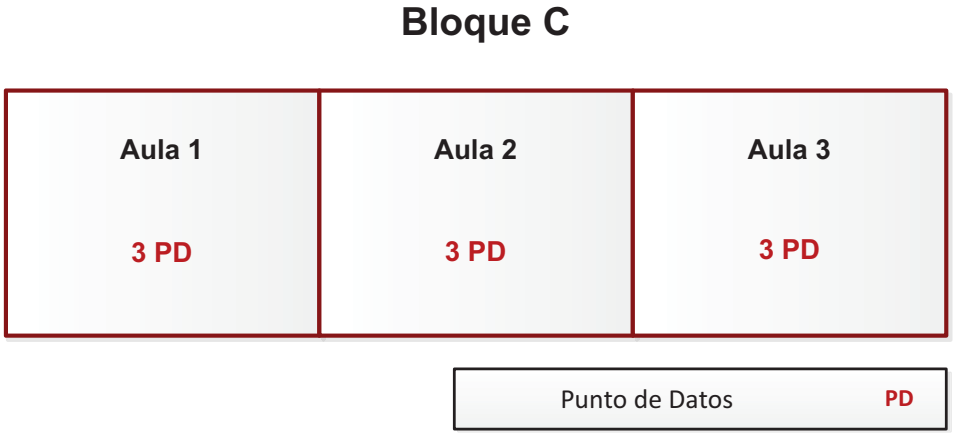


Figura 3.5: Esquema de distribución de los puntos de red en el Bloque C

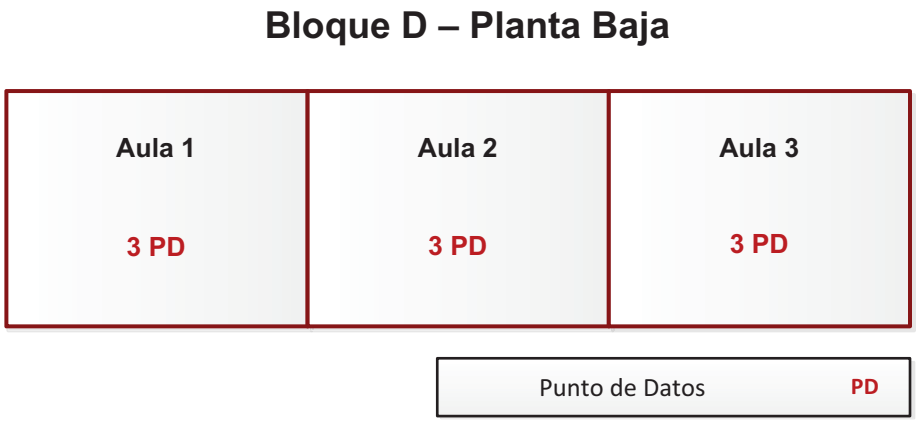


Figura 3.6: Esquema de distribución de los puntos de red en el Bloque D–Planta Baja

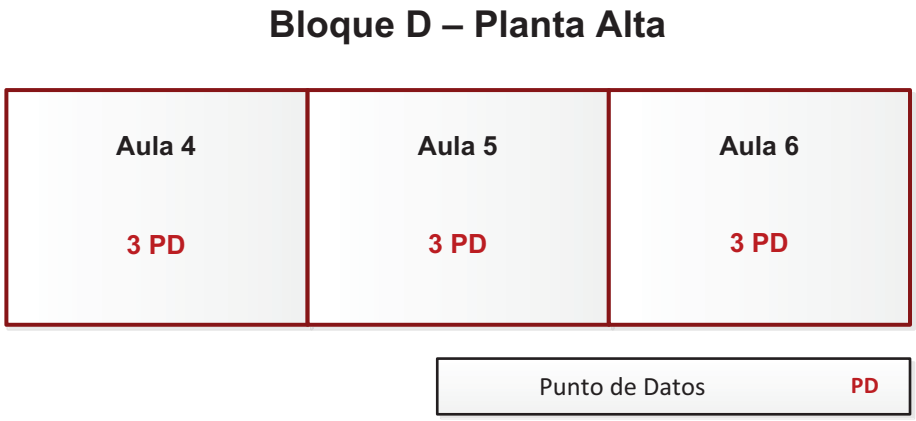


Figura 3.7: Esquema de distribución de los puntos de red en el Bloque D–Planta Alta

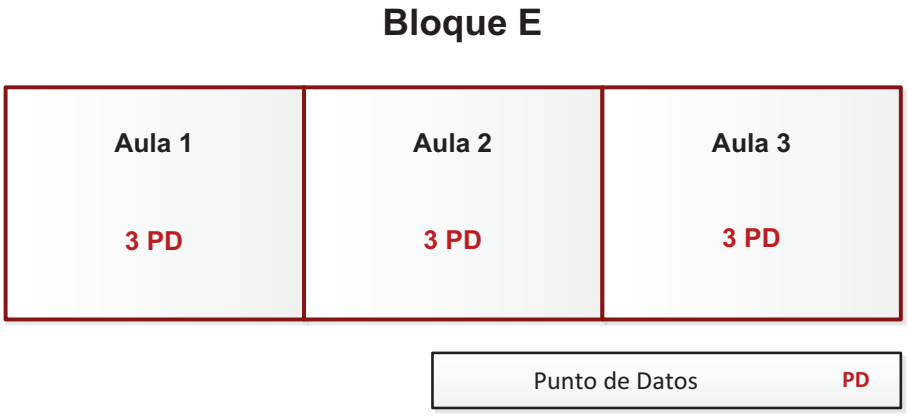


Figura 3.8: Esquema de distribución de los puntos de red en el Bloque E

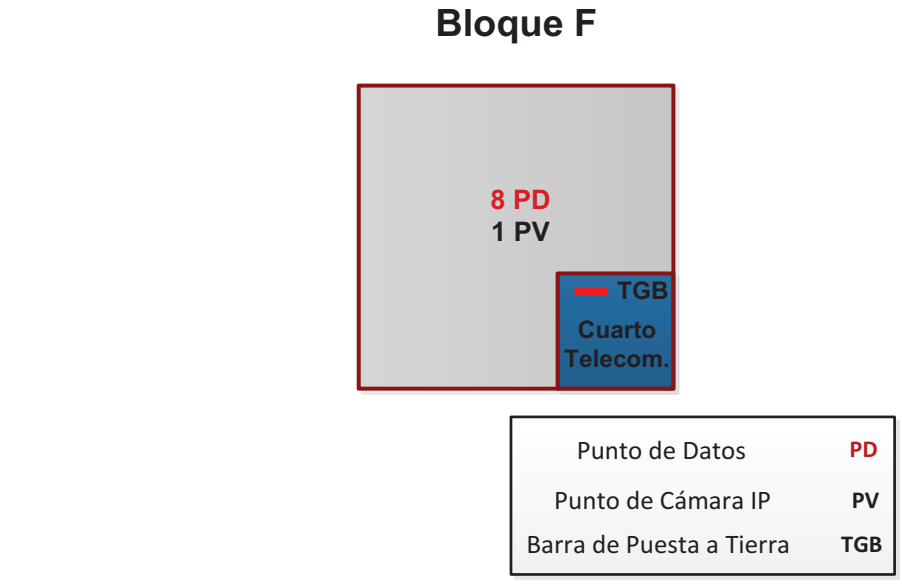


Figura 3.9: Esquema de distribución de los puntos de red en el Bloque F

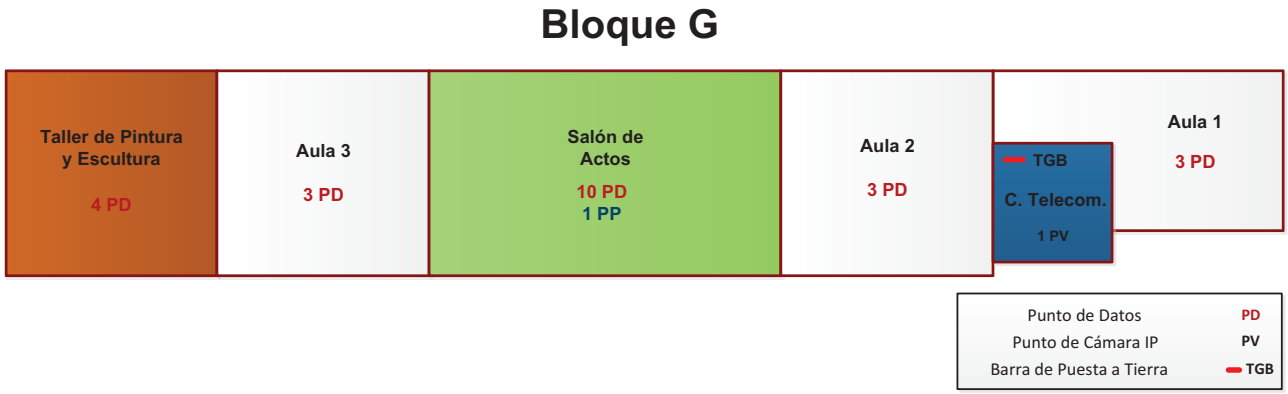


Figura 3.10: Esquema de distribución de los puntos de red en el Bloque G

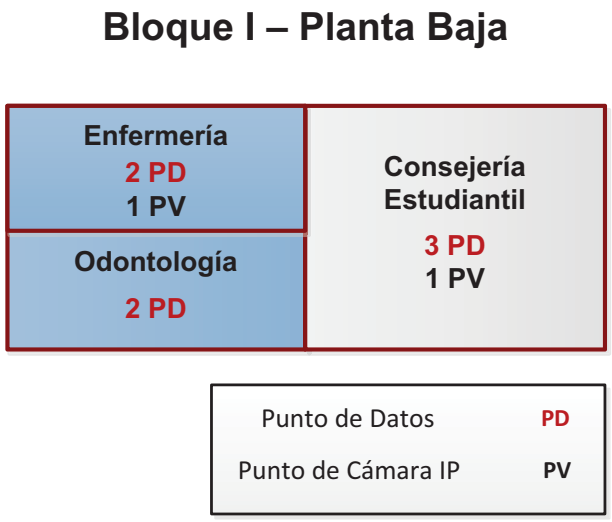


Figura 3.11: Esquema de distribución de los puntos de red en el Bloque I-Planta Baja

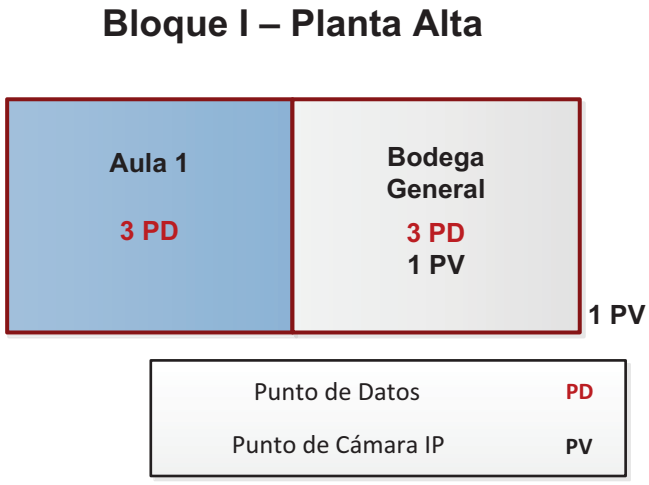


Figura 3.12: Esquema de distribución de los puntos de red en el Bloque I-Planta Alta

Figura 3.13: Esquema de distribución de los puntos de red en el Bloque H

En la Tabla 3.17 se muestran un resumen de la cantidad de puntos de red que se tiene en cada uno de los Bloques del CFD.

RESUMEN DE SALIDAS DE TELECOMUNICACIONES DEL CFD				
Bloque	**Área**	**Tipo de punto**	**No. de puntos/área**	**No. de puntos/bloque**
Bloque A – Planta Baja	Aula 1	Datos	3	50
	Aula 2	Datos	3	
	Aula 3	Datos	3	
	Aula 4	Datos	3	
Bloque A – Planta Alta	Vicerrectorado	Datos	4	
	Sala de Reuniones	Datos	4	
		Video	2	
	Rectorado	Datos	4	
	Secretaría	Datos	6	
		Video	1	
	Colecturía	Datos	6	
		Video	1	
	Biblioteca	Datos	12	
		Video	1	
Bloque B –Planta Baja	Aula 1	Datos	3	84
	Aula 2	Datos	3	
	Aula 3	Datos	3	
	Aula 4	Datos	3	
Bloque B –Planta Alta	Aula 5	Datos	3	
	Aula 6	Datos	3	
	Lab. Comp. 1	Datos	31	
		Video	1	
		Proyector	1	
	Lab. Comp. 2	Datos	31	
		Video	1	
		Proyector	1	
Bloque C	Aula 1	Datos	3	9
	Aula 2	Datos	3	
	Aula 3	Datos	3	
Bloque E	Aula 1	Datos	3	9
	Aula 2	Datos	3	
	Aula 3	Datos	3	

Tabla 3.17: Resumen de las Salidas de telecomunicaciones del CFD (cont…)

RESUMEN DE SALIDAS DE TELECOMUNICACIONES DEL CFD				
Bloque	**Área**	**Tipo de punto**	**No. puntos/área**	
Bloque D – Planta Baja	Aula 1	Datos	3	18
	Aula 2	Datos	3	
	Aula 3	Datos	3	
Bloque D – Planta Alta	Aula 4	Datos	3	
	Aula 5	Datos	3	
	Aula 6	Datos	3	
Bloque F	Inspección	Datos	8	9
		Video	1	
Bloque G	Aula 1	Datos	3	25
		Video	1	
	Aula 2	Datos	3	
	Aula 3	Datos	3	
	Salón de Actos	Datos	10	
		Proyector	1	
	Taller Pintura	Datos	4	
Bloque I – Planta Baja	Enfermería	Datos	2	17
		Video	1	
	Odontología	Datos	2	
	Consejería Estudiantil	Datos	3	
		Video	1	
Bloque I – Planta Baja	Aula 1	Datos	3	
	Bodega General	Datos	3	
		Video	2	
Bloque H	Lab. de Física	Datos	3	29
		Video	1	
		Proyector	1	
	Lab. de Química	Datos	3	
		Video	1	
		Proyector	1	
	Lab. de Biología	Datos	3	
		Video	1	
		Proyector	1	
	Aula 1	Datos	3	
	Sala de Prof.	Datos	8	
	Taller Carpint.	Datos	3	
Total de puntos de red				250

Tabla 3.17: Resumen de las Salidas de telecomunicaciones del CFD

3.3.1.1 Diseño de los Subsistemas de Cableado Estructurado

3.3.1.1.1 Área de Trabajo

El área de trabajo se extiende desde la salida de telecomunicaciones hasta la ubicación del equipo que utilizan los usuarios de red. En este subsistema se debe especificar el tamaño promedio que debe tener el patch cord para la conexión del usuario a la red LAN; las características con las que debe cumplir este cable deben ser:

- Cable UTP cat. 5E terminado en fábrica
- Cumplir con la norma ANSI/TIA 568-C.2
- Resistencia a altas temperaturas, desgaste mecánico y protección contra tensiones del cable.
- Longitud de 2 metros.

3.3.1.1.2 Subsistema de Cableado Horizontal

El Subsistema de Cableado Horizontal es aquel ubicado desde el área de trabajo hasta el Cuarto de Telecomunicaciones. Al ser el CFD una institución educativa fiscal que no posee un presupuesto para realizar mejoras o cambios importantes en sus instalaciones, se recomienda realizar la implementación de un SCE de bajo costo; es por ello, que se realizará el tendido del cableado por medio de canaletas y bandejas de cableado sobre techo falso. Los radios de curvatura que se tendrá no será menor a 4 veces el diámetro del cable y se utilizarán amarres tipo velcro para agrupar el cableado dentro de cualquier tipo de canalización.

a) Canaletas

Para el tendido del cableado horizontal en aulas y oficinas de los bloques A, B, C, D, F e I se utilizarán canaletas decorativas, debido a que estas instalaciones no poseen techo falso, ni tuberías por medio de pared, por las que pueda tenderse el cableado.

Todas las canaletas decorativas que saldrán desde el Cuarto de Equipos y por las cuales se distribuye el cableado hacia las oficinas y aulas estarán ubicadas a la

altura del techo de las mismas (2.5 metros de altura) para evitar el fácil acceso y manipulación del cableado por personal no autorizado; una vez dentro de oficinas y aulas las canaletas bajarán a ras de piso cuidando siempre que las mismas pasen desapercibidas y no causen molestias en la movilidad dentro de las instalaciones. Las cajas de revisión se usarán en las derivaciones de la canaleta principal hacia oficinas o aulas y en secciones rectas cuya longitud exceda los 30 metros.

Las dimensiones de las canaletas decorativas y cajas de revisión serán las apropiadas para que solo tengan ocupada el 40% de su capacidad máxima, dejando espacio para el crecimiento futuro.

Las canaletas a utilizar deben estar hechas de materiales auto extinguibles, con resistencia a los rayos UV, humedad y al estrés mecánico.

b) Bandejas de Cable

Los bloques E, G y H están conformados por aulas de una sola planta con cubiertas fabricadas con estructuras de hierro, que van a ser aprovechadas para la sujeción de las bandejas de cableado. Se utilizarán las dimensiones de bandeja de cableado adecuadas para no superar el 25% de la capacidad de las mismas. Para las bajantes del cableado desde la bandeja de cables hasta el nivel de suelo se utilizarán canaletas decorativas.

c) Salidas de Telecomunicaciones

Las Salidas de Telecomunicaciones en lugares como oficinas y la Biblioteca de la institución harán uso de una Salida de Telecomunicaciones Multi-Usuario (*MUTO*) para permitir la flexibilidad en el modo de distribución de las estaciones de trabajo sin tener que cambiar la instalación del cableado horizontal. Las Salidas de Telecomunicaciones en el resto de las instalaciones de la institución usarán faceplates de uno y dos puertos de tipo RJ-45, algunas de estas salidas se encontrarán elevadas a una altura mínima de 2 metros sobre el piso, pues serán utilizadas para la conexión de proyectores asegurados en el techo. Para las cámaras de seguridad existirá cableado que se conectará directamente a ellas desde el Cuarto de Telecomunicaciones más cercano sin ninguna otra conexión.

Los faceplates a usar deben tener las siguientes características:

- Porta etiquetas transparente para identificación del punto
- Cubre polvos abatible
- Diseño adecuado para instalación horizontal o vertical

Los jacks deben cumplir con las siguientes especificaciones:

- Tipo de conector frontal RJ-45
- Diseñado para instalación en faceplates planos y angulares
- Para configuraciones de conexión T568A y T568B
- Cumplir con la norma ANSI/TIA 568-C.2

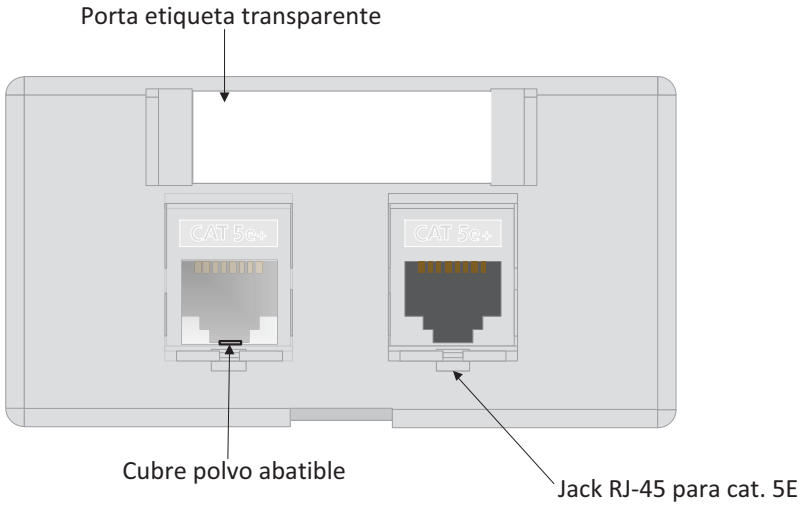


Figura 3.14: Esquema de una salida de telecomunicaciones

3.3.1.1.3 Subsistema de Cableado Vertical

El Subsistema de Cableado Vertical también llamado Backbone es aquel que conecta los dispositivos de conectividad de los Cuartos de Telecomunicaciones y Cuarto de Equipos. El Backbone usará cable UTP cat. 6 de tipo CMR y que cumpla con las normas UL-444 para tener una protección contra estrés mecánico, exposición al calor, al frío y a la humedad.

El cableado vertical que baje de los cuartos de telecomunicaciones o de equipos ubicados en la segunda planta se canalizarán por medio de conduit PVC de 4” recubierto por una estructura de cemento para asegurar su integridad, estos

conduits deben sobresalir una altura de 10 cm sobre el nivel del piso en cada uno de estos cuartos.

El cableado vertical entre edificios se canalizará por medio de tubería PVC de 3” y ésta a su vez correrá dentro de tubería de cemento de 4” enterrada a 1 metro de profundidad con cajas de revisión en los extremos por donde el cableado entra a estas tuberías.

Los extremos de las tuberías estarán sellados con material anti fuego para prevenir el avance de un incendio.

3.3.1.1.4 Cuarto de Equipos

El Cuarto de Equipos es aquel donde se encuentran los dispositivos de conectividad pertenecientes a la institución y aquellos que los proveedores de servicio de Internet y telefonía instalan; en este espacio también se encuentran los servidores de las aplicaciones que se ofrecen a los usuarios del CFD.

El Cuarto de Equipos estará ubicado junto a la oficina de Colecturía en el Bloque A del CFD, a esta área llegará el cableado vertical proveniente de los cuartos de telecomunicaciones y el cableado horizontal de los puntos de red del Bloque A. El Cuarto de Equipos dará servicio a 67 puntos de red y a él entrarán 73 cables de cat. 5e y cat.6 que pertenecen al cableado horizontal y vertical.

		5e	6	$6A_1$	$6A_2$
Average OD		.185"	.230"	.330"	.300"
Cable Tray*	2" x 6"	111	72	35	42
	4" x 8"	298	192	93	113
	6" x 20"	1116	722	350	424

Tabla 3.18: Capacidad de Bandeja de Cables (# de cables) llenada al 25% [PW26]

Esta área estará separada de las oficinas por paredes de hormigón con una dimensión de 5.7 m x 2.8 m y una altura de 2.5 m, con una puerta metálica de dimensiones 0.9m de ancho x 2m de alto asegurada con cerradura. El piso de esta área será de cerámica y las ventanas que existen en el lugar deben ser cerradas para evitar polvo que pueda dañar los equipos.

La distribución del cableado dentro del área del Cuarto de Equipos se realizará por medio de bandejas de cableado sujetas al techo, que tendrán el tamaño apropiado para que solo el 25% de su capacidad esté ocupada, y según la Tabla 3.18 se deberá ocupar una bandeja de 2”x6”.

Todos los patch cords para la conectividad entre los dispositivos de red instalados dentro de un rack deben cumplir con las siguientes características:

- Terminados en fábrica
- Cumplir con la norma ANSI/TIA 568-C.2
- Resistencia a altas temperaturas, desgaste mecánico y protección contra en los extremos contra tensiones
- Longitud de 1.2 metros

Los patch panels utilizados en todos los cuartos de equipos y de telecomunicaciones deben cumplir con las siguientes especificaciones:

- Terminados en fábrica
- Cumplir con las norma ANSI/TIA 568-C.2
- Patch panel para montaje en rack de 19” con terminal para conexión a tierra.

De ser posible en todos los casos se dejará un espacio de 80 cm en la parte delantera y trasera del rack para tener un óptimo acceso a las conexiones del cableado y equipos de conectividad.

En el Cuarto de Equipos se contará con un rack abierto que cumpla las siguientes características:

- Rack de 42 U de 19” y 31” de profundidad, con patas niveladoras
- 2 patch panel de 48 puertos
- 2 organizadores de cables horizontales de 2U.
- 2 organizadores de cables verticales
- 2 bandejas horizontales fijas de 18” de profundidad
- 2 barras multi-contactos de 1U con 6 tomacorrientes, 120V, 15 A con protección anti sobrecarga y borneras para conexión a tierra
- 2 Paneles de Ventiladores de 120 V de 2U
- El rack también debe poseer una bornera para su conexión a tierra

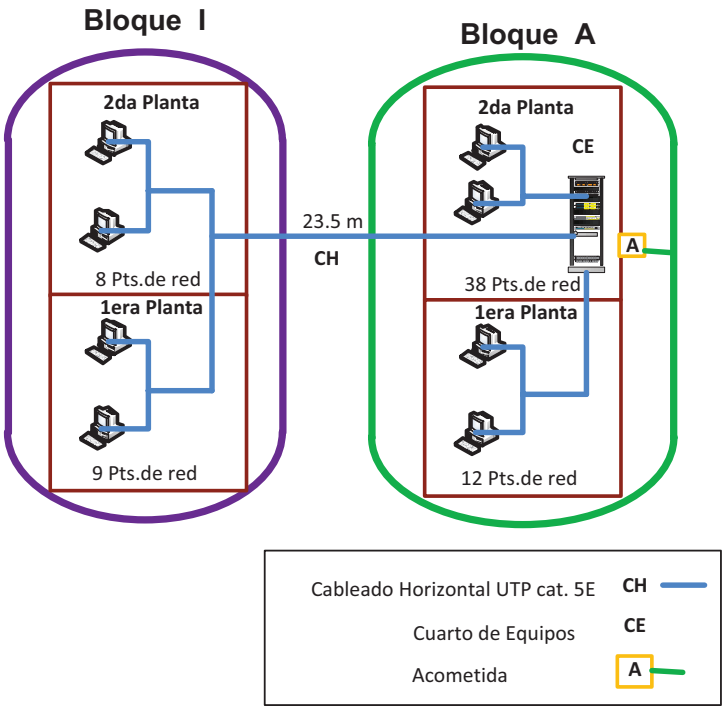


Figura 3.15: Esquema del cableado que llega al Cuarto de Equipos

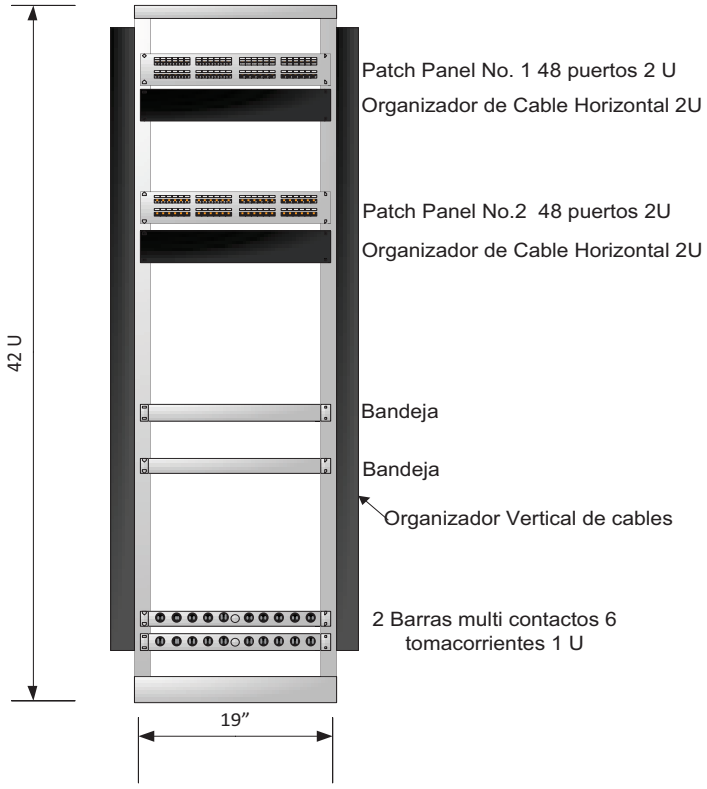


Figura 3.16: Esquema de la distribución del rack del Cuarto de Equipos

3.3.1.1.5 Cuartos de Telecomunicaciones

Para la ubicación de los Cuartos de Telecomunicaciones se debe considerar el número de estaciones de trabajo por cada edificación de la institución y la distancia desde el último punto de red de una edificación hasta el Cuarto de Equipos. Siguiendo estos parámetros se implementarán 3 Cuartos de Telecomunicaciones, el primero cercano a los laboratorios de Computación que brindará servicio a los puntos de red del Bloque B; el segundo estará dentro de un aula del Bloque G, brindando servicio a los puntos de red de los bloques G, E y H; y el tercero estará ubicado dentro del bloque F dentro de un rack cerrado montado en la pared y brindará servicio a los puntos de red de los bloques C, D y F; y por último los puntos de red del bloque A se conectan directamente al Cuarto de Equipos.

A continuación se muestra un diagrama en el que puede observar la ubicación relativa y las distancias que separan a cada Cuarto de Telecomunicaciones del Cuarto de Equipos ubicado en el Bloque A.

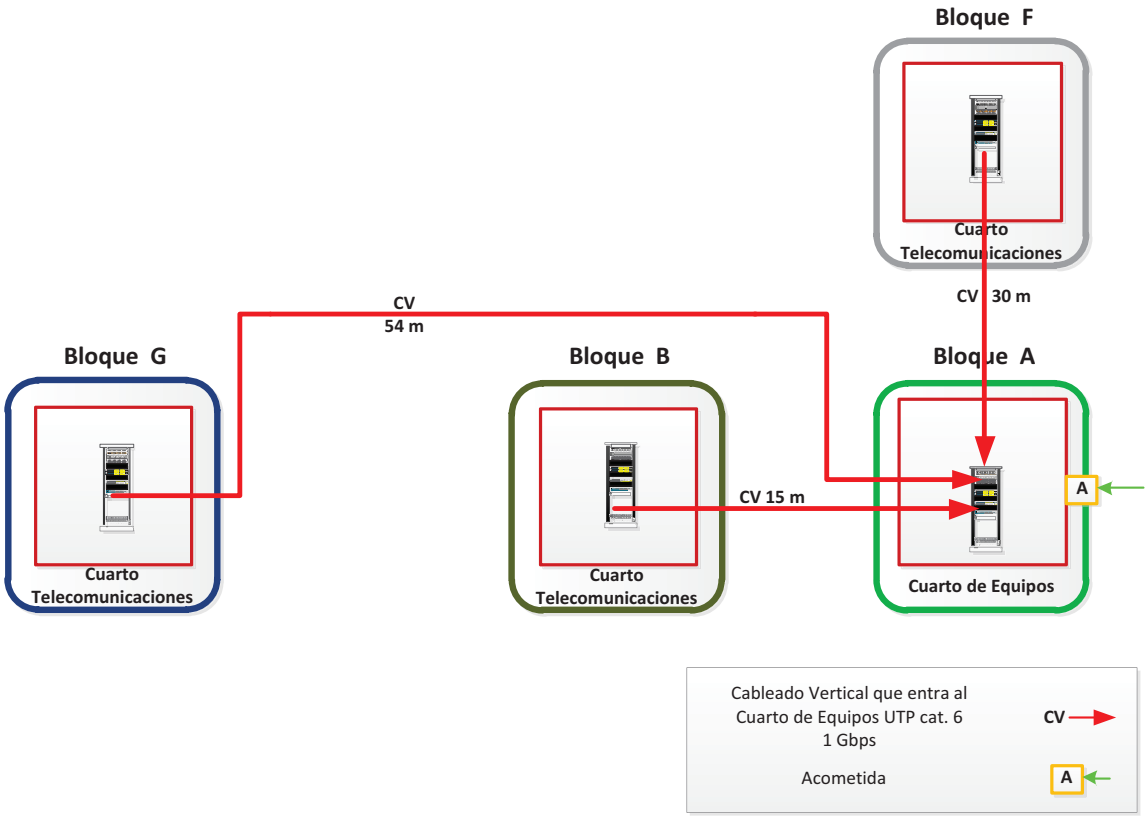


Figura 3.17: Diagrama de la ubicación de los Cuartos de Telecomunicaciones

Cuarto de Telecomunicaciones Bloque B:

El Cuarto de Telecomunicaciones del Bloque B tendrá paredes de bloque prensado, piso de cerámica y con dimensiones de 3 m de largo, 2 m de profundidad y 2.5 m de alto. La entrada a esta área será por medio del laboratorio de computación ubicada en el aula 7, a través de una puerta metálica con 2 m de altura y 0.9m de ancho asegurada con cerradura.

Este cuarto de telecomunicaciones brindará servicio a los 84 puntos de red que existen en el Bloque B del CFD, de los cuales 20 puntos de red se encontrarán en los laboratorios de computación pues se prevé que se aumentará el número de ordenadores en estos sitios para poder tener un estudiante por computadora, y con estas 10 salidas de telecomunicaciones disponibles para cada laboratorio se llegará a tener un número de puntos que se aproxima a la cantidad de estudiantes que reciben clases en estos laboratorios.

Para la conexión de los laboratorios de computación se reutilizarán los switches NEXXT que el colegio posee, ya que se observó que tanto la velocidad de acceso como la velocidad de backbone de estos switches son suficientes para manejar el flujo de datos total que generará la navegación en Internet y el acceso a las aulas virtuales por parte de los estudiantes. El resto de puntos de red de este bloque estarán conectados a switches administrables que permitan configurar un trato diferenciado para el tráfico de voz y de video, pues desde estos puntos se podrá tener acceso a servicios en que se transmita datos de voz o de video. Todos los switches mencionados estarán instalados dentro un rack abierto dentro del Cuarto de Telecomunicaciones B.

La bandeja de cables que se usará dentro del cuarto de telecomunicaciones del Bloque B según la Tabla 3.18 deberá ser de 2”x6” ya que debe transportar 91 cables de red.

El rack abierto de éste cuarto de telecomunicaciones cumplirá con las siguientes características:

- Rack de 42 U de 19” y 31” de profundidad, con patas niveladoras y borneras para conexión a tierra

- 2 Patch panel de 48 puertos
- 2 organizadores de cables horizontales de 2U.
- 2 organizadores de cables verticales de 6 pies
- 1 bandeja horizontal fija de 18” de profundidad
- 2 barras multi-contactos de 1U con 6 tomacorrientes, 120V, 15 A con protección anti sobrecarga y borneras para conexión a tierra

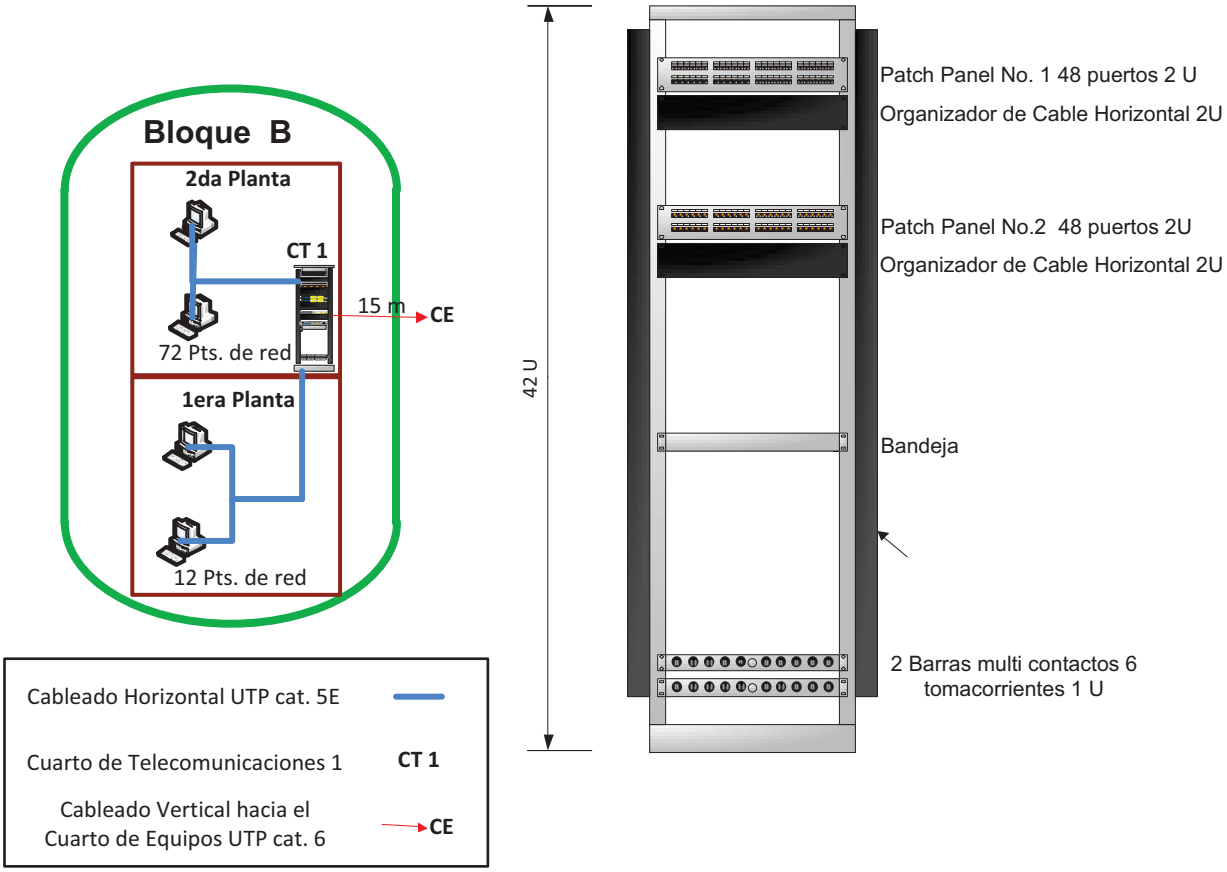


Figura 3.18: Esquema del cableado y distribución del rack del Cuarto de Telecomunicaciones del Bloque B

Cuarto de Telecomunicaciones Bloque G:

El Cuarto de Telecomunicaciones ubicado en el Bloque G será construido con paredes de bloque prensado, piso de cerámica y tendrá unas dimensiones de 3m de largo, 3m de profundidad y 2.3m de altura; con una puerta metálica de 2m de alto por 0.9m de ancho asegurada con cerradura.

Al Cuarto de Telecomunicaciones proporciona conectividad a 9 puntos de red del Bloque E, 25 puntos de red del Bloque G, y 29 puntos de red en el Bloque H.

Para manejar el cableado que entra al cuarto de telecomunicaciones se utilizará una bandeja de cables de una dimensión de 2"x6" ya que deberá soportar 63 cables de red categoría 5E, este resultado es obtenido luego de la suma de los cables de red de los Bloques E, G, H.

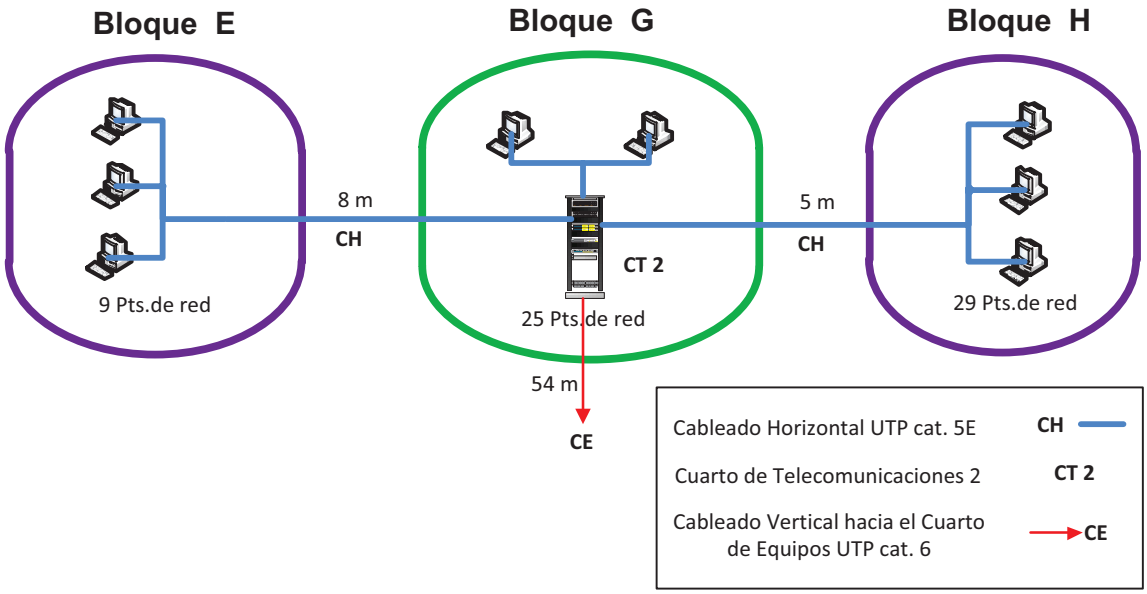


Figura 3.19: Esquema del cableado que ingresa al Cuarto de Telecomunicaciones del Bloque G

Los equipos de conectividad que van a funcionar dentro de este cuarto de telecomunicaciones deberán estar instalados en un rack abierto que cuente con las siguientes características:

- Rack de 42 U de 19" y 31" de profundidad, con patas niveladoras y borneras para conexión a tierra
- 2 Patch panels de 48 puertos
- 2 organizadores de cables horizontales de 2U.
- 2 organizadores de cables verticales de 6 pies
- 1 bandeja horizontal fija de 18" de profundidad
- 1 barra multi-contactos de 1U con 6 tomacorrientes, 120V, 15 A con protección anti sobrecarga y borneras para conexión a tierra.

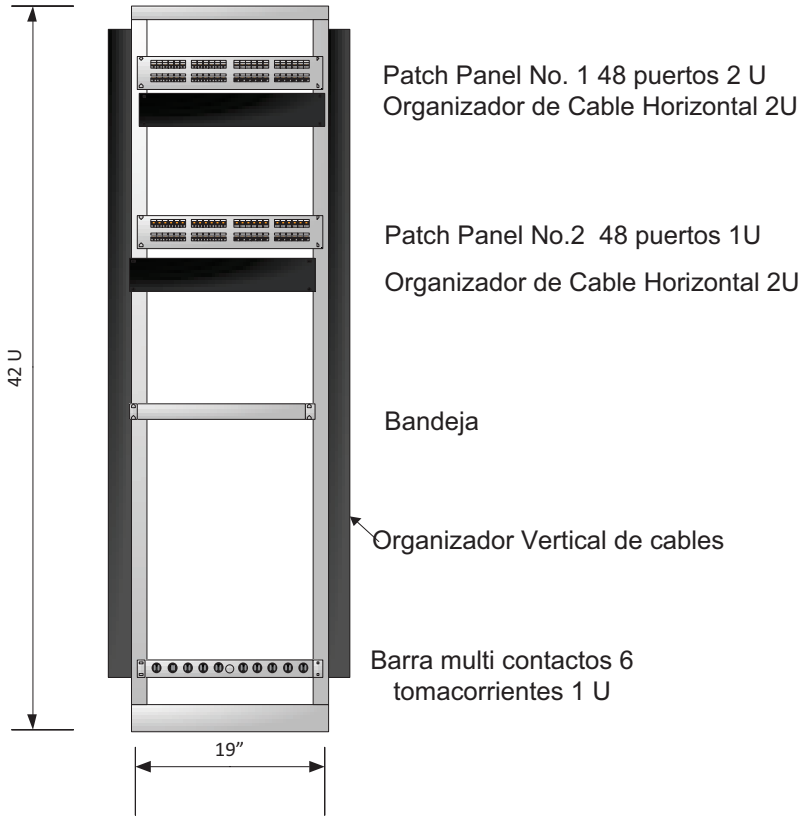


Figura 3.20: Esquema de distribución del rack del Cuarto de Telecomunicaciones del Bloque G

Cuarto de Telecomunicaciones Bloque F:

Al estar bastante alejados los bloques C, D y F del Cuarto de Equipos se vio la necesidad de colocar un cuarto de telecomunicaciones dentro de uno de estos tres bloques para que a través de los equipos contenidos en este cuarto se pueda brindar conectividad a los puntos de red de esos bloques.

Se recomienda utilizar el Bloque F para albergar los equipos de conectividad debido a que está asegurado tanto en sus ventanas como su puerta con protecciones metálicas.

Este cuarto de telecomunicaciones deberá dar servicio a 9 puntos de red del Bloque C, 18 puntos del Bloque D y 9 puntos del Bloque F, es decir en total brinda conectividad a 36 puntos de red.

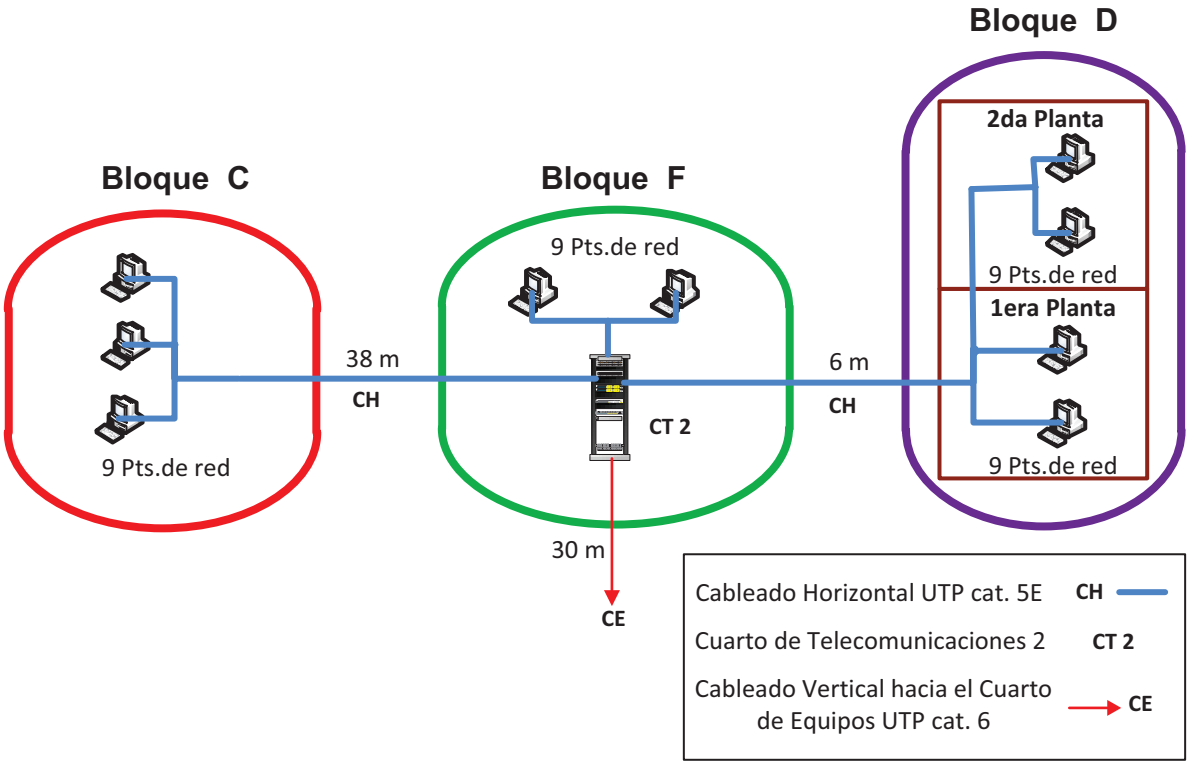


Figura 3.21: Esquema de cableado que ingresa al Cuarto de Telecomunicaciones del Bloque F

Para colocar los dispositivos de conectividad se usará un rack de piso cerrado con paneles desmontables con cerradura debido a que no estará dentro de un espacio dedicado para dispositivos de red por cuestiones del espacio disponible. Las características que el rack debe cumplir son las siguientes:

- Rack cerrado con paneles desmontables con cerradura de 24 U de 19" y 31" de profundidad y borneras para conexión a tierra
- 2 Paneles de ventiladores
- 1 Patch panel de 48 puertos
- 1 Patch panel de 24 puertos
- 1 organizador de cables horizontal de 2U
- organizador de cable vertical tipo anillo independientes
- 1 barra multi-contactos de 1U con 6 tomacorrientes, 120V, 15 A con protección anti sobrecarga y borneras para conexión a tierra

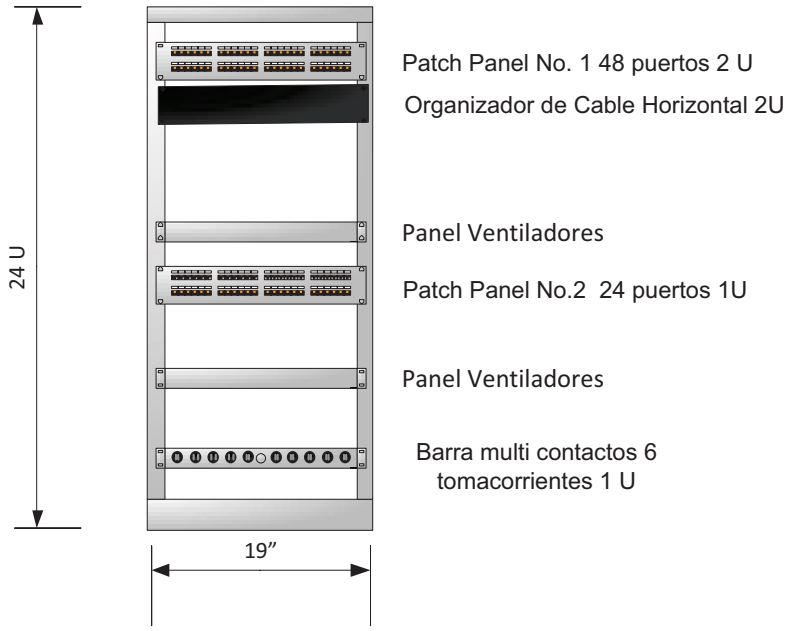


Figura 3.22: Esquema de distribución del rack del Cuarto de Telecomunicaciones del Bloque F

3.3.1.1.6 Entrada de Servicios

La Entrada del cableado de los Servicios provistos por ISP's y compañía telefónica se realizará de manera aérea pues la empresa CNT usa los postes de tendido eléctrico para la distribución de su cableado de fibra óptica y telefonía analógica.

3.3.1.2 Administración y Etiquetado del SCE[P1]

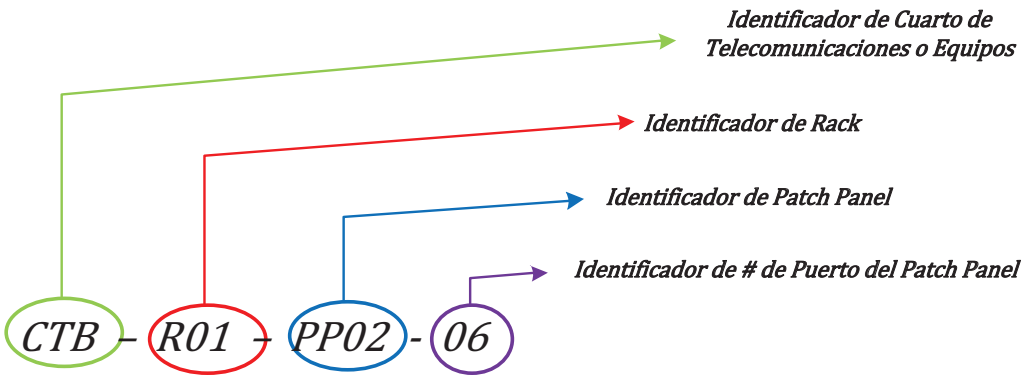
Siguiendo la norma EIA/TIA 606-A, se deben etiquetar con una identificación única a todos los elementos del SCE como:

- Cables
- Rutas de acceso de telecomunicaciones (conduit, firestops, etc.)
- Cuartos de telecomunicaciones y de equipos
- Locaciones de conexión a tierra y uniones (TMGB, TGB, TBB).
- Equipo de conectividad.
- Edificio.
- Cables y rutas de entrada de servicios
- Salidas de telecomunicaciones

Las identificaciones de los diferentes elementos del SCE deberán seguir una nomenclatura común, para lo cual, se seguirá el siguiente orden de izquierda a derecha: identificador del Cuarto de Telecomunicaciones o de Equipos, identificación de rack, identificación de patch panel y número de puerto de patch panel. Luego de ello se agruparán los cables con cintas de velcro según la zona a los cuales éstos se dirijan.

$$Id.\,Cuarto\ de\ Telecomuniciones/Equipos - Id.\,Rack - \ Id.\,Patch\ Panel - \#\ Puerto\ en\ Patch\ Panel$$

Una identificación quedaría de la siguiente manera:



El significado de la anterior identificación es: *El cable que tenga esta identificación se encontrará conectado al Puerto No. 6 del Patch Panel No. 2 del Rack No. 1 del Cuarto de Telecomunicaciones del Bloque "B".*

Otro ejemplo; el identificador para un cable que está conectado al Puerto No. 35 de Patch Panel No. 1 del Rack No. 1 del Cuarto de Equipos sería:

$$CE - R01 - PP01 - 35$$

El cableado de backbone entre edificios deberá identificar a más de los identificadores de Cuartos de Equipos y de Telecomunicaciones los identificadores de los bloques de edificación donde estos cuartos se encuentren.

Estos identificadores se imprimirán de manera térmica sobre etiquetas adhesivas de coloraciones adecuadas según el tipo de terminación al que pertenezca el elemento a marcar.

Código de Colores de Campos de Terminación	
Tipo de Terminación	**Color**
Punto de demarcación	Naranja
Conexión de red del lado del cliente	Verde
Equipo común (PBX, Multiplexor, Servidor)	Púrpura
Backbone de primer nivel	Blanco
Backbone de segundo nivel	Gris
Cableado Horizontal (solo extremo de los Cuartos de Telecomunicaciones)	Azul
Backbone entre edificios	Marrón
Circuitos Auxiliares (Alarmas de Seguridad)	Amarillo
Circuito de Alarma de incendio	Rojo

Tabla 3.19: Código de colores según el campo de terminación

Se debe crear una documentación en la que se encuentren los detalles de identificación de punto de red, tipo de cable, longitud y equipo de conexión.

3.3.1.3 Puesta a Tierra[P6, PW20, PW21]

La infraestructura de Puesta a Tierra sigue el estándar ANSI/EIA/TIA 607-A el cual protege de sobre tensiones y electricidad estática que pueda dañar a los dispositivos de telecomunicaciones del cuarto de Equipos, el Cuarto de Telecomunicaciones y la Entrada de Servicios.

Los elementos de la infraestructura de Puesta a Tierra son:

- TMGB (*Telecommunicactions Main Grounding Bar*) Barra Principal de Puesta a Tierra
- TGB (*Telecommunicactions Grounding Busbar*) Barra de Puesta a Tierra
- TBB (*Telecommunication Bonding Backbone*) Unión Vertical de Telecomunicaciones

Características que debe tener el sistema de Puesta a Tierra de telecomunicaciones son:

- Las barras de Puesta a Tierra deberán ser de cobre.
- La TMGB debe tener una dimensión mínima de 100 mm de ancho y 6mm de grosor.
- La TMGB debe estar ubicada lo más cercano a la entrada de servicios.
- La TGB debe tener una dimensión mínima de 50 mm de ancho y 6mm de grosor.
- La barra de Puesta a Tierra debe estar aislada del soporte de empotramiento y dejará al menos 50 mm de espacio entre ésta y la pared donde está instalada.
- Las dimensiones y espacio mínimo entre los agujeros de conexión y empotramiento de las barras de puesta a tierra TMGB y TGB deben tener las medidas que se muestran en el Anexo 13.
- Se instalarán barras de Puesta a Tierra dentro de los Cuartos de Telecomunicaciones para las conexiones de los equipos ubicados en estas áreas.
- Para realizar las conexiones en las barras de Puesta a Tierra se usará líquido antioxidante en los contactos para evitar la corrosión y la resistencia de contacto. Los cables deben usar contactos de presión para los extremos de conexión.
- Los conductores de la unión vertical de las barras de Puesta a Tierra (TBB) van a ser conducidos por tuberías y canaletas no metálicas.
- Los conductores usados como unión vertical de telecomunicaciones serán de cable 1 AWG desnudo debido a la distancia entre las barras de Puesta a Tierra. Este dato se basa en la tabla de relación entre tamaño de cable y la longitud del mismo que se puede ver en el Anexo 13.
- La TMGB estará conectada a una malla compuesta de 3 varillas copperweld de 2 m de longitud y 16 mm de diámetro.
- Las varillas estarán enterradas al menos a 50 cm de profundidad en un terreno tratado con gel químico para aumentar la conductividad del suelo. La separación entre electrodos deberá ser al menos 4 veces a la longitud de la varilla copperweld. La resistencia eléctrica que deberá presentar el suelo no debe superar los 5 Ω.

- La unión entre conductor y la malla de puesta a tierra deberá hacerse con soldadura exotérmica para asegurar la menor resistencia de contacto.

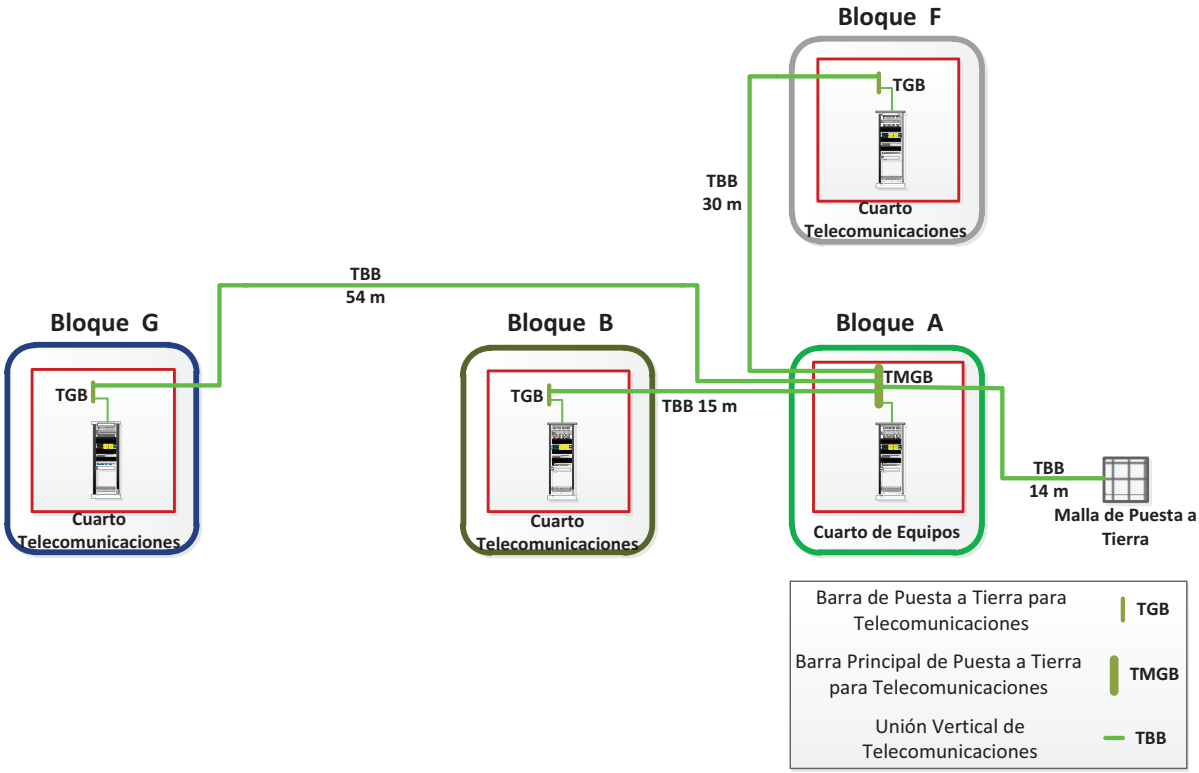


Figura 3.23: Esquema de ubicación de la Malla de Puesta a Tierra del CFD

3.3.1.4 UPS y Generador Eléctrico [P7, PW22]

El lugar donde se encuentra el CFD está dentro de una zona de fábricas e industrias, por lo que la red eléctrica que da servicio a la institución está expuesta a grandes variaciones de voltaje que han causado daño a los dispositivos de conectividad, entre estos dispositivos están el servidor HP Proliant D160 G y la central telefónica analógica, los que fueron quemados cuando hubo una sobretensión en las líneas eléctricas. Es por ello que se vio la necesidad de contar con dispositivos que proteja a los equipos de conectividad que integran la red de datos de la institución y que brinden la energía eléctrica necesaria para que las actividades del colegio se sigan realizando con normalidad; por lo que se optó por una solución doble es decir un UPS que mantenga funcionando los equipos de conectividad, la telefonía IP y la video seguridad durante el tiempo suficiente como para que un generador eléctrico sea encendido y alimente a estos equipos durante al menos unas 6 horas.

El equipo que se recomienda usar es un UPS de tipo On-Line que brindará protección ante sobretensiones, picos, rayos y cualquier otra perturbación eléctrica que pueda presentarse; además, de poder usarse como una fuente de energía redundante en un período de tiempo suficiente como para guardar la información y apagar apropiadamente los equipos de conectividad, y estaciones de trabajo.

Para los cálculos de la capacidad del UPS se deberán tomar en cuenta las computadoras y teléfonos IP presentes en las oficinas administrativas, los servidores, los dispositivos de conectividad del Cuarto de Equipos y las cámaras IP.

Para obtener la capacidad que el UPS deberá sumar las potencias en Voltiamperios (*VA*) de cada dispositivo que estará conectado al UPS; en el caso de que un equipo como un computador no disponga del dato de potencia en Voltiamperios se deberá realizar el siguiente cálculo, en el que la potencia en Voltiamperios es un 40% mayor a la potencia del equipo en Watios:

$$Potencia\ \ VA\ = Potencia\ W\ * 1.4$$

$$Potencia\ [VA] = 200\ W\ * 1.4 = 280\ [\mathrm{VA}]$$

En la Tabla 3.20 se muestra el cálculo de la capacidad mínima que el UPS deberá tener.

Cálculo de la Capacidad del UPS					
Equipos	**Número**	**Voltaje [V]**	**Potencia [W]**	**Potencia [VA]**	**Potencia Total [VA]**
Pc's	5	120	200	280	1400
Switch Acceso para Teléfonos y Cámaras IP	1	120	715	1001	1001
Switch de Acceso	3	120	200	280	840
Switch de Core	2	120	350	490	980
Servidores	3	120	500	700	2100
Router	1	120	350	490	490
Access Point	2	120	16	22.4	44.8
				Total	6855.8

Tabla 3.20: Cálculo de la capacidad del UPS del Cuarto de Equipos

Según el resultado obtenido sobre la cantidad de potencia consumida por los equipos de conectividad y estaciones de trabajo del personal administrativo se recomienda sobredimensionar la capacidad del UPS en un 30% para evitar con esto una sobrecarga en el UPS. La selección de un UPS de 10 KVA de capacidad garantizará al menos 12 minutos de funcionamiento de todos los equipos en caso de un corte eléctrico y con este tiempo se puede echar un generador eléctrico que permita alimentar a estos equipos.

El generador deberá tener una potencia de al menos 10KVA ya que la potencia del UPS al que estarán conectados los equipos de conectividad es de esa capacidad, además el generador debe poder funcionar por al menos 6 horas ya que con este tiempo se supliría casi por completo la jornada laboral de la institución y es tiempo prudente para que el suministro eléctrico se restablezca por completo.

3.3.1.4.1 Características Técnicas del UPS y del Generador Eléctrico

A continuación se encuentran las características técnicas que deberá tener el UPS:

- Como se dijo en el punto 3.3.1.4 la capacidad mínima con la que deberá contar el UPS es de 10 KVA, con la posibilidad de añadir al menos tres bancos de baterías externas con el objetivo de que el equipo pueda abastecer con energía a un tiempo mayor en caso de ser necesario.
- Los bancos de baterías deben estar completamente sellados, no deben necesitar mantenimiento y deben poder añadirse fácilmente al UPS.
- Para que los equipos conectados al UPS no se vean afectados por los cambios de voltaje que suceden en la transferencia entre el suministro de energía de la red eléctrica al suministro por baterías del UPS se utilizará el mecanismo de doble conversión online que garantiza que los equipos conectados al UPS no sufrirán daños por la variaciones de tensión o corriente en este cambio.
- El UPS deberá contar con luces indicadoras que ofrezcan información sobre el estado de las baterías, nivel de carga de las mismas y funcionamiento general del UPS.

- Para tener un mayor nivel de control sobre el funcionamiento del UPS se deberá contar con acceso a una interfaz gráfica de administración, por lo que el UPS deberá contar con un puerto Ethernet para la comunicación con una computadora.
- Ya que todos los equipos de conectividad y periféricos deberán estar conectados a Tierra, todos lo tomacorrientes del UPS deberán estar conectados al sistema de Tierra del colegio.
- Debido a que el voltaje de la red eléctrica del país y a que los dispositivos de red que se comercializan trabajan con el voltaje de 120V a una frecuencia de 60 Hz, el UPS también debe poder trabajar a este voltaje y frecuencia.
- Los dispositivos como computadoras, servidores y equipos de conectividad son susceptibles ante las distorsiones del voltaje y la frecuencia del suministro eléctrico, es por ello que el UPS debe garantizar una distorsión de voltaje menor o igual al 3% y una variación de frecuencia salida máxima del 4%; ya que si se superan estos valores los equipos conectados al UPS pueden presentar fallas en su funcionamiento.
- El generador debe tener una potencia mínima de 10KVA con un voltaje de salida de 120V, 60 Hz, con el encendido por medio de ignición eléctrica con batería.
- El generador debe poder funcionar con su reserva de combustible llena por al menos 6 horas consecutivas.
- EL generador debe poseer un tablero de indicadores para combustible, temperatura, batería y aceite, y
- El generador debe tener entradas para conectores eléctricos tipo B e I ya que son los más ocupados por los equipos de conectividad en el país.

3.3.1.5 Materiales utilizados en el SCE

Definida la topología física, los enrutamientos del cableado y los materiales que se ocuparán dentro de los Cuartos de Equipos, Telecomunicaciones, Área de Trabajo y Puesta a Tierra, se procederá a realizar una lista con el cálculo

aproximado de la cantidad de materiales que se necesitará para la implementación del SCE, misma que servirá posteriormente para la cotización.

Para las salidas de telecomunicaciones se dejará 30 cm de holgura en el cable en caso de requerir mantenimiento. Para los Cuartos de Telecomunicaciones se dejará 3m de holgura para la conexión al patch panel y 2m para la conexión con equipos activos. También se debe tomar en cuenta que se dejará cableado horizontal tendido, que se utilizará en el futuro para satisfacer las necesidades de crecimiento en el número de puntos red.

En el Anexo 12 se encuentra el cálculo de la cantidad de cable de datos, canaletas plásticas, tuberías para cableado vertical, bandejas de cables, cableado de puesta a tierra, número de patch panels, patch cords y otros accesorios de rack. En la Tabla 3.21 se muestran los resultados de los materiales y cantidades aproximadas necesarias para la implementación del SCE.

LISTA DE MATERIALES DEL SCE			
	Tipo de Material	**Uni.**	**Cantidad**
Cableado	Cableado cat. 5E	m	14504
	Cableado cat. 6	m	1960
	Patch Cord de 1.2 m cat. 5E	u	275
Canalización	Canaleta de ½" (35x17mm)	m	265
	Canaleta de ¾" (60x25mm)	m	309
	Canaleta de 1" (62x40mm)	m	51
	Canaleta de 1 ½" (100x52mm)	m	130
	Codo Interior ½"	u	24
	Codo Interior ¾"	u	21
	Codo Interior de 1 ½"	u	4
	Codo Exterior de ½"	u	4
	Codo Exterior de ¾"	u	4
	Sección Tipo "T" ¾"	u	16
	Sección Tipo "T" 1"	u	4
	Sección Tipo "T" 1 ½"	u	4
	Sección Tipo "L" ½"	u	12
	Sección Tipo "L" ¾"	u	39

Tabla 3.21: Lista de materiales del SCE (cont…)

LISTA DE MATERIALES DEL SCE			
	Tipo de Material	**Uni.**	**Cantidad**
Canalización	Sección Tipo “L” 1”	u	4
	Sección Tipo “L” 1 ½”	u	6
	Faceplate de 2 puertos	u	83
	Faceplate de 1 puerto	u	85
	Jack cat.5E punch down	u	260
	Caja para instalación de faceplate	u	168
	Cajas de revisión	u	19
	Tubería PVC de 4”	m	77
	Tubería de Fibro-cemento de 4” simple	m	55
	Tubería de Fibro-cemento de 4” doble	m	45
	Bandeja de Cables metálica de 2”x6”	m	136
	Otros (Tornillos, tacos, cintas sujetadoras de cable, material antifuego, etc)	-	-
Cuartos de Equipos y Telecomunicaciones	Rack abierto de piso 19” y 42 U	u	3
	Rack de piso cerrado con paneles desmontables de 19” y 24 U	u	1
	Patch Panel cat. 5E de 24 puertos para rack de 19” (1 U)	u	1
	Patch Panel cat. 5E de 48 puertos para rack de 19” (2 U)	u	7
	Patch Panel cat. 6 de 24 puertos par rack de 19”	u	1
	Organizador de cables horizontal plástico de 19” (2 U)	u	8
	Organizador de cables vertical de 6 pies de altura	u	6
	Organizador de cables tipo anillos independientes	u	10
	Barra eléctrica 6 toma de corrientes 19” (1 U)	u	6
	Panel de ventiladores 120V (2 U o 3U)	u	2
	Bandeja Metálica de 18” de profundidad (2U)	u	4
Puesta a Tierra	Cable 1 AWG	m	113
	Barra de cobre	u	4
	Varilla Copperweld 16mm diámetro	u	3
	Gel para tratar el suelo donde estará la malla de tierra	gl	2
	Otros (conectores de presión, tuercas, tornillos, antioxidante, soldadura exotérmica)	-	-

Tabla 3.21: Lista de materiales del SCE

3.3.2 REDISEÑO DE RED LAN

Para el rediseño de la red LAN del CFD se tendrá como objetivo el llegar a tener una red convergente, en la que el tráfico de voz, datos y video puedan transmitirse simultáneamente sin ningún tipo de problemas como: retrasos, cuellos de botella, lazos de conmutación, incompatibilidades de funcionamiento.

Para ello los equipos de conectividad a escoger deberán cumplir con las siguientes características:

Escalabilidad y Flexibilidad

La velocidad de acceso a la que funcionará la LAN del CFD será de 100 Mbps (Fast Ethernet – 100Base-TX) y como previsión para el futuro crecimiento en el número de puntos de red necesarios, se dejará puntos de red adicionales en las áreas donde se prevé que el crecimiento será inmediato como por ejemplo se dejará 20 puntos de red adicionales repartidos en los Laboratorios de Computación; y además en caso de ser necesario el tendido adicional de cable de red se deja libre el 60% de las canaletas usadas para este propósito, con lo cual, se asegura que funcionará al menos 10 años sin tener que realizar cambios importantes.

Los equipos de conectividad como switches, routers y servidores estarán dimensionados para soportar las aplicaciones y novedades tecnológicas que aparezcan dentro de un período de 5 años sin tener que sufrir ningún tipo de modificación.

Pero además, tendrán la posibilidad de permitir ampliaciones o la incorporación de nuevos dispositivos que trabajen en conjunto con ellos, para mediante esto aumentar su desempeño y capacidades, prolongando su vida útil y asegurando una inversión económica.

Confiabilidad y Disponibilidad

La red LAN debe ser capaz de brindar confiabilidad y disponibilidad, para lo cual, se utilizarán enlaces redundantes entre los equipos de conectividad de las capas

de acceso y núcleo-distribución; también se buscarán equipos de conectividad que funcionen como un conjunto de dispositivos apilables, aumentando así la tolerancia a fallas del sistema; además, todos los equipos de los cuartos de telecomunicaciones, cuarto de equipos y los servicios de red estarán monitoreados de forma automática con un software de monitorización que utiliza el protocolo SNMP, para en caso de detectar anomalías en el funcionamiento se puedan solucionar oportunamente.

Para aumentar la confiabilidad y disponibilidad de la red se utilizará equipos que garanticen que su tiempo medio entre fallos mínimo cubra el período para el cual se está diseñando la red, es decir al menos 5 años de uso continuo.

La disponibilidad de los servicios de red se asegurará mediante un servidor backup en el que se alojarán las principales aplicaciones de red para poder ofrecer servicio sin interrupción a los usuarios del CFD. Los servicios que se prevé tener dentro de éste servidor serán los necesarios para el funcionamiento de la navegación en Internet, página web, aula virtual, correo electrónico, telefonía IP y video seguridad ya que estos son los servicios de mayor utilización.

También para asegurar la disponibilidad se buscarán marcas de equipos que ofrezcan garantías y apoyo técnico dentro del país para tener una pronta reparación y solución a inconvenientes de funcionamiento de los dispositivos de conectividad.

Seguridad

Para asegurar los datos que se transmitirán por medio de la red LAN y controlar el acceso de los usuarios a los servicios y aplicaciones que se ofrecerán dentro de la red, se utilizará VLANs con las que se fraccionará a la red en distintos grupos, entre los cuales no podrán comunicarse excepto que sea estrictamente necesario; también se usarán aplicaciones de filtrado de contenidos y firewall basado en software que protegerán a la red de ataques y accesos no autorizados. Para la seguridad de cada estación de trabajo en especial de los computadores del personal administrativo se usarán cuentas de acceso que se cambiarán periódicamente, antivirus de licencia gratuita en cada estación, intercambio de correos y archivos con la utilización de protocolos seguros, y backups periódicos

de los documentos y archivos importantes dentro de dispositivos de almacenamiento portátil que serán solamente utilizados por el administrador de la red para éste propósito.

Para proteger los objetos de valor que se tengan dentro las instalaciones del CFD se instalará un sistema de video seguridad, con el que las cámaras IP además de capturar video se podrán usar como detectores de movimiento pudiendo disparar una acción en cuanto el movimiento sea detectado, como por ejemplo una llamada hecha por medio de la central telefónica IP que alerte sobre una intrusión en las instalaciones del colegio.

3.3.2.1 Arquitectura de la red LAN

La estructura de la red LAN se basará en el modelo jerárquico de capas de acceso-distribución-núcleo, pues permite tener una mayor escalabilidad, redundancia, seguridad, facilidad de mantenimiento y por lo tanto un mejor rendimiento.

Debido a la reducida dimensión de la red del CFD (250 puntos de red), se condensarán las capas de distribución y núcleo para que funcionen como una sola, quedando solo dos capas en las que se deben dimensionar los equipos de conectividad, según los requerimientos que se tiene en cada una de estas capas.

En la capa de núcleo-distribución se buscará equipos de conectividad que permitan el enrutamiento entre VLANs, la configuración de listas de acceso para controlar el tráfico que puede circular por la red; también deberá proporcionar mecanismos para brindar calidad de servicios a los datos de voz y video, y, debe tener un gran nivel de confiabilidad y disponibilidad. A través de estos equipos pasará todo el tráfico que se dirija hacia los servidores de la institución y hacia el Internet.

En la capa de acceso se necesita dispositivos de conectividad que ofrezcan calidad de servicio al tráfico de voz y video, que permita el uso de VLANs asignadas a los puertos, que brinden seguridad basada en puerto y que manejen protocolos que eviten lazos de conmutación. A estos equipos se conectarán las

estaciones de trabajo, los teléfonos IP, las impresoras de red y otros dispositivos que tengan que conectarse a la red.

Los equipos de conectividad deberán poseer las características necesarias para ofrecer confiabilidad, disponibilidad, escalabilidad, flexibilidad y seguridad.

Los dispositivos de conectividad que conformarán la red activa del colegio serán switches de capa 2 y capa 3 con características que permitan brindar calidad de servicio los flujos de datos de voz y video que recorrerán la red la institución educativa.

Capa de Acceso

Los switches de la capa de acceso estarán ubicados dentro de los Cuartos de Telecomunicaciones y dentro del Cuarto de Equipos. El número de puertos y la velocidad de los *enlaces de* Uplink de estos equipos dependerán del número de usuarios que existan en cada área a la que servirán.

Los equipos de conectividad serán del tipo apilable para obtener mayor flexibilidad, escalabilidad y confiabilidad en la red.

- *Cuarto de Telecomunicaciones Bloque B:*

En el Cuarto de Telecomunicaciones del Bloque B se utilizarán los dos switches NEXXT de acceso de 24 puertos (10/100 Mbps) no configurables que el CFD posee en éste momento, y que se utilizarán para brindar servicio a las computadoras de los laboratorios de computación (42 computadoras), donde los estudiantes solo intercambiarán flujos de datos con Internet y el aula virtual, por lo que, no requieren la diferenciación de los flujos de la información de voz, datos y video.

Para dar servicio a los demás puntos de red presentes en éste bloque, entre los que se cuenta con: 40 puntos de datos-voz; se utilizarán dos switches de 24 puertos Fast Ethernet configurables que se adquirirán con las características necesarias para diferenciar y priorizar el flujo de información de voz, video y datos. Los 2 puntos de red de las cámaras IP que se encontrarán en el Bloque B

estarán conectados directamente con el Cuarto de Equipos ya que recibirán energía a través del cable de red y el switch al que estén conectados a su vez recibirá energía del UPS.

Los dispositivos dentro de este Cuarto de Telecomunicaciones se conectarán a los equipos de red de la Capa de Distribución-Núcleo por medio de enlaces Uplink de 1 Gbps.

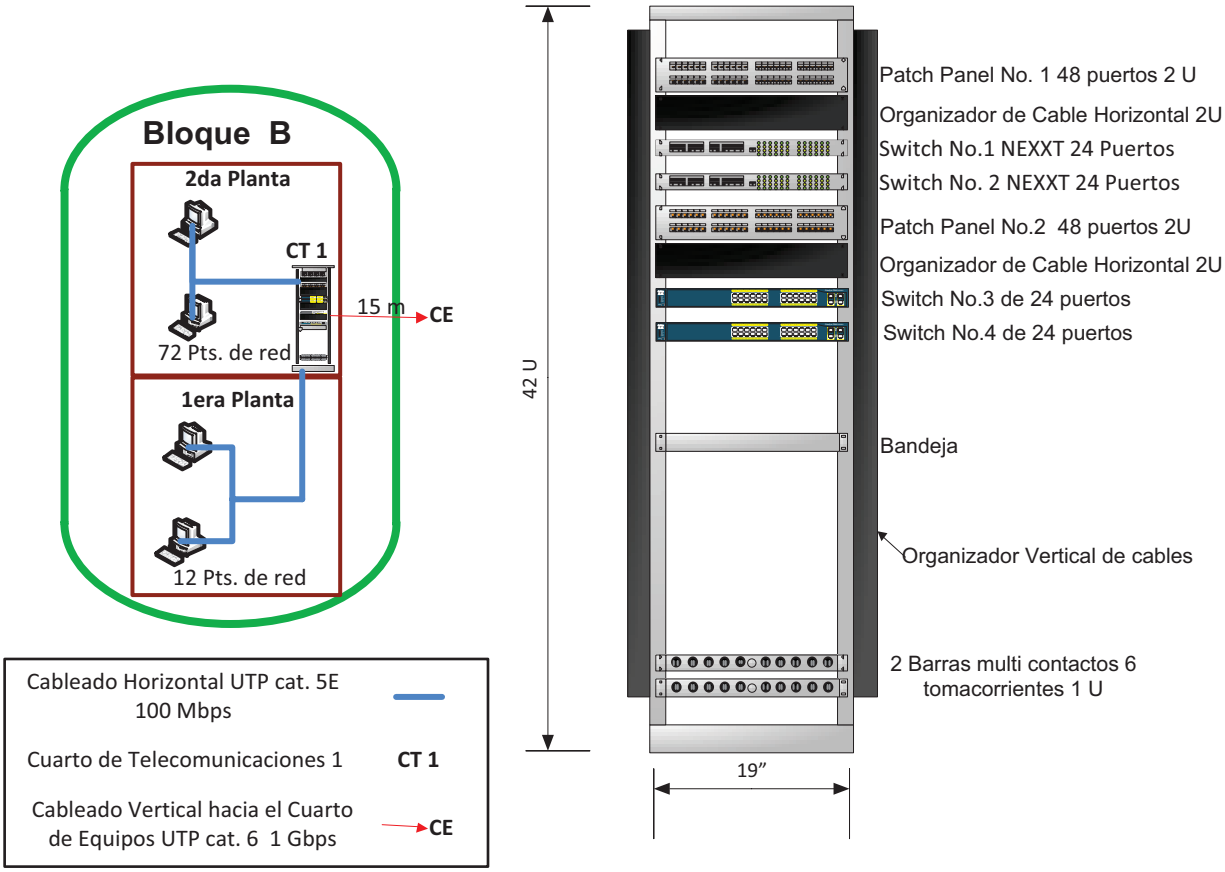


Figura 3.24: Esquema de la distribución de dispositivos de conectividad en el rack del Cuarto de Telecomunicaciones del Bloque B

- *Cuarto de Telecomunicaciones Bloque G:*

En este Cuarto de Telecomunicaciones se encontrarán los equipos de conectividad que darán servicio a los puntos de red ubicados en las aulas y otros ambientes dentro de los Bloques E, G y H del CFD.

En estos bloques existen 4 puntos dedicados para proyectores en red, 4 puntos para cámaras de video y 59 puntos de voz-datos; por lo que, se ha considerado la

utilización de tres switches configurables de 24 puertos Fast Ethernet. La cámara IP presente dentro del Cuarto de Telecomunicaciones del Bloque G no se conectará a los switches presentes en este cuarto sino que se conectarán directamente al Cuarto de Equipos pues esta cámara estará conectada a un dispositivo de red que recibe energía del UPS.

Los switches de este Cuarto de Telecomunicaciones se conectarán a los equipos de la Capa de Distribución-Núcleo con un de enlace Uplink de 1 Gbps.

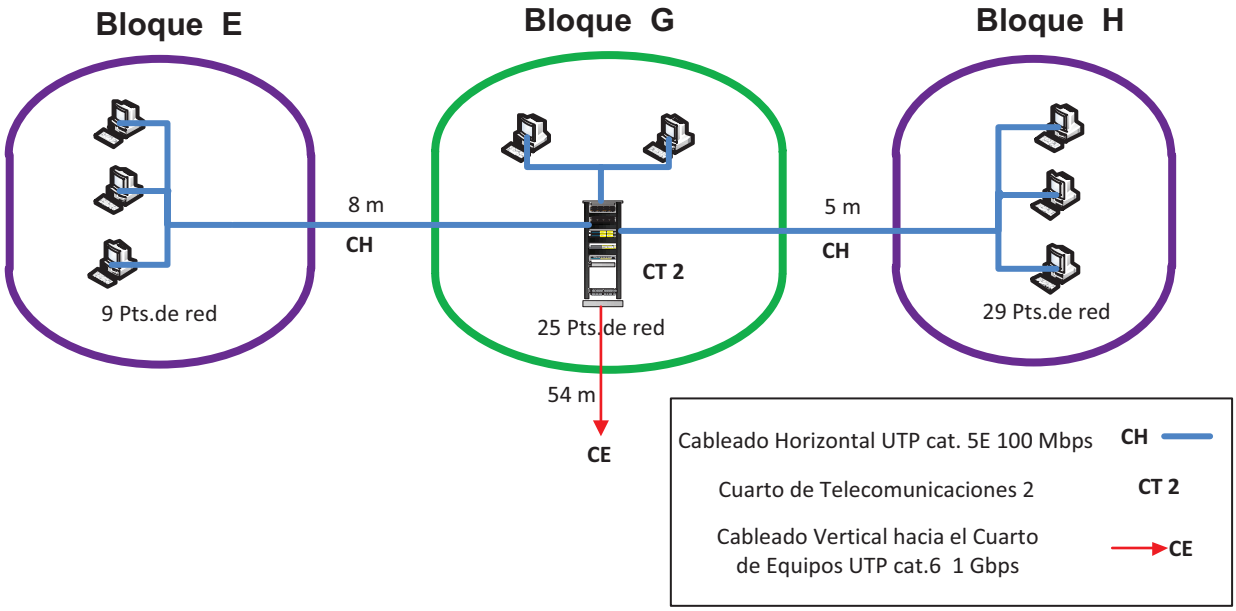


Figura 3.25: Esquema del cableado en el Cuarto de Telecomunicaciones del Bloque G

- *Cuarto de Telecomunicaciones Bloque F:*

El Cuarto de Telecomunicaciones del Bloque F se encontrarán los equipos de conectividad que brindarán servicio a los puntos de red ubicados dentro de los bloques C, D y F; entre los cuales se tiene 35 puntos de voz-datos; el punto de red que corresponde a la cámara IP del Bloque F estará conectada directamente con el Cuarto de Equipos pues esta cámara recibirá energía por medio del cable de red. Con esto en mente se ha decidido utilizar dos switches configurables de 24 puertos Fast Ethernet; estos switches se conectarán a los equipos de conectividad de la Capa de red de Distribución-Núcleo con enlaces Uplink de una velocidad de 1 Gbps.

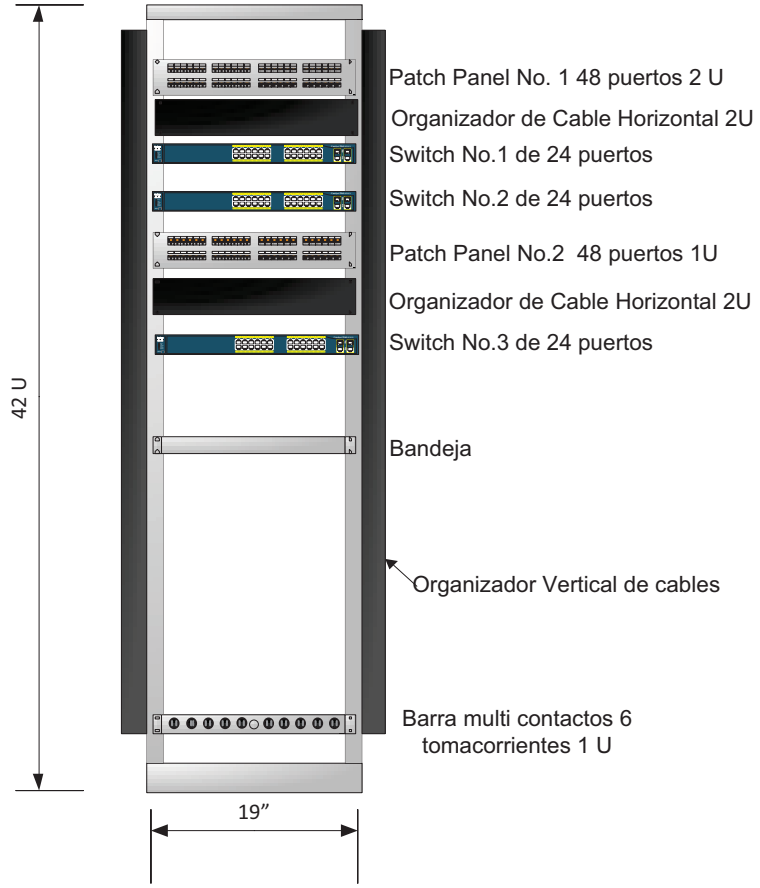


Figura 3.26: Esquema de la distribución de dispositivos de conectividad en el rack del Cuarto de Telecomunicaciones del Bloque G

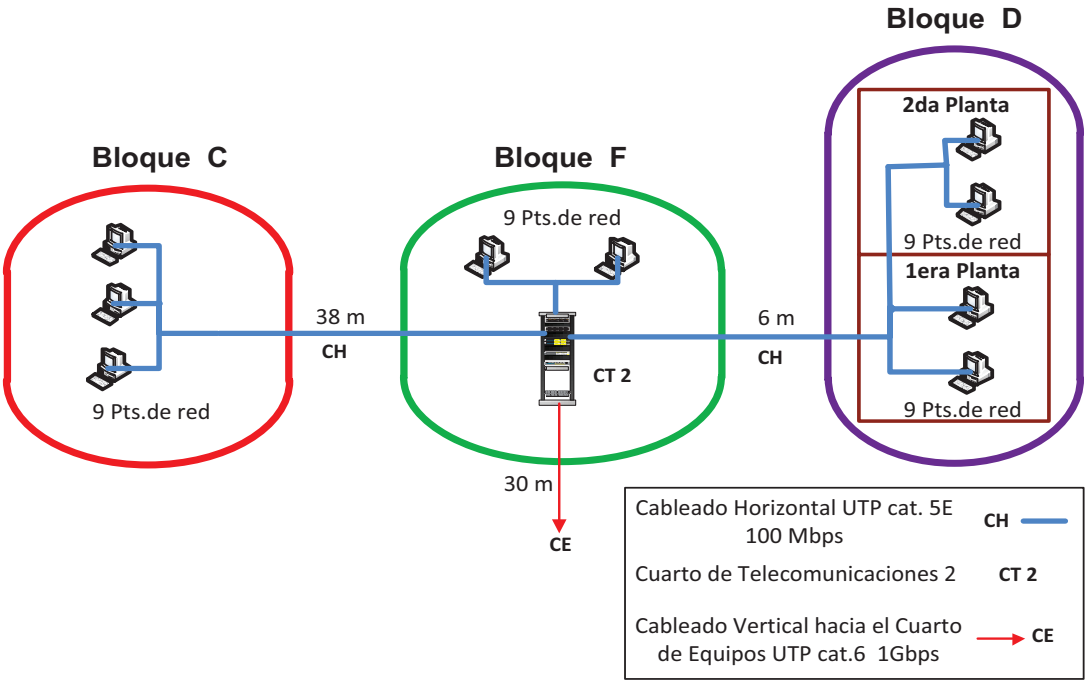


Figura 3.27: Esquema del cableado en el Cuarto de Telecomunicaciones del Bloque F

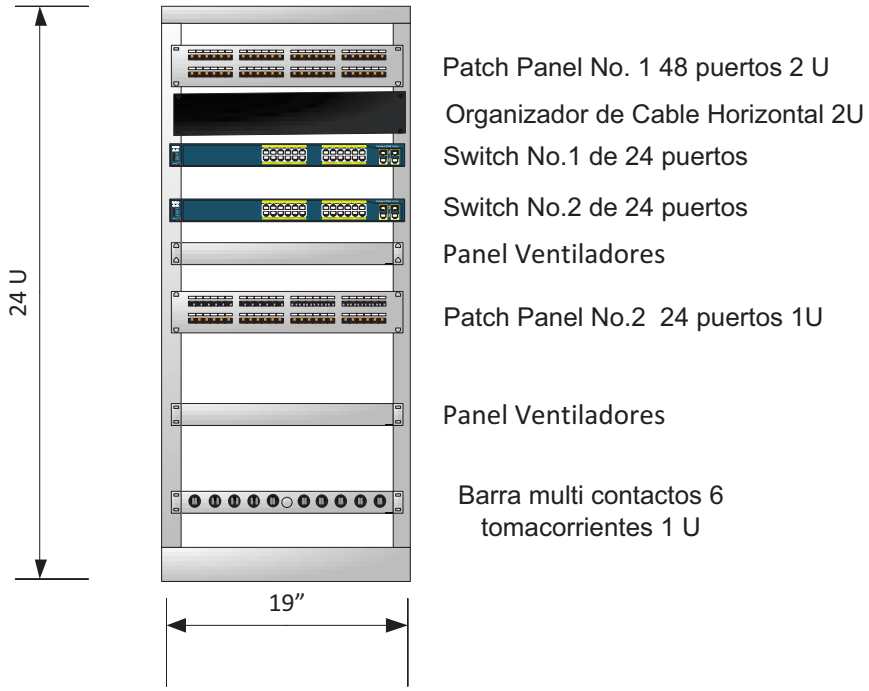


Figura 3.28: Esquema de la distribución de dispositivos de conectividad en el rack del Cuarto de Telecomunicaciones del Bloque F

- *Cuarto de Equipos:*

En el Cuarto de Equipos del CFD se encontrarán también equipos de conectividad de capa de acceso, que darán servicio a los puntos de red de aulas y oficinas de los bloques A e I. En estos puntos de red se tienen 14 puntos para cámaras IP y 58 puntos de voz-datos.

Debido a que se tienen en total 58 puntos de red se usará cuatro switches de 24 puertos Fast Ethernet, conectándose a la Capa de Distribución-Núcleo por medio de enlaces de Uplink de 1 Gbps. Uno de los switches deberá contar con características de PoE[33], ya que dispositivos como las cámaras y teléfonos IP recibirán energía por medio del cable de red, esto permitirá usar estos dispositivos sin necesidad de buscar una toma eléctrica y además en caso de un corte de energía estarán respaldados por el UPS.

Capa de Distribución-Núcleo

El switch de Distribución-Núcleo se encontrará dentro del área del Cuarto de Equipos. Este switch debe tener la capacidad de enrutamiento inter VLANS,

priorización de tráfico, alta velocidad de conmutación, capacidad de funcionar de manera apilable, configuración de listas de acceso por puerto, dirección MAC y dirección IP; y soporte para protocolos de enrutamiento no propietarios como RIPv1, RIPv2. A este equipo se conectarán los switches de acceso y los servidores, por lo que, debe tener al menos 24 puertos Gigabit Ethernet.

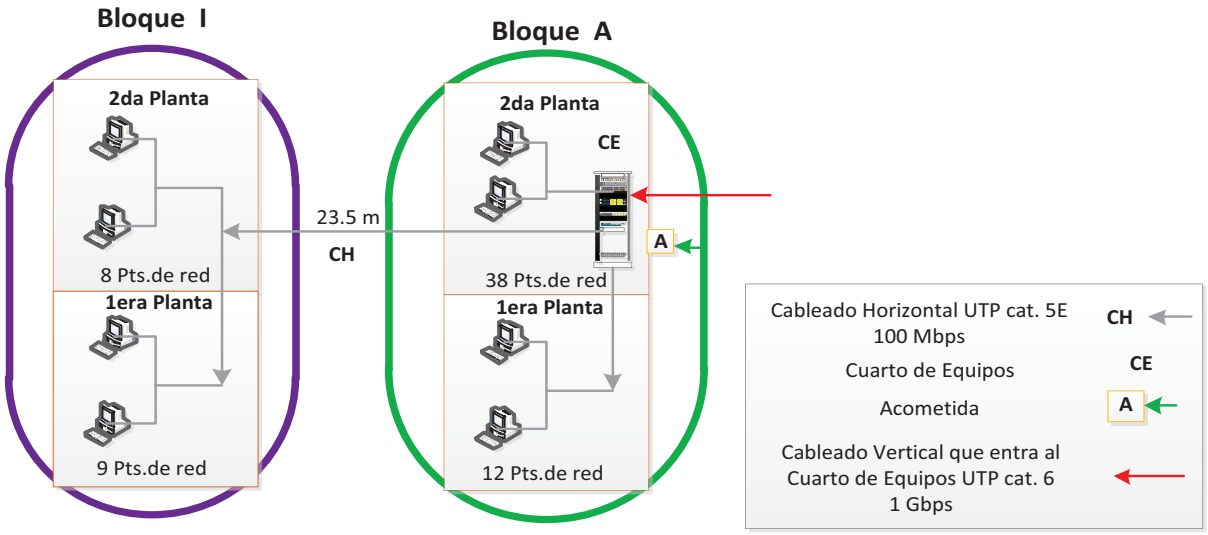


Figura 3.29: Esquema del cableado del Cuarto de Equipos

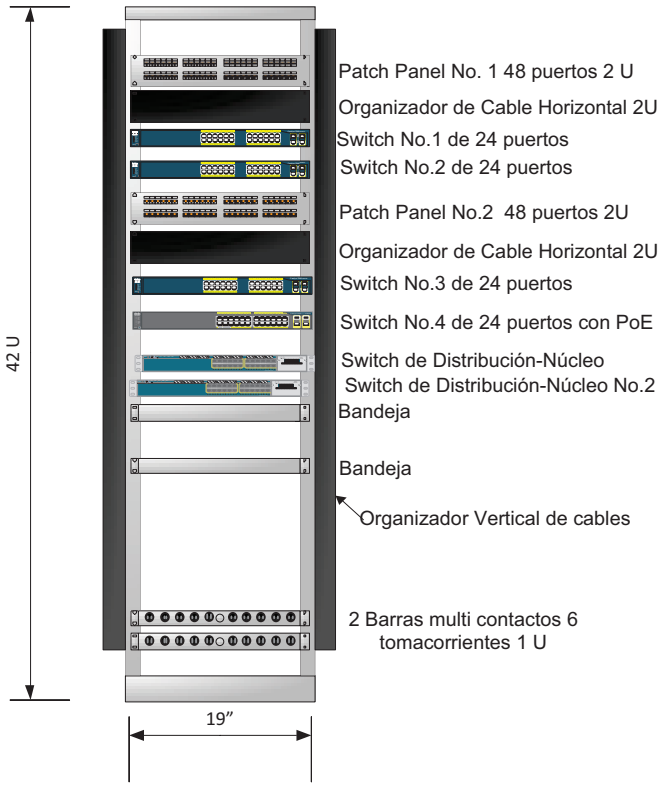


Figura 3.30: Esquema de la distribución de dispositivos de conectividad en el rack del Cuarto de Equipos

En la siguiente tabla se muestra un resumen del número de puntos de red que estarán ocupados en los switches de cada cuarto de Telecomunicaciones y de Equipos, y además se muestra el número de puntos de red libres para el crecimiento futuro de la red.

CAPA DE ACCESO		
	# de Puntos de red	**# puntos de red libres para escalabilidad**
Cuarto de Equipos	72	24
Cuarto de Telecomunicaciones Bloque B	82	14
Cuarto de Telecomunicaciones Bloque G	62	10
Cuarto de Telecomunicaciones Bloque F	35	13
CAPA DE DISTRIBUCIÓN-NÚCLEO		
	# de Puntos de red	**# puntos de red para escalabilidad**
Cuarto de Equipos	16	32

Tabla 3.22: Resumen del número puntos de red y puntos para crecimiento futuro

3.3.2.2 Características técnicas de los dispositivos de conectividad de la LAN

Características de los Switches de la Capa de Acceso

Los switches de Capa de Acceso deberán tener las siguientes características:

- Funcionar en las capas 1 y 2 del modelo OSI, pues su trabajo solo consiste en dar conectividad a los usuarios de la red.
- Once de los switches deben ser de 24 puertos Fast Ethernet.
- Para aumentar la escalabilidad, disponibilidad y flexibilidad de la red los switches de la capa de acceso deberán poder trabajar de manera apilable, con lo cual se tendría la ventaja de una gestión centralizada para todos lo switches pertenecientes a una pila.

- Todos los puertos de los switches deberán configurarse automáticamente para la conexión de cables de red directos o cruzados para evitar problemas de conectividad debido a esta característica.
- Los switches deberán contar con al menos un puerto de Uplink de 1 Gbps de velocidad; ya que ésta velocidad supera por mucho al ancho de banda de backbone que se estima se utilizará en la red (para más detalles ver Tabla 3.16) y permitirá tener un gran margen de ancho de banda disponible para el crecimiento futuro del tráfico que ocupe cada usuario, garantizando que no existirán cuellos de botella.
- Todos los dispositivos de conectividad deberán montarse en racks para su funcionamiento, es por ello que se debe buscar switches que puedan ser instalados dentro de racks de 19” de ancho y 31” de profundidad.
- Para soportar el tráfico de voz, datos y video los switches deberán contar con mecanismos como priorización de tráfico (IEEE 802.1p) basada en el campo de priorización de servicio, en dirección IP, en número de puerto TCP/UDP. Para facilitar la configuración de los puertos que tienen conectados teléfonos IP los switches deberán poder utilizar configuración automática de cada uno de éstos puertos.
- Debido que en los switches se conectarán equipos que pertenecerán a diferentes subredes por ejemplo administración, docentes, teléfonos y cámaras IP, etc.; los switches deberán poder utilizar VLANS para separar el tráfico de cada subred y disminuir el tráfico de broadcast innecesario.
- La administración de los equipos deberá poderse hacer mediante consola de comandos e interfaz web, y para la monitorización del equipo deberá soportar el protocolo SNMPv3.
- Para evitar lazos de conmutación por errores en las conexiones los switches deben soportar los protocolos STP (*Spanning Tree Protocol*), RSTP (*Rapid Spanning Tree Protocol*).
- Como medidas de seguridad los switches deben ser capaces de tener filtros por medio de listas de acceso generales y por puerto, autenticación para entrada a la consola de administración por medio RADIUS, y además

deberán tener medidas para evitar ataques por medio del envenenamiento DNS, IGMP y ARP que son los tipos de ataques más comunes para las redes LAN.

Comparación entre switches de Acceso

Para los equipos de conectividad en la Capa de Acceso se ha decidido buscar entre dos marcas de equipos con presencia en el mercado nacional (Cisco y HP) y que ofrecen una gran variedad de dispositivos de red orientados a grandes y pequeñas empresas.

Para la comparación se escogieron dos modelos de switches que poseen características de funcionamiento similares para poder realizar una comparación que permita sacar las mejores características de cada uno de los dispositivos.

Al comparar los dos switches de acceso se pudo observar la clara superioridad del dispositivo Cisco WS-2960-24PC-L en aspectos como el funcionamiento de forma apilable con conexiones de mayor velocidad, puertos de Uplink con mayor número de opciones de tecnologías de capa física para escoger y con velocidades de entre 1Gbps y 10Gbps, y posee un mayor número de configuraciones y funcionalidades para la priorización del tráfico. Es por ello que se recomienda a los equipos Cisco WS-C2960-24PC-L, WS-C2960-24TC-L (switch con PoE) como switches de acceso en la red del CFD. En el Anexo 14 se muestra en detalle la comparación de las características técnicas de los switches vistos en la Tabla 3.23.

Características del Switch de la Capa de Distribución-Núcleo

Para la comparación de los equipos de conectividad a usarse en las capas de Acceso y Distribución-Núcleo, se han elegido dos marcas de prestigio en el mercado nacional: Cisco y HP; luego de realizar una comparación de las características esenciales de los equipos se elegirá al dispositivo que presente más ventajas y cuyas capacidades técnicas sean superiores.

SWITCH DE ACCESO		
CARACTERÍSTICAS	**EQUIPOS**	
	WS-C2960-24PC-L 	**HP 2530-24G(J9776A)** 
Puertos fullduplex (10Base-T, 100Base-TX) auto sensibles	Sí	Sí
Soportar 2 puertos SFP[35]+ como enlaces Uplink.	Sí	Sí
Velocidad Back Plane	50Gbps	31Gbps
Priorización de tráfico por IEEE 802.1p	Sí	Sí
Priorización de tráfico por MAC, dirección IP, número de puerto y VLAN	Sí	No
Capacidad para funcionar de manera apilable	Sí	Sí
Listas de Acceso basadas en MAC, IP, VLAN y Puerto TCP/UDP	Sí	No
Spanning Tree Protocol (IEEE802.1d), Rapid Spanning Tree (IEEE802.1w) y Multiple SpanningTree(IEEE802.1s)	Sí	Sí
VLANS (IEEE 802.1q)	Sí	Sí
Configuración automática del Puerto en la VLAN de telefonía	Sí	No
Agregación de Enlace (IEEE 802.3ad)	Sí	Sí
Administración SSHv2	Sí	No
Administración por interfaz web	Sí	Sí
Autenticación RADIUS	Sí	Sí
Soporte de SNMP v2c, v3	Sí	Sí
Soporte de RMON	Sí	Sí
Protección DHCP snooping	Sí	Sí
Protección ARP spoofing	Sí	Sí
IGMP snooping	Sí	No
Fuente de poder redundante	No	No
Garantía	De por vida	De por vida
Soporte especializado dentro de Ecuador	Sí	Sí

Tabla 3.23: Comparación de características técnicas entre dos marcas de equipos a usarse en la capa de Acceso [PW36, PW37]

El switch de Capa de Distribución-Núcleo deberá contar con las siguientes características:

- Deberá funcionar en la capa 1, 2 y 3 del modelo ISO/OSI, ya que, deberán tener la capacidad de enrutar el tráfico inter VLANS.
- Tendrá 24 puertos full duplex de velocidad 1000 Mbps debido a que esta es la velocidad que tienen los enlaces de Uplink de los switches de acceso.
- El switch deberá poder trabajar de manera apilable para ofrecer escalabilidad y flexibilidad para el aumento y administración de los equipos de Distribución-Núcleo.
- Deberá poder montarse en racks de 19” para su funcionamiento.
- Deberá soportar protocolos de enrutamiento no propietarios como RIPv1, 2 para poder enrutar el tráfico entre VLANS y tráfico que necesite enrutamiento especial.
- Deberá soportar las mismas características que los switches de acceso que garanticen la calidad de servicio para el tráfico de voz y datos, es decir deberá soporta la priorización de tráfico (IEEE 802.1p) y Diffserv.
- Sus puertos deberán poder configurarse para funcionar como enlaces troncales debido a que desde los switches de acceso el tráfico de varias VLANS viene por el mismo enlace.
- La administración de los equipos deberá poderse hacer mediante consola de comandos e interfaz web, y para la monitorización del equipo deberá soportar el protocolo SNMPv3.
- Para evitar lazos de conmutación por errores en las conexiones los switches deben soportar los protocolos STP (*Spanning Tree Protocol*), RSTP (*Rapid Spanning Tree Protocol*).
- Como medidas de seguridad los switches deben ser capaces de tener filtros por medio de listas de acceso generales y por puerto, autenticación para entrada a la consola de administración por medio RADIUS, y además deberán tener medidas para evitar ataques por medio del envenenamiento DNS, IGMP y ARP que son los tipos de ataques más comunes para las redes LAN.

SWITCH DE DISTRIBUCIÓN - NÚCLEO		
CARACTERÍSTICAS	**EQUIPOS**	
	WS-C3750X-24T-S 	**HP 2910-24G al (J9145A)** 
Puertos fullduplex (10Base-T, 100Base-TX, 1000Base-T) auto sensibles	Sí	Sí
Velocidad de Back Plane	50Gbps	70Gbps
Soportar 2 puertos SFP+ como enlaces Uplink.	Sí (2 puertos en varias tecnologías)	Sí (4 puertos en varias tecnologías)
Enrutamiento	RIPv1/v2, OSPF, EIGRP, BGP, e IS-IS. OSPFv3 y EIGRPv6.	Enrutamiento estático, RIPv1 y RIPv2.
Priorización de tráfico por 802.1p	Sí	Sí
Priorización de tráfico por MAC, dirección IP, número de puerto y VLAN	Sí	Sí
Capacidad para funcionar de manera apilable	Sí (hasta 9 switches)	Sí (hasta 16 switches)
Listas de Acceso por MAC, dirección IP, número de puerto TCP/UDP	Sí	No (no puede hacer ACL por MAC)
Spanning Tree Protocol (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w) y Multiple Spanning Tree (IEEE 802.1s)	Sí	Sí
VLANS (IEEE 802.1q)	Sí	Sí
Agregación de Enlace (IEEE 802.3ad)	Sí	Sí
Administración SSHv2	Sí	No
Administración por interfaz web	Sí	Sí
Autenticación RADIUS	Sí	Sí
Soporte de SNMP v2c, v3	Sí	Sí
Soporte de RMON	Sí	Sí
Protección DHCP snooping	Sí	Sí
Protección ARP spoofing	Sí	Sí
IGMP snooping	Sí	No
Fuente de poder redundante	No	No
Garantía	De por vida	De por vida
Soporte especializado dentro de Ecuador	Sí	Sí

Tabla 3.24: Comparación de características técnicas entre dos marcas de equipos a usarse en la capa Distribución -Núcleo

Luego de hacer una comparación de las características más importantes entre los equipos de las dos marcas elegidas se ha elegido al Switch Cisco WS-C3750X-24T-S como la opción más recomendable para que cumpla la función de switch de Distribución – Núcleo para la red LAN del CFD, pues posee más opciones de configuración para otorgar calidad de servicio a los flujos de datos de video y voz, tiene mejores capacidades de enrutamiento, posee un mejor sistema para las fuentes de poder redundantes y su sistema de apilamiento no ocupa puertos Uplink para la interconexión. En el Anexo 14 se muestra en detalle la comparación de las características técnicas de los switches vistos en la Tabla 3.24.

3.3.2.3 Plan de Direccionamiento IP y VLANS

Al analizar la estructura organizacional del CFD, se determinó que existen tres grupos bien definidos de usuarios en la red local de la institución, y basándose en esta división se definirán la estructura lógica de red y la asignación de VLANS; mecanismos mediante los cuales se busca facilitar la administración, la segmentación de tráfico y aumentar la seguridad de la red mediante restricciones de comunicación entre las estaciones que pertenezcan a distintas VLANS.

3.3.2.3.1 VLANS

La red del CFD estará segmentada a nivel de la capa 2 del modelo ISO/OSI por medio de VLANS que estarán asignadas de acuerdo con la estructura organizacional del establecimiento educativo. Para ello, los equipos de conectividad de las Capas de Acceso y de Distribución-Núcleo deberán soportar el estándar IEEE 802.1Q.

VLAN / NOMBRE	No. De Identificación
ADMINISTRACIÓN DE RED / CFDADMIN	3
SERVIDORES / CFDSERV	5
ESTUDIANTES / CFDEST	10
PROFESORES / CFDPROF	20
PERSONAL ADMINISTRATIVO / CFDPADM	30
TELEFONÍA IP /CFDVOIP	40
VIDEO SEGURIDAD /CFDVID	50
INVITADOS /CFDINV	60

Tabla 3.25: Nombres y número de identificación de las VLANS

En la VLAN de ADMINISTRACIÓN DE RED se encontrarán todos los equipos de conectividad (switches, access point, etc.) a los que se les asignará una dirección IP dentro del rango establecido en esta VLAN y servirá para el acceso a las interfaces de administración y configuración de estos equipos.

En la VLAN SERVIDORES estarán los servidores de DHCP, DNS, Directorio, etc., a los que solo los usuarios de la intranet tendrán acceso. Los servidores de E - Mail, Página Web y Aula Virtual se encontrarán dentro de una zona desmilitarizada (DMZ) pues deberán permitir el acceso de usuarios desde Internet.

Las VLANS de PROFESORES y PERSONAL ADMINISTRATIVO tendrán acceso a su propia VLAN y a la VLAN SERVIDORES para obtener acceso a todos los servicios que se ofrecen dentro de la red. Para los puertos pertenecientes a la VLAN PERSONAL ADMINISTRATIVO se tendrá el acceso a la VLAN TELEFONÍA pues estos usuarios poseerán teléfonos IP conectados junto con los computadores de cada estación.

La VLAN ESTUDIANTES será utilizada para todas las conexiones inalámbricas y alámbricas usadas por alumnos del CFD; éstos puntos de red solo tendrán conectividad con las PC’s que se encuentren dentro de ésta VLAN y además tendrá acceso a los servidores Proxy, Web y Aula Virtual de la red de la institución.

La VLAN TELEFONÍA se creó con el objetivo de segmentar todo el tráfico de voz para priorizarlo con respecto al tráfico de datos que fluye dentro la red.

La VLAN VIDEO SEGURIDAD se configurará para los puertos a los que estarán conectados las cámaras IP que conformarán el sistema de video seguridad IP del CFD.

La VLAN INVITADOS estará destinada para los usuarios que deseen acceder a Internet desde la Sala de Reuniones del colegio por medio de un Access Point. Esta VLAN solo podrá comunicarse con los equipos dentro de la misma VLAN y con el servidor Proxy de la red para brindar la salida a Internet.

3.3.2.3.2 Direccionamiento

Para el direccionamiento IP se utilizarán subredes creadas mediante VLSM (V*ariable Length Subnet Mask*). Para determinar el tamaño de cada subred se utilizará el número de usuarios de red que se proyectó tener en los próximos 5 años y además se asumirá que todos los puntos de red de las aulas estarán dentro de la VLAN de PROFESORES.

DIRECCIONAMIENTO			
VLAN	**# de Usuarios**	**Dir. De Subred / Máscara de Subred**	**# de Direcciones Utilizables**
PROFESORES	180	172.16.0.0/24	254
ESTUDIANTES	80	172.16.1.0/25	126
PERS. ADMINISTRATIVO	50	172.16.1.128/26	62
ADMINISTRACIÓN DE RED	20	172.16.1.192/27	30
INVITADOS	15	172.16.1.224/27	30
VIDEO SEGURIDAD	17	172.16.2.0/27	30
TELEFONÍA IP	13	172.16.2.32/27	30
SERVIDORES	5	172.16.2.64/28	14

Tabla 3.26: Direccionamiento IP

3.3.3 DISEÑO DE LA RED INALÁMBRICA

La red inalámbrica brindará principalmente acceso a Internet a profesores, alumnos e invitados en lugares donde exista dificultad al acceso a puntos de red y se necesite de conectividad de forma temporal y solo en áreas específicas del colegio. Por ello, se ha definido que las áreas principales dentro del CFD donde se requiere de una cobertura inalámbrica permanente son:

- La segunda planta del Bloque A (Biblioteca y Áreas Administrativas).
- El Salón de Actos ubicado en el Bloque G.
- La Sala de Profesores ubicada en el Bloque H.

En cada una de estas áreas se analizará el tipo de construcción del edificio, los elementos físicos y otras redes inalámbricas que puedan causar interferencia, estimar el tamaño del área que se quiere cubrir y el número máximo de usuarios que se espera tener simultáneamente con el objetivo de determinar la cantidad de

Access Points que se necesiten, la potencia que deben tener, el tipo de antenas a utilizar y la frecuencia de funcionamiento de la red inalámbrica.

Se crearán 3 Identificadores de Red (SSID) que estarán asociadas a las VLANS de ESTUDIANTES, PROFESORES-PERSONAL ADMINISTRATIVO e INVITADOS. La utilización de VLANS separadas permitirá tener un control más específico en los permisos que tendrán los usuarios de cada red inalámbrica.

3.3.3.1 Segunda Planta Bloque A

En esta planta se encuentran las oficinas administrativas y la biblioteca de la institución, distribuidas en un espacio de 6 x 36 metros. El área está dividida en 4 secciones por muros de bloques de cemento, mientras que dentro de cada uno de éstos ambientes las divisiones están hechas de láminas de madera.

En cuanto al número de usuarios se tomó en cuenta que en esta área cada usuario cuenta con un computador conectado de manera cableada a un punto de red, por lo que, se estima que en el área administrativa se tendrá un máximo de 10 usuarios inalámbricos. En la parte donde funciona Biblioteca se estima que se tendrá un máximo de 12 usuarios conectados de manera inalámbrica, ya que, esta sección está diseñada para unos 15 estudiantes.

Para determinar si existe interferencia por la existencia de redes inalámbricas vecinas, se realizó el Site Survey Pasivo[36] del área. En la tecnología 802.11b/g/n se pudo identificar que los canales 1 y 6 no están siendo utilizados en esta zona; mientras que en la tecnología 802.11a no se encontró ninguna red inalámbrica funcionando. Los informes completos del Site Survey hecho en el CFD se encuentran en el Anexo 15.

3.3.3.1.1 Red WLAN en la Segunda Planta Bloque A

Se observó que los estudiantes estarán siempre conectados en el área de Biblioteca, mientras que profesores, invitados y personal administrativo se conectarían a la red inalámbrica al otro extremo de esta planta (Sala de Reuniones y oficinas administrativas); por lo que, se reutilizará el Access Point D-Link DIR 655 que la institución posee para que brinde servicio inalámbrico

exclusivamente a los estudiantes en la zona de Biblioteca, estando toda esta parte de la red dentro de la VLAN de estudiantes (ESTUDIANTES).

Para el acceso inalámbrico de los profesores, invitados y personal administrativo se utilizará otro Access Point que soporte la configuración de múltiples VLANs (PROFESORES-PERSONAL ADMINISTRATIVO e INVITADOS) y que estará ubicado dentro del Cuarto de Equipos.

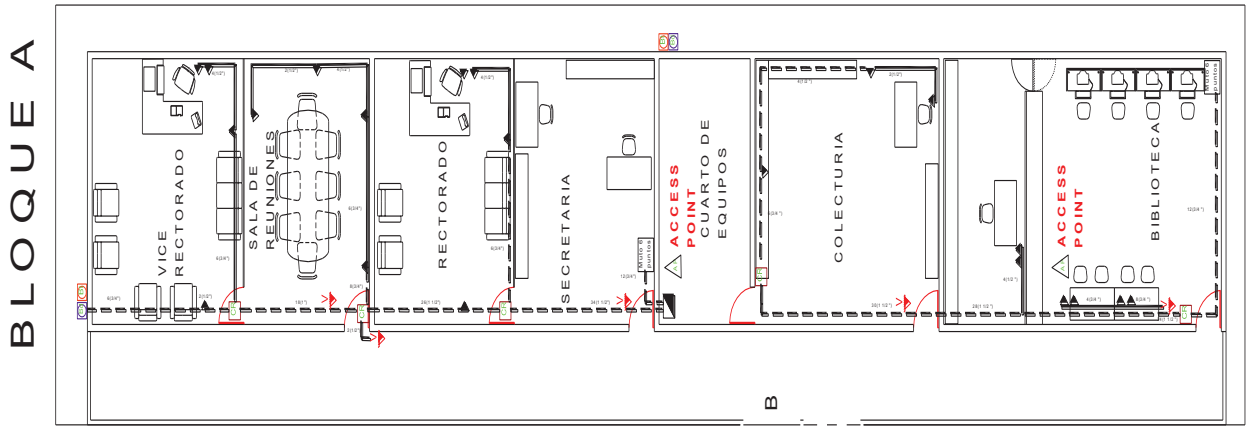


Figura 3.31: Ubicación Access Point Segunda Planta Bloque A

Considerando el tipo de construcción, la forma y extensión de esta zona, se recomienda que la red inalámbrica funcione con las tecnologías 802.11 b/g/n.

El Access Point de Biblioteca trabajará en el Ch. 1, a una potencia de 15 dBm utilizando antenas dipolo y con una conexión alámbrica 100Base-TX. El Access Point del Cuarto de Equipos trabajará en el Ch. 6, con una potencia de transmisión de 20 dBm, con antenas dipolo y conexión alámbrica 100Base-TX.

3.3.3.2 Salón de Actos

Esta zona es utilizada para eventos como conferencias, cursos y actos especiales; con espacio para unas 140 personas de los cuales la mayor parte serán profesores y personas externas a la institución. Las dimensiones de éste salón es de 8,5 metros de ancho x 15 metros de largo.

Si se considera que el 40% de los 140 usuarios se conectan inalámbricamente se tendrá unos 56 usuarios conectados a los Access Point se esta área usando la red para acceder principalmente al servicio de Internet.

En éste salón no existe materiales que puedan interferir o degradar la señal utilizada por la red inalámbrica, pero si existe la presencia de algunas redes inalámbricas externas en la tecnología 802.11 b/g/n con un nivel de señal medio (-60 dBm) ocupando el canal No. 11; en la tecnología inalámbrica 802.11a no se encontró ninguna red inalámbrica funcionando.

3.3.3.2.1 Red WLAN en el Salón de Actos

Por el número de usuarios en el área se recomienda usar dos Access Points con el objetivo de brindar un nivel de servicio adecuado, distribución de la carga y permitir la utilización de ésta red para otras aplicaciones en el futuro.

Se recomienda usar la tecnología 802.11 b/g/n (Ch. 1 y Ch. 6) con una potencia de transmisión de 15 dBm, utilizando antenas dipolo y con una conexión alámbrica 100Base-TX. Estos Access Points estarán sujetos a las estructuras metálicas de techo del salón y separados entre sí por una distancia de 7 metros aproximadamente. Debido a la ubicación de éstos Access Points la alimentación eléctrica se realizará mediante PoE.

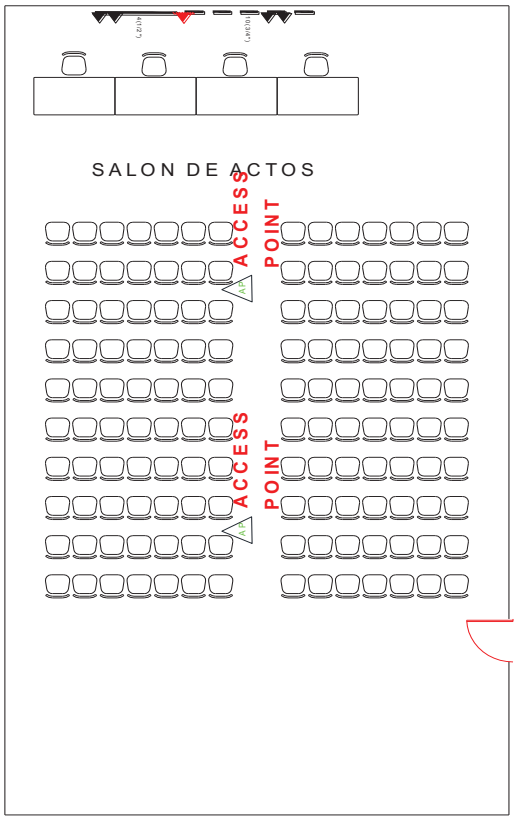


Figura 3.32: Ubicación Access Point Salón de Actos

3.3.3.3 Sala de Profesores

La Sala de Profesores es el área donde los docentes del colegio se reúnen para trabajar en actividades afines al ámbito académico, por lo que, las principales aplicaciones a las que se tendrán acceso desde esta área serán la navegación en Internet, las Aulas Virtuales y el correo electrónico.

En esta área de 38 m^2 se pueden tener hasta 20 personas sentadas con sus respectivas laptops, y según los resultados que se obtuvieron de las encuestas aplicadas a los docentes, gran parte de ellos adquirirán en poco tiempo laptops para realizar sus labores académicas; tomando en cuenta esto y sabiendo que en la Sala de Profesores existirán 8 puntos de red cableados, se estima que por lo menos se tendrán 15 usuarios conectados inalámbricamente.

En cuanto a interferencias que puedan existir se identificó que en la tecnología inalámbrica 802.11 b/g/n se tiene una leve presencia de redes externas que ocupan el canal No. 11 (potencia de -66 dBm) para transmitir sus datos; en la tecnología 802.11a no se detectaron redes funcionando. La interferencia que pudo haberse tenido por la cercanía de esta área al Taller Mecánico del colegio quedó descartado, debido a que ahora esta área se utiliza como bodega de pupitres.

3.3.3.3.1 Red WLAN en la Sala de Profesores

Al tener un número reducido de usuarios que van a utilizar las aplicaciones de Internet y Aula Virtual, se decidió utilizar un Access Point, trabajando con la tecnología 802.11 b/g/n (Ch. 6) con una potencia de transmisión de 15 dBm, utilizando antenas dipolo y con una conexión alámbrica 100Base-TX. Este Access Point estará sujeto a las estructuras metálicas del techo de la sala, la alimentación se realizará mediante PoE.

Por último se debe aclarar que no se realizó un Site Survey Activo para ninguna de las zonas donde se ha destinado la instalación de Access Points debido a que las áreas de cobertura de este servicio se encuentran directamente junto o debajo de la ubicación de donde se encontrarán funcionando los Access Points.

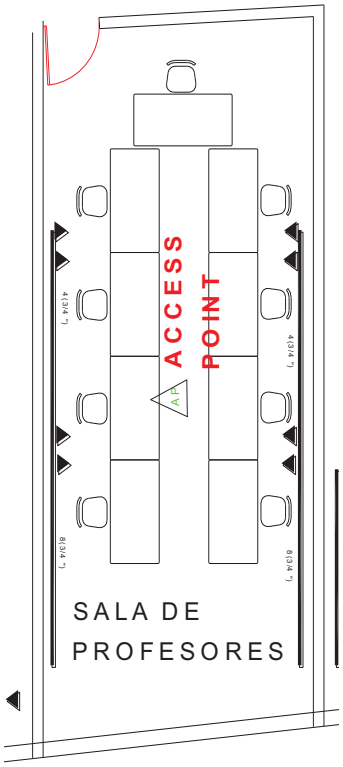


Figura 3.33: Ubicación Access Point Sala de Profesores

3.3.3.4 Seguridad en la WLAN

Al ser la red WLAN un punto vulnerable a ataques externos e intrusiones peligrosas para la integridad de la red del colegio, se deberán tomar medidas que protejan y minimicen al máximo las posibilidades de que los ataques produzcan daño.

Para evitar que los usuarios cercanos geográficamente a la institución puedan detectar fácilmente la red inalámbrica del colegio se va a deshabilitar la publicación del SSID de estas redes; además los nombres con los que funcionarán las redes inalámbricas de estudiantes, profesores e invitados no tendrán relación alguna con el CFD. Otra razón para ocultar el SSID es para que solo el administrador de red sea capaz de poder configurar el acceso a las redes inalámbricas, excepto en el caso de la red de los Estudiantes, que podrán configurarla de forma autónoma.

Para la asociación de un usuario a una red inalámbrica se utilizará el estándar de seguridad WPA2 (*Wi-Fi Protected Access 2*) y el algoritmo de cifrado AES

(*Advanced Encryption Standard*); además, se usarán claves de 10 caracteres alfanuméricos y no alfanuméricos con un período de validez de 6 meses.

A las VLANS de INVITADOS y ESTUDIANTES solo se les permitirá el acceso a Internet; la VLAN de PROFESORES tendrá habilitado el acceso a Internet y transferencia de archivos, correo electrónico y aulas virtuales; y la VLAN de PERSONAL ADMINISTRATIVO tendrá acceso a Internet, correo electrónico, transferencia de archivos, y los servicios de correo electrónico institucional.

3.3.3.5 Características Técnicas de Access Points

El Access Point D-Link DIR 655 será reutilizado para la Biblioteca de la institución y estará trabajando solo dentro de la VLAN ESTUDIANTES.

Los Access Points a utilizarse en el Cuarto de Equipos, Salón de Actos y Sala de Profesores deberán tener las siguientes características:

- Los Access Points deberán trabajar en la frecuencia de 2.4 Ghz debido a que con esta frecuencia se puede abarcar un área mayor y se tiene menor atenuación debido a obstáculos entre el AP y un usuario. Además como se mostró en el Site Survey pasivo la utilización de la tecnología 802.11b/g/n es totalmente posible pues casi no existe interferencia en esa banda de frecuencias.
- Para la conexión con la red cableada se deberá contar con un puerto de 100 Mbps de velocidad, ya que es una velocidad suficiente si se toma en cuenta que la mayor cantidad de tráfico solo estará destinado a la navegación en Internet con una velocidad de 210 Kbps por usuario. También este puerto deberá poder configurarse automáticamente ante conexiones directas o cruzadas.
- Debido a que la ubicación de los AP's será en lugares donde no exista toma corrientes, estos equipos deberán tener la capacidad tomar energía por medio del cable de red.
- Para tener un mayor control sobre la zona que estará cubierta por el AP y poder cambiar de antena en el caso de que se necesite una mayor potencia o un diferente patrón de radiación, las antenas de los AP's

deberán estar montadas en el exterior del dispositivo y unidas por medio de conectores RP-SMA.

- Ya que en algunas zonas como el salón de actos se tendrá que dar cobertura a un área un poco amplia, la potencia de transmisión deberá ser 20 dBm o mayor.
- Como las conexiones inalámbricas podrán utilizarse para las conexiones de docentes, administrativos e invitados, el AP deberá ser capaz de configurar varias redes inalámbricas y asociar cada red a una VLAN diferente para con esto poder separar cada tipo de tráfico.
- Para permitir la diferenciación de tráfico de video, del tráfico de datos el AP deberá contar con mecanismos como priorización de tráfico (IEEE 802.1p) y diferenciación de tráfico.
- Como medidas de seguridad se deberá poder utilizar como método de autenticación a WPA2 y con algoritmo de cifrado AES. Adicionalmente deberá soportar el método de autenticación por medio del protocolo EAP y un servidor RADIUS en caso de que se quiera aumentar el nivel de seguridad de la red.
- Permitirá realizar un filtrado por direcciones MAC para evitar que personas ajenas al colegio traten de acceder a la red por medio de la WLAN.
- El AP permitirá funcionar como servidor DHCP y DNS, pero también deberá poder funcionar como repetidor DHCP para poder reenviar las peticiones al servidor DHCP del colegio.
- La administración de los AP's podrá hacerse por medio de una interfaz gráfica web, o por consola con la utilización de Telnet o SSH.
- Los AP's deberán soportar el protocolo SNMP para la monitorización del equipo.

Al observar la comparación de las características técnicas de los dos dispositivos de red se recomienda la utilización del Access Point HP MSM410 (J9427C) debido a que presenta las mismas funciones que el equipo Cisco pero lo supera en aspectos como el menor consumo de energía, lo cual es importante pues se va a utilizar PoE para alimentar a estos dispositivos, además posee una interfaz alámbrica de 1 Gbps que asegurará que en caso de que se requiera de un

servicio de red que ocupe un mayor ancho de banda se podrá seguir utilizando este equipo sin problemas de cuellos de botella. Para ver más detalles sobre las características técnicas que se muestran en la Tabla 3.27 mirar el Anexo 16.

ACCESS POINT		
CARACTERÍSTICAS	**EQUIPOS**	
	Cisco AIR-AP1261N-x-K9 	**HP MSM410 (J9427C)** 
Soporte de estándares IEEE 802.11 b/g/n, con certificado Wi-Fi	Sí	Sí (802.11 a/b/g/n)
Puerto WAN fullduplex (10Base-T, 100Base-TX) auto sensible	Sí (1 puerto)	Sí (1 puerto hasta 1Gbps)
Power over Ethernet (IEEE 802.3af)	Sí (15.4 W)	Sí (8 W)
Configuración de múltiple SSID y difusión de SSID.	Sí	Sí
VLANS (IEEE 802.1q)	Sí	Sí
Soporte de DHCP	Sí	Sí
Soporte para QoS: 802.1p y Diffserv	Sí	Sí
Antenas Desmontables con conector RP-SMA,	Sí	Sí
Potencia de Transmisión 20dBm	Sí (23 dBm)	Sí (23 dBm)
Autenticación: RADIUS/EAP-TLS, EAP-TTLS, EAP-MD5	Sí (RADIUS incorporado)	Sí
Soporte de WPA2 Personal y Enterprise	Sí	Sí
Filtrado por direcciones MAC, dirección IP y puerto	Sí	Sí
Métodos de Cifrado AES y TKIP	Sí	Sí
SNMP v1/v2c/v3	Sí	Sí
Administración por Http, Https, Telnet, SSH y consola	Sí	Sí(No Telnet, ni SSH)

Tabla 3.27: Comparación de características técnicas entre dos marcas de APs para usar en la red WLAN

3.3.4 DISEÑO SISTEMA DE TELEFONÍA IP

Debido a las fallas en el funcionamiento de la central telefónica analógica que posee el CFD, se ha considerado tomar en cuenta en el diseño, la futura implementación de un sistema de telefonía IP que brinde más servicios y venga a reemplazar al sistema de telefonía existente. Este nuevo sistema de telefonía deberá cumplir con el decreto ejecutivo 1014 que impulsa el uso de plataformas de software libre dentro de los sistemas y equipamientos informáticos.

3.3.4.1 LAN

El sistema de Telefonía IP demanda ciertas características de funcionamiento a los equipos de conectividad que componen la LAN para garantizar la calidad de este servicio; pensando en ello la LAN deberá cumplir con las siguientes características:

- Los switches de acceso y distribución-núcleo deberán contar con mecanismos de priorización del tráfico de voz y de configuración de VLANS separadas para voz y datos.
- El suministro de energía a los teléfonos IP se hará por medio de PoE (*Power over Ethernet*).
- Para facilitar la clasificación y priorización del tráfico de voz todos los teléfonos IP se configurarán utilizando un servidor DHCP con direcciones IP dentro del rango de una subred exclusiva para ellos y pertenecerán a la VLAN TELEFONIA.
- Todo el sistema de telefonía estará conectado a un UPS (*Uninterruptible Power Supply*) para que en caso de que la red eléctrica pública falle las comunicaciones internamente y con el exterior sigan funcionando durante un tiempo aproximado de 12 minutos, y en caso de que el servicio eléctrico no haya vuelto para el final de este período de tiempo se utilizará la energía que el generador eléctrico va a producir y que estará destinado entre otras cosas a mantener el servicio de telefonía IP funcionando.

3.3.4.2 Central Telefónica IP

La central telefónica IP es un hardware o software que permite la comunicación telefónica mediante el uso de las redes de datos. Los dispositivos usados para la comunicación en la telefonía IP son llamados teléfonos IP cuya identificación es la dirección IP que tiene configurado cada uno de ellos.

Entre las ventajas que ofrece la telefonía IP están servicios como identificación de llamadas, servicio de espera, buzón de voz, cuentas de voz seguras, interconexión entre troncales telefónicas digitales que permite intercomunicar lugares separados geográficamente por medio de Internet, de manera transparente para el usuario y a un costo menor. Otra ventaja de la telefonía IP es su capacidad de poder enviar información de video y voz codificada simultáneamente para realizar video llamadas.

Las características con las que deberá cumplir la central telefónica IP son:

- Facilidad para la configuración de cuentas de usuario y funcionalidades.
- Permitir un nivel de escalabilidad para crecer en el número de usuario y de llamadas simultáneas.
- Capacidad para utilizar bases de datos para almacenar las cuentas de usuario y registros de llamadas.
- Permitir funcionamiento de las cuentas de usuario dentro de un directorio LDAP.
- Capacidad para la conexión con la PSTN con la utilización de canales E1/T1 o por medio de líneas telefónicas individuales.
- Funcionalidades para asignar permisos para llamadas locales, nacionales, internacionales y hacia celulares con la utilización de perfiles de usuario.
- Funcionalidades de temporizador para restringir la duración de las llamadas con varios avisos que adviertan que la llamada está por terminar.
- Cuentas de usuario móviles y seguras con la utilización de passwords individuales para cada usuario.

- Capacidad para conferencias entre varias terminales telefónicas a la vez.
- Utilización de codecs de voz de licencia gratuita como el codec G.711, GSM e IAX; y licencias privadas como el codec G.729.
- Permitir los protocolos de señalización SIP y H.323.
- Capacidad para la implementación de un menú de bienvenida interactivo (IVR, *Interactive Voice Response*) para las llamadas que recibe el colegio.
- Función de contestadora automática en caso de que el usuario no conteste o se encuentre ausente; y almacenamiento de los mensajes de voz en cuentas individuales.
- Acceso mediante menús interactivos a la cuenta de usuario personal, mensajes de voz y directorio telefónico.
- Permitir al usuario poder crear su propio saludo para el correo de voz, además de permitirle poder cambiar sus claves de seguridad.
- Posibilidad de poder intercomunicarse con otras centrales telefónicas IP por medio de enlaces datos para poder realizar llamadas sobre IP entre dos lugares geográficamente separados y así disminuir el costo que representan estas llamadas.
- Encriptación para el tráfico de voz y de control de la central telefónica que fluye por la red para garantizar la privacidad en las llamadas.
- Permitir la interacción de la central telefónica con otros servicios como por ejemplo el servicio de video seguridad.
- Permitir la agregación de más funcionalidades por medio de agregación de módulos.

3.3.4.2.1 Alternativas de Software

Asterisk es una aplicación de software libre que permite tener funcionalidades de central telefónica sobre un servidor de comunicaciones con diferentes sistemas operativos como BSD, MAC OS X, Windows, etc. Entre las características que trae Asterisk están el buzón de voz, menús de voz interactivos, seguridad y

portabilidad de cuentas telefónicas, conferencias, distribución de llamadas automáticas y la posibilidad de utilizar módulos escritos en script de formato Asterisk o en cualquier otro lenguaje de programación soportado por Linux.

GNU Gatekeeper software libre multiplataforma que permite implementar un servidor VoIP y videoconferencia basado en el proyecto OpenH323 que provee una implementación de código abierto del estándar de la ITU H.323. Entre sus características están el soporte de almacenamiento de cuentas en archivos y bases de datos SQL, poseer una interfaz gráfica y soporte para IPV6 entre otras.

CARACTERÍSTICAS	SERVIDOR	
	Asterisk	**GNU Gatekeeper**
Facilidad	Fácil	Complejo
Almacenamiento en bases de datos	Sí (Las cuentas y los registros telefónicos)	Sí (las cuentas de usuario)
Utilización de canales E1/T1 y líneas telefónicas analógicas	Sí	Sí
Soporte LDAP	Sí	Sí
Funcionalidad de permisos con perfiles de usuario	Sí	No (solo puede asignar permisos por cada cuenta)
Codecs voz soportados	G.711, GSM, G.729, H323, IAX2	G.711
Protocolos de señalización	SIP, H323, IAX2	H.323
Creación de menús de voz	Sí	No
Contestadora y mensajes de voz	Sí	N.D.(*No Disponible*)
Comunicación entre centrales telefónicas IP	Sí	Sí
Encriptación del tráfico de voz y de señalización	Sí	No
Permite la interacción y generación automática de llamadas por medio de comandos	Sí	No
Estructura modular para añadir servicios	Sí	No
Soporte y Documentación	Muy Buena	Buena
Licencia	GPL	GPL

Tabla 3.28: Comparación de las características técnicas del software para Central Telefónica IP[PW38, PW39]

Luego de analizar las ventajas que ofrece cada alternativa se decidió utilizar Asterisk como central telefónica y Gateway IP, debido a su gran escalabilidad y robustez. Asterisk ofrece soporte para la mayor cantidad de protocolos de transporte y señalización de tráfico de voz y video sobre IP, posibilita agregar funcionalidades por medio de la agregación de módulos y además posee una gran cantidad de documentación en línea.

3.3.4.3 Teléfonos IP

En la Tabla 3.29 se muestran las características mínimas que los teléfonos IP deberán contar:

- Ya que cada punto de red que tendrá un teléfono IP conectado también prestará servicio a un computador, los teléfonos IP a utilizar deberán tener 2 interfaces de red de 100 Mbps, una de ellas para conectarse a la salida de telecomunicaciones y el otro para conectarse a la estación de trabajo.
- Los puertos deben poder detectar y configurarse automáticamente en conexión directa o cruzada para evitar errores de conectividad debidas a la incorrecta utilización de los patch cords de conexión.
- Los terminales telefónicos deben tener funciones de: transferencia, parqueo, reenvío, historial de llamadas y llamada en espera.
- Soporte del codec de voz G.711 ya que es el codec de mayor utilización en la telefonía IP.
- Soporte del protocolo de señalización SIP pues es el más difundido en la telefonía IP y provee las funcionalidades indispensables para concretar una llamada sobre IP.
- Como el servicio de telefonía es indispensable para las actividades del personal administrativo del colegio se utilizarán teléfonos IP que puedan recibir energía por medio del cable de red con el objetivo de que en caso de exista una falla en el suministro eléctrico, los teléfonos reciban energía del UPS por medio del switch al que estarán conectados; además con esta forma de alimentación se puede instalar un teléfono casi en cualquier lugar del colegio.
- La configuración de las direcciones IP de los teléfonos en red, debe poder hacerse con clientes DHCP.

- El teléfono IP al actuar como un switch intermedio entre la estación de trabajo conectada a él y los dispositivos de conectividad del colegio; éste debe garantizar que el flujo de datos que se dirige hacia su estación de trabajo debe pasar sin ser cambiado en ninguna cabecera ya que si no fuera así los servicios como las VLANS no podrían funcionar correctamente.
- La administración del teléfono IP y sus configuraciones deben poder realizarse por medio de una interfaz gráfica IP y también por medio de menús de configuración integrados en el teléfono.
- Permitir la actualización de su software por medio del protocolo Http, pues con estas actualizaciones permitirán arreglar cualquier imperfección que pueda surgir en el funcionamiento del teléfono.

TELÉFONO IP		
CARACTERÍSTICAS	**EQUIPOS**	
	Cisco SIP Phone 3911 	**HP 3500B (JC505A)** 
2 Interfaces fullduplex auto sensible (10Base-T, 100Base-Tx) para computador y conexión a LAN	Sí	Sí
Soporte de PoE (IEEE 802.3af)	Si (15.4W)	Sí (6.4W)
Funcionalidades: Llamada en espera, Transferencia de llamada, Altavoz, Conferencia, Remarcado	Sí	Sí
Display	Blanco/Negro de 144x32 pixeles	Display de 85mm x 28mm
Soporte de clientes DHCP	Sí	Sí
Soporte de VLANS (IEEE 802.1Q)	Sí	N.D.
Soporte 802.1p	Sí	Sí
Soporte de protocolos de señalización	SIP	SIP
Soporte de Codecs G.711, G729A/B	G.711 y G.729a	G.711, y G.729ab
Configuración Web y Menú integrado	Sí	Sí

Tabla 3.29: Comparación de características técnicas entre Teléfonos IP de dos marcas distintas que se usarán en la Telefonía IP [PW40, PW41]

Luego de observar la comparación de las características de estos dos equipos, se pudo ver que tienen funcionalidades similares, por lo que para tomar una decisión se consideró el hecho de que los switches de acceso a los que van a estar conectados éstos teléfonos IP serán de marca Cisco, y para no tener un mal funcionamiento debido a incompatibilidades entre marcas distintas y por facilidad para la administración y creación de configuraciones se decidió usar una misma línea de fabricante, por esta razón se sugiere al teléfono IP Cisco 3911 para que sea utilizado en el sistema de telefonía del CFD.

3.3.4.4 Dimensionamiento de Servidor de Telefonía [PW27, PW28, PW29]

El servidor que alojará la central telefonía IP deberá tener las siguientes características:

- Ya que la central telefónica va a prestar servicio a 13 terminales IP, la carga de trabajo será baja, es por ello, que se le dará los requerimientos mínimos de memoria RAM de 2 GB y un procesador de cuatro núcleos a 2 GHz.
- El espacio libre en disco mínimo deberá ser de 89 MB, considerando que se va a tener alrededor de 13 casilleros de voz y que se tendrá espacio para 15 minutos de grabación para cada uno usando el códec de voz G.711 que proporciona una tasa de bits de 64 Kbps[PW30].
- Para tener conectividad con la PSTN el servidor deberá tener una tarjeta FXO de al menos 4 puertos.
- Para que la central telefónica IP pueda trabajar con teléfonos analógicos se instalará también una tarjeta FXS de mínimo 4 puertos; con esto se podrá reutilizar algunos de los teléfonos analógicos con los que cuenta la institución.
- Para evitar que el servidor quede sin funcionar debido a fallas en la fuente de energía, el servidor deberá poder contar con una fuente de energía redundante.

3.3.5 DISEÑO DEL SISTEMA DE VIDEO SEGURIDAD

Las medidas de seguridad física con las que cuenta el CFD son deficientes, ya que no se cuenta con seguridad privada para su resguardo y solo se tiene protecciones metálicas para las oficinas y laboratorios de computación dejando todas las otras áreas del colegio desprotegidas, es por ello que en las encuestas aplicadas a profesores y personal administrativo se puede observar la preocupación sobre la seguridad de los activos fijos e información que posee la institución. Debido a esto se consideró diseñar un sistema de video seguridad que permita solventar esta necesidad del CFD.

Las características con las que debe contar el servidor de video seguridad se listan a continuación:

- Capacidad para funcionamiento de las cámaras IP en diferentes perfiles, en cada uno de los cuales la cámara se comporte de una manera diferente; el objetivo es poder automatizar el comportamiento de las cámaras IP según la hora del día y el día de la semana.
- El servidor de video seguridad debe soportar el envío y configuración de patrones de movimiento para aquellas cámaras que tengan esa característica.
- Permitir el uso de las cámaras IP como detectores de movimiento, y en caso de que se detecte algo se pueda interactuar por medio de comandos con otro servicio de red como por ejemplo la central telefónica IP para que se cree una llamada alertando de la detección de movimiento.
- El sistema de video vigilancia debe permitir configurar en detalle la sensibilidad en la detección de movimiento para evitar que se produzcan alertas en falso.
- Los videos del sistema de vigilancia se podrán ver por medio de un monitor web que permita observar tanto los videos tomados en vivo, como también los eventos pasados en los que se haya detectado movimiento por medio de las mismas cámaras.

- Todo el tráfico que se intercambie con el monitor de video seguridad deberá estar encriptado para proteger la información de videos y cuentas de usuario de esta interfaz.

3.3.5.1 Servidor de Video Seguridad

3.3.5.1.1 Alternativas de Software

ZoneMinder es una aplicación de software libre para monitoreo de video de cámaras de CCTV, cámaras USB, cámaras IP, que permite configurar y observar las capturas de video por medio de una interfaz gráfica web. ZoneMinder tiene la funcionalidad de detección de movimiento. Los videos se almacenan por defecto en una base de datos MySQL permitiendo el acceso, revisión, pausa y acercamiento digital a los videos en vivo y a videos anteriormente registrados.

Motion es una aplicación de software libre para monitorear señales de video de una o más cámaras USB o IP. Motion posee una interfaz gráfica web para la configuración de cada una de las cámaras que tiene configuradas y permite ver en vivo cada cámara en una ventana diferente del navegador web. Las capturas cuando no se detecta movimiento se realizan como imágenes y solo al detectar movimiento se inicia la captura de video.

Características	Servidor	
	ZoneMinder	Motion
Configuración de Perfiles de funcionamiento	Sí	No
Envío de comandos de movimiento a la cámara IP	Sí	No
Utilizar cámaras para detectar movimiento y ejecutar comandos de consola	Sí	Sí
Nivel de configuración de la sensibilidad de la detección de movimiento	Alto	Medio
Monitor Web, con capacidad de ver videos guardados	Sí	No
Encriptación del tráfico de video y de cuentas de usuario	Sí	Sí

Tabla 3.30: Comparación de las características del software para servidor de video seguridad[T1, T2]

Se ha escogido a ZoneMinder como servidor de video seguridad, ya que, tiene una fácil configuración para añadir nuevas cámaras y para el funcionamiento del servicio; además, permite ahorrar espacio de almacenamiento en el disco duro, pues permite configurar de forma detallada las capturas durante y luego de que se detecte movimiento en la zona; así como también permite la observación de varias fuentes de video dentro de una misma pantalla y permite el envío de comandos para el movimiento de las cámaras IP lo que es muy necesario para las aplicaciones de video seguridad.

3.3.5.2 Cámaras IP

A continuación se muestran las características mínimas que las cámaras IP deberán tener:

- Ya que las cámaras IP van a ser ubicadas en lugares donde no existe el acceso a toma corrientes, las cámaras IP deberán poder recibir energía eléctrica por medio del cable de red.
- Los codecs de video que deben soportar son MJPEG y MPEG-4 ya que son los más difundidos para la utilización en transmisiones de video seguridad.
- Ya que se debe poder mirar en los monitores en condiciones de luz y de oscuridad, las cámaras IP deben tener leds infrarrojos que se activen cuando las condiciones de luz sean pobres.
- Se podrá configurar de manera detallada la calidad de video, el tamaño de cuadro y la cantidad de cuadros por segundo que se van a capturar, esto para poder definir exactamente las condiciones de video que se necesiten para observar claramente las imágenes en el monitor de video seguridad.
- La configuración de los parámetros deberá poder hacerse por medio de una interfaz gráfica web.
- Se deberá poder actualizar el software por medio del protocolo Http para reparar las imperfecciones que puedan aparecer en el funcionamiento de la cámara debido a errores del firmware.

CÁMARA IP PARA INTERIORES		
CARACTERÍSTICAS	**EQUIPO**	
	Cisco CIVS-IPC-2521V 	**D-Link DCS-6111** 
1 Interfaz fullduplex auto sensible (10Base-T, 100Base-Tx)	Sí	Sí
Soporte de PoE (IEEE 802.3af)	Sí (14.4 W)	Sí (11 W)
Soporte de Codecs de video	H.264, MPEG-4 y MJPEG	MPEG-4, MJPEG.
Ajuste de Lente de Cámara	Paneo: 340° Cabeceo: 160° Campo de Visión: Horizontal: 22°-76° Vertical: 17°-56°	Paneo: 350° Cabeceo: 85° Campo de Visión: Horizontal: 63.3° a 17.9° Vertical: 46.5° a 13.5°
Detección de movimiento y disparo de acción	Sí	Sí
Configuración Manual de Tasa de Bits, Tamaño de imagen y Número de cuadros por segundo	720x480/576@30/25 ips 704x480/576@30/25 ips 352x240/288@30/25 ips	Tamaño de imagen, bit rate y números de cuadros por segundo pueden ajustarse.
Configuración vía HTTPS, HTTPS	Sí	Sí
Actualización vía HTTP	Sí	Sí (también por FTP)
Compatibilidad con Sistemas de Video Seguridad de software libre	N.D.	Soporte para configuraciones dentro de aplicaciones de video seguridad de software libre

Tabla 3.31: Comparación de características técnicas entre Cámaras IP internas de dos marcas distintas para el sistema de video seguridad del CFD[PW42, PW43]

Un aspecto importante que se consideró para escoger las cámaras IP fue su compatibilidad con la aplicación de video seguridad de software libre ZoneMinder; además otro aspecto importante evaluado fue la capacidad de ajustar sin restricciones los parámetros de tamaño de imagen y número de cuadros por segundo, y que la cámara cuente con el codificador MJPEG. Al evaluar estos aspectos en la Tabla 3.31 se evidenció que la cámara IP D-Link DCS-6111 es la que mejor cumple con los requisitos, por lo que es la que recomienda para su uso dentro de las oficinas e instalaciones del colegio.

Además de las características que ya se mencionaron anteriormente las cámaras IP externas deberán cumplir con los siguientes requisitos:

- Deberán estar protegidas dentro de un estuche especialmente hecho para resistir a la intemperie. La base inferior del estuche tendrá la forma de un domo y estará polarizada para ocultar los movimientos de la cámara.
- Las cámaras IP externas deben poder moverse y enfocar objetos para aumentar así el rango de visión de la cámara y registrar con más detalles los acontecimientos sospechosos. Para el movimiento horizontal se debe mover al menos 300º y para el movimiento vertical debe poder moverse unos 170º.
- Las cámaras externas deberán poder recibir comandos desde su interfaz de administración y desde la aplicación de video vigilancia para tener un control completo sobre las zonas que se vayan a capturar en video.
- Las cámaras externas deben ser revisadas periódicamente para comprobar si su protección no ha sufrido daños.

Para evaluar cuál es la mejor cámara IP que se puede instalar en el perímetro del colegio se tomó en cuenta los requerimientos como: la compatibilidad de la cámara para el funcionamiento con el sistema de video vigilancia ZoneMinder; también se analizó las capacidades de zoom óptico y digital, la sensibilidad a la luz de la cámara y la configuración sin restricciones del tipo de códec a utilizar, del número de cuadros por segundo, y del tamaño de imagen que ofrece la cámara. Luego de considerar los aspectos anteriores se pudo ver que la cámara IP D-Link 6818 es la que mejor cumple con ellos, y es por esto que se la recomienda para su utilización en la vigilancia externa del colegio. En la Tabla 3.32 se muestra la comparación de las características técnicas más relevantes de las cámaras externas.

Las ubicaciones de las cámaras IP dentro de las instalaciones del colegio están especificadas dentro la Tabla 3.14 de este capítulo, y para observar gráficamente su ubicación ver el Anexo 11.

CÁMARA IP PARA EXTERIORES		
CARACTERÍSTICAS	**EQUIPO**	
	Cisco CIVS-IPC-2930 	**D-Link DCS-6818** 
1 Interfaz fullduplex auto sensible (10Base-T, 100Base-Tx)	Sí	Sí
Soporte de PoE (IEEE 802.3af)	Sí (15.4 W)	Sí (20 W)
Soporte de Codecs de video	H.264, MPEG-4 y MJPEG	MPEG-4, MJPEG.
Soporte para grabación diurna y nocturna	Iluminación Mínima: 0.55 lux at 1/60 seg (color) 0.018 lux at 1/2 seg (color) 0.00018 lux at 1/2 seg (B/W)	Iluminación Mínima: F1.4 @ 1.5flux
Ajuste de Lente de Cámara	Paneo: 360° Cabeceo: -2° a +92° Campo de Visión: Horizontal: 22°-76° Vertical: 17°-56° Zoom: 35x óptico y 12x digital	Paneo: 5° a 400° Cabeceo: -10° a 190° Campo de Visión: Horizontal: 63.3° a 17.9° Vertical: 46.5° a 13.5° Zoom: 36x óptico y 12x digital
Detección de movimiento y disparo de ación	Sí	Sí
Configuración Manual de Tasa de Bits, Tamaño de imagen y Número de cuadros por segundo	Tamaño de imagen: 704 x 480 352 x 240 704 x 576 Cuadros por segundo: 30, 25, 24, 15, 12.5, 12, 10,8, 7.5, 6, 5, 4, 3, 2, 1	Tamaño de imagen, bit rate y números de cuadros por segundo pueden ajustarse.
Condiciones ambientales, Protección IP6	Temperatura: -51°C a 50°C Protección IP6	Temperatura: -20°C a 50°C Protección IP6
Configuración vía HTTPS, HTTPS	Sí	Sí
Actualización vía HTTP	Sí	Sí (también por FTP)
Compatibilidad con Sistemas de Video Seguridad de software libre	N.D.	Soporte para configuraciones dentro de aplicaciones de video seguridad de software libre

Tabla 3.32: Comparación de características técnicas entre Cámaras IP externas de dos marcas distintas para en el sistema de video seguridad del CFD[PW44, PW45]

3.3.5.3 Dimensionamiento de Servidor de Video Seguridad

Para el servidor de video seguridad se debe considerar que se usarán capturas en formato de imagen y solo se tomarán videos en caso de que se detecte movimiento en la zona vigilada. Los videos tendrán un tamaño de imagen de 320x240@15 IPS en calidad media, y se tiene un flujo de datos de video igual a 1.6 Mbps.

Se considera que las horas en las que se debe tener grabaciones completas son en las horas en las que no existe ningún personal dentro del colegio, por lo que el tiempo de grabación sería de 16 horas diarias con lo que se obtiene que diariamente se ocuparían 10.73 GB de espacio de almacenamiento por cámara y se ocuparían 182.39 GB de espacio por las 17 cámaras IP aproximadamente. Si se desea tener un registro de los últimos 7 días el espacio en disco necesario sería de 1.25 TB.

Para dimensionar el procesador y la memoria RAM se usará los parámetros que son recomendados por el programa ZoneMinder[T1]. El procesador mínimo del servidor debe ser un Dual Core de 1.5 GHz, y la memoria RAM será de 1 GB.

El servidor de video seguridad deberá montarse dentro de un rack en el Cuarto de Equipos, por lo que éste debe tener un ancho de 19” y una profundidad menor a 31”.

3.3.6 SERVICIOS DE LA INTRANET

El CFD al ser una institución pública, se encuentra en proceso de migración del software propietario hacia el Software Libre, por lo que, los servicios de red deberán cumplir con este requisito.

Para asegurar el correcto funcionamiento de los servicios que se ofrecerán dentro de la red LAN del CFD, es necesario realizar un análisis de los diferentes paquetes de Software Libre que existen en el mercado, para obtener los criterios necesarios y escoger aquellos servicios y aplicaciones que tengan las mejores características.

3.3.6.1 Plataforma para la implementación de los servicios de red

Para la implementación de los servicios de red se usará un sistema operativo basado en GNU/LINUX, por ser plataformas confiables, seguras, con mucha documentación publicada y de acceso gratuito.

3.3.6.1.1 Alternativas de Software

Las alternativas de plataformas para la instalación de los servicios de red son:

CentOS (*Community Enterprise Operating System*) es un sistema operativo creado por personas voluntarias que compilan el código fuente que la empresa privada Red Hat libera para cumplir los términos de la Licencia Pública General GNU. Es por ello, que CentOS es muy similar a las distribuciones Red Hat Enterprise Linux, pero su desventaja es que al ser creado por voluntarios no se ofrece mantenimiento, ni asistencia técnica especializada tal como poseen las distribuciones ofrecidas por Red Hat, dificultando los procesos de instalación y actualización de sus paquetes.

RedHat Enterprise Linux es un sistema operativo que se compone de software libre que es desarrollado y mantenido por la empresa Red Hat. Esta distribución Linux es una de las más seguras y estables que existen en la actualidad, pero su desventaja es que tanto el sistema operativo y las actualizaciones de paquetes en formato binario usable solo son accesibles para aquellos que se hayan suscrito por medio de un pago anual.

Debian es un sistema operativo que nace de un proyecto orientado a crear una distribución de software libre por medio de la colaboración de desarrolladores de todo el mundo, que escriben y depuran cada componente del sistema operativo de forma separada, pero siempre manteniendo una gran atención a la calidad del producto final. Esta distribución es estable, segura, confiable y ofrece actualizaciones de sus paquetes de forma permanente.

Ubuntu es un sistema operativo mantenido por la empresa privada Canonical, y es distribuido bajo la licencia GNU. Al estar respaldado por una empresa esta distribución tiene una gran compatibilidad con un sinnúmero de plataformas de hardware de fabricantes como Dell, HP, Intel, etc.; además ofrece ventajas como

tener distribuciones Ubuntu orientadas exclusivamente para servidores que reciben actualizaciones de seguridad constantes durante un tiempo máximo de 5 años, y al cabo del mismo puede ser actualizado de forma automática y gratuita a una distribución más actualizada. Otras ventajas que tiene esta distribución son el ofrecer una gran cantidad de documentación oficial y no oficial en línea y la instalación y actualización de paquetes por medio de los servidores oficiales de Ubuntu en Internet.

3.3.6.1.2 Selección de alternativa

Una vez considerado las ventajas y desventajas que cada una de las distribuciones posee, se llegó a la decisión de usar la distribución Ubuntu, debido a que es una de las más difundidas en el mundo, está orientada a servidores, tiene una amplia compatibilidad con un sinnúmero de plataformas de hardware de diferentes fabricantes, existe mucha documentación en idioma español para realizar consultas, brinda un servicio de instalación y actualizaciones de seguridad para la mayor parte de paquetes de los servicios de red, y puede ser obtenido de forma gratuita desde servidores oficiales en Internet.

3.3.6.2 Servidor DNS (*Domain Name System*)

El servicio DNS almacena nombres de dominio y los relaciona con sus direcciones IP, y viceversa. Este servicio es usado por las aplicaciones clientes que necesitan traducir los nombres de dominio de recursos ubicados en redes externas y obtener su dirección IP para con ello poder acceder a esos recursos.

3.3.6.2.1 Alternativas de Software

Las alternativas de software para el servicio de DNS son las siguientes:

BIND9 (*Berkeley Internet Name Domain*) es el servidor DNS más usado en Internet. Ésta es una versión totalmente nueva pues el código fue escrito desde cero para superar las dificultades de auditoría del código presentes en versiones anteriores. Incorpora la utilización de DNSSEC (*DNS Securty Extensions*) para asegurar el intercambio de la información DNS y TSIG (*Transaction SIGnatures*) usado principalmente como forma de autenticación en la transferencia de zonas

entre servidor DNS primario y secundario. Esta aplicación es usada en condiciones de altos volúmenes de peticiones, brindando gran nivel de fiabilidad.

DJBDNS implementación DNS creada por Daniel J. Bernstein, con el objetivo de hacer énfasis en la seguridad. Su característica más relevante es su arquitectura de software modular que hace que su código sea menos extenso y complejo. Debido a su arquitectura modular DJBDNS está compuesto por diversos programas que se encargan cada uno de una función específica de la resolución DNS, lo que proporciona mayor velocidad de respuesta a las peticiones.

PowerDNS servidor DNS que posee dos partes; un proceso usado como servidor autoritativo que solo responde con los dominios de los que tiene conocimiento, y otro proceso que actúa como servidor DNS recursivo que se encarga de hacer las consultas a otros servidores DNS autoritativos en Internet. PowerDNS también tiene la característica de usar varias formas de almacenamiento de registros de dominio, desde los archivos de configuración en texto, hasta bases de datos MySQL, Oracle, etc.

La alternativa elegida para el servidor de nombres de dominio es BIND 9, pues es la más robusta de todas las alternativas analizadas, además, está respaldado por la ISC (*Internet Systems Consortium*) que es una organización sin fines de lucro, que desarrolla aplicaciones de código abierto de alta calidad y que participa de forma activa en la creación de nuevos estándares de la IETF; además, la ISC ofrece una gran cantidad de documentación, mantenimiento y actualizaciones de seguridad para sus aplicaciones.

Servidor	Características						
	Autoritativo	Recursivo	Esclavo	Caching	IPV6	DNSSEC	TSIG
BIND 9	Sí	Sí	Sí	Sí	Sí	Sí	Sí
DJBDNS	Sí	Sí	Sí	Sí	No	No	No
PowerDNS	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Tabla 3.33: Comparación del software para servidor DNS[PW46, PW47, PW48]

3.3.6.3 Servidor DHCP (*Dynamic Host Configuration Protocol*)

La configuración de direcciones IP, máscara de red, puerta de enlace, direcciones

DNS y otros datos en computadores y otros dispositivos conectados a la red, se lo hará de forma automática utilizando un servidor DHCP. También este servidor reservará las direcciones IP para la configuración manual de otros dispositivos de red como servidores.

3.3.6.3.1 Alternativas de Software

ISC DHCP servidor DHCP creado por la organización sin fines de lucro ISC. Servidor diseñado para trabajar en ambientes de producción con un alto nivel de fiabilidad. Al estar respaldado por la ISC posee documentación, actualizaciones de seguridad y de versión de forma continua.

Dual DHCP DNS Server es un servidor DHCP creado para trabajar de forma conjunta con un servidor DNS local para tener siempre actualizada y congruente la información de nombre de dominio y dirección IP de cada dispositivo que se encuentre conectado a la red local.

El software elegido para que cumpla con la función de servidor DHCP en la red es ISC DHCP, pues es el más utilizado en el mundo y el que cuenta con mayor respaldo de sus creadores en aspectos de documentación, foros de ayuda y actualizaciones; además, cuenta con mayor número de opciones de configuración de funcionamiento y tiene compatibilidad con el servidor DNS BIND, pues es desarrollado por la misma organización.

Servidor	Características					
	Múltiples Redes y Subredes	DHCP Relay	Asignación por MAC	Configuración de Nombres de Dominio	Trabaja con Servidor DNS	Listas de acceso al servicio por MAC
ISC DHCP	Sí	Sí	Sí	Sí	Sí	Sí
Dual DHCP DNS	Sí	Sí	Sí	Sí	Sí	No

Tabla 3.34: Comparación del software para servidor DHCP[PW49, P8]

3.3.6.4 Servidor de Correo Electrónico

El servicio de correo electrónico es de gran importancia debido a los múltiples documentos, avisos, acuerdos y reglamentos que deben darse a conocer al

personal administrativo y docente de la institución; y, aunque en este momento los servicios de página Web y correo se encuentran funcionando dentro de un hosting, en el futuro será necesario migrar estos servicios a servidores propios del CFD.

3.3.6.4.1 Alternativas de Software

QMail servidor de correo creado por Daniel J. Bernstein, diseñado pensando en la seguridad; además, es considerado uno de los mejores servidores de correo pues permite realizar el envío de un número considerable de correos de manera paralela, y garantizando que los correos que llegan hasta el servidor serán entregados.

SendMail servidor de correo utilizado para el envío seguro de correo, con una gran capacidad de configuración en todos los aspectos relacionados con el manejo de correo electrónico, incluyendo en sus opciones la clase de protocolo de envío utilizado.

Postfix es un servidor de correo diseñado para tener las características comunes de los otros servidores de correo, pero además, posee otras ventajas adicionales como la facilidad de configuración, soporte de tecnologías como MySQL, LDAP, etc., fácil integración con antivirus, soporta direccionamiento IPv6 y un gran rendimiento en situaciones de elevada demanda del servicio.

Servidor	Características							
	SMTP	POP3	IMAP	POPS	SMTPS	SSL	Almacena-miento Base de Datos	Almacena-miento Sistema de Archivos
QMail	Sí	Sí	No	No	No	No	No	Sí
SendMail	Sí	No	No	No	Sí	No	Sí	Sí
Postfix	Sí	No	No	No	Sí	Sí	Sí	Sí

Tabla 3.35: Comparación del software para el servidor de Correo Electrónico[P9, PW50, PW51]

Según las características analizadas de las diferentes alternativas de software para el servidor de correo electrónico se eligió a Postfix con Dovecot. Las razones

para la elección de esta aplicación es su diseño modular orientado a la seguridad, a la facilidad de configuración, su soporte para bases de datos LDAP y MySQL, etc., y la utilización de protocolos seguros para el envío de correo.

3.3.6.5 Servidor de Directorio

El servicio de directorio es una base de datos especializada, en la que se almacena información sobre los usuarios de una red, y los recursos que existen en ésta, permitiendo tener una gestión descentralizada sobre los permisos de uso y acceso a estos últimos.

El servicio de directorio estará funcionando como un servidor de autenticación para los usuarios de la red, permitiendo tener una administración centralizada, dinámica y flexible de los privilegios y restricciones que cada uno de los usuarios tenga sobre los recursos de la misma.

3.3.6.5.1 Alternativas de Software

OpenLDAP-Samba es un conjunto de aplicaciones usada para integrar un sistema de directorio Linux a una red de estaciones que funcionan con sistema operativo Windows. OpenLDAP es una implementación de código abierto del protocolo LDAP (*Lightweight Directory Access Protocol*) que permite almacenar de manera jerárquica información acerca de cuentas de usuario, cuentas de equipos, cuentas de administrador, etc. Samba es un conjunto de servicios y protocolos que permite interoperabilidad entre redes Linux y Windows, y es el que actúa como controlador principal de dominio.

389 Directory Server es un servidor LDAP implementado a partir del código liberado por la empresa Red Hat, por lo que es exactamente igual al servidor Red Hat Directory Server. Está diseñado para utilizarse en ambientes de alta demanda, con soporte para funcionar con los protocolos LDAPv3, SSLv2, TLS, fácil replicación para brindar alta disponibilidad, e interfaz gráfica para configuraciones.

Apache Directory Server es un servidor de directorio escrito en su totalidad en el lenguaje de programación Java, que soporta el uso de los protocolos LDAPv3 y

LDAP Kerberos 5. Esta aplicación tiene como característica principal el uso de triggers, procedimientos almacenados, consultas y vistas en el directorio LDAP y es capaz de una alta concurrencia de peticiones. Apache Directory Server es creado por la misma organización que creó y mantiene a Apache Http Server.

Servidor	Características					
	LDAPv2, LDAPv3	SSLv3	TLSv1	Replicación	Compatibilidad con Active Directory	Interfaz Gráfica
OpenLDAP -Samba	Sí	Sí	Sí	N-Way Multi-Master	Sí	Sí (Web)
389 Directory Server	Sí	Sí	Sí	Multi-Master	Sí	Sí (Java)
Apache Directory Server	Sí	Sí	Sí	Multi-Master	Sí	Sí (Java)

Tabla 3.36: Comparación del software para el servidor de Directorio[PW52, PW53, PW54]

De las opciones de software analizadas se eligió a OpenLDAP-Samba como el servidor de directorio debido a que es un servidor de muy buenas prestaciones, con una gran penetración en el mercado, abundante documentación oficial y actualizaciones frecuentes publicadas por la organización OpenLDAP.

3.3.6.6 Firewall

El servidor de Firewall es el encargado de permitir o negar el acceso de los usuarios desde o hacia nuestra red local, protegiendo a los recursos de la red de intrusiones y ataques; además, se encargará de realizar el enmascaramiento y desenmascaramiento de las direcciones IP privadas con la IP pública al navegar por Internet.

Debido a cuestiones de presupuesto y a la urgencia de implementar este servicio, se ha decidido usar un Firewall basado en software libre que estará funcionando sobre el servidor HP que posee el CFD. Ya que, se va a instalar una distribución Linux dentro de este servidor, se va a usar la herramienta de software Shorewall que se basa en el sistema Netfilter (*iptables*) que viene incluido en el núcleo de

Linux. Esta herramienta brinda una forma más amigable de configurar las reglas de Firewall y que permite usar todas las potencialidades presentes en Netfilter.

3.3.6.7 Servidor FTP (*File Transfer Protocol*)

El servidor FTP es necesario para compartir los archivos y documentos que tengan un tamaño demasiado grande para ser enviados por medio de correo electrónico entre las distintas oficinas del CFD, permitiendo tener estos documentos y archivos organizados dentro de un directorio común, controlando los permisos de lectura y escritura sobre los mismos. A este directorio solo tendrán acceso usuarios que posean las cuentas autorizadas para ello.

3.3.6.7.1 Alternativas de Software

Servidor	Características					
	SSL/TLS	IPv6	Control de Ancho de Banda	Listas de Acceso	Vitalización de servidor FTP	Licencia
Pure-FTPd	Sí	Sí	Sí	Sí	Sí	GPL
Vsftpd	Sí	Sí	Sí	Sí	Sí	GPLv2
ProFTPd	Sí	Sí	Sí	Sí	Sí	GPL

Tabla 3.37: Comparación del software para el servidor FTP[PW55, PW56, PW57]

Pure-FTPd servidor FTP de licencia libre, que se enfoca principalmente en la seguridad, manteniendo siempre su código bajo pruebas de nuevas vulnerabilidades. Aplicación robusta y fiable que soporta conexiones SSL (*Secure Sockets Layer*)/TLS (*Transport Layer Security*).

Vsftpd es un servidor FTP muy usado por empresas de software como Red Hat, Debian; siendo uno de las aplicaciones más seguras, robustas y confiables que existe en el mercado. Esta aplicación tiene una gran número de configuraciones que permiten tener un alto grado de control sobre la velocidad máxima de bajada y subida de archivos, direcciones IP que pueden tener acceso y configuración de cuentas virtuales entre otras opciones.

ProFTPd al desarrollar esta aplicación se tuvo como objetivo brindar el mayor número de opciones de configuración. Entre las características de funcionamiento

está la capacidad de usar conexiones SSL/TLS, conectarse con servidores LDAP, correr como un usuario sin privilegios de administrador, etc.

Se ha escogido a Vsftpd como servidor FTP para la red de CFD, pues muestra las características más completas en aspectos como seguridad, actualizaciones, documentación, opciones de configuración, confiabilidad y robustez.

3.3.6.8 Servidor Proxy Web

El servidor Proxy será utilizado para el acceso a páginas Web en Internet, de las estaciones presentes en la red interna del CFD, además, también cumplirá las funciones de controlar el acceso a estas páginas, controlar los horarios de uso de Internet y controlar las descargas de archivos.

Este tipo de servidor almacena las páginas Web con más número de consultas y las almacena en su cache para que la próxima vez que un cliente requiera esa página, la respuesta la dé el servidor proxy local permitiendo disminuir el ancho de banda necesario para dar servicio a toda la red.

3.3.6.8.1 Alternativas de Software

Squid es un cache proxy creado por Squid Software Foundation. Entre sus características más importantes están el poder realizar un control de acceso basado en dirección IP o MAC, trabajar con cache jerárquico distribuido en varios servidores para acelerar el acceso a la información, control de acceso a páginas web por URL (*Uniform Resource Locator,* Localizador Uniforme de Recursos) o por palabras clave previamente configuradas, y capacidad de funcionar como proxy transparente.

Privoxy es un servidor proxy web, que no almacena información de páginas web en su memoria cache, más bien tiene capacidad para modificar el contenido de páginas web, administrar las cookies, hacer control de acceso, funcionar como proxy transparente, eliminar anuncios, banners y ventanas emergentes no deseadas.

Luego de analizar las características de las aplicaciones se ha escogido a Squid como servidor proxy web, pues es una implementación más robusta y confiable,

con respaldo de una organización mejor estructurada, con mayor cantidad de documentación y características de funcionamiento más completas.

Servidor	Características					
	Almacenamiento de pág Web en memoria Caché	IPv6	Control de Acceso	Filtro de Banners y Anuncios	SSL	Licencia
Squid	Sí	Sí	Sí	Sí	Sí	GPL
Privoxy	No	Sí	Sí	Sí	No	GPL

Tabla 3.38: Comparación del software para servidor Proxy Web[PW58, PW59]

Además se instalará la herramienta SARG que permitirá mostrar detalladamente la cantidad de tráfico, las páginas web visitadas, y el horario de navegación de cada uno de los usuarios de la red, que permitirá al administrador de red saber si el enlace de Internet se usa de forma responsable.

3.3.6.9 Monitor de Red

Es una herramienta de software que permite al administrador de la red poder ubicar problemas y actividad sospechosa en el funcionamiento de los servicios y de los dispositivos de conectividad, al permitirle realizar un seguimiento y análisis del comportamiento de la red basándose en los registros que esta herramienta presenta.

Por medio de la utilización de eventos esta herramienta permite lanzar alertas por diferentes medios dirigidos a advertir al personal que administra la red sobre mal funcionamiento y caída de los servicios o dispositivos de red.

3.3.6.9.1 Alternativas de Software

Zenoss es una herramienta de la empresa Zenoss inc. con licencia GPL v2. Su principal característica es el uso de una interfaz gráfica basada en el lenguaje de programación PHP que brinda una gran facilidad para su instalación y configuración. Al igual que Nagios también puede añadir nuevas funcionalidades por medio de plugins.

Nagios herramienta de software de código abierto más utilizada en el mundo, debido a su estabilidad, madurez y soporte que ofrece. Esta herramienta puede monitorizar protocolos como HTTP, FTP, SSH, SMTP, POP3, etc.; puede monitorizar los recursos de hardware de estaciones con diferentes sistemas operativos, notifica a usuarios definidos cuando existe algún problema en la red mediante correo electrónico, y posee una interfaz gráfica basada en web para mostrar el estado de la red, informes y gráficas de funcionamiento.

Luego de analizar las ventajas que presenta cada una de las opciones tal como se muestra en la Tabla 3.39, se eligió a Nagios como el software de monitorización de red, pues es el software más confiable, estable, con más fuentes de documentación, permite observar un gran número diferente de estadísticas y con muchas opciones de configuración.

Servidor	Características				
	Monitoreo por Syslog	**Notificación de problemas automático**	**Interfaz Gráfica**	**Soporte**	**Licencia**
Zenoss	Sí	Vía Email a uno o varios usuarios	Permite configuraciones y muestra informes y gráficas del estado de la red	Sí	GPL
Nagios	Sí (con plugins)	Vía Email, Busca personas, SMS	Muestra informes y gráficas del estado de la red	Sí(Gran cantidad de información en español)	GPL

Tabla 3.39: Comparación del software para Monitor de red[PW60, PW61]

3.3.6.10 Aula Virtual

Una Aula Virtual, es un software mediante el cual se simula una clase real en la que se desarrollan actividades como preguntas al profesor, presentación de trabajos, toma de exámenes, discusiones con compañeros sobre temas tratados en clase, etc.; todo esto mediante el uso de un ordenador.

El aula virtual otorgará a los estudiantes del CFD una manera de acceder a recursos académicos y herramientas que les permita asimilar, profundizar y

compartir los conocimientos recibidos durante las horas de clase. Hasta la adquisición de un servidor dedicado para este servicio, se usará el servidor HP para el uso de un aula virtual para los cursos de computación, a los que se tendrá acceso solo desde el interior del colegio.

3.3.6.10.1 Alternativas de Software

ATutor sistema de e-learning desarrollado con el objetivo de lograr accesibilidad y adaptabilidad. Este software está basado en el ambiente web, trabaja en múltiples sistemas operativos (Windows, Linux, Solaris), tiene soporte en muchos idiomas (incluyendo español).

Chamilo herramienta de software libre para la gestión de e-learning, muy popular en el mundo entre instituciones educativas, especialmente universidades. Está auspiciada por la asociación sin fines de lucro Chamilo, cuyo objetivo es asegurar la disponibilidad y calidad de educación a bajo costo. Entre las características de este sistema de gestión están: el tener una red social incorporada, seguimiento del progreso de cada usuario, exámenes controlados por tiempo, generación automática de certificados, arreglo rápido de alertas de seguridad.

Servidor	Características			
	Facilidad de uso	Utilidades	Seguridad	Licencia
ATutor	Media	Exámenes, calificaciones, recursos, chat, foro, tareas, etc.	Rápido arreglo de bugs	GPL
Chamilo	Media	Exámenes, tareas, recursos, calificaciones	Rápido arreglo de bugs	GPL
Moodle	Media	Módulos de tareas, recursos, exámenes, calificaciones, foros, chat, grupos de trabajo, etc	Desarrollado para ser robusto frente ataques. Rápido arreglo de bugs	GPL

Tabla 3.40: Comparación del software para Aula Virtual[PW62, PW63, PW64]

Moodle es un sistema de gestión de e-learning desarrollado por Moodle Comunity. Moodle fue creado para incentivar al estudiante a ser partícipe activo en la creación de conocimiento y no ser solo un espectador; en cuanto a las

características del software, están el soporte de múltiples idiomas, posee una gran cantidad de módulos con los cuales se puede crear cuestionarios, tareas, subir recursos, crear foros, o crear grupos de trabajo.

Luego de analizar las opciones para el software de aula virtual, se ha decidido usar a Moodle debido a la gran cantidad de documentación en español que existe en línea, por las múltiples utilidades que ofrece dentro de sus cursos y constantes actualizaciones de sus versiones.

3.3.6.11 Servidor Web

El servidor web será el encargado de responder a las peticiones hacia la página web institucional, también permitirá acceder al aula virtual, a reportes del monitor de red, y cualquier otro servicio que dependa de éste para su presentación.

Se considera que la principal carga del servidor vendría de las peticiones desde Internet hacia la página web institucional, por lo que, se ha decidido implementar la misma dentro de un hosting rentado para liberar de carga al servidor con el que cuenta actualmente la institución.

Para el resto de servicios como aula virtual e interfaces gráficas del monitor de red y proxy web, se utilizará el servidor HP, con el que cuenta en este momento la institución. Se recomienda que en el futuro se adquiera un servidor de mayores prestaciones, para alojar la página web junto con las aulas virtuales dentro de la red del colegio.

3.3.6.11.1 Alternativas de Software

Apache HTTP es un servidor web HTTP de código abierto con licencia Apache 2.0 que ofrece gran cantidad de opciones de configuración, bases de datos para autenticación, de estructura modular, soporta el uso de HTTPS y es multiplataforma.

Apache Tomcat es un servidor web HTTP de código abierto desarrollado por la *Apache Software Foundation* al igual que Apache HTTP, cuya característica que lo diferencia con este último es su soporte de Java Servlets.

HTTP Cherokee es un servidor web HTTP desarrollado sobre lenguaje C por la comunidad Cherokee bajo licencia GPL. Entre sus funcionalidades está el soporte de PHP, CGI, SSL/TLS; métodos de autenticación como en texto plano, htpasswd, htdigest; y tiene un interfaz de administración web.

Servidor	Características					
	Autenticación	HTTPS	CGI	Java Servlets	Consola de Administración	Licencia
Apache HTTP	Plain, htpasswd, htdigest, PAM	Sí	Sí	Sí	Sí	Apache 2.0
Apache Tomcat	Plain, htpasswd, htdigest, PAM	Sí	Sí	Sí	Sí	Apache 2.0
HTTP Cherokee	Plain, htpasswd, htdigest, PAM	Sí	Sí	Sí	Sí	GPL

Tabla 3.41: Comparación del software para servidor Web[PW65, PW66, PW67]

Se ha decidido utilizar Apache HTTP como servidor web, debido a que es un software maduro, estable y seguro, con gran cantidad de documentación y múltiples opciones de configuración.

3.3.7 DIMENSIONAMIENTO DE SERVIDOR

Una vez determinadas las aplicaciones a utilizar en los servicios de red, se procederá a determinar los requerimientos de procesamiento, cantidad de memoria, capacidad de almacenamiento y disponibilidad que deben tener los servidores de comunicaciones.

El servidor de DNS y DHCP son los servicios que consumen menor cantidad de recursos de memoria y almacenamiento en disco, pues van a dar servicio a solo unas decenas de estaciones de red, por lo que, se ha definido un espacio de 512 MB en disco y 128 MB en memoria RAM.

Para dimensionar los requerimientos del servidor de correo, se debe considerar varios factores como: el funcionamiento junto con el servidor de antivirus para

escanear cada correo electrónico que se envíe; además, se debe tomar en cuenta que cada usuario tendrá un buzón de correo de un tamaño de 500MB y que el número de clientes en el presente y en el futuro de este servicio serán alrededor de 71 usuarios. Con esta información se calcula que el espacio necesario en disco para este servicio es de 34.7 GB. La cantidad de memoria que se usará en este servicio debido a la poca cantidad de usuarios será igual a 256 MB[PW31] que es lo mínimo que se recomienda tener para el funcionamiento de un servidor de correo.

El dimensionamiento de los recursos necesarios para el funcionamiento del servidor web considerará la carga de página web institucional, si se espera tener un máximo de 2 peticiones simultáneas y se considera que cada petición va a consumir 25 MB[PW32] de memoria RAM, entonces el total de memoria RAM necesaria sería 50 MB; para evitar que este servicio deje de responder debido a la falta de memoria se ha definido que se requiere 512 MB para el funcionamiento de la página web; de la misma manera se calcula para el aula virtual, en éste caso se espera tener hasta 64 usuarios simultáneos, con esto se calcula que la memoria necesaria para poder responder a las peticiones del aula virtual es 1.28 GB; en total la cantidad de memoria necesaria para el servidor web es igual a 1.78 GB. Para el espacio en disco necesario para este servicio se tomará el espacio recomendado por Apache que es 1 GB.

El servidor FTP será usado para la compartición de documentos, la descarga de reglamentos y disposiciones oficiales. Este servicio será usado por el personal administrativo y docente de la institución. Si se considera que se tendrán 50 documentos o archivos dentro de la carpeta de FTP y cada uno tiene un tamaño de 10 MB, entonces el espacio necesario en el disco del servidor deberá ser de 500 MB. Ya que este servicio no va a ser utilizado con mucha demanda se recomienda que se utilice 128 MB[PW33] de memoria RAM que es la cantidad mínima recomendada.

Para el servicio de directorio se tomará en cuenta la cantidad de usuarios y estaciones de red que van a ser administrados. Para este caso se dimensionará para un número de 100, entre usuarios y estaciones de red, por lo que, se

considera separar 512 MB en disco y 256 MB en memoria RAM considerando que la mayor parte de peticiones van a realizarse al inicio de la jornada laboral.

El servicio de proxy web tendrá que ser dimensionado teniendo en cuenta que éste debe ser capaz de filtrar las peticiones de todos los usuarios del CFD que están y que desean acceder a Internet, y además, tendrá la tarea de almacenar en cache las páginas web más visitadas por los usuarios. Para el cálculo de la cantidad de memoria RAM se calculará en base a los resultados que se pueden ver en los informes del servidor proxy; si el día en que más tráfico se registró 10 GB, y se sabe que un 10% de éste tráfico fue respondido desde los registros de cache del proxy, por lo que se considera que un 5% de esto va a estar almacenado en la memoria RAM y el otro 5% se almacenará dentro del disco, por lo que se tiene que se necesitan 512 MB en memoria RAM y 512 MB de espacio en disco para el funcionamiento del servidor proxy[PW34].

Otro de los servicios que va estar siempre con gran cantidad de carga de trabajo será el servidor Firewall, pues depende de éste el realizar la traducción de direcciones IP privadas a IP públicas y viceversa, además, de filtrar las conexiones permitidas y no permitidas desde y hacia Internet. Es por ello, que se recomienda el utilizar valores mayores a los recomendados para el funcionamiento del firewall, es decir se recomienda utilizar 512 MB y 512 MB en disco.

El servicio de monitor de red Nagios va a estar siempre haciendo comprobaciones del correcto funcionamiento de muchos dispositivos y servicios de red, por lo que, se consideró que se debe dimensionar 256 MB en RAM y 512 MB de espacio en disco para almacenamiento de los registros.

Debido a que el uso del servidor SSH y el generador de reportes SARG serán utilizados ocasionalmente y que el único autorizado a utilizar estos servicios será el administrador de la red, se los tomará en cuenta junto con el dimensionamiento de memoria y espacio en disco necesario para el sistema operativo, por lo que, se destina 128 MB en memoria RAM y 10 GB de espacio en disco duro[PW35] que son los valores recomendados por Ubuntu. A continuación se muestra en la Tabla

3.42 la cantidad de memoria RAM y de espacio en disco necesario por cada una de los servicios de red.

Servidor	Memoria [MB]	Disco [GB]
Sistema Operativo (Ubuntu Server)	128	10
ISC DNS y ISC DHCP	128	0.5
Postfix – Dovecot - ClamAv	256	34.7
HTTP Apache Server	512	1
Moodle	1822	5
vsftp	128	1.2
OpenLDAP-Samba	256	0.5
Squid	512	0.5
Shorewall(iptable)	512	0.5
Nagios	256	0.5
TOTAL:	4510	54.4

Tabla 3.42: Tamaño de memoria RAM y espacio en disco duro para cada servidor de la red del CFD

Una vez ya obtenidos la cantidad de memoria RAM y tamaño en disco duro mínimos para el funcionamiento de cada servidor, se listarán las características mínimas que deben tener los servidores de comunicaciones:

- El servidor deberá poder instalarse en un rack de 19”x 31” por lo que debe tener 19” de ancho y máximo 31” de profundidad.
- Debido a que los servicios como el firewall, el proxy y el servidor web necesitan de una alta capacidad de procesamiento y a que estos servicios son los que tiene más demanda se recomienda el usar un procesador de cuatro núcleos con una velocidad mayor a 1.5 GHz.
- Como se pudo ver en la Tabla 3.42 un disco duro de 500 GB es más que suficiente, y con ello se deja un margen muy amplio para que se pueda ocupar con información de nuevos programas o funcionalidades que se instalen en el servidor. Además de ello para el caso en que se necesite usar más espacio de almacenamiento el servidor debería aceptar la instalación de al menos 2 discos duros más de 1 TB de capacidad.

- La memoria RAM que se necesita en este momento como se vió en la Tabla 3.42 es de 4.5GB, pero el servidor debe poder expandir esta memoria a al menos 8 GB para asegurar que se podrá usar este servidor para que funcionen otros servicios de red.
- El servidor deberá tener al menos un puerto USB y un lector de discos DVD para que se puedan realizar las operaciones como la instalación del sistema operativo o la instalación de software por medio del USB.
- Utilizar fuentes de poder redundantes para evitar que el servidor falle por un mal funcionamiento en éste componente.

3.3.8 COSTO REFERENCIAL DE LA SOLUCIÓN

Luego de concluido la fase de diseño de la red convergente de voz, datos y video, se procederá a presentar un presupuesto referencial de la solución según los equipos y materiales elegidos.

3.3.8.1 Costo del Sistema de Cableado Estructurado y Puesta a Tierra

El costo referencial del Sistema de Cableado Estructurado toma en cuenta los costos de materiales e instalación. El desglose de los costos de cada material utilizado en la red se encuentra en el Anexo 19.

Descripción	Valor Total ($)
Cableado	15050,82
Canalización	10921,91
Materiales para el Cuarto de Equipos y Cuartos de Telecomunicaciones	3139,76
Puesta a Tierra, UPS y Generador Eléctrico	12763,26
Servicios	
Instalación y prueba del Sist. De Cableado Estruct.	10468,93
Sub Total	52344,68
IVA (12%)	6281,36
Total	58626,04

Tabla 3.43: Costo referencial del Sist. de Cableado Estructurado para el CFD

3.3.8.2 Costo de los equipos activos de conectividad y servidor de comunicaciones

En la Tabla 3.44 se muestran los costos referenciales de los switches de las capas de Acceso y Distribución-Núcleo, los Access Points y sus respectivos módulos adicionales a utilizar en la solución presentada en el diseño de red, además se incluyeron los costos de instalación, configuración y soporte para éstos equipos de conectividad.

COSTO REFERENCIAL EQUIPOS DE CONECTIVIDAD				
ITEM	**Descripción**	**Cant.**	**Valor Unitario ($)**	**Valor Total ($)**
Switch de Acceso				
WS-C2960-24TC-L	Catalyst 2960 24 10/100 + 2T/SFP LAN Base Image	10	1726,67	15540,03
WS-C2960-24PC-L	Catalyst 2960 24 10/100 PoE + 2 T/SFP LAN Base	1	3326,67	3326,67
Switch de Distribución-Núcleo				
WS-C3560X-24T-S	Catalyst 3560X 24 Port Data IP Base	1	5733,33	5733,33
Access Point				
HP MSM410 (J9427C)	802.11a/b/g/n Standalone AP; Ext Ant; 1 RJ45 1000Base-T	4	652.8	2503,2
Servicios				
Configuración	Instalación y configuración de los equipos	1	600,00	600,00
			Sub Total	29429,9
			IVA (12%)	3531,58
			Total	32961,48

Tabla 3.44: Costo referencial de los equipos de conectividad para el CFD

En cuanto a la selección del servidor de comunicaciones se revisó primero las características técnicas del servidor HP Proliant DL160 G6 con el que cuenta el CFD, y se pudo observar que éste servidor es perfectamente capaz de funcionar con todos los servicios de red que se plantearon instalar en la red existente de la institución; además se vio que éste equipo soporta la expansión de su memoria

RAM hasta 192 GB y la expansión de su espacio de almacenamiento hasta 4 TB, por lo que existe la posibilidad de repotenciar éste servidor para hacer funcionar también sobre él los sistemas de telefonía y video seguridad IP que se plantearon en el diseño.

El servidor de backup tendrá instalado los servicios necesarios para brindar navegación en Internet, servicio de telefonía, correo electrónico y video seguridad, pues son las aplicaciones con más demanda en la red, es por esto que éste equipo tendrá iguales características que el servidor que posee el colegio actualmente pero ya con las mejoras de repotenciación.

COSTO REFERENCIAL DE LOS SERVIDORES DEL CFD				
ITEM	**Descripción**	**Cant.**	**Valor Unitario($)**	**Valor Total ($)**
Servidor de Backup				
HP DL160 G6 E5620	Servidor HP DL160 G6 1 Procesador Intel Xeon QuadCore 2.4GHz, 8GB RAM, 2 HD SATA de 1 TB 3.5", 2 puertos GigabitEthernet, 3 años de garantía	1	2348,13	2348,13
Repotenciación del servidor HP DL160 del CFD				
HP 500658-B21	Memoria HP 4GB (1x4 GB) DDR3 1333MHz 2RX4 PC3-10600R-9 Compatible con: DL1000, DL160 G6, DL160se G6, DL170h G6, DL180 G6, DL320 G6, DL360.	2	280,34	560,68
HP 507772-B21	Unidad de disco duro HP LFF 1 TB 3 G SATA de 7.200 rpm (3,5 pulg.) sin conexión en caliente, Midline, 1 año garantía	4	426,18	1704,72
HP 394791-B21	PCI-E Multifunction Gigabit Server Adapter. 10/100/1000 Ethernet.	2	565,76	1131,52
Servicios				
Instalación y Configuración	Instalación y configuración de los equipos	1	300,00	300,00
			Sub total	6045,05
			IVA (12%)	725,41
			Total	6770,46

Tabla 3.45: Costo referencial de los servidores HP para el CFD

En la Tabla 3.45 se muestra el costo referencial del servidor de backup que tiene 8GB en RAM, 2 TB de disco duro, y un procesador Intel Xenon de 2.4 GHz; además en este total también se suma el precio de dos memorias de 4 GB y 4 discos de 1 TB que servirán para repotenciar el servidor de comunicaciones que posee el CFD, y así aumentar su memoria a 12 GB y tener 4 TB en disco duro que serán suficientes para soportar el funcionamiento de todos los servicios de red que se expusieron en la fase de diseño; además se deberá tomar en cuenta el costo de la instalación y configuración de las nuevas partes del servidor.

3.3.8.2.1 Costos del Sistema de Telefonía IP y Video Seguridad

A continuación se muestran los costos referenciales de los teléfonos y las cámaras IP a utilizar en los sistemas de Telefonía IP y Video Seguridad que se definieron en el diseño, además también se toma en cuenta el costo de la instalación y la configuración de los equipos dentro de la red del CFD.

COSTO REFERENCIAL DE TELÉFONOS IP Y CÁMARAS DE SEGURIDAD				
ITEM	**Descripción**	**Cant.**	**Valor Unitario($)**	**Valor Total($)**
Teléfonos IP				
Cisco 3911	Cisco UC Phone, Fast Ethernet, PoE, Display Black/White	7	115,33	807,31
Cámaras IP				
D-Link DCS-6111	D-Link SECURICAM Day & Night, PoE, Camera with WDR Sensor and Infra-red LEDs	15	247,65	3714,75
D-Link DCS-6818	D-Link SECURICAM Day & Night, High Speed, Tipo Domo, PoE, Zoom opt. 36x dig. 12x; con patrones automáticos de movimiento	2	1890,00	3780,00
Servicios				
Instalación y Configuración	Instalación de las cámaras IP exteriores.	1	150,00	150,00
			Sub Total	8452,06
			IVA (12%)	1014,24
			Total	9466,30

Tabla 3.46: Costo referencial de los Teléfonos y Cámaras IP

3.3.8.3 Costos de operación y mantenimiento

Los costos de operación de la red son gastos que periódicamente deberán pagarse, como por ejemplo las mensualidades por el servicio de Internet y por las líneas telefónicas.

*Ya que en el diseño se utilizan el mismo número de líneas telefónicas que en la actualidad el colegio posee; para el cálculo del costo anual de éstas líneas telefónicas se realizó un análisis sobre la tarifas que se ha están pagando y con estos valores se obtuvo que cada mes se paga aproximadamente $14 por cada línea, este valor multiplicado por las tres líneas telefónicas y por doce meses da como resultado $504.

COSTOS DE OPERACIÓN	
Descripción	**Valor Total ($)**
Costo anual del enlace primario (7 Mbps, relación 1:1, Disponibilidad 99.8% FO)	10108.89
Costo anual de los 3 Modems en Postpago (2 GB de navegación, velocidad de 7.2 Mbps a 21.6 Mbps)	240,00
Costo anual de las líneas telefónicas analógicas*	504,00
Salario del Administrador de la red	13712,09
Total	24564,97

Tabla 3.47: Costos referenciales de operación

COSTOS DE MANTENIMIENTO	
Descripción	**Valor Total ($)**
Soporte técnico equipos de conectividad	600,00
Soporte técnico equipos de Telefonía IP	250,00
Soporte técnico a servidor HP	500,00
Soporte técnico a UPS	300,00
Soporte técnico y mantenimiento cámaras IP	240,00
Total	1890,00

Tabla 3.48: Costos referenciales de mantenimiento

Los costos de mantenimiento suponen los costos por soporte técnico que se pueda necesitar luego del año de servicio técnico gratuito que da el fabricante. Entre estos costos están la revisión preventiva y reparación de los equipos por personal técnico de la empresa fabricante de los equipos de conectividad o su representante en el país; estos costos serán anuales.

3.3.8.4 Costo Total de la Solución

En el costo total de la solución se contempla la adquisición, instalación y configuración del sistema de cableado estructurado, puesta a tierra, servidore, switches, cámaras IP y Access Points que se determinaron como parte del rediseño de la red del CFD.

COSTO TOTAL DE LA SOLUCIÓN	
Descripción	**Valor Total ($)**
Cableado Estructurado, Puesta a Tierra y UPS	58626,04
Equipos de Activos (Switches, Access Point y Servidor de Comunicaciones)	39731,94
Telefonía IP y Video Seguridad	9466,30
Total	107824,28

Tabla 3.49: Costo Total de la solución

3.3.9 DIAGRAMA DE RED

El diagrama de red de la solución planteada se muestra en la Figura 3.34.

3.4 POLÍTICAS DE SEGURIDAD

Las políticas de seguridad permiten a los usuarios de red proteger la información sensible y evitar intrusiones en los equipos de la red.

Para proteger los servicios de red, la información y la documentación sensible se deben dictar normas que indiquen cuáles serán los procedimientos para la instalación de nuevo software, el uso de las cuentas de usuario, el uso del correo electrónico, la navegación en Internet y el uso e instalación de hardware.

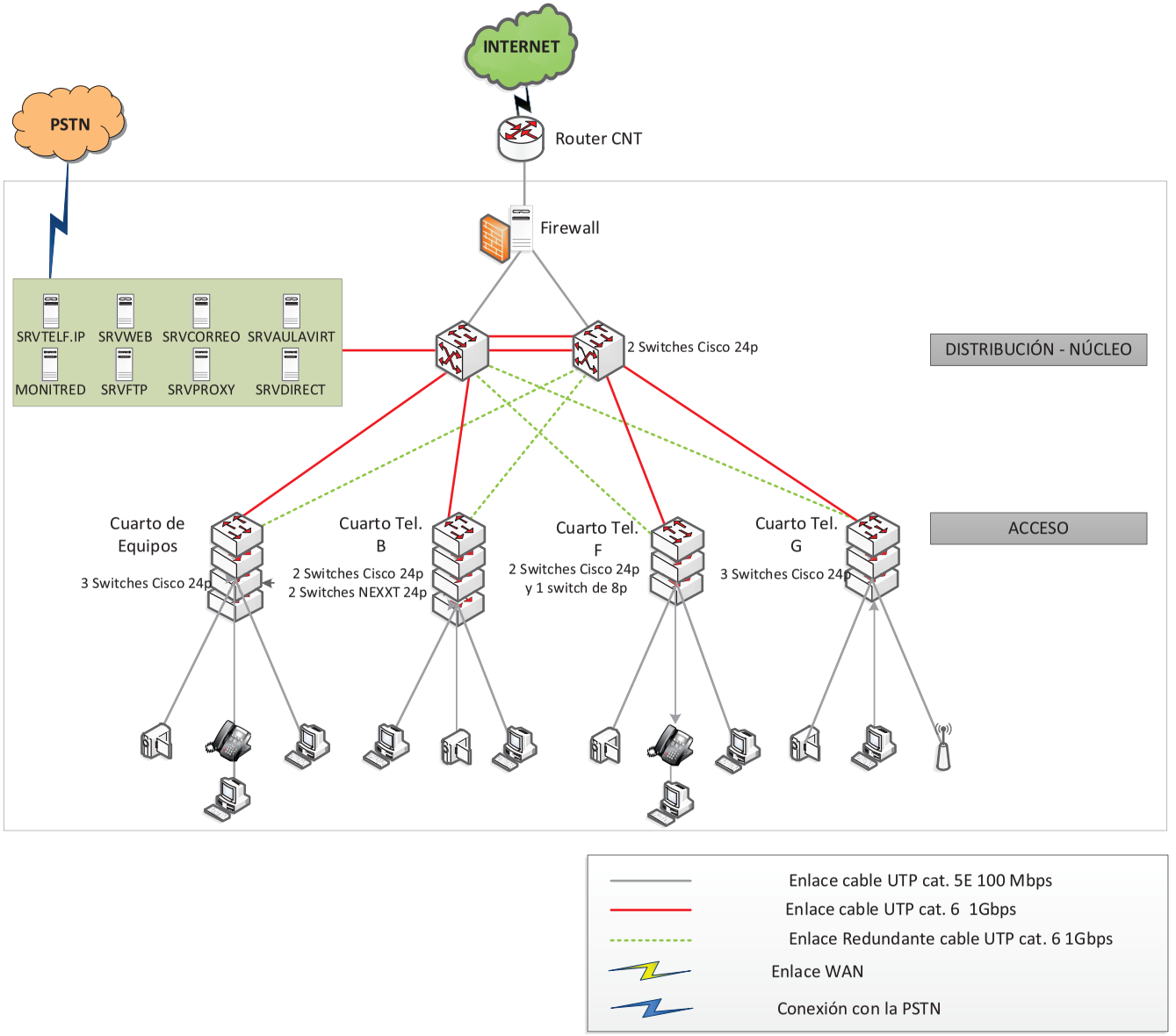


Figura 3.34: Diagrama de Red

3.4.1 POLÍTICAS PARA EL MANEJO DE CUENTAS DE USUARIO

- Cada usuario es responsable de mantener en secreto sus credenciales personales que le fueron entregadas por el Administrador de la red.
- Las contraseñas tendrán una validez de 45 días, y deberán ser cambiadas por el usuario antes de su fecha de caducidad.
- Los credenciales de usuario que no hayan sido usadas por un período de 1 mes serán desactivadas y si se desea reactivarlas deberá extender una solicitud al Administrador de red.
- En caso de que un usuario deje de trabajar en la institución sus credenciales deberán ser desactivadas el mismo día en que el usuario dejó el trabajo.
- Las credenciales de los equipos de conectividad y servicios de red especiales como por ejemplo monitor de video seguridad solo serán conocidas por el administrador de la red; y las contraseñas de estas cuentas deberán contar con letras mayúsculas, minúsculas, números y caracteres no alfanuméricos.
- La configuración de las cuentas para el acceso a la red inalámbrica solo lo podrá hacer el administrador de la red, y este llevará una documentación en la que conste el nombre del dueño de la laptop o dispositivo móvil(IPad, Tablet) junto con la dirección MAC del mismo para tener un control más detallado sobre los usuarios autorizados a conectarse inalámbricamente.

3.4.2 POLÍTICAS PARA LOS SERVICIOS DE RED

- El servicio de Internet en laboratorios, biblioteca y aulas del colegio solo deberá ser usado para fines académicos. El personal administrativo solo podrá usar Internet para realizar las actividades relacionadas con su trabajo.
- Se prohíbe la descarga de archivos de música, video o datos que no sean de interés para las actividades del colegio, y si es necesario la descarga de

algún archivo especial se deberá hacer una solicitud al Administrador de red indicando la razón por la que es necesario esta descarga.

- Se negará la navegación a sitios web relacionados con: redes sociales, comercio electrónico, entretenimiento, violencia y pornografía.
- Se prohíbe el uso del correo institucional para el uso personal. El uso adecuado de este servicio es responsabilidad del dueño de la cuenta.
- El usuario no deberá usar la cuenta de correo para el envío de cadenas o correo spam.
- El usuario no deberá abrir correos o archivos adjuntos sospechosos.
- La utilización adecuada del sistema telefónico será responsabilidad del usuario.
- El administrador de la red podrá controlar los privilegios de las cuentas de telefonía de todos los usuarios.
- Cada usuario es responsable de la información que maneja y solo aquella información indispensable se compartirá con otros usuarios.

3.4.3 POLÍTICAS PARA EL SOFTWARE Y HARDWARE

- Los usuarios de red no podrán realizar instalaciones de nuevo software sin autorización previa, para lo que deberá presentar una solicitud en la que conste la utilidad de la aplicación y la razón por la que es necesario su instalación.
- Cualquier software que se instale no deberá violar los derechos de propiedad intelectual.
- Se prohíbe el uso o instalación de hardware que no pertenezca a la institución.
- La información importante que se encuentra almacenada dentro de las estaciones de trabajo del personal administrativo deberá tener respaldos quincenales dentro de dispositivos de almacenamiento móviles como discos duros externos a los cuales solo tendrán acceso el administrador de

la red; para el acceso a estos datos se deberá realizar la solicitud al administrador de red.

- Los backups de los servicios, cuentas de usuario, videos de seguridad, correos electrónicos, archivos y documentos en el servidor primario dentro del servidor de Backup se harán los fines de semana ya que en estos días no se realiza ninguna actividad dentro de la institución y así no se interrumpirá el funcionamiento normal de la red debido a cualquier desperfecto que se produzca mientras se realiza este procedimiento.

3.4.4 POLÍTICAS DE ACCESO FÍSICO

- Solo el administrador de la red tendrá las llaves para el acceso a los cuartos de telecomunicaciones y de equipos.
- El Administrador de la red es responsable por los equipos dentro de los cuartos de telecomunicaciones y de equipos; y si es necesario que personal externo ingrese a estas áreas se deberá pedir autorización al Administrador de la red.

3.4.5 PENALIZACIONES

- Aquellos usuarios que no cumplieran con las políticas de los servicios de red, o el uso del software y hardware serán sancionados con la suspensión temporal del servicio de red en cuestión (3 días), y con una amonestación escrita.
- Si la persona desobedeciera tres veces las políticas antes mencionadas se deberá quitar los privilegios para el uso de los servicios para ese usuario; o se desinstalará el software que utiliza para violar las reglas siempre y cuando este dentro de una computadora perteneciente a la institución, caso contrario solo se negará el acceso a la red a ese usuario.
- En caso de detectar el uso de la instalación de hardware en las computadoras pertenecientes al colegio, estos dispositivos serán confiscados y devueltos solo al final de la jornada, esto aplica para

cualquier dispositivos externo que se trajera a la institución excepto para memorias USB.

- El uso incorrecto del servicio de correo electrónico será sancionado con la suspensión temporal (3 días) de la cuenta de correo.
- Si un estudiante es sorprendido descargando o visitando páginas web prohibidas el encargado del laboratorio de computación donde se haya detectado este comportamiento deberá enviar una nota de atención al representante del estudiante; en caso de que esto suceda en la Biblioteca el encargado de esta hará cumplir de la misma manera las reglas de uso correcto de las computadoras presentes en ésta área.
- Si el estudiante realiza un uso incorrecto del Internet inalámbrico, la laptop o dispositivo móvil de ese alumno quedara temporalmente (2 semanas) bloqueada para la conexión a la red.

CAPÍTULO IV

IMPLEMENTACIÓN Y PRUEBAS EN LA INFRAESTRUCTURA DE RED

4.1 INTRODUCCIÓN

Al momento una las necesidades más importantes del CFD es la instalación de un sistema operativo libre en su servidor HP Proliant DL160, que se encuentra sin funcionar porque el sistema operativo que posee instalado es una versión de prueba de Windows Server que no permite usar sus funcionalidades de manera apropiada.

Una vez el servidor esté funcionando se instalarán y configurarán los servicios de red que según las encuestas que se aplicaron a los usuarios, son las más necesarias en la actualidad en el colegio. Los servicios a implementar serán: DHCP, DNS, proxy, correo, transferencia de archivos, aula virtual, SSH, directorio, firewall, página web, monitor de red y generador de reportes de navegación en Internet.

Además, se realizarán pruebas de cada uno de los servicios de red que se van a implementar y se describirán los problemas que se presentaron al momento de la instalación y puesta a punto de cada uno de estos servicios, así como también cual fue la solución para cada problema.

4.2 IMPLEMENTACIÓN Y PRUEBAS DE SERVICIOS DE RED

La infraestructura de comunicaciones se implementará utilizando Software Libre, con las opciones de software que fueron analizadas en la etapa de diseño. Se usará el sistema operativo *Ubuntu* Server *10.04 LTS*; esta es una distribución orientada para empresas medianas y grandes, lo que permitirá cumplir con las necesidades presentes y futuras del colegio.

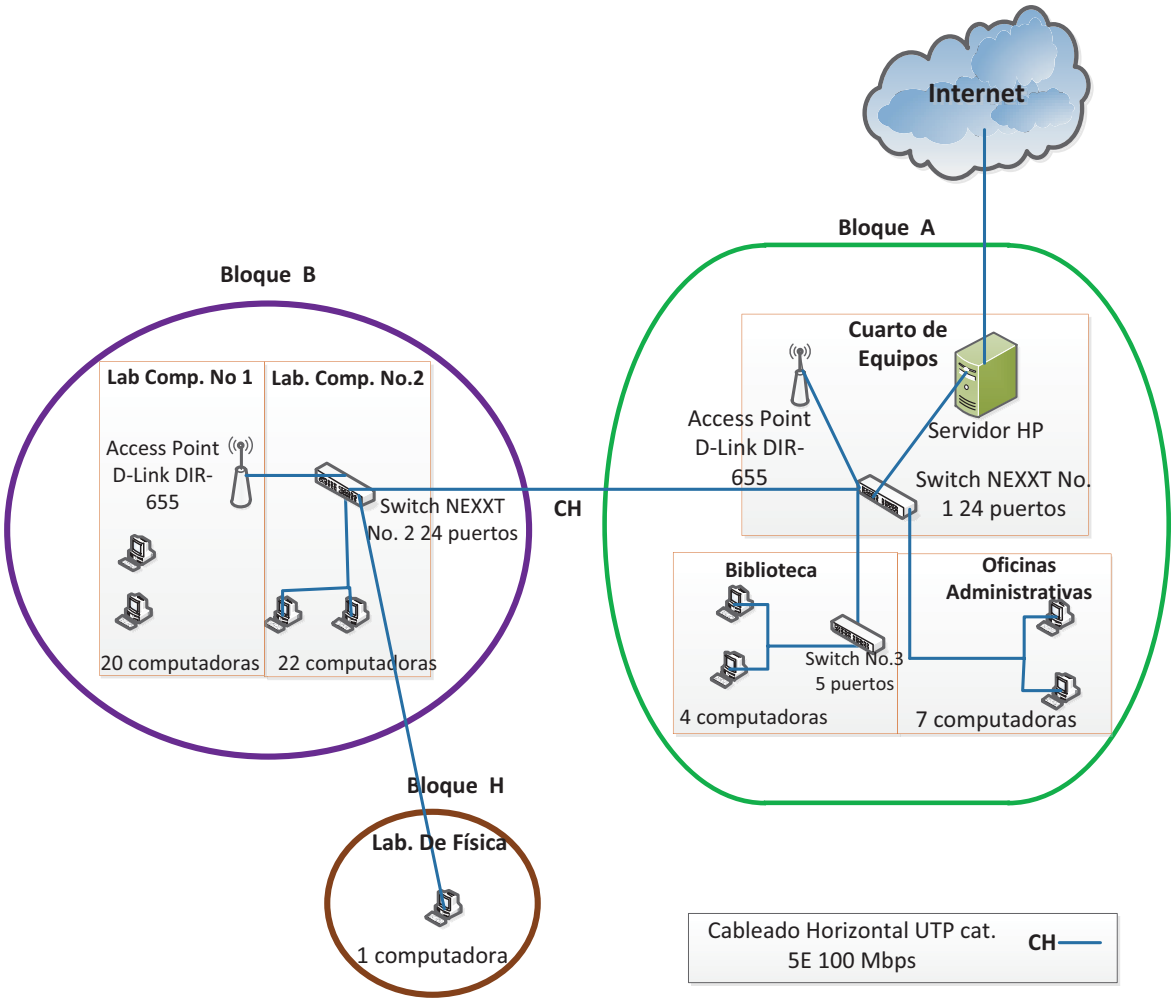


Figura 4.1: Diagrama de Red actual del CFD

La infraestructura de comunicaciones constará de los siguientes servicios:

- Servidor DHCP
- Servidor DNS
- Servidor de Directorio
- Firewall.
- Servidor Proxy
- Servidor de correo electrónico
- Servidor FTP
- Servidor SSH
- Servidor de Aula Virtual
- Monitor de Red
- Generador de Reportes del Proxy
- Página Web

La instalación y configuración de *Ubuntu Server* se encuentra explicada en el Anexo 20.

4.2.1 SERVIDOR DHCP

El servidor DHCP será implementado usando la aplicación Internet Systems Consortium DHCP, mediante el cual se asignará dinámicamente las direcciones IP a computadoras, laptops y teléfonos IP; mientras que los otros dispositivos de conectividad y servidores de comunicaciones se configurarán con direcciones IP fijas de forma manual.

4.2.1.1 Configuración

El servidor DHCP estará configurado como servidor autoritativo y se podrá asignar direcciones IP a equipos que se encuentren fuera del dominio del colegio. Además, pensando en que todos las computadoras del colegio poseerán un nombre único dentro del dominio, se configurará al servidor DHCP para que automáticamente actualice las lista DNS de la relación entre el nombre del computador y su dirección IP asignada ese momento.

El principal archivo de configuración del Servidor DHCP se encuentra en el directorio: /etc/dhcp3/dhcpd.conf. Dentro de este archivo se especificarán el rango de direcciones IP que se van a difundir mediante DHCP a los hosts clientes. Además, se puede especificar qué host específicos como: Impresoras IP, y Proyectores IP, sean configurados siempre con una misma dirección IP para facilitar las tareas de administración de éstos equipos. En la Figura 4.2 se muestra las líneas del archivo en las que se configura los puntos descritos anteriormente.

Se observa que el rango de IP’s que se configura de manera dinámica por DHCP va desde 192.168.0.30 a 192.168.0.250; el resto de IP’s están disponibles para que sean configuradas de forma fija. En las últimas líneas de este archivo se indica un mecanismo para aquellos dispositivos como impresoras IP a las que se les va a asignar de forma automática una misma IP cada vez que lo solicite, por ejemplo a “impresora” la IP 192.168.0.29 cada vez que éste pida una dirección IP

mediante DHCP, al detectar que la petición viene con la MAC 00:24:2B:65:54:84, este método ayudará al control y administración de ésta clase de dispositivos.

```
############################################################
#       Configuracion de las zonas                         #
############################################################

zone localdomain. {
        primary 127.0.0.1;
        key rndc-key;
}

zone  0.168.192.in-addr.arpa. { #Zona para la resolucion Inversa de DNS
        primary 192.168.0.1; #IP del Servidor DNS
        key rndc-key;
}

zone fdaquilema. { #Zona para la resolucion de DNS
        primary 192.168.0.1; #IP del Servidor DNS
        key rndc-key;
}

shared-network redlocal {
        subnet 192.168.0.0 netmask 255.255.255.0 { #Subred que se va a anunciar en DHCP
                option routers 192.168.0.1; #IP del Router o Gateway de la red LAN
                option subnet-mask 255.255.255.0;
                option broadcast-address 192.168.0.255; #IP de Broadcast de la Red LAN
                option domain-name-servers 192.168.0.1; #IP del Servidor DNS
                option ntp-servers 200.23.51.205, 132.248.81.29, 148.234.7.30; #IPs de
Servidores NTP gratuitos en Internet
                range 192.168.0.30 192.168.0.250; #Rango de direcciones a asignar por DHCP a los
clientes

        }
```

Figura 4.2: Archivo de configuración DHCP

En el archivo /etc/default/dhcp3-server se configura la interfaz del servidor por la cual se van a escuchar las peticiones DHCP de los clientes, en la Figura 4.3 se muestra cómo quedará este archivo de configuración.

```
#####################################################################
#     Ubicaion: /etc/default/dhcp3-server              #
#                                                 #
#####################################################################
# Defaults for dhcp initscript
# sourced by /etc/init.d/dhcp
# installed at /etc/default/dhcp3-server by the maintainer scripts

#
# This is a POSIX shell fragment
#

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="eth1" #Interfaz por la cual el servidor DHCP va a escuchar
```

Figura 4.3: Archivo de configuración de interfaces de red que escuchan peticiones DHCP

Todos los archivos de configuración que se editaron para poner a punto el servidor DHCP se encuentran en el Anexo 21.

4.2.1.2 Pruebas

Para probar que el servidor DHCP se encuentra funcionando correctamente se utilizará el comando de consola *ifconfig* dentro un computador cliente y la respuesta que se obtuvo fue la siguiente:

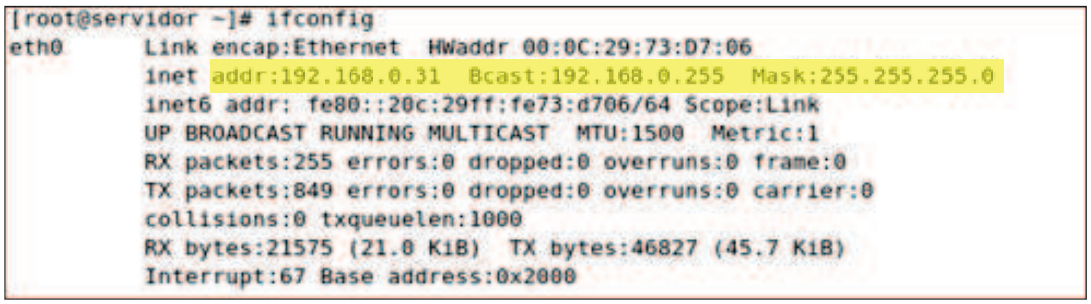


Figura 4.4: Asignación dinámica de IP

4.2.2 SERVIDOR DNS

El servidor DNS a instalar será Bind9 (*Berkeley Internet Name Domain*). Todos los usuarios de la LAN podrán realizar peticiones de resolución de nombres de dominio a este servidor.

4.2.2.1 Configuración

En este servidor se definirán los nombres de dominio y direcciones IP que corresponden a los distintos servidores de la institución como: servidor de Directorio, servidor de E-Mail, servidor FTP, etc.

Es muy importante que el nombre y dirección IP del servidor de Directorio estén bien configurados, pues si no es así las computadoras no podrán unirse al dominio, especialmente si se está usando el sistema operativo Windows en la estación cliente.

Las configuraciones de las direcciones IP de los servidores y sus nombres de dominio se realizan en los archivos: /var/cache/bind/db.fdaquilema.zone, /var/cache/bind/db.0.168.192.in.addr.arpa.zone. En las Figuras 4.5 y 4.6 se puede observar las configuraciones de estos archivos.

```
#####################################################################
#     Ubicacion Archivo: /var/cache/bind/db.fdaquilema.zone      #
#                                                                   #
#####################################################################
$TTL 86400 ; 1 dia
@               IN      SOA     servidor.fdaquilema.    root.fdaquilema. (
                2009081501 ; numero de serie
                28800 ; tiempo refresco (8 horas)
                7200 ; tiempo entre reintentos (2 horas)
                604800 ; tiempo que expira la zona si deja de resolver (1 semana)
                86400 ; tiempo total de vida (1 dia)
                )
@               IN      NS      servidor.fdaquilema.
@               IN      A       192.168.0.1
@               IN      MX      10 mail
```

Figura 4.5: Archivo db.fdaquilema.zone.

```
#####################################################################
#Ubicacion Archivo: /var/cache/bind/db.12.168.192.in.addr.arpa.zone   #
#                                                                     #
#####################################################################

$TTL 86400 ; 1 dia
@               IN      SOA     servidor.fdaquilema.    root.fdaquilema. (
                2009081501 ; numero de serie
                28800 ; tiempo refresco (8 horas)
                7200 ; tiempo entre reintentos (2 horas)
                604800 ; tiempo que expira la zona si deja de resolver (7 dias)
                86400 ; tiempo total de vida (1 dia)
                )
@               IN      NS      servidor.fdaquilema.
1               IN      PTR     servidor.fdaquilema.
```

Figura 4.6: Archivo db.0.168.192.in.addr.arpa.zone.

En el archivo /etc/bind/named.conf.options se configuran por seguridad una lista de direcciones de red de confianza a las que se puede responder a las peticiones DNS, en este caso solo se responde a las IP's que pertenecen a la LAN del CFD; además, se configuró como forwarders a los servidores DNS de CNT (*Corporación Nacional de Telecomunicaciones*), para que solo a estos servidores se envíen las peticiones de nombres de dominio que el servidor local no conozca en ese instante.

En la Figura 4.7 se muestra la configuración de este archivo. Todos los archivos de configuración relevantes en la configuración del servidor DNS editados y con comentarios se encuentran en el Anexo 22.

```
//////////////////////////////////////////////////////////////////////////
//          Ubicación archivo: /etc/bind/named.conf.options             //
//                                                                       //
//////////////////////////////////////////////////////////////////////////

// ACL para la Red Local
acl "red-local" {
                127.0.0.1/32;
                192.168.0.0/24;
                };

options {
        directory "/var/cache/bind";
        dump-file "/var/cache/bind/data/cache_dump.db";
        statistics-file "/var/cache/bind/data/named_stats.txt";
        memstatistics-file "/var/cache/bind/data/named_mem_stats.txt";
        // Indica que solo se debe contestar peticiones a las IP de la Red Local
        allow-recursion { red-local; };
        allow-query     { red-local; };

        // Forwarders son Direcciones IP de los Servidores DNS que da el ISP
        forwarders { 200.24.194.82; };

        // Se indica que primero se reenvia la peticion a las IP de forwaders
        forward first;
        auth-nxdomain no;    # conform to RFC1035
};
```

Figura 4.7: Archivo /etc/bind/named.conf.options

4.2.2.2 Pruebas

Para probar que el servidor DNS se encuentra funcionando correctamente se utilizará el comando de consola *nslookup* para observar los servidores de correo electrónico del dominio. En la Figura 4.8 se muestra el resultado de la consulta.

```
root@servidor:/home/sebas# nslookup -q=mx
> fdaquilema
Server:         192.168.0.1
Address:        192.168.0.1#53

fdaquilema      mail exchanger = 10 mail.fdaquilema.
```

Figura 4.8: Consulta de Servidor de Correo del domino fdaquilema

4.2.3 SERVIDOR DE DIRECTORIO

El servidor de Directorio permite una administración centralizada de las cuentas de usuario y de permisos de acceso o negación de los servicios de red que se ofrecen en la intranet.

Para que el servicio de Directorio pueda ser utilizado por computadores con sistemas operativos Windows y Linux, se optó por utilizar los programas de software libre OpenLDAP y SAMBA, pues para su correcto funcionamiento es necesario que estas dos aplicaciones funcionen de manera conjunta, para que aquellas computadoras que posean el sistema operativo Windows puedan autenticarse dentro del directorio LDAP por medio de los protocolos (NBSS, NBNS) que el servicio SAMBA ofrece para la integración de las redes Windows con Linux.

El servicio de Directorio será utilizado para almacenar las cuentas de los usuarios autorizados para acceder a las PC's ubicadas en los Laboratorios de Computación.

4.2.3.1 Configuración

Primero se configurará el árbol de directorio dentro de OpenLDAP. Los datos que se deben definir son el dominio LDAP, la ubicación del administrador LDAP:

- dc= fdaquilema
- cn=admin,dc=fdaquilema

dc es el nombre del dominio de la institución, y *cn* es el nombre distinguido del administrador del árbol LDAP. La configuración de éstos parámetros y de las unidades organizativas (*Usuarios, Grupos, Computadoras, etc*) se realizan dentro del archivo /etc/ldap/init.ldif.

Dentro del archivo /etc/ldap/slapd.conf se deberá indicar que se va a usar una representación del árbol LDAP que será compatible con SAMBA, además, se establece el nombre distinguido del administrador del árbol LDAP y su contraseña, lo que va a permitir poder crear una base de datos para el dominio del colegio y con las unidades organizativas que se configuró en el archivo /etc/ldap/init.ldif. En la Figura 4.9 se observa parte de la configuración del archivo slapd.conf.

Una vez editado el archivo de configuración de LDAP con las contraseñas y nombre distinguido del administrador del Dominio LDAP, se debe crear el árbol

LDAP. Para verificar que el árbol se creó correctamente se hace una consulta al mismo usando comandos de consola, en la Figura 4.10 se observa el resultado de una consulta que devuelve todo el árbol LDAP.

```
# Features to permit
#allow bind_v2

# Schema and objectClass definitions
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
# Se incluye la siguiente linea indicando que se va a Usar un esquema SAMBA
include         /etc/ldap/schema/samba.schema
include         /etc/ldap/schema/misc.schema

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile                 /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
argsfile                /var/run/slapd/slapd.args

modulepath              /usr/lib/ldap
moduleload          back_bdb
sizelimit 500
tool-threads 1
backend                 bdb
database            bdb

# The base of your directory in database
# Es la Base del Directorio LDAP
suffix              "dc=fdaquilema"

rootdn              "cn=admin,dc=fdaquilema"
rootpw              {SSHA}HkyIZjBSf7UzbBh8P8Bao6wAhQ9XGzRF
```

Figura 4.9: Archivo de Configuración OpenLDAP

```
root@servidor:/home/sebas# ldapsearch -xLLL -b "dc=fdaquilema" | less
dn: dc=fdaquilema
objectClass: top
objectClass: dcObject
objectClass: organizationalUnit
dc: fdaquilema
ou: Colegio Fernando Daquilema

dn: cn=admin,dc=fdaquilema
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

dn: ou=Users,dc=fdaquilema
objectClass: top
objectClass: organizationalUnit
```

Figura 4.10: Verificación del árbol LDAP

En la configuración del servidor SAMBA se debe especificar que será el encargado de la autenticación de usuarios Windows, y que se pueda realizar la compartición de archivos entre los ambientes Windows y Linux. Los siguientes parámetros se establecieron en la configuración:

- Se indica la ubicación de la base de datos LDAP a la cual SAMBA hará referencia.
- Se definen las interfaces que escucharán y divulgarán que existe un servidor SAMBA como Controlador Primario de Dominio.
- Se define el nombre común del administrador del directorio LDAP.
- Se especifica que SAMBA actuará como servidor WINS.
- Se crea un directorio para compartir archivos al que solo podrán acceder los usuarios que pertenezcan al grupo de laboratorios. En este directorio solo el administrador LDAP tendrá permisos de escritura, todos los demás usuarios solo tienen permisos de lectura.
- No se permitirá tener perfiles de usuario móviles, es decir, cada computador tendrá credenciales de usuario únicas que solo servirán para el acceso a ésa estación.

En la Figura 4.11 se muestra el archivo de configuración principal de SAMBA: /etc/samba/smb.conf, donde se observa la definición de la dirección IP del servidor LDAP y del nombre de dominio que verán las computadoras con sistema operativo Windows.

```
#============================================================================
#     Ubicacion archivo: /etc/samba/smb.conf                                #
#============================================================================
[global]

     # Domain name ..
     workgroup = FDAQUILEMA

     # Server name - as seen by Windows PCs ..
     netbios name = SERVIDOR

     # Digo que interfaces va a escuchar el servidor SAMBA
     # y de que redes se va a aceptar conexiones y a anunciar al Servidor
     interfaces = lo eth1
     hosts allow = 127.0.0.1 192.168.0.0/24
     hosts deny = 0.0.0.0/0
     remote announce = 192.168.0.255

     # Administrador del Dominio
     admin users = admin, root, @"Domain Admins"
```

Figura 4.11: Archivo /etc/samba/smb.conf

Para que OpenLDAP y SAMBA funcionen de manera conjunta son instaladas algunas herramientas adicionales con el paquete *smbldap-tools*. Los principales archivos de configuración de estas herramientas son: /etc/smbldap-tool/smbldap.conf en donde se configura el nombre de Domino, la IP del servidor LDAP, el puerto por el cual se harán las peticiones al Servidor LDAP, la raíz del árbol LDAP, el tipo de cifrado de la clave LDAP, el directorio donde se crearán las carpetas personales de los usuarios de red, etc.

El otro archivo de configuración de *smbldap-tools* es el /etc/smbldap-tools/smbldap_bind.conf, en este archivo se va a configurar el usuario Administrador del árbol LDAP y su contraseña. La contraseña fue borrada de la imagen por seguridad.

```
##############################################################################
#     Ubicacion archivo: /etc/smbldap-tools/smbldap_bind.conf                #
##############################################################################
############################
# Credential Configuration #
############################
# Notes: you can specify two differents configuration if you use a
# master ldap for writing access and a slave ldap server for reading access
# By default, we will use the same DN (so it will work for standard Samba
# release)
slaveDN="cn=admin,dc=fdaquilema"
slavePw="       "
masterDN="cn=admin,dc=fdaquilema"
masterPw="       "
```

Figura 4.12: Archivo /etc/smbldap-tools/smbldap_bind.conf

Configuración de Clientes:

En los laboratorios de computación del CFD se manejan los sistemas operativos Windows 7 y Ubuntu, por lo que, a continuación se mostrarán los mecanismos para añadir estas computadoras dentro del dominio LDAP.

- *Windows XP y 7:*

  Cambios necesarios para que Windows se una a un Dominio SAMBA PDC:

  Cambios en Opciones de Seguridad de Directivas locales:

  Ir a Panel de control → Sistema y Seguridad → Herramientas Administrativas → Directiva de seguridad local → Directivas locales → Opciones de seguridad.

1. En **Seguridad de red: Nivel de autenticación de LAN Manager,** configurar la opción: “enviar respuestas LM y NTML”.

2. En **Seguridad de red: Seguridad de sesión mínima para clientes NTML basados en SSP y Seguridad de red**, marcar la opción: ‘seguridad de sesión mínima para servidores NTML basados en SSP’, deshabilitar “Requerir cifrado de 128-bit”.

Cambios en el Registro de Windows:

Para editar el registro se debe ejecutar la aplicación *Regedit.exe.*

1. En la ruta HKEY_LOCAL_MACHINE\System\CurrentControlSet\ Services\LanmanWorkstation\Parameters, se añadirá como DWORD la entrada **DomainCompatibilityMode** con valor **1** y también como **DWORD** la entrada **DNSNameResolutionRequired** con valor **0**.

Si se quiere utilizar perfiles móviles, omitir el siguiente paso. Si se quiere utilizar perfiles locales, se requieren añadir las siguientes entradas en el registro de Windows.

2. Y para que Windows use perfiles locales en lugar de perfiles remotos, se debe añadir en la ruta HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Syste m como **DWORD** la entrada **LocalProfile** con valor **1**, y añadir también como **DWORD** la entrada **ReadOnlyProfile** con valor **1**.

Nota: Además de estos cambios se debe asegurar que el Firewall de Windows y Firewall del Antivirus permita conexiones por los puertos 339, 445, 137, 138 y 139 de los protocolos de transporte TCP y UDP.

- *Cliente Linux (Ubuntu):*

Primero se instalará la aplicación cliente de LDAP:

```
root~#apt-get install ldap-auth-client
```

Al hacer la instalación se pedirá contestar varias preguntas, las respuestas deben ser:

```
LDAP server Unifor Resource Identifier: ldap://(ip del servidor
LDAP)
Distiguished name of the search base: (base del dominio, ejmp:
dc=fdaquilema)
LDAP versión to use: 3
Make local root Database admin: Yes
Does the LDAP database require login? No
LDAP account for root: cn:****, dn=fdaquilema
LDAP root account password: <password del Administrador LDAP>
```

Luego de esto se editará el archivo:/etc/ldap.conf y copiarlo dentro del directorio /etc/ldap/. Aquí se va a configurar la IP del Servidor LDAP, y el nombre del usuario Administrador del árbol LDAP. A continuación se muestra parte de la configuración.

```
# Multiple hosts may be specified, each separated by a
# space. How long nss_ldap takes to failover depends on
# whether your LDAP client library supports configurable
# network or connect timeouts (see bind_timelimit).
host 192.168.0.1

# The distinguished name of the search base.
base dc=fdaquilema

# Another way to specify your LDAP server is to provide an
uri ldap://192.168.0.1/
# Unix Domain Sockets to connect to a local LDAP Server.
#uri ldap://127.0.0.1/
#uri ldaps://127.0.0.1/
#uri ldapi://%2fvar%2frun%2fldapi_sock/
# Note: %2f encodes the '/' used as directory separator

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
#binddn cn=proxyuser,dc=padl,dc=com

# The credentials to bind with.
# Optional: default is no credential.
#bindpw secret

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
rootbinddn cn=admin,dc=fdaquilema
```

Figura 4.13: Archivo de Configuración LDAP Cliente Linux

Por último, se deberá configurar la autenticación para que al momento de iniciar sesión se haga hacia el Servidor LDAP antes de hacerse contra las credenciales

de usuarios creados localmente en la PC. Para configurar esto se debe crear un archivo en el directorio: /etc/auth-client-config/profile.d/open_ldap.

```
###############################################################################
#     Ubicacion archivo: /etc/auth-client-config/profile.d/open_ldap       #
###############################################################################

[open_ldap]
nss_passwd=passwd: compat ldap
nss_group=group: compat ldap
nss_shadow=shadow: compat ldap
nss_netgroup=netgroup: nis
pam_auth=auth          required                    pam_env.so
        auth                sufficient              pam_unix.so likeauth nullok
        auth                sufficient              pam_ldap.so use_first_pass
        auth                required                   pam_deny.so
pam_account=account      sufficient            pam_unix.so
       account               sufficient              pam_ldap.so
       account                required                 pam_deny.so
pam_password=password          sufficient          pam_unix.so nullok md5 shadow
use_authtok
        password                    sufficient           pam_ldap.so use_first_pass
        password                         required                  pam_deny.so
pam_session=session      required                    pam_limits.so
        session                  required                 pam_mkhomedir.so
skel=/etc/skel/ umask=0077
        session                  required              pam_unix.so
        session                  optional               pam_ldap.so
```

Figura 4.14: Archivo de Configuración de Autenticación de Logeo Ubuntu

Todos los archivos de configuración del servidor de Directorio editados y con comentarios se encuentran en el Anexo 23.

4.2.3.2 Pruebas

Para probar el funcionamiento del servidor de Directorio OpenLDAP-SAMBA se configurará a un computador que usa el sistema operativo Windows XP para que se una al dominio FDAQUILEMA; este proceso deberá registrar el nombre del computador dentro del grupo Computadores y las credenciales del usuario que tendrá permitido el acceso a este computador estarán registradas en el Grupo Usuarios de la Base LDAP.

En el proceso para unir el computador al dominio de la red, también se especificará las credenciales únicas con las que un usuario podrá acceder al computador; estas credenciales deben haber sido creadas con anterioridad por el administrador de red en la base LDAP.

En la Figura 4.16 se observa que el dominio al que ahora pertenece el computador es FDAQUILEMA, comprobando que el computador ha ingresado al

dominio de la institución. En esta fase se presentaron varios problemas con la conexión y envío de información de autenticación por los protocolos NBNS (*NetBios Naming Service*), NBSS (*NetBios Session Service*), debido a que en los cortafuegos del servidor y del computador cliente tenían cerrado estos puertos, pero una vez añadidos estos puertos a las reglas del cortafuegos no existieron problemas para adherir el computador al dominio de la red.

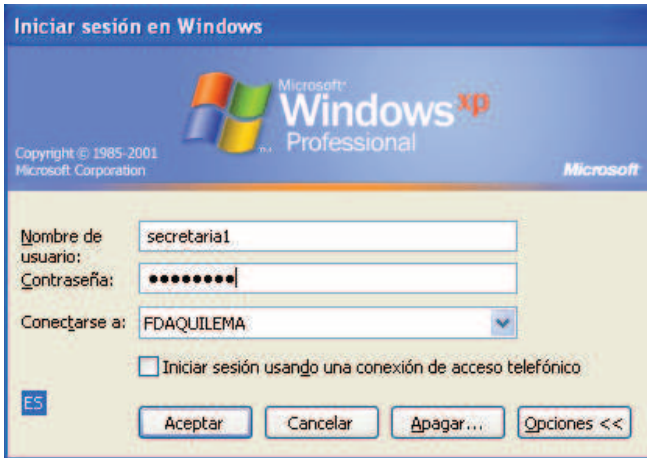


Figura 4.15: Acceso de un usuario al computador dentro del Dominio FDAQUILEMA

Figura 4.16: Comprobación de unión al dominio FDAQUILEMA

4.2.4 FIREWALL

El Firewall permitirá filtrar el tráfico hacia el Internet y hacia la LAN que pasa por las Interfaces del servidor, con el fin de asegurar que no se permitan ataques o intrusiones no deseadas hacia la información interna o a los dispositivos pertenecientes al colegio. Otra de las funciones que realizará el Firewall es el cambio de Direcciones IP Locales a Direcciones IP Públicas y viceversa, para que los equipos de la red local puedan navegar en Internet.

Para configurar el Firewall se utilizará Shorewall, el mismo que permite de manera más simple el configurar el firewall 'iptables' que por defecto viene en la mayoría de distribuciones Linux.

4.2.4.1 Configuración

En el firewall se configurará tres zonas, la zona de Internet, la zona de firewall y la zona de la LAN; con estas zonas se definirán las reglas y políticas que el servidor seguirá en el filtrado de tráfico.

Los archivos en los que se define cómo actuará el firewall frente al tráfico que cursa por las dos interfaces de red del servidor son: /etc/shorewall/interfaces, /etc/shorewall/policy y /etc/shorewall/rules.

En el archivo /etc/shorewall/interfaces se definirá que solo la interfaz eth1 que se conecta a la LAN podrá intercambiar tráfico DHCP, además, en este archivo se configurará que todo el tráfico que provenga o se dirija hacia las direcciones IP consideradas maliciosas que estarán definidas dentro del archivo /etc/shorewall/blacklist será desechado.

```
net   eth0       detect          blacklist
loc   eth1       detect          dhcp,blacklist
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

Figura 4.17: Archivo de configuración de interfaces

Para tener un control completo sobre los puertos que estarán abiertos hacia Internet y hacia la red local, primero se va a bloquear todo el tráfico que provenga desde éstos dos orígenes, esto se lo configura dentro del archivo

/etc/shorewall/policy. En la Figura 4.18 se observa cómo quedará el archivo de políticas de red.

```
# Politica de Trafico originado en el Firewall(fw) hacia la red LAN(loc) y hacia
# el Internet(net) que ACEPTA ese trafico desde los dos origenes
fw          all         ACCEPT

# Politica de Trafico originado en Internet(net) hacia el Firewall(fw) y hacia
# la red LAN(loc) que RECHAZA este trafico SIN enviar una notificaion de error
# hacia el usuario que lo origino
net         all         DROP        info

# Politica de Trafico originado en la LAN(loc) hacia el Firewall(fw) y hacia
# el Internet(net) que RECHAZA el trafico y envÃa una notificaion de error
# hacia el usuario que lo origino
loc         all         REJECT          info
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

Figura 4.18: Archivo de configuración de Políticas

Por último en el archivo /etc/shorewall/rules se especificarán los puertos de red que se abrirán para el tráfico proveniente desde Internet (*net*) y desde la LAN(*loc*) hacia el Firewall (*fw*), de este modo se restringe el intercambio de tráfico.

Los únicos puertos que se abrirán para el tráfico desde la red local hacia el firewall son: HTTP, HTTPS, DNS, SMTP, SMTPS, IMAP, IMAPS, SAMBA, LDAP, NetBios, FTP, SSH.

Todos los archivos de configuración del Firewall editados y con comentarios explicativos se encuentran en el Anexo 24.

4.2.4.2 Pruebas

En el CFD se definió que en los laboratorios de computación el uso de las redes sociales estará prohibido, por lo cual, éstas páginas web estarán bloqueadas dentro de éstas áreas; para ello se definirán las direcciones IP de éstos sitios web seguros dentro del archivo /etc/shorewall/blacklist para su bloqueo. En la Figura 4.19 se puede ver que la petición de conexión a la página segura de Facebook está siendo rechazada por el Firewall.

4.2.5 SERVIDOR PROXY

El Servidor Proxy Web será configurado usando Squid, mismo que brindará formas de controlar la navegación en Internet de los usuarios de la LAN del CFD.

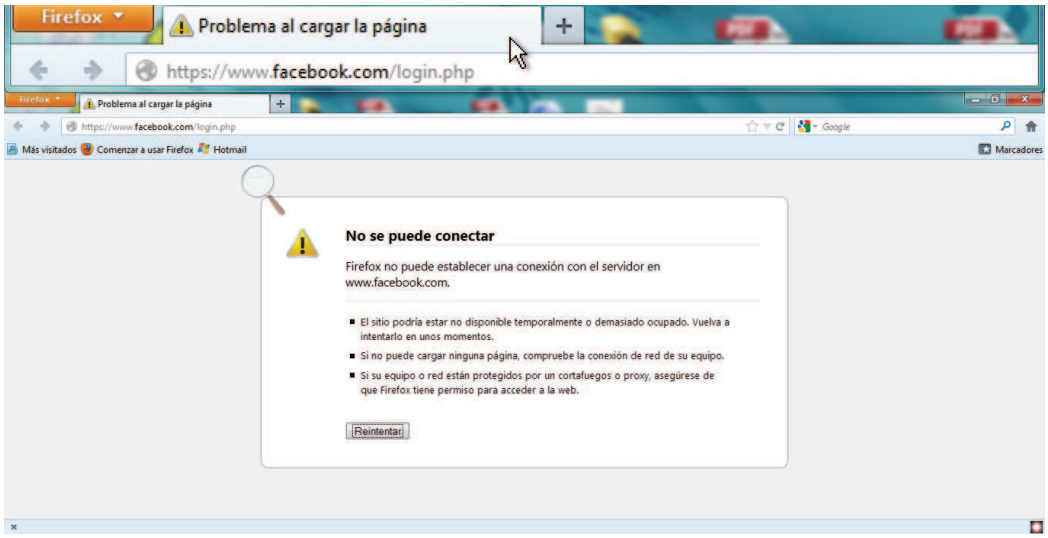


Figura 4.19: Filtrado de Conexiones a páginas seguras de Redes Sociales

Debido a que existen diferentes tipos de usuarios en la red, se los agrupará en dos clases: los estudiantes y profesores solo podrán navegar en Internet hasta la hora de cierre del colegio (15h00 PM); y el Personal Administrativo que podrá navegar sin limitaciones de tiempo, ya que, estos usuarios suelen quedarse en sus oficinas sobre la hora de salida oficial.

Como política de la institución se bloqueará el ingreso a páginas no relacionadas con temas educativos como: juegos, descargas, pornografía, redes sociales, etc., normas que se implementarán usando las funcionalidades que posee el Servidor Proxy.

Otra de las funciones importantes del Servidor Proxy es el guardar en disco las páginas web más buscadas por los usuarios del CFD para responder más rápidamente y ahorrar el ancho de banda que se usaría en estas peticiones.

El Servidor Proxy estará funcionando de forma transparente para el usuario por lo que no será necesaria la configuración de su dirección IP en los navegadores Web de los clientes.

4.2.5.1 Configuración

Para diferenciar los dos tipos de usuarios que tendrá la red se ingresarán las direcciones MAC de las computadoras del personal administrativo dentro de una lista ubicada en el directorio: /etc/squid3/listas/macslibres. Todas las otras

direcciones MAC que el servidor Proxy detecte pertenecerán a estudiantes y profesores.

```
#Recommended minimum configuration:
acl all src all
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32
acl red-local src 192.168.0.0/24

#
# Esta linea se puede ser usada para que los
# usuarios que no tengan RESTRICCIONES sean
# identificados por sus MACs en vez de  usar
# las IPs como en la linea Anterior a esta
acl macsLibres arp "/etc/squid3/listas/macsLibres"

acl expresiones-denegadas url_regex "/etc/squid3/listas/expresiones-denegadas"
acl dominios-denegados dstdomain "/etc/squid3/listas/dominios-denegados"
acl descargas-denegadas urlpath_regex "/etc/squid3/listas/descargas-denegadas"

# ACL para que solo se pueda conectar a internet de
# Lunes a Viernes en horario de 7AM a 3PM
acl horario time MTWHF 07:00-15:00
```

Figura 4.20: Archivo de Configuración de Servidor Proxy

El archivo de configuración principal del servidor Proxy es /etc/squid3/squid.conf; dentro de este archivo se definirán las reglas de control sobre la navegación Web como el bloqueo de páginas web prohibidas, el horario de navegación permitido, descargas prohibidas; además, también se especifica que reglas van a ser aplicadas para cada grupo de usuarios (Estudiantes-Profesores y Personal Administrativo). En la Figura 4.20 se muestra las líneas del archivo de configuración en la que se definen las reglas de control de navegación Web.

Para el bloqueo de páginas web prohibidas se hará uso de la lista /etc/squid3/listas/dominios-denegados en la que constarán los nombres de dominio de estas páginas; en la lista /etc/squid3/listas/expresiones-denegadas estarán las expresiones tales como: xxx, taringa, etc. cuya búsqueda o presencia en el URL estarán prohibidas; y por último la lista /etc/squid3/listas/descargas-denegadas que contendrá las extensiones de los archivos cuya descarga estará denegada, con excepción de los archivos de extensiones: .docx, .doc, .xls, .xlsx, .ppt, .pps, .pdf que podrán ser descargados.

Los archivos de configuración del servidor Proxy editados y comentados se encuentran en el Anexo 25.

4.2.5.2 Pruebas

Dentro de las pruebas hechas al servidor Proxy existieron problemas con el funcionamiento de forma transparente del mismo, pues para ello era necesario que el Firewall del servidor cumpla la función de reenviar todas las peticiones dirigidas al puerto 80 hacia el puerto por el que escucha Servidor Proxy (puerto 8080); el error encontrado luego de hacer varias pruebas estuvo en la sintaxis de la regla del Firewall que permitía hacer esta redirección del tráfico, ya que, al escribirla no se usó correctamente las tabulaciones y esto provocó que la regla sea ignorada por el Firewall, haciendo imposible que el servidor Proxy pueda funcionar de manera transparente; una vez editada la regla del cortafuegos el servidor Proxy funcionó de manera transparente sin contratiempos.

Para mostrar el funcionamiento de las reglas de navegación Web se realizará una petición a la página web de descargas *www.taringa.net*, misma que consta dentro de la lista de nombres de dominios denegados. En la Figura 4.21 se observa que al realizar la petición el Servidor Proxy bloquea la misma y nos muestra un mensaje que indica que el acceso a la página web está denegado, pero que en caso de que esta acción no sea correcta, se puede contactar al e-mail del administrador de la red.

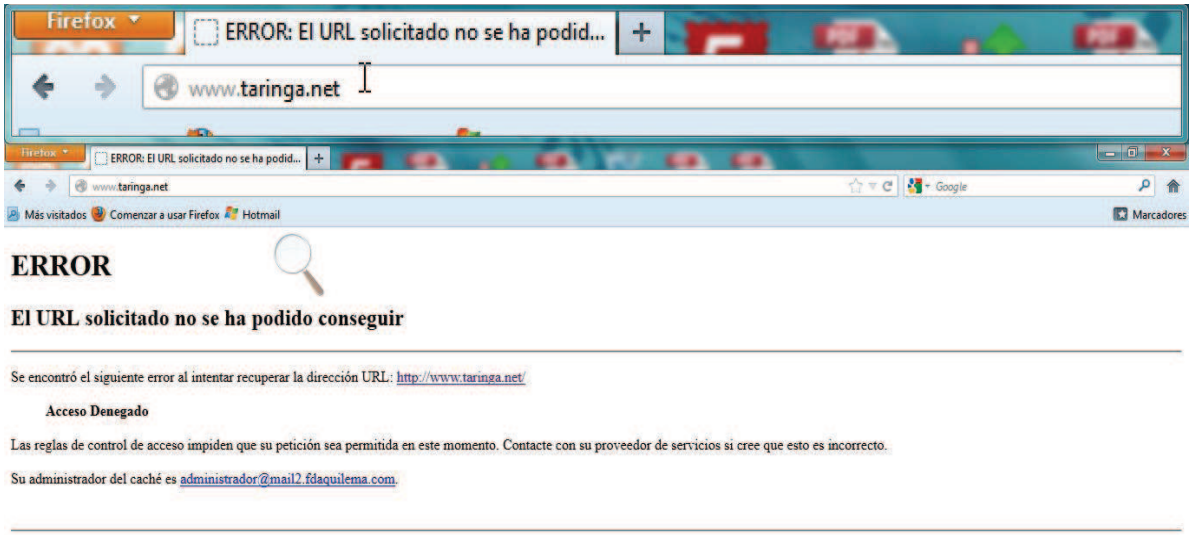


Figura 4.21: Comprobación de funcionamiento de Servidor Proxy

4.2.6 SERVIDOR DE CORREO ELECTRÓNICO

El servidor de Correo Electrónico estará configurado usando Postfix-Dovecot; además, se usará ClamAV para el escaneo automático de los e-mails que sean recibidos. Todo el tráfico de correo usará los protocolos seguros SMTPS e IMAPS para garantizar la confidencialidad e integridad de la información.

Como otra medida de seguridad se usará la aplicación de correo de software libre Mozilla Thunderbird que solo será configurado por el administrador de la red en las computadoras del Personal Administrativo.

Se definió además las políticas de tamaño máximo de buzón de correo por usuario de 500 MB y tamaño máximo de archivos adjuntos de 5.5 MB. Para enviar archivos de mayor tamaño se podrá usar el servidor de intercambio de archivos.

4.2.6.1 Configuración

El archivo de configuración de Postfix es el /etc/postfix/main.cf, dentro del mismo se configura el nombre del servidor de correo, el dominio con el que los correos serán enviados, los dominios de correo que se va a considerar de entrega local, el tamaño máximo del buzón de correo, el tamaño máximo por cada correo incluyendo el archivo adjunto y el filtrado del contenido de los correos por parte de ClamAV. En la Figura 4.22 se observan las líneas del archivo de configuración donde se declaran las características de configuración detalladas anteriormente.

```
myhostname = mail.fdaquilema
mydomain = fdaquilema
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = servidor.fdaquilema, servidor.localdomain, localhost.localdomain,
localhost, fdaquilema
relayhost =
mynetworks = 127.0.0.0/8 192.168.0.0/24
# Tamanio max. del buzon de correo. Este caso 5MB
mailbox_size_limit = 5242880
# Tamanio max. de un correo electronico
message_size_limit = 5242880
```

Figura 4.22: Archivo de Configuración Postfix

Para que el antivirus ClamAV escanee los emails se deberá editar el archivo /etc/postfix/master.cf para que los emails sean enviados hacia ClamAV desde el servidor de correo, y para que estos correos puedan retornar al servidor de correo desde ClamAV se necesita editar el archivo /etc/clamsmtpd.conf.

En el archivo de configuración de Dovecot (/etc/dovecot/dovecot.conf) se configurará el protocolo IMAPS como el usado por defecto para la recepción de los correos, la autenticación usando SSL, y la ubicación de la carpeta de correo del usuario dentro del servidor.

Los archivos de configuración de Postfix, Dovecot y ClamAV completos y con comentarios explicativos se encuentran en el Anexo 26.

4.2.6.2 Pruebas

Al momento de configurar la aplicación Thundebird se notó que el servicio de Dovecot dejaba de funcionar de manera inesperada, lo que afectaba en la recepción de E-mails en los clientes. Al revisar los logs de este servicio se detectó que el problema radicaba en que este servicio era muy sensible a los cambios repentinos en la marca de tiempo del servidor, misma que estaba siendo actualizada tomando como referencia a un servidor de tiempo de nivel 1 por medio del comando *ntpdate* ejecutado automáticamente por el demonio *crontab;* esta actualización causaba que la marca de tiempo varíe en ocasiones en hasta 7 segundos, provocando a su vez la caída del servicio Dovecot. Para remediar este problema se instaló el servicio *ntpd,* el cual de forma automática sincronizará el tiempo del servidor sin causar variaciones importantes en los valores del tiempo.

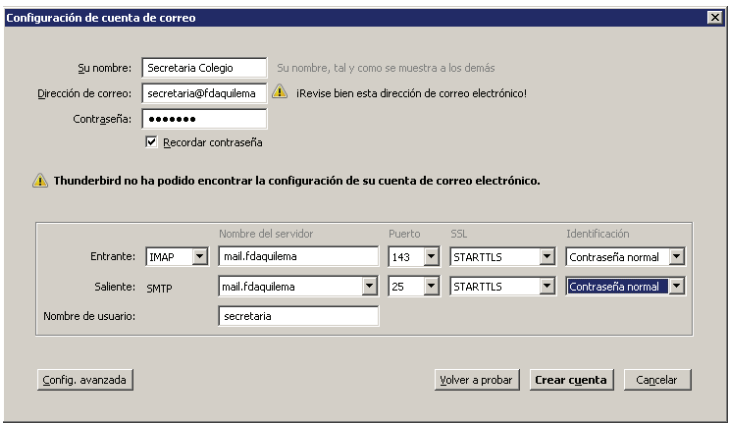


Figura 4.23: Configuración de cuenta de Correo en cliente Thundebird

En la Figura 4.23 se muestra la configuración manual de una cuenta de correo usando la aplicación de software libre Mozilla Thunderbird, en la que se observa que la autenticación del usuario se realiza utilizando el protocolo seguro TLS (*Transport Layer Security*).

Ahora para verificar que los correos se están enviando correctamente se enviará un correo desde el servidor del CFD hacia un correo de Gmail. En la Figura 4.24 se muestra el contenido y la dirección de correo al que se envía el e-mail; y en la Figura 4.25 se muestra como llegó este correo a la cuenta de Gmail.

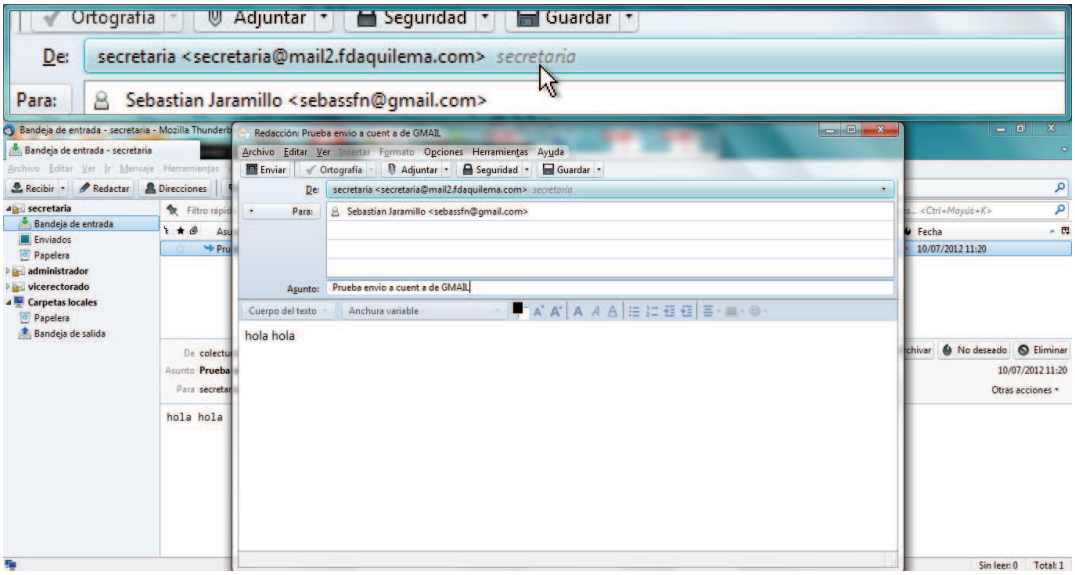


Figura 4.24: Envío de e-mail desde correo del CFD

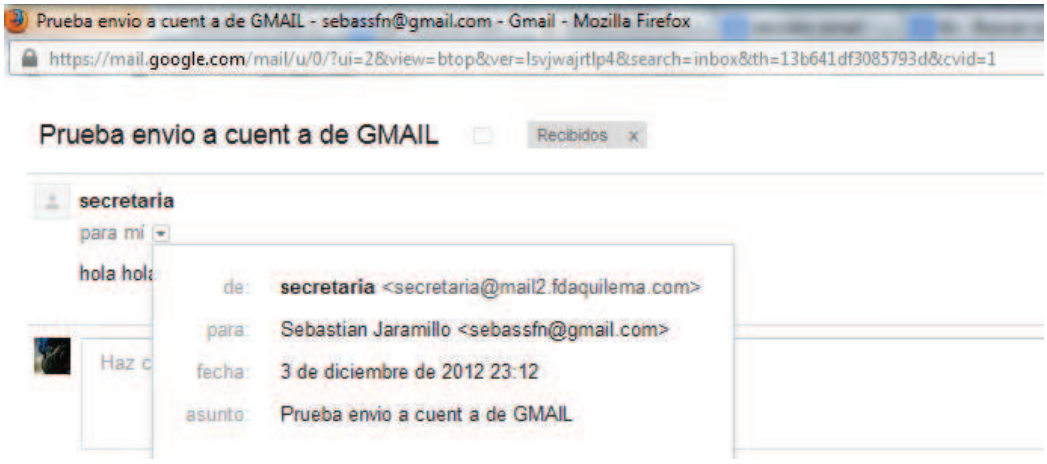


Figura 4.25: Recepción de e-mail desde correo del CFD

4.2.7 SERVIDOR FTP

El servidor FTP se configurará con Vsftp y se usará para compartir archivos que tengan un tamaño demasiado grande para ser enviados por medio de correo electrónico entre varios usuarios del personal administrativo. Para ello se creará dos cuentas con diferentes tipos de permisos, la cuenta de Administrador servirá para dar mantenimiento a la carpeta FTP "/home/compartida/" que será donde reposarán los archivos que se quieran compartir; esta cuenta tendrá permisos para borrar los archivos que estén usando espacio innecesariamente dentro de esta carpeta. La cuenta 'compartida' es la cuenta que tendrán todos los usuarios del personal administrativo que necesiten compartir archivos entre ellos, los usuarios de esta cuenta podrán grabar y leer archivos dentro de esta carpeta pero no podrán ejecutar estos archivos.

Como medida de seguridad solo el administrador de la red instalará y configurará los clientes FTP dentro de los computadores de los usuarios del personal administrativo que necesite intercambiar archivos; el cliente FTP a instalar será la aplicación de software libre FileZilla. También como otra medida de seguridad se obligará que la autenticación de usuarios y transferencia de archivos se realicen utilizando el protocolo TLS.

4.2.7.1 Configuración

El servidor FTP además deberá cumplir con las siguientes características para asegurar la seguridad e integridad de la información del CFD:

- No se permitirá el acceso a usuarios anónimos.
- Todo ingreso y cambio realizado en el servidor de archivos será registrado en el archivo de logs de Vsftp. Si se registra más de 4 intentos fallidos de autenticación la dirección IP desde la cual se está realizando esta acción será bloqueada durante 1 día, antes de que pueda otra vez intentar autenticarse en este servicio.
- Los dos únicos usuarios que tendrán acceso a este servicio serán los usuarios Administrador y Compartida.

Todas las características antes mencionadas se configuran dentro del archivo /etc/vsftpd.conf. En la Figura 4.26 se observa algunas líneas en las que se configura la negación de acceso a los usuarios que no consten dentro de la lista /etc/vsftpd.user_list, en la que solo estarán los usuarios Administrador y Compartida; también se observan las líneas de configuración para la autenticación e intercambio de archivos usando obligatoriamente el protocolo TLS.

```
# archivo: /etc/vsftpd.users_list a los que se deberÃ¡ermitir el Logeo a FTP
userlist_enable=YES
tcp_wrappers=YES
#Indica que si no esta el Usuario especificado en el archivo
# /etc/vsftpd.user_list, entonces no podra hacer Login al servidor FTP
userlist_deny=NO

# Especificar cualquier rango arbitrario, y estrecho, de puertos para conexion al
# Servidor por FTP Explicito
pasv_min_port=60200
pasv_max_port=60208

# Habilita el soporte de TLS/SSL
ssl_enable=YES

# Indica que se va a usar Algoritmos de cifrado altos, si no se pone esta linea
# La autenticacion TLS Explicita no Funciona con el Cliente FTP Filezilla
ssl_ciphers=HIGH

# Deshabilita o habilita utilizar TLS/SSL con usuarios anÃ³os
allow_anon_ssl=NO

# Obliga a utilizar TLS/SSL para todas las operaciones, es decir,
# transferencia de datos, y autenticaciÃ³e usuarios locales.
# Establecer el valor NO, hace que sea opcional utilizar TLS/SSL.
force_local_data_ssl=YES
force_local_logins_ssl=YES

# Se prefiere TLSv1 sobre SSLv2, y SSLv3
ssl_tlsv1=YES
```

Figura 4.26: Archivo de Configuración de Vsftp

En caso de que los intentos de autenticación fallen más de cuatro ocasiones, el servicio Fail2Ban será el encargado de monitorear el archivo de logs de Vsftp y bloquear por un período de 24 horas a la dirección IP origen desde la cual se realizan las peticiones de autenticación fallidas; además Fail2Ban enviará un e-mail al administrador de la red avisando sobre el bloqueo de la dirección IP por haber excedido el número de intentos fallidos en la autenticación FTP.

Los archivos de configuración de Vsftp completos y con comentarios explicativos se encuentran en el Anexo 27.

4.2.7.2 Pruebas

Al tratar de configurar los clientes usando la aplicación de software libre FilleZilla ocurrió un error en la autenticación de los usuarios utilizando una conexión TLS, luego de investigar la causa dentro de los foros oficiales de la aplicación FilleZilla se encontró que el problema es el algoritmo de cifrado que por defecto utiliza Vsftd, ya que, éste ya no era soportado por el cliente FilleZila; la solución al problema es especificar el algoritmo de cifrado dentro del archivo de configuración /etc/vsftpd.conf de la siguiente manera:

ssl_ciphers=HIGH

Luego de colocar la línea anterior la autenticación y la transferencia de archivos usando conexiones seguras con el protocolo TLS funcionan normalmente. En la Figura 4.27 se observa como el usuario Compartida puede ver solo los archivos dentro de su propia carpeta.

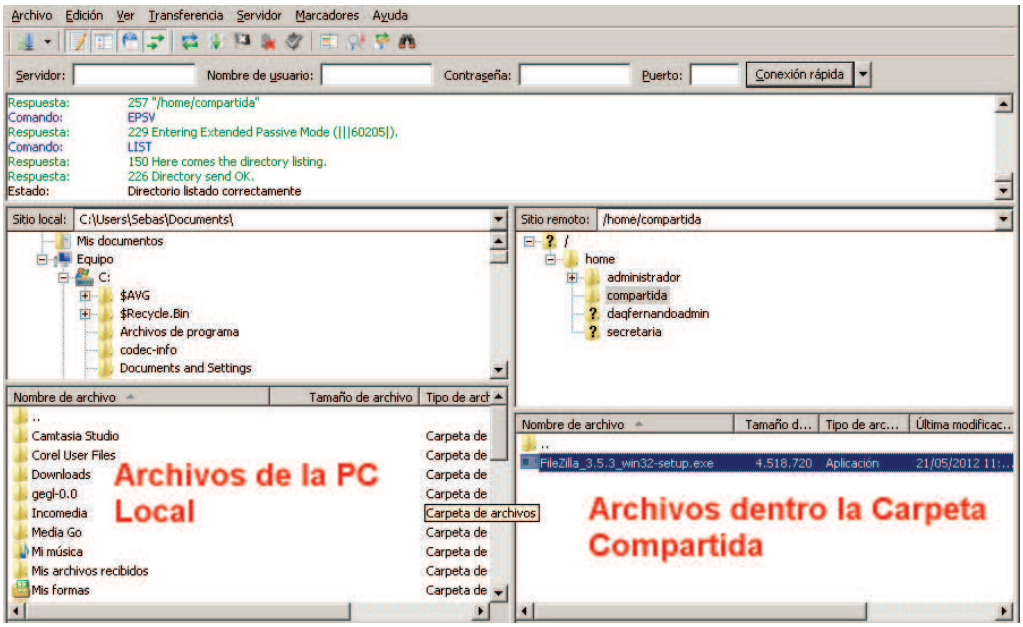


Figura 4.27: Cliente FileZilla conectado al servidor FTP

4.2.8 SERVIDOR SSH

El servidor SSH estará configurado sobre OpenSSH, mismo que se monta al instalar el sistema operativo Ubuntu Server en el servidor. Este servicio permitirá acceder a una consola de comandos segura de forma remota.

Para incrementar el nivel de seguridad se deberá implementar los siguientes puntos:

- El servicio SSH funcionará dentro de un puerto no conocido, del que solo tendrá conocimiento el administrador de la red.
- Solo el administrador de red podrá ingresar vía SSH.
- Se permitirán solo 2 intentos para autenticación antes que la conexión con el servidor SSH se cierre; además, solo se tendrá 30 segundos para digitar el usuario y el password antes de que la conexión expire.
- No se permitirá la autenticación del usuario *root.*
- Si se excede los 3 intentos fallidos de autenticación se bloqueará la dirección IP en el puerto usado por un período de 24 horas.

4.2.8.1 Configuración

La configuración de todos los puntos anteriormente descritos se realizarán dentro del archivo /etc/ssh/sshd_config. En la Figura 4.28 se muestra parte de este archivo de configuración, en el que se puede ver que el tiempo límite que tiene un usuario para autenticarse es de 30 segundos, que el usuario *root* no puede acceder vía SSH y que se tiene máximo 2 intentos para autenticarse antes de que la conexión con el servidor SSH expire entre otras configuraciones.

```
# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 30
PermitRootLogin no
StrictModes yes
MaxAuthTries 2

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile     %h/.ssh/authorized_keys
```

Figura 4.28: Archivo de Configuración de OpenSSH

Para el bloqueo de la dirección IP que ha fallado más de tres veces en la autenticación se usará nuevamente el servicio Fail2Ban, y de la misma manera

que con el servidor FTP también se enviará una notificación por e-mail al administrador de la red con la dirección IP que ha sido bloqueada.

Los archivos de configuración de OpenSSH completos y comentados se encuentran en el Anexo 28.

4.2.8.2 Pruebas

Para probar el funcionamiento del servidor SSH se iniciará una sesión remota con las credenciales del administrador de red, y se accederá directamente al directorio propio de este usuario.

Figura 4.29: Verificación de funcionamiento de servidor SSH

4.2.9 SERVIDOR DE AULA VIRTUAL

El servidor de Aula Virtual estará configurado utilizando Moodle y éste a su vez usará el servidor Web Apache2 para mostrar en el navegador los cursos virtuales.

Considerando que existirán tres tipos de usuarios que accederán al Aula Virtual, se les asignará diferentes roles con permisos de acceso y configuración distintos.

A continuación se describen los permisos que cada tipo de usuario tendrá:

- **Administrador**.- Este usuario tendrá completo control sobre el sitio web. Entre los permisos más importantes que posee están: será el único que puede definir políticas de seguridad, crear y borrar cursos, crear y borrar usuarios, asignar cualquier rol a un usuario, instalar nuevas funcionalidades y editar cualquier actividad como: Lecciones, Foros, Cuestionarios.

- **Profesor**.- Este usuario podrá crear y editar actividades como: Lecciones, Tareas, Foros, Cuestionarios, etc. dentro de un curso establecido; además podrá matricular usuarios con el rol de Estudiante; podrá poner calificaciones y promover estudiantes.
- **Estudiante**.- Tendrá permisos de crear y editar Foros, enviar mensajes a otros alumnos del curso en el que está matriculado, participar en las actividades que han sido activadas por el profesor del curso y será capaz de editar sus datos de usuario.

Entre los ajustes de seguridad que se deberán definir son: la utilización de conexiones HTTPS, la prohibición de entrada en los cursos a los usuarios que se identifiquen como invitados, y, prohibir la utilización de contraseñas que no contengan al menos 1 letra mayúscula, 1 letra minúscula y 1 carácter no alfa numérico.

4.2.9.1 Configuración

Para realizar las configuraciones se debe primero ingresar las credenciales de Administrador del Aula Virtual que viene configurado por defecto, una vez se ingresa a la interfaz de configuración por razones de seguridad se procederá a cambiar las credenciales del usuario Administrador, tal como se muestra en la Figura 4.30.

Para la configuración del Idioma se debe ingresar en la siguiente ruta Language/Language Packs, ahí se deberá buscar el paquete de Español – Internacional y descargarlo, al terminar automáticamente se instalará el paquete de Idioma. Para definir que el lenguaje por defecto será el Español se deberá ingresar en la sección Language/Language Settings.

Lo próximo a configurar serán las políticas de seguridad del sitio web, aquí se configurará: la autenticación vía HTTPS, la longitud mínima de las contraseñas será de 8 caracteres con letras mayúsculas, minúsculas, dígitos y caracteres no alfanuméricos.

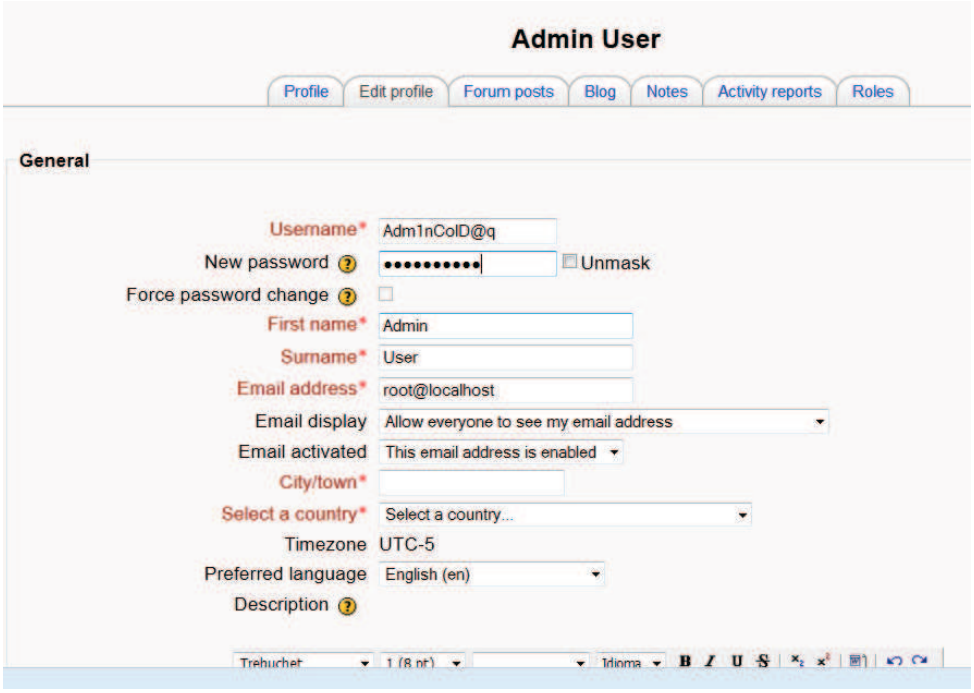


Figura 4.30: Cambio de datos de la credencial de Administrador

Para la configuración de los perfiles de usuario se debe ingresar la ruta Usuarios/Permisos/Definir Roles; en la Figura 4.31 se observa la pantalla de configuración de los roles que puede ser asignados a los usuarios dentro del Aula Virtual. En esta misma sección se pueden editar con más detalle los permisos que cada uno de los perfiles tendrá.

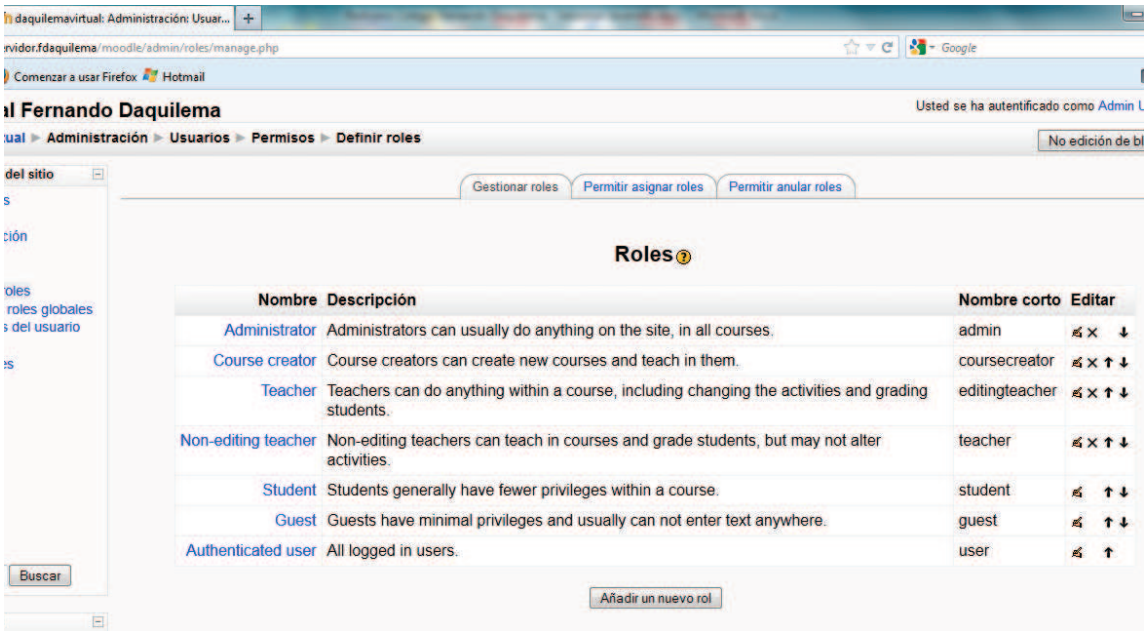


Figura 4.31: Edición de los roles de usuario en el Aula Virtual

Por último, será necesario definir la zona horaria en la que el país se encuentra para actualizar la hora y fecha con la que funcionarán las Aulas Virtuales. Esto se configurará en la ruta Ubicación/Ajustes de ubicación; en la Figura 4.32 se observa la definición de la zona horaria UTC-5.

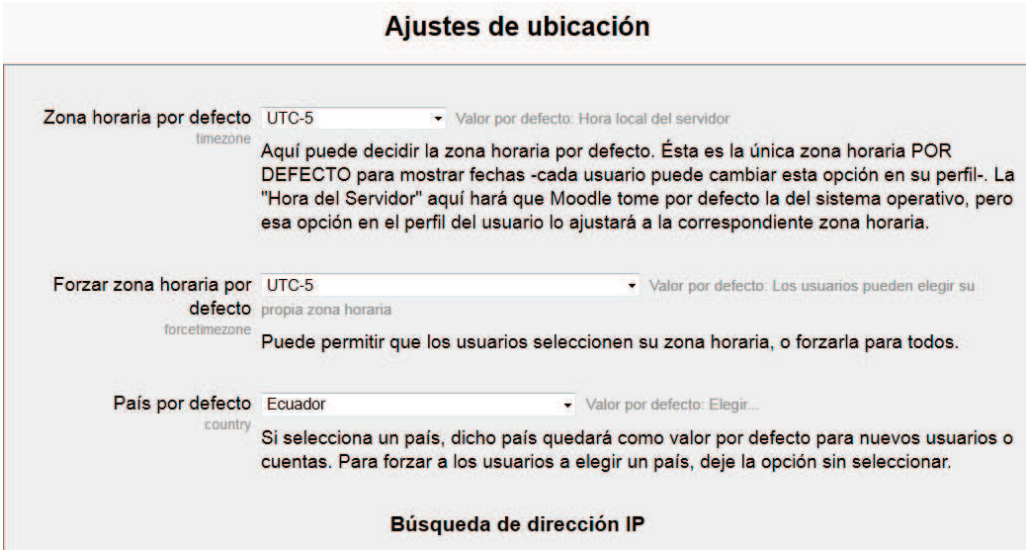


Figura 4.32: Configuración de zona horaria

4.2.9.2 Pruebas

En la Figura 4.33 se muestra el curso para la clase de computación al ingresar con el perfil de Profesor. Se observa que el lado izquierdo aparecen las opciones para matricular alumnos, añadir nuevas actividades e ingresar recursos para que los estudiantes puedan descargarlos.

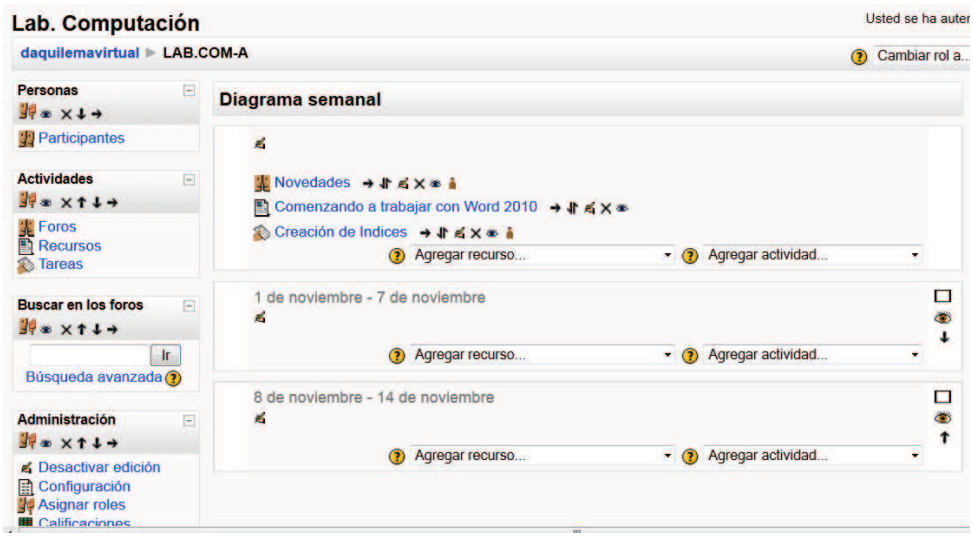


Figura 4.33: Diseño y edición de recursos en el curso de Lab. de Computación

4.2.10 MONITOR DE RED

El Monitor de Red es una herramienta de software que permite al administrador de la red poder ubicar problemas y actividad sospechosa en el funcionamiento de los servicios y de los dispositivos de conectividad, al permitirle realizar un seguimiento y análisis del comportamiento de la red, basándose en los registros que esta herramienta presenta. El Monitor de Red a configurar usará la aplicación de código abierto Nagios.

Se monitoreará todos los servicios que estarán funcionando en la red del CFD (DHCP, DNS, Proxy, Correo Electrónico, FTP, SSH, HTTP) además de los parámetros como utilización del CPU, utilización de memoria y número de procesos activos del servidor de comunicaciones. Las notificaciones de la caída de algunos de los servicios, o alertas que indiquen mal funcionamiento en los parámetros de carga del servidor serán notificados vía e-mail al administrador de la red.

4.2.10.1 Configuración

Para una mejor forma de administración y monitoreo, Nagios permite agrupar los hosts que se van a monitorear, esta definición de los hosts que pertenecen a un cierto grupo se realiza dentro del archivo /etc/nagios3/conf.d/hostgroups_nagios 2.cfg, la configuración deberá ser parecida a la mostrada en la Figura 4.34. A estos grupos de hosts se les puede definir servicios comunes a monitorizar como por ejemplo carga de CPU o utilización de memoria, esta configuración se encuentra dentro del archivo /etc/nagios3/conf.d/services_nagios2.cfg.

```
# Some generic hostgroup definitions

# A simple wildcard hostgroup
define hostgroup {
        hostgroup_name  all
                alias           All Servers
                members         *
        }

# A list of your Debian GNU/Linux servers
define hostgroup {
        hostgroup_name  debian-servers
                alias           Debian GNU/Linux Servers
                members         localhost
        }
```

Figura 4.34: Configuración de grupos de Hosts a monitorizar

Ahora se deben definir las direcciones IP, alias y nombre de host (este nombre debe ser el mismo que se utilizará en la línea *members* si es que se quiere agregar el host a un grupo); dentro de éste archivo también se pueden definir servicios a monitorizar para éste host. Todas estas definiciones se configurarán dentro de un archivo de texto plano que se guarde dentro del directorio /etc/nagios3/conf.d/. En la Figura 4.35 se muestra la definición del nombre, alias y dirección IP con la que se identificará en Nagios al servidor de comunicaciones.

```
define host{
        use                     generic-host            ; Name of host template to use
        host_name               localhost
        alias                   localhost
        address                 127.0.0.1
        }

# Define a service to check the disk space of the root partition
# on the local machine.  Warning if < 20% free, critical if
# < 10% free space on partition.

define service{
        use                             generic-service         ; Name of service
template to use
        host_name                       localhost
        service_description             Disk Space
        check_command                   check_all_disks!20%!10%
        }
```

Figura 4.35: Configuración de datos de un host a monitorear

Para que las alertas y notificaciones de caída de servicios se envíen por e-mail al administrador de la red se debe hacer un par de configuraciones en el servicio Postfix. Dentro del archivo /etc/postfix/main.cf se deberá configurar las siguientes líneas:

smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl/passwd
smtp_sasl_security_options = noanonymous

Y dentro del archivo /etc/postfix/sasl/passwd se deben colocar las credenciales de buzón de correo del administrador de la red. El password del correo del administrador está borrada de la siguiente imagen por seguridad.

```
[smtp.fdaquilema]:[redacted] administrador@fdaquilema:[redacted]
```

Figura 4.36: Configuración de credenciales del Buzón de Correo del Administrador de Red Postfix

Por último se configurará Nagios para que sepa que debe enviar las notificaciones al buzón de correo electrónico del administrador, esto se lo hará dentro del archivo /etc/nagios3/conf.d/contacts_nagios2.cfg. En la Figura 4.37 se muestra como deberá quedar este archivo de configuración.

```
##############################################################################
##############################################################################
#
# CONTACTS
#
##############################################################################
##############################################################################

# In this simple config file, a single contact will receive all alerts.

define contact{
        contact_name                    root
        alias                           Root
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    w,u,c,r
        host_notification_options       d,r
        service_notification_commands   notify-service-by-email
        host_notification_commands      notify-host-by-email
        email                           administrador@fdaquilema
        }
```

Figura 4.37: Configuración de contacto para envío de notificaciones

Para brindar mayor seguridad en el intercambio de la información de claves de acceso y la información de monitorización que viaja por la LAN se usará el protocolo HTTPS en las páginas web del Monitor de Red.3

4.2.10.2 Pruebas

En la Figura 4.38 se muestra la salida que entrega el Monitor de Red Nagios sobre el estado del servicio SSH que se ejecuta dentro del hosts de alias Localhost (servidor de comunicaciones).

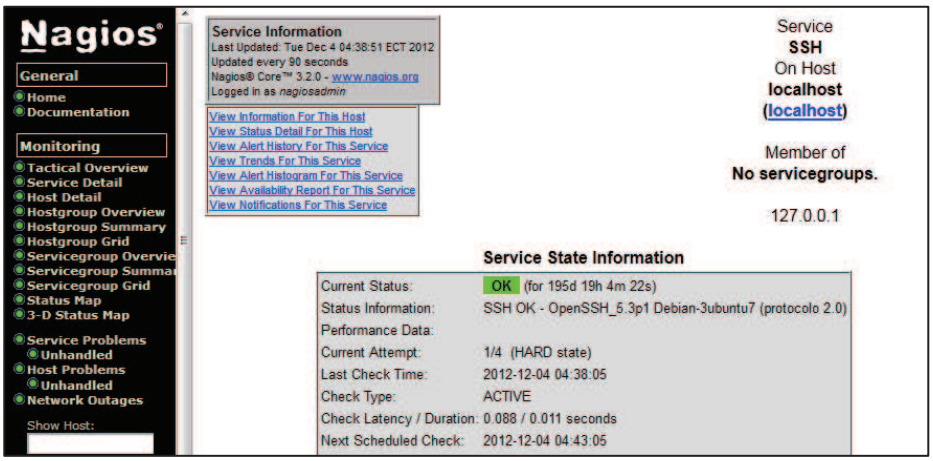


Figura 4.38: Monitorización del servicio SSH

4.2.11 GENERADOR DE REPORTES DEL PROXY

Se consideró la instalación de un Generador de Reportes de la actividad del servidor Proxy al observar la necesidad de tener informes sobre las páginas web que los alumnos, profesores y personal administrativo visitan regularmente, y que a su vez brinda la posibilidad de verificar que no existan páginas web que siendo prohibidas no hayan sido bloqueadas aún.

Este generador de reportes es una herramienta de software libre llamado SARG (*Squid Analysis Report Generator*) que crea reportes Web, a los que se tendrá acceso solo mediante la presentación de un usuario y password autorizados que serán enviados de forma cifrada para proteger esta información.

A esta herramienta se la configurará para generar reportes diarios, semanales y mensuales sobre las páginas web más visitadas, la cantidad de tráfico que fue respondido directamente por el Proxy desde su caché y la cantidad de tráfico web entrante y saliente.Los archivos de configuración de la aplicación web SARG completos y comentados se encuentran en el Anexo 29.

4.2.11.1 Configuración

En el archivo /etc/sarg/sarg.conf se realizarán las configuraciones de idioma, directorios donde se guardarán los reportes, se indicará la ubicación del archivo de logs del servidor Proxy, desde el que se sacarán dichos reportes y se definirá que se guardarán un máximo de 150 reportes que equivalen a tener un registro del tráfico web de un período de 6 meses anteriores a la fecha actual.

```
language Spanish

# TAG:  access_log file
#       Where is the access.log file
#       sarg -l file
#
access_log /var/log/squid3/access.log

# TAG: graphs yes|no
#    Use graphics where is possible.
#           graph_days_bytes_bar_color blue|green|yellow
#
graphs yes
graph_days_bytes_bar_color orange

# TAG:     title
#    Especify the title for html page.
#
title "Squid User Access Reports"
```

Figura 4.39: Archivo de Configuración SARG

Para que los reportes se generen automáticamente se deberá crear tres archivos de texto plano que contendrán las instrucciones para que la herramienta SARG cree los tres diferentes tipos de reportes (diarios, semanales y mensuales); en la Figura 4.40 se observa el script que contiene el archivo encargado de generar los reportes diarios.

```
#daily :
#======
#!/bin/bash
#Obtener la fecha actual
TODAY=$(date +%d/%m/%Y)
#Obtener la fecha del día anterior
YESTERDAY=$(date --date "1 day ago" +%d/%m/%Y)
#Creación del reporte diario
sarg -n /var/log/squid3/access.log -o /var/www/squid-reports/daily -z -d $YESTERDAY-
$TODAY
/usr/sbin/squid3 -k rotate
exit 0
```

Figura 4.40: Script para generar reporte diario del servidor Proxy

Una vez creados estos archivos, se procede a utilizar el servicio *crontab* para automatizar la ejecución de estos scripts diariamente, semanalmente y mensualmente según sea el caso.

Para evitar que cualquiera dentro de la red ingrese a los reportes usando el navegador web, se creará el archivo /etc/apache2/sites-avaliable/sarg.conf en el que se va a especificar que los únicos usuarios que tienen permitido el ingreso al directorio donde se encuentran los reportes web serán aquellos que sean usuarios de la LAN del CFD y puedan autenticarse con las credenciales autorizadas; además, en este archivo se configurará los directorios de los certificados y llaves que el servidor Web usará para la conexión SSL.

```
NameVirtualHost *:443
<VirtualHost *:443>
    ServerAdmin administrador@fdaquilema.com
    ServerName proxy.fdaquilema.com
    DocumentRoot /var/www/squid-reports

    # Parametros para configuraciones SSL y certificados
    SSLEngine on
    SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eN
ULL
    SSLCertificateFile /etc/ssl/certs/serverssl.crt
    SSLCertificateKeyFile /etc/ssl/private/serverssl.key
    #SSLCACertificateFile /etc/ssl/certs/cacert.pem

    <Directory /var/www/squid-reports/>
      Options Indexes FollowSymLinks MultiViews
      AllowOverride None
      Order allow,deny
      allow from all

      # Permitir solo autenticacion a usuarios autorizados
      AuthType Basic
      AuthName "Solo Usuarios Autorizados"
      AuthUserFile /var/www/claves-sarg
```

Figura 4.41: Archivo de configuración /etc/apache2/sites-avaliable/sarg.conf

4.2.11.2 Pruebas

En la figura 4.42 se muestra un reporte diario en el que se puede ver los usuarios que navegaron en Internet, la cantidad de tráfico consumido por cada uno y el tráfico total consumido en el día; además de esto también se puede apreciar que este reporte viaja cifrado, pues la conexión Web usa el protocolo HTTPS.

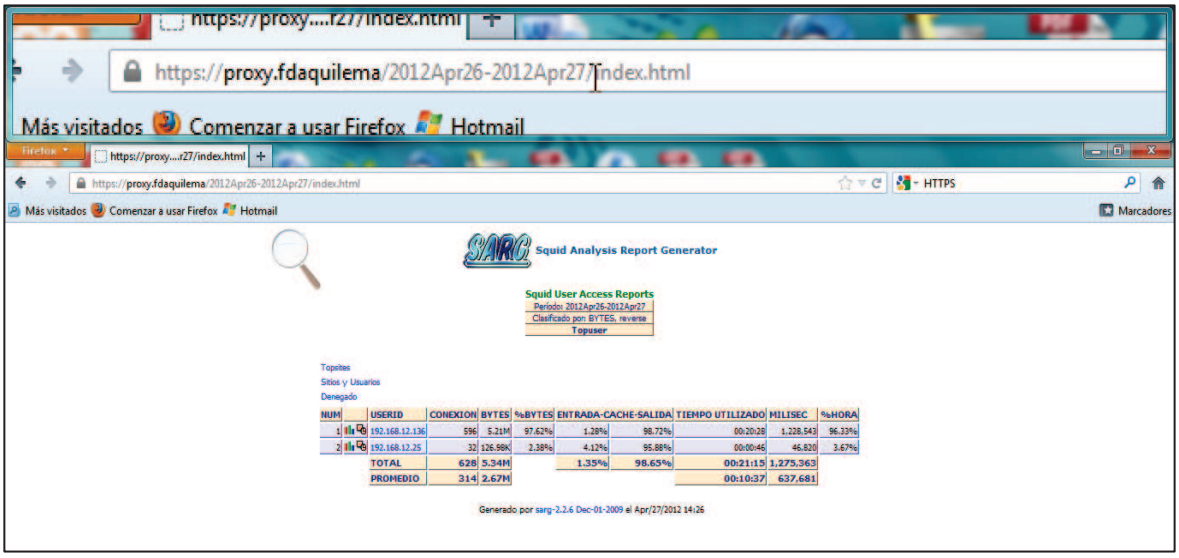


Figura 4.42: Reporte de Tráfico del servidor Proxy

4.2.12 PÁGINA WEB

Para la creación de la página web de la institución se decidió usar la aplicación de software libre Joomla que ofrece una plataforma completa para la creación, configuración, edición y administración de un portal web.

Este portal web tendrá como objetivo ser una ventana para que los alumnos, profesores, padres de familia y visitantes de Internet puedan acceder a información sobre noticias, eventos, actividades e información relevante en relación al CFD. Con este objetivo se diseñará el sitio web para tener las siguientes secciones:

- Inicio: en esta sección se encontrarán las noticias, avisos y eventos próximos que van a realizarse en la institución de modo que sean de fácil acceso para todos los visitantes.

- Programas Pedagógicos: en esta sección se presentarán los modelos pedagógicos y mallas curriculares con las que trabaja el colegio.
- Historia: en esta sección se presentarán temas relacionados con la vida de Fernando Daquilema, la historia de la institución, etc.
- Contactos: en esta sección aparecerá información sobre la ubicación, teléfonos y horarios de atención de las diferentes oficinas de la institución; además se contará con un mecanismo para enviar correos electrónicos al administrador de la red para aquellos visitantes que deseen contactarse con las autoridades del colegio.
- Profesores: en esta sección se encontrará información solo relevante a los profesores y personal administrativo de la institución.

4.2.12.1 Configuración

La configuración, administración y edición del portal web se hace desde el panel de control de Joomla, en esta sección el primer paso es definir una plantilla sobre la cual se va a editar los artículos y colocar nuevos módulos; para ello se ingresa al menú Gestor de Plantillas y luego se hace click en el ícono que aparece en la columna *Defecto* para que sea esta plantilla la que se use en el sitio web.

Figura 4.43: Panel de Control Joomla

Una vez definido la plantilla se puede comenzar a crear artículos (noticias, novedades, etc.) que van a ser publicados en el sitio web, para ello debemos ir a la pestaña *Contenido ->Gestor de Artículos* y aparecerá un listado de artículos creados en el sitio web y si están publicados o no. Para la creación de un nuevo

artículo se debe hacer click en el icono *Nuevo* que parece a la derecha del título de ésta ventana. Para publicar o quitar un artículo basta con hacer click en el ícono que se encuentra en la columna *Estatus* y cambiarlo de color verde al color rojo. Al finalizar la edición de un artículo se hace click en *Guardar y Cerrar*.

Figura 4.44: Gestor de Artículos Joomla

Con los artículos ya creados se definen los menús que se tendrán en la página; cada sección que se definió que tendría la página va a estar representada con un menú. Para crear un menú se debe ingresar a *Menús -> Menú Principal*, y aparecerá una ventana con una lista de los menús y submenús creados en la página web. De la misma manera que con los artículos para publicar o quitar un menú se debe hacer click en el ícono que aparece en la columna *Estatus*.

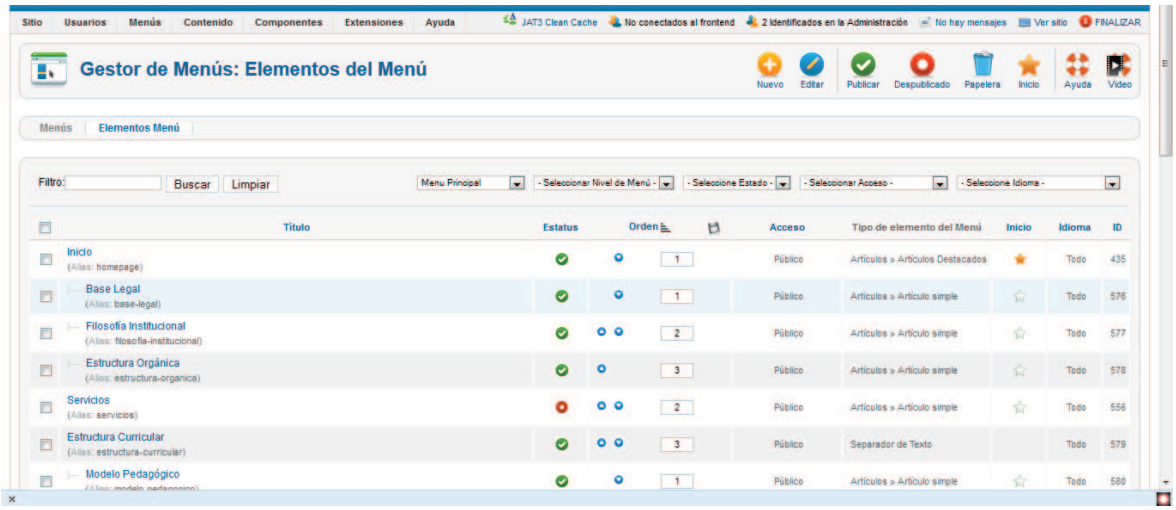


Figura 4.45: Gestor de Menús Joomla

Para crear un nuevo menú se debe hacer click en el ícono de nombre *Nuevo* en la parte derecha del nombre de la ventana *Gestor de Menús*, y aparecerá una ventana de configuración del nuevo menú a crear. Entre las configuraciones que se van a hacer está el definir el tipo de menú a crear, como por ejemplo un menú simple que va a ser un enlace a un artículo que se creó anteriormente, o puede ser solo un menú principal desde el cual se van a desplegar sub menús; otra configuración a hacer es definir si es un Menú Principal o si va a actuar como un sub menú dentro de un Menú Principal padre;al finalizar las configuraciones se hace click en *Guardar y Cerrar.*De esta manera se van a ir creando cada menú y submenús que tendrá la página web.

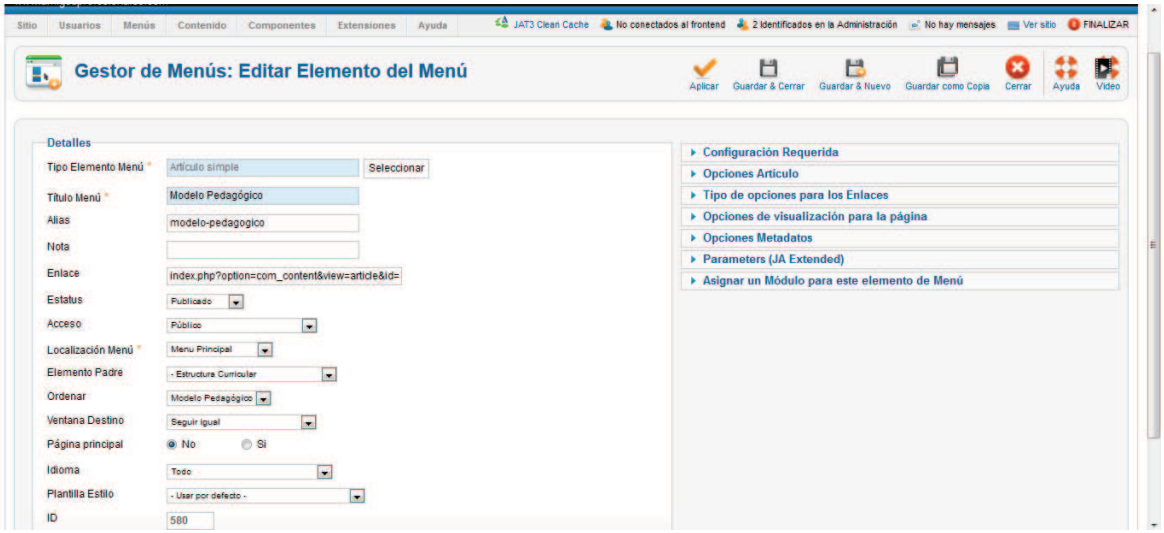


Figura 4.46: Configuración de un Menú de página web Joomla

Entre los módulos que vienen instalados en Joomla se encuentra el módulo de Calendario, este módulo permite identificar fechas en las que se quiera indicar noticias, eventos o actividades que se vayan a desarrollar en el colegio.

Para crear un nuevo el módulo como el de Calendario que pueda publicarse en la página web se debe ingresar al menú *Extensiones -> Gestor de Módulos, y hacer* click en el ícono *Nuevo* y aparece una ventana que pide seleccionar el tipo de módulo a crear, en éste caso se selecciona el tipo *JEvents Calendar*, luego parece una ventana de configuración para el nuevo módulo, aquí se configura el nombre del módulo, la posición del mismo es decir la posición que va a ocupar el módulo dentro de la página web, también se definen las páginas en que se va a

poder publicar este módulo; al finalizar las configuraciones se hace click en *Guardar y Cerrar.* Del mismo modo se añadirán los módulos Buscar, pie de página, últimas noticias, visor de imágenes y visor de noticias.

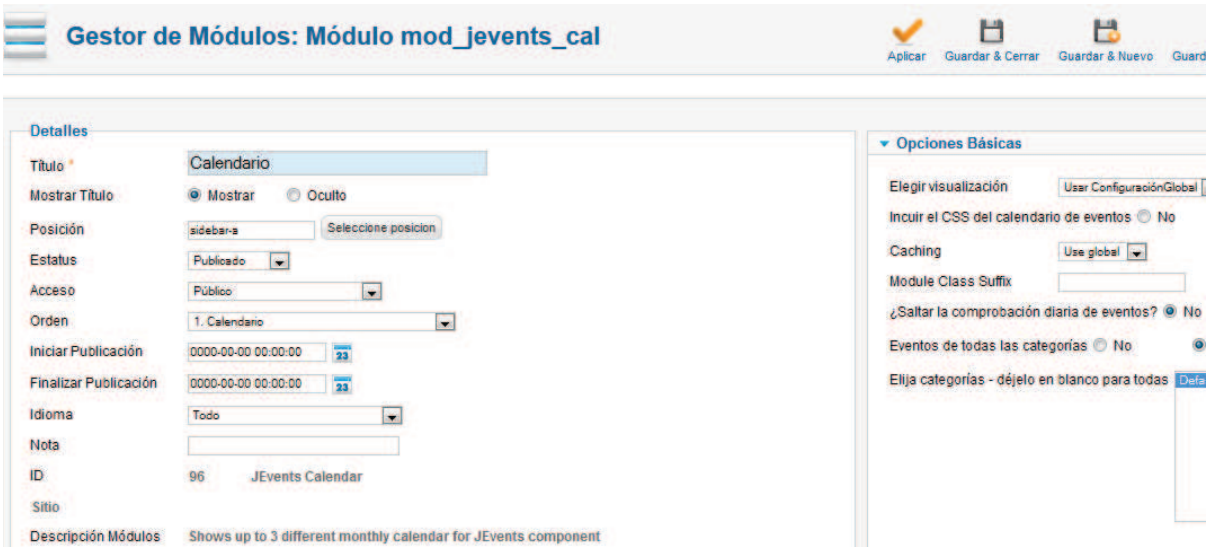


Figura 4.47: Configuración de un nuevo módulo

Para publicar un módulo en la página web se debe ingresar al menú *Extensiones -> Gestor de Módulos* y aparecerá una ventana con todos los módulos que se han agregado, para aquellos que se encuentran publicados su *Estatus* estará en color verde.

Figura 4.48: Gestor de Módulos de página web Joomla

4.2.12.2 Pruebas

En la Figura 4.49 se puede observar los módulos de banner de imágenes, los menús de Inicio, estructura curricular, historia, horario de atención y acceso de profesores. La página web del CFD tiene el siguiente nombre de dominio www.fdaquilema.com.

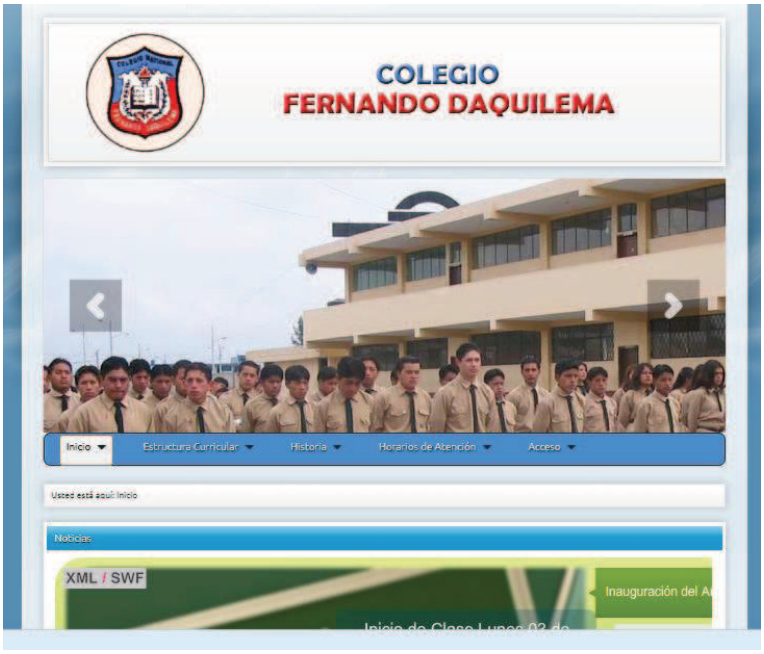


Figura 4.49: Página Web CFD

4.2.13 PRUEBAS DE VIDEO CONFERENCIA Y VIDEO SEGURIDAD EN EL PROTOTIPO DE RED

A más de los servicios de red anteriormente presentados, dentro del prototipo de red se instalaron los servicios de: video conferencia por medio de Asterisk y video seguridad con ZoneMinder para mostrar el funcionamiento de estos dos servicios.

4.2.13.1 Video conferencia con Asterisk

El servicio de video conferencia se lo implementó usando el servidor Asterisk. Esta es una aplicación de licencia GPL (licencia libre) que tiene las funcionalidades de una central telefónica, entre sus características más sobresalientes están: el buzón de voz, el menú de bienvenida interactivo, cuentas de usuario protegidas con contraseñas, el soporte integrado de varios codecs de

voz y video (G.711, GSM, G.722, G723.1, G728, G729, H.261, H.263, H.262p, H264), cuentas de usuario móviles para usarse desde cualquier teléfono IP presente en la red, y restricciones en el plan de marcado para dar permisos a cada usuario con respecto al tipo de llamadas que puede realizar.

4.2.13.1.1 Configuración

El archivo /etc/asterisk/sip.conf es donde se guardan las cuentas de usuario, sus contraseñas y se configura el contexto al cual estará asociado cada usuario.

En la Figura 4.50 se muestra parte del archivo /etc/asterisk/sip.conf en el que se puede apreciar las diferentes características que una cuenta SIP puede tener; entre ellas están:

- *Type* de la cuenta SIP, en el ejemplo de la Figura 4.50 se encuentra en modo 'friend' pues se trata de un softphone o teléfono IP; pero si fuera la cuenta para comunicarse con otra central telefónica IP este parámetro sería tipo 'peer', que tiene como un parámetro obligatorio el especificar en la configuración la dirección IP de la central telefónica remota para lograr la comunicación con ella.
- Otro parámetro importante es *secret,* con este parámetro se indica la contraseña que se va a usar para autenticar a este usuario con Asterisk.
- Las siguientes 5 líneas de la configuración que inician con las palabras *disallow* y *allow* indican que solo se permite el uso de los codecs G.711a, G711u y GSM para audio, y H.264 para video.
- El parámetro *context* es muy importante pues con este se indica a que extensiones y números telefónicos puede llegar éste usuario.
- Por último están *mailbox* y *setvar,* el primero sirve para indicar cuál es la cuenta de buzón de voz del usuario y el otro parámetro sirve para crear una variable que estará asociada siempre con la cuenta SIP de este usuario, y que es utilizada dentro de la funciones declaradas en el archivo /etc/asterisk/extensions.conf.

En el archivo /etc/asterisk/extensions.conf se configuran los números de extensión asociados con cada cuenta de usuario creada en 'sip.conf'; también en este archivo se crean los diferentes contextos a los cuales pueden ingresar o no los usuarios dependiendo de sus privilegios; y además aquí se puede configurar el mensaje de bienvenida interactivo.

En la figura 4.51 se muestran los contextos y la creación de los números de extensión que se van a utilizar, por ejemplo la cuenta 'sebas' tiene asociado el número de extensión '500'; también se debe notar que todos los números de extensión fueron creados dentro del contexto *[phones]* aunque el usuario sebas tiene como *contex* el nombre 'intranet-out-loc-nac-cel' y si se mira debajo del contexto *phones* se puede ver otros contextos que a su vez tienen dentro declarados los contextos de *phones, locales, nacionales, etc.,* esto sirve para que el usuario 'sebas' tenga acceso a las extensiones internas y a las llamadas de tipo local, nacional y celular.

```
[sebas]
type=friend
secret=12345
disallow=all
allow=ulaw
allow=alaw
allow=gsm
;allow=h261
;allow=h263
allow=h264
qualify=yes     ; Permite a Asterisk saber si el usuario sigue estando en linea
                ; al enviar regularmente un paquete SIP (2000 ms).
nat=no          ; No hay NAT.
host=dynamic    ; Dispositivo se registrara con el servidor.
context=intranet-out-loc-nac-cel  ; Contexto predefinido (ver . extensions.conf)
directmedia=yes ; Para que la informacion de voz se envie con el mismo codec por toda la red
mailbox=505@correo_voz_colegio ; Indica la cuenta de Buzon de Voz del usuario y el contexto
setvar=SIPACC=sebas ; Se crea una variable que se usara dentro de la macro de buzon de voz y
                    ; para localizar el archivo que conetiene la contrasenia del usuario para
                    ; realizar llamadas nacionales.
```

Figura 4.50: Archivo /etc/asterisk/sip.conf

A través de los contextos se puede restringir los permisos que cada usuario tiene para hacer llamadas locales, nacionales o a celulares. Otra opción importante es el uso de *Macros,* la mismas que son como un procedimiento que ejecuta un código dado; las macros se pueden crear tal como se declaran los contextos pero la diferencia está en que los macros usan las variables que se les envía para ejecutar su código.

```
[phones]
exten => 505,1,Macro(buzon,${EXTEN},sebas)
exten => 500,1,Macro(buzon,${EXTEN},sruiz)
exten => 501,1,Macro(buzon,${EXTEN},eperez)
exten => 502,1,Macro(buzon,${EXTEN},amunioz)
exten => 503,1,Macro(buzon,${EXTEN},cpaez)
exten => 504,1,Macro(buzon,${EXTEN},mroca)

;Contexto que posee permisos para realizar llamadas en la intranet.
[intranet]
include => phones

;Contexto que posee permisos para realizar llamadas en la intranet y Locales.
[intranet-out-loc]
include => phones
include => locales

;Contexto que posee permisos para realizar llamadas en la intranet, Nacionales y Locales.
[intranet-out-loc-nac]
include => phones
include => nacionales
include => locales
```

Figura 4.51: Archivo /etc/asterisk/extensions.conf

En la Figura 4.51 se muestra que los números de extensión de *phones* usan una macro que se llama *buzon* y que envía como datos el número de extensión y el nombre de la cuenta SIP del usuario, estos datos serán usados para que en caso de que el destinatario de la llamada esté desconectado o no conteste se cree un mensaje de voz al cual solo el usuario podrá acceder mediante el número de extensión y una contraseña que es diferente de la usada en la cuenta SIP.

Por último para que las cuentas de correo funcionen se debe declarar las cuentas de buzón de voz dentro del archivo /etc/asterisk/voicemail.conf, estas cuentas deben estar también dentro de un contexto en este caso *correo_voz_colegio*, y dentro de este se especifica la contraseña del buzón, el nombre del dueño de esa cuenta y la dirección de email asociada que servirá para el caso en que se necesite enviar al usuario vía correo electrónico la grabación de voz que tiene en su buzón.

```
[correo_voz_colegio]
500 => 12345,Saul Ruiz,sruiz@fdaquilema
501 => 12345,Esteban Perez,eperez@fdaquilema
502 => 12345,Andrea Minioz,amunioz@fdaquilema
503 => 12345,Carlos Paez,cpaez@fdaquilema
504 => 12345,Marco roca,mroca@fdaquilema
505 => 12345,Sebastian Jaramillo,sjaramillo@fdaquilema
```

Figura 4.52: Cuentas del buzón de voz

Para que las grabaciones de voz se envíen por correo se necesita cambiar las siguientes líneas dentro del archivo /etc/asterisk/voicemail.conf. En la línea *attach* del archivo 'voicemail.conf' se debe colocar 'yes' para que la grabación de voz del buzón sea enviada adjunta al email; también se puede editar cual será el asunto, mensaje y el formato de la fecha que tendrá el correo que se envíe. En la Figura 4.53 se puede apreciar cada uno de los parámetros que se explicaron para habilitar el envío de correos con los mensajes de voz.

Los archivos de configuración de Asterisk que han sido editados se encuentran completos en el Anexo 30.

```
; Indica que el e-mail enviado al usuario contendra el mensaje de voz adjunto a este
attach = yes

;Asunto y mensje que contedrÃ¡n los emails enviados
emailsubject=Nuevo mnesaje de voz de ${VM_CALLERID}
emailbody=Saludos ${VM_NAME} recibido el ${VM_DATE}
emaildateformat=%A %B %d, %Y
```

Figura 4.53: Archivo /etc/asterisk/voicemail.conf

4.2.13.1.2 Pruebas

Para realizar la prueba se utilizó el softphone de licencia GPL Ekiga para Windows, y se realizaron video llamadas entre dos máquinas. Los resultados se pueden observar en la Figura 4.54.

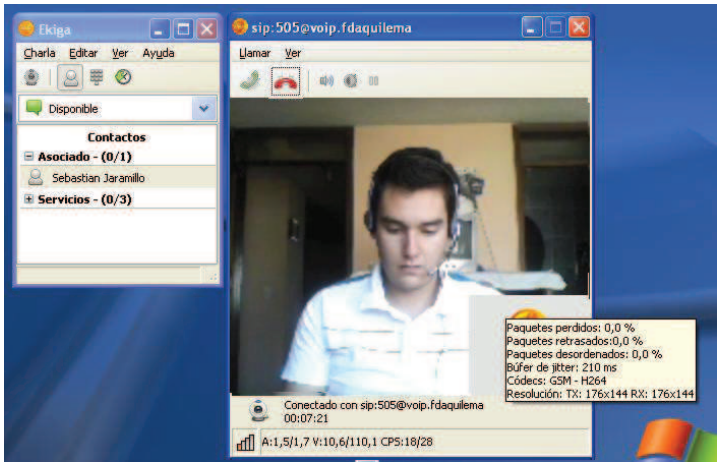


Figura 4.54: Video llamada con Asterisk

En la figura anterior se pude apreciar la video llamada que se realiza, además se pueden ver los parámetros que el softphone Ekiga brinda sobre los paquetes

perdidos, paquetes retrasados, paquetes desordenados, los codecs utilizados y la resolución de imagen que se muestra.

4.2.13.2 Video seguridad

Para el servidor de video seguridad se ocuparon dos cámaras IP que se comunican con el servidor de video seguridad ZoneMinder. Entre las capacidades que tiene ZoneMinder está la detección de movimiento mediante la comparación y contabilización de cuantos cuadros de la imagen son diferentes, haciendo así que cámaras que no tienen esta funcionalidad pueda usarse como detectores de movimiento, y, apenas se detecte algo se puede crear una grabación de la alerta para su revisión posterior.

4.2.13.2.1 Configuración

La configuración de ZoneMinder se realiza todo por una interfaz web por lo que es fácil y rápido unir una nueva cámara y ponerla a funcionar. Para agregar una nueva cámara se debe primero hacer click en *Agregar Nuevo Monitor* y aparecerá una nueva ventana como se muestra en la Figura 4.55, en esta ventana las pestañas más importantes son *General* y *Origen.*

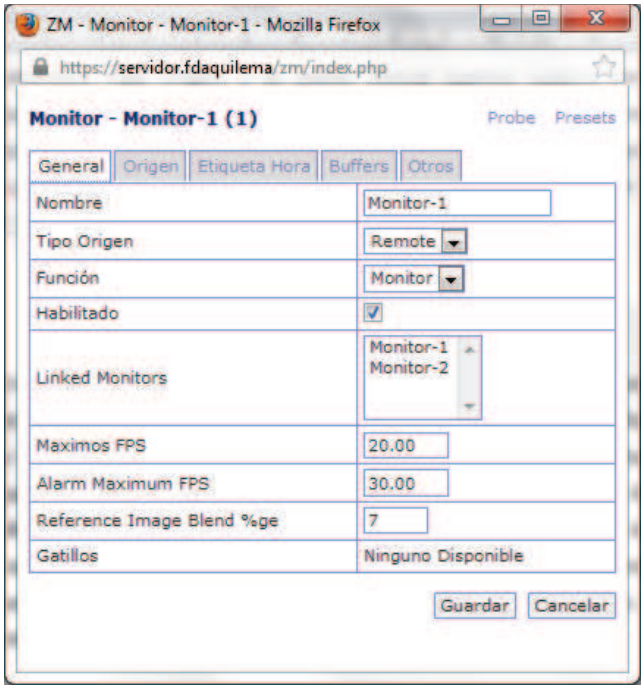


Figura 4.55: Pestaña General de la ventana para añadir un monitor

En la pestaña *General* se especifica: el nombre del monitor (*Nombre*), en el parámetro *Tipo Origen* se declara si la cámara está instalada en el mismo servidor o si es una cámara IP en ese último caso se coloca 'Remote'; también en esta pestaña se puede colocar cuantos cuadros por segundo se quieren mostrar en los monitores aun cuando el número de cuadros por segundo que la cámara entregue sea mayor, así como también se pude especificar cuantos cuadros por segundo se pueden ver en el monitor en caso de que se haya disparado una alarma.

En la pestaña *Origen* se especifica el método de autenticación con la cámara IP utilizando el parámetro *Remote Method*, en el parámetro *Nombre Servidor* se especifica el nombre de usuario y contraseña para acceder a la cámara IP, el puerto por donde escucha la cámara IP para ingresar a su interfaz de configuración se lo coloca en *Puerto Servidor Remoto,* y por último se especifica la ruta que se debe seguir para obtener la imagen que captura la cámara, esto se coloca en *Enlace Servidor Remoto;* los otros parámetros de esta pestaña sirven para configurar el tamaño de cuadro de la imagen y cambiar la orientación de la misma.

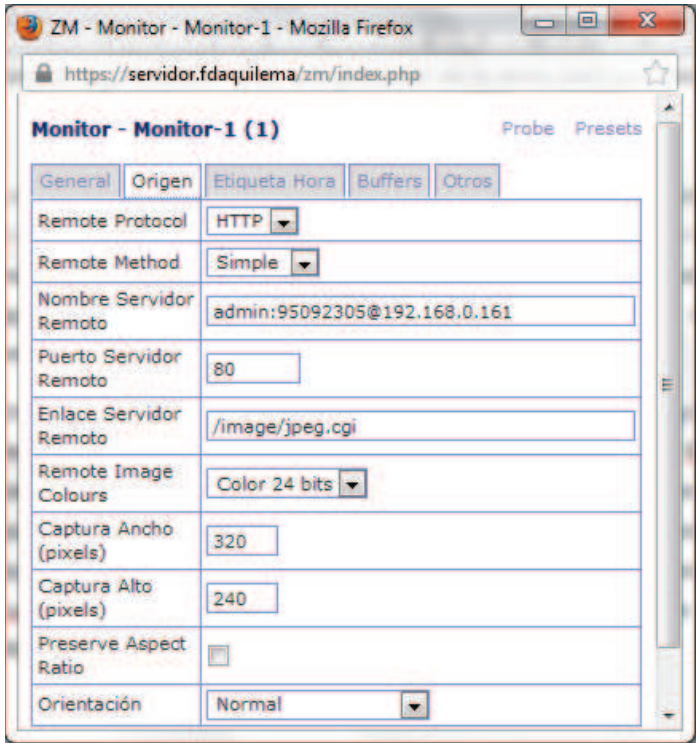


Figura 4.56: Pestaña Origen de la ventana para añadir un monitor

Para poder crear videos al detectar movimiento se debe crear un *Filtro*, para ello se hace click en *Filters* en la ventana principal de ZoneMinder, y aparecerá una ventana como la que se presenta en la Figura 4.57; en esta ventana se puede especificar muchos tipos de filtros que pueden involucrar solo a un monitor o a varios de ellos y pueden dispararse según si se cumplen o no todas las condiciones que se especifiquen en el filtro.

Para crear estas condiciones que usará el filtro a crear se tiene varios menús, en el primer menú contando desde arriba a la izquierda se puede especificar: un nombre de monitor, un identificador, una fecha, hora o día de la semana; luego en el menú a la derecha de este último se puede escoger una condición lógica como 'mayor que', 'igual que', 'menor que', 'distinto', etc., y finalmente se coloca el valor a comparar; de la misma manera se pude seguir añadiendo más comparaciones lógicas y uniéndolas entre ellas con operaciones lógicas de 'Y' u 'O'.

Para el caso del ejemplo de Figura 4.57 se va crear un filtro que sea activado por Monitor-1 cuando los cuadros de alarma (Alarm Frames) tengan un número mayor que 30 y que al momento que se cumpla este filtro se cree un video (*Create video for all matches*).

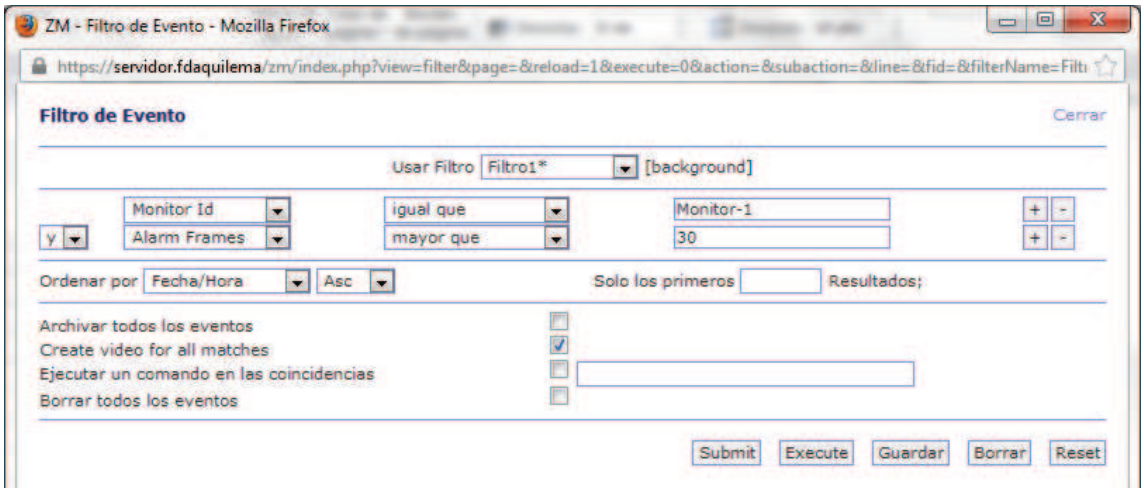


Figura 4.57: Ventana para crear filtros

4.2.13.2.2 Prueba

Primero se va a mostrar los videos que se toman con las dos cámaras en un monitor tipo grilla, para lo cual se debe hacer click en *Cámara Múltiple* en la ventana principal de ZoneMinder.

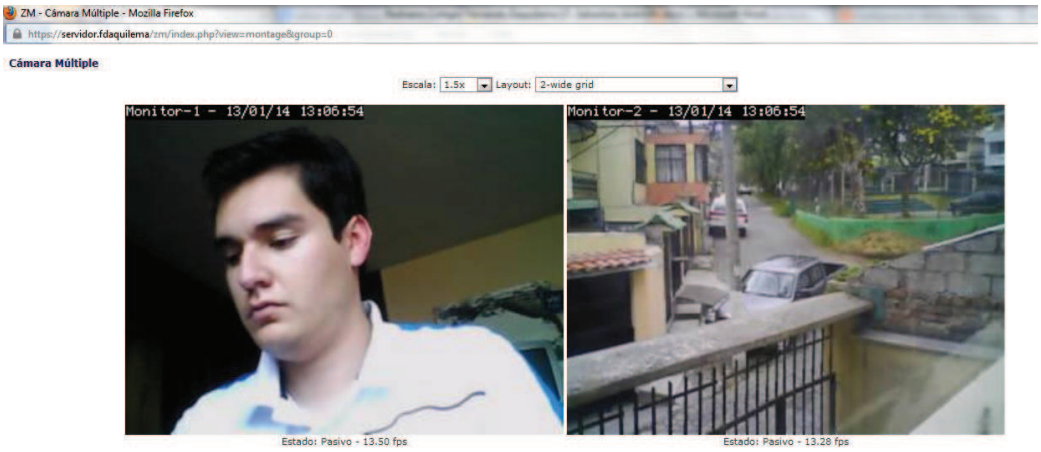


Figura 4.58: Monitor de cámaras múltiples

Ahora se va a probar el filtro que se creó anteriormente, para hacerlo se debe cambiar el modo de funcionamiento del Monitor-1 al modo de detección de movimiento 'Modetect' y luego hay que realizar un movimiento para que se dispare la alarma y se grabe un video del incidente. En la Figura 4.59 se puede observar como aparece en la lista un evento de 10.7 segundos de duración, y para poder observar este evento guardado solo se debe hacer doble click sobre él. En la Figura 4.60 se puede ver la reproducción del video, en esta ventana se puede pausar, retroceder y adelantar los videos que se observan.

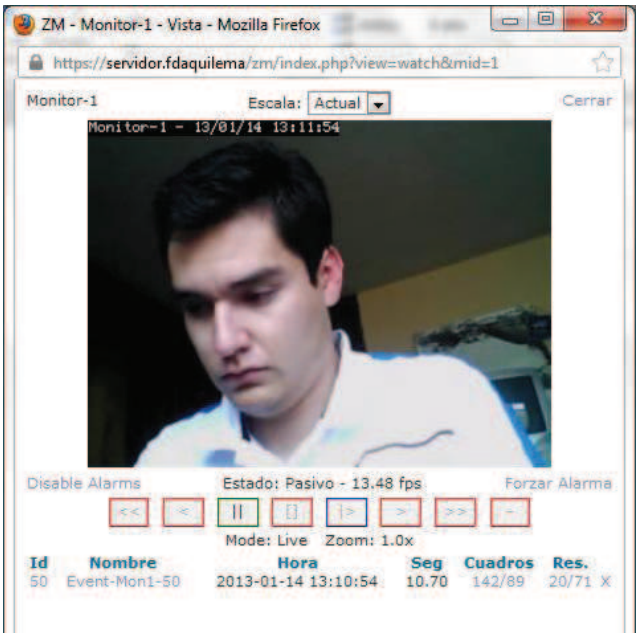


Figura 4.59: Video de alarma creado por el filtro puesto al Monitor-1

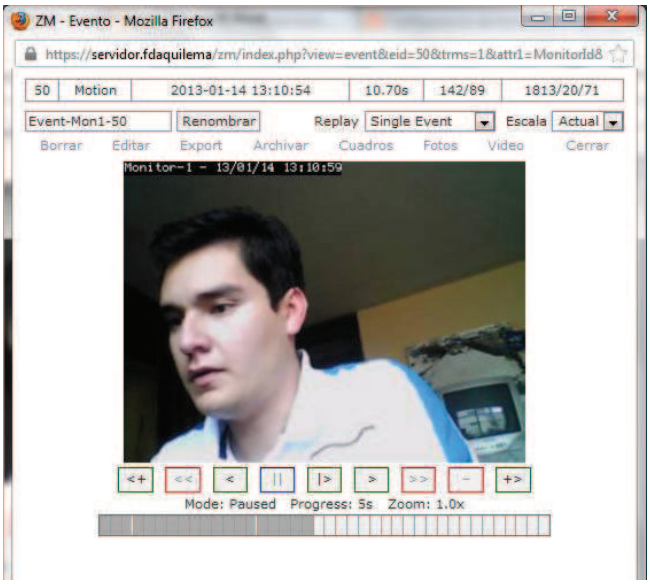


Figura 4.60: Reproducción del video de alarma grabado por el Monitor-1

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Es muy importante diseñar un sistema de cableado estructurado que cumpla con los lineamiento definidos por las normas TIA-568.C pues la mayor parte de fallas en el funcionamiento de la red actual se deben a la mala implementación y la falta de etiquetamiento en los cables de red, lo que no permite la pronta localización y reparación de fallas de funcionamiento del cableado de red.

- Los equipos de conectividad deben funcionar dentro de cuartos de telecomunicaciones fuera del alcance de los usuarios de la red, ya que si no es así pueden aparecer problemas debido a la manipulación de las conexiones o de los equipos de red por parte de personal no autorizado.

- El tener una topología de red sin una estructura definida no permite tener escalabilidad ni flexibilidad lo que causa dificultades al momento en que se requiere aumentar el número de equipos de conectividad con el fin de brindar servicio a un mayor número de puntos de red, pues no existe un orden específico para este crecimiento y no se tiene claro las funciones que específicas con las que cada equipo deberá cumplir.

- El seguir una topología basada en las capas de Núcleo, Distribución y Acceso hace que la red sea mucho más escalable y flexible ya que se conoce las funciones y características que los equipos pertenecientes a cada una de las capas deberá tener, haciendo más fácil la búsqueda y determinación de los equipos de conectividad más adecuados para las necesidades de la red.

- La implementación de un Sistema de Puesta a Tierra para los equipos de conectividad es de gran importancia para el CFD, pues con este sistema se protegerá a estos equipos de las variaciones de voltaje que la red eléctrica sufre, y que en veces anteriores ya causaron daño al servidor con el que cuenta el colegio; además como complemento a este sistema se deberá instalar un UPS 10 KVA y contar con un generador que serán un respaldo ante cortes eléctricos, permitiendo continuar las actividades normales en las estaciones de trabajo y equipos de conectividad evitando pérdidas de información y daños en los equipos.

- Por los resultados obtenidos luego de los cálculos sobre el ancho de banda que consumiría cada usuario de la red se concluyó que la velocidad de acceso de 100 Mbps permitirá soportar todos los servicios de red con los que contará el CFD sin saturarse.

- Luego del análisis sobre el ancho de banda ocupado en el enlace de Internet que tiene contratado el CFD se concluyó que el enlace se encuentra está saturado especialmente en el enlace de bajada pues la velocidad registrada supera por 0.5 Mbps a la velocidad que el enlace posee; es por esto que luego de realizar un análisis sobre el uso de Internet y el número de usuarios simultáneos que se tendrá usando este servicio se recomienda que se contrate un enlace de 7 Mbps.

- El tráfico de red multiservicios requiere que se realice un trato diferenciado para los datos pertenecientes a la voz y el video; para asegurar la calidad del servicio se deben implementar configuraciones que den prioridad a estos flujos de tráfico en todos los elementos de la red que intervienen en la comunicación, es decir desde los terminales telefónicos IP y pasando por los switches de las diferentes capas de la red.

- Entre las más grandes ventajas de la telefonía IP están su escalabilidad que solo depende de las características técnicas con la que cuente el

servidor en la que se instale la central telefónica IP; también está su capacidad para la comunicación entre varias centrales telefónicas IP al mismo tiempo que permite bajar mucho los costos de telefonía en los casos en que se tenga sucursales remotas y se necesite la comunicación entre ellas haciendo que el costo de esta comunicación solo dependa de la capacidad del enlace de datos que la empresa tenga contratado para la comunicación entre las centrales IP; los servicios adicionales como el buzón de voz, los menús de voz interactivos y el control detallado de cada cuenta de usuario.

- El sistema de telefonía deberá tener 3 líneas analógicas para la comunicación con la PSTN, este dato se obtuvo a partir del análisis de número de llamadas por hora que se tiene en la institución, con un porcentaje de bloqueo 1% y siguiendo el modelo Erlang B.

- El usar un sistema de video seguridad por medio software tiene muchas ventajas frente a otras implementaciones que utilizan hardware para dirigir el video de las cámaras hacia un monitor; entre las ventajas que ofrece la video seguridad por software es que posee muchas opciones para obtener diferentes de comportamientos del sistema de video; permite usar y calibrar la sensibilidad para la detección de movimiento mediante el análisis continuo del video que se capta, y además permite interactuar con los servidores por medio de comandos de consola que se pueden ejecutar automáticamente.

- Los sistemas de vigilancia con cámaras IP permiten tener cámaras que envían la información de manera inalámbrica como alámbrica, y a más de ello permite usar el cableado de la red de datos existente para enviar la información de video y brindar alimentación eléctrica a la cámara en el caso de que esta se encuentre en un lugar donde no exista tomas eléctricas, estas características le dan a la vigilancia IP una gran flexibilidad y escalabilidad.

- La utilización de backups periódicos de los servicios de red como de la información sensible que el personal administrativo maneja, va a dar a los usuarios la garantía de que los servicios de red van a estar funcionando permanentemente y que su información va a estar segura aun cuando exista algún percance con las computadoras con las que trabajan.

5.2 RECOMENDACIONES

- Para la implementación de este proyecto es necesario contar con un plan de acción que permita adquirir los equipos y servicios de manera gradual, para ajustarse con el presupuesto asignado por la institución para este propósito. Por lo que se recomienda seguir los siguientes pasos para la implementación de la red:

    - Instalación del Sistema de Cableado Estructurado y Puesta a Tierra
    - Adquisición de los switches, Access Points, UPS, y repotenciación del Servidor de Comunicaciones
    - Configuración de Servicios
    - Configuración de VLANs, permisos y filtros de tráfico
    - Adquisición de Teléfonos y Cámaras IP
    - Configuración de la Central Telefónica IP y Sistema de Video Vigilancia

- Los equipos a adquirir para la infraestructura de comunicaciones deberán tener la garantía del fabricante y del proveedor; indicando claramente el tiempo de respuesta ante un fallo, necesidad de reparación o cambio del equipo.

- Se recomienda la contratación de un ingeniero de soporte, ya que, aunque se ha diseñado la infraestructura de red para una fácil administración, es

necesario contar con una persona de forma permanente que se haga cargo de la administración de los servicios y de soporte técnico a los usuarios de la red.

- Se recomienda crear un archivo físico en el que se encuentren registrados todas las instalaciones, cambios y configuraciones creadas en lo equipos de conectividad y el servidor de comunicaciones; este documento servirá como guía sobre el estado de la red para cualquier persona que se encargue de la administración de la misma.

- Se debe calendarizar mantenimientos anuales a los equipos de conectividad, servidor y UPS, para asegurar que se encuentran en buenas condiciones y detectar posibles problemas que puedan aparecer a futuro.

- Se recomienda el almacenamiento de la información de video seguridad en varios lugares, para evitar la pérdida de la información en caso de que el disco duro del servidor sufra algún daño o falle.

- Se recomienda el uso de conexiones SSL para la autenticación e intercambio de información sensible de la institución, como por ejemplo el intercambio de información de correo electrónico, intercambio de archivos mediante FTP, acceso a los informes del monitor de red, etc.; este mecanismo garantizará la confidencialidad e integridad de las cuentas de usuario e información que se intercambia.

REFERENCIAS BIBLIOGRÁFICAS

Libros:

[L1] A. Tanembaum, D. Wetherall, *Redes de Computadoras,* Prentice – Hall, 5ta edición, 2010.

[L2] W. Stallings, *Comunicaciones y Redes de Computadoras,* Prentice – Hall, 9na edición, 2010.

Folletos:

[F1] P. Hidalgo, Folleto de *Redes TCP/IP,* 2008.

[F2] M. Vinueza, P. Hidalgo, Folleto de *Redes de Área Local,* 2008.

[F3] S. Sinche, Folleto de *Redes LAN Inalámbricas,* 2009

[F4] P. Hidalgo, Folleto de *Sistemas de Cableado Estructurado,* 2009.

Publicaciones:

[P1] Tempo, Quick Reference Guide TIA/EIA 606A*,* 2010.

[P2] A. Fuentes, Folleto de *Telefonía IP Análisis, Diseño e Implementación*, 2009.

[P3] J. Joskowicz, *Voz, Video y Telefonía sobre IP,* Ing. Eléctrica, Univ. de la República, Montevideo, Uruguay, 9na edición, 2011, [En línea]. Disponible en: http://iie.fing.edu.uy/ense/asign/ccu/material/docs/Voz%20Video%20y%20Telefonia%20sobre%20IP.pdf

[P4] P. Shade, *VoIP Analisys Fundamentals with Wireshark*, 2010, [En línea]. Disponible en: http://sharkfest.wireshark.org/sharkfest.12/presentations/BI-7_VoIP_Analysis_Fundamentals.pdf

[P5] M. Alvarez, *Video sobre IP*, VITELSA, 2002, [En línea]. Disponible en: http://pendientedemigracion.ucm.es/info/multidoc/multidoc/cursos/verano/material/BLESA_JOSE%20ANTONIO/VideosobreIP.ppt

[P6] Norma ANSI/EIA/TIA 607-A. TIA, *Commercial Building Grounding (Earthing) and Bonding Requirements For Telecommunications,* Washington DC*,* 2002

[P7] Institute of Electrical and Electronics Engineers, *Powering and Grounding Electronic Equipment (IEEE 1100),* Washington DC*,* 2005

[P8] Dual DHCP DNS, *Dual DHCP DNS Server Installation and Configuration Manual,* 2010

[P9] J. Levin, *QMail,* United States of America, Marzo del 2004

Tesis:

[T1] J. Noguera, J. Vásquez. *Diseño e implementación de un circuito cerrado de televisión con cámaras ip inalámbricas y monitoreo remoto, notificación de eventualidades mediante el uso de un servidor para la grabación de video bajo Linux usando zoneminder para el laboratorio* de informática del edificio de Eléctrica-Química, Julio 2011, pag: 93 Tabla 2.13, [En línea]. Disponible en: http://bibdigital.epn.edu.ec/bitstream/15000/3947/1/CD-3718.pdf

[T2] O. Zambrano, A. Toala. *Implementación de un Sistema de Vigilancia utilizando una Web Cam, Asterisk y Teléfonos Grandstream*, 2009, [En línea]. Disponible en: http://www.dspace.espol.edu.ec/bitstream/123456789/8039/3/tesis.pdf

Páginas Web:

[PW1] Sin Autor, *Pila OSI de ISO*, Wikipedia, Abril 30 del 2012, [En línea]. Disponible en:http://upload.wikimedia.org/wikipedia/commons/thumb/7/7d/Pila-osi-es.svg/300px-Pila-osi -es.svg.png

[PW2] Sin Autor, *Encapsulación TCP/IP*, Junio 05 del 2012, [En línea]. Disponible en:http://www.textoscientificos.com/imagenes/redes/encapsulacion-tcp-ip.gif

[PW3] Sin Autor, SNAP in IEEE 802, Wikipedia, Septiembre 07 del 2012, [En línea]. Disponible en: http://upload.wikimedia.org/wikipedia/commons/a/ae/Snap_en_ _ieee802.gif

[PW4] Sin Autor, *Modelo de Referencia 802.11*, Noviembre 12 del 2012, [En línea]. Disponible en: http://cfile3.uf.tistory.com/image/122D47274AD8743 2151537

[PW5] Sin Autor, *Link Layer*, Junio 07 del 2012, [En línea]. Disponible en: http://www.technicalhowto.com/Networking/tcpip/images/wireless-ess.jpg

[PW6] Sin Autor, *Canales Wifi*, Junio 07 del 2012, [En línea]. Disponible en: http://img77.imageshack.us/img77/8585/80211boverlapdq6.png

[PW7] Sin Autor, *Dirección IP*, Mayo 11 del 2012, [En línea]. Disponible en: http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP

[PW8] Sin Autor, *Elementos de 568 C.0*, Junio 15 del 2012, [En línea]. Disponible en: http://2.bp.blogspot.com/_rM8VQ3CkAww/TNI32unrlII/AAAAAAAAACI/ffjqu8OUOcc/s1600/Dibujo3.bmp

[PW9] Sin Autor, *Parámetros de Rendimiento de Fibra Óptica*, Junio 06 del 2012, [En línea]. Disponible en: http://3.bp.blogspot.com/_rM8VQ3CkAww/TL-pXgOHFOI/AAAAAAAAABM/VxbScqSwPAs/s320/1.png

[PW10] Sin Autor, *Diagrama Cableado Estructurado*, Junio 15 del 2012, [En línea]. Disponible en: http://www.felipereyesvivanco.com/wp-content/uploads/2012/02/diagrama-Cabl-estruc.gif

[PW11] Sin Autor, *Normas T56A-T568B*, Junio 16 del 2012, [En línea]. Disponible en: http://4.bp.blogspot.com/-_IP7lHe0c-Y/UKPgnS-YVVI/AAAAAAAAABI/BewC4JasQDg/s200/cable-de-red-normas-t568a-t568b_1.gif

[PW12] Sin Autor, *Enlace extremo a extremo*, Junio 18 del 2012, [En línea]. Disponible en: http://www.fibraopticahoy.com/imagenes/2009/11/Figura-11-%E2%80%93-El-canal-representa-el-enlace-extremo-a-extremo-que-conecta-transmisor-y-receptor.jpg

[PW13] Sin Autor, *Comunicación y Tecnología: H.323 como jugando*, Julio 31 del 2013, [En línea]. Disponible en: https://lh4.googleusercontent.com/-jxfGjlAnoyg/TYuF_zlVc0I/AAAAAAAAAEo/_a1k0TFwXNs/s400/Arquitectura+H.323.bmp

[PW14] Cisco, *Components of SIP*, Junio 24 del 2012, [En línea]. Disponible en: http://www.mobilelife.eu/OSU/ece599/sip.jpg

[PW15] VoIP Foro, *Tabla Resumen Codecs*, Noviembre 20 del 2012, [En línea]. Disponible en: http://www.voipforo.com/codec/codecs.php

[PW16] GNU Project, *A Quick Guide to GPLv3*, Noviembre 25 del 2012, [En línea]. Disponible en: http://www.gnu.org/licenses/quick-guide-gplv3.html

[PW17] Linux Information Project, *BSD License Definition*, Noviembre 25 del 2012, [En línea]. Disponible en: http://www.linfo.org/bsdlicense.html

[PW18] Ministerio de Empleo y Seguridad España, *Encuestas: Metodología para su utilización*, Noviembre 22 del 2012, [En línea]. Disponible en: http://www.insht.es/InshtWeb/Contenidos/Documentacion/FichasTecnicas/NTP/Ficheros/201a300/ntp_283.pdf

[PW19] Moodle.org, *Cuantos usuarios soporta Moodle*, Diciembre 12 del 2012, [En línea]. Disponible en: https://moodle.org/mod/forum/discuss.php?d=157923

[PW20] *Puesta a Tierra de las Instalaciones*, Diciembre 04 del 2012, [En línea]. Disponible en: http://www.marcombo.com/Descargas/8496334147-INSTALACIONES%20EL5C3%89CTRICAS%20DE%20INTERIOR/UNIDAD%2010.pdf

[PW21] Para-Rayos, *Manual de Puesta a Tierra Thor-Gel*, Diciembre 04 del 2012, [En línea]. Disponible en: http://www.para-rayos.com/datos/gel20061.pdf

[PW22] Computer Protection Technology, *Sizing UPS*, Diciembre 07 del 2012, [En línea]. Disponible en: http://www.cptups.com/sizing.htm

[PW23] F. Félix, *Servidor – Linux Reporte de Navegación de Usuarios SARG*, Diciembre 12 del 2012, [En línea]. Disponible en: ftp://www.avmeiecuador.com/pub/manuales/mikrotik/mikrotik/SARG-VILCANET-Nov-2011.pdf

[PW24] D. Marcano.(s/f). *Conceptos y Elementos Básicos del Tráfico en Telecomunicaciones,* 21 Noviembre del 2012, [En línea]. Disponible en: http://departamento.pucp.edu.pe/ingenieria/images/documentos/seccion_telecomunicaciones/Capitulo%205%20Modelos%20de%20Trafico.pdf

[PW25] E. Magaña, E. Izkue. *Comunicaciones y Redes de Computadores: Problemas y Ejercicios Resueltos,* 21 de Noviembre del 2012, [En línea]. Disponible en: http://books.google.com.ec/books?id=GlP058nlPa4C&pg=

PA62&lpg=PA62&dq=tabla+erlang+b&source=bl&ots=q4TzAI0NX8&sig=ptjqbzlCCXx_zCxT3nb39Fhnh_k&hl=es&sa=X&ei=h8VyUfraK4Hc8wTiooFQ&ved=0CH8Q6AEwDQ#v=onepage&q=tabla%20erlang%20b&f=false

[PW26] Levinton. *CAT 6A Reference Guide*. (Cap. 2), pag. 11. 24 de Septiembre del 2012, [En línea]. Disponible en: http://www.leviton.com/OA_HTML/ibcGetAttachment.jsp?cItemId=d9GnxKOzUAGOmEq4cFvGQ&label=IBE&appName=IBE&minisite=10251

[PW27] Sin Autor, *Preparing a System for Asterisk*, 30 de Noviembre del 2012. Disponible en: http://www.asteriskdocs.org/en/3rd_Edition/asterisk-book-html-chunk/asterisk-InstallationPlanning.html

[PW28] VoIPForo, *Codecs : g711, g729, iLBC, gsm*; 02 deDiciembre del 2012, [En línea]. Disponible en: http://www.voipforo.com/codec/codecs.php

[PW29] VoIPInfo.org.*Dimensionig a Asterisk System,* 02 de Diciembre del 2012, [En línea]. Disponible en: http://www.voip-info.org/wiki/view/Asterisk+dimensioning

[PW30] Sin Autor*. Dimensionig a Asterisk System,* 02 de Diciembre del 2012, [En línea]. Disponible en: http://technet.microsoft.com/es-ec/library/aa998670%28v=exchg.141%29.aspx

[PW31] Linux Para Todos*. Servidor de Correo Electrónico,* 04 de Diciembre del 2012, [En línea]. Disponible en: http://www.linuxparatodos.net/portal/staticpages/index.php

[PW32] S.A*. web server maximum number of users apache can handle?,* 05 de Diciembre del 2012, [En línea]. Disponible en: http://stackoverflow.com/questions/10747548/web-server-maximum-number-of-users-apache-can-handle

[PW33] Linux Para Todos. *Servidor FTP,* 15 de *Junio* del 2012, [En línea]. Disponible en: http://www.linuxparatodos.net/portal/staticpages /index.php?page=servidor-ftp

[PW34] Novell Incorporated. *SUSE Linux Enterprise Server Administration Guide,* 24 de Julio del 2012, [En línea]. Disponible en: http://doc.opensuse.org/products/draft/SLES/SLES-admin_sd_draft

[PW35] Ubuntu Documentation Team. *Preparing to install,* 24 de Julio del 2012, [En línea]. Disponible en: https://help.ubuntu.com/10.04/serverguide/preparing-to-install.html#id2829267

[PW36] Cisco.*Cisco Catalyst 2960-S and 2960 Series Switches with LAN Base Software,* 25 de Agosto del 2012, [En línea]. Disponible en: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/product_data_sheet0900aecd80322c0c.html

[PW37] HP. *HP 2530 Switch Series,* 25 de Agosto del 2012, [En línea]. Disponible en:http://h17007.www1.hp.com/us/en/networking/products/switches/HP_2530_Switch_Series/index.aspx#tab=TAB3

[PW38] Sin Autor. *Customize with Asterisk Features,* 12 de Mayo del 2012, [En línea]. Disponible en: http://www.asterisk.org/get-started/features

[PW39] Sin Autor. *GNU Gatekeeper - a free VOIP Gatekeeper for H.323,* 12 de Mayo del 2012, [En línea]. Disponible en: http://www.gnugk.org

[PW40] Cisco. *Cisco Unified SIP Phone 3911,* 16 de Junio del 2012, [En línea]. Disponible en: http://www.cisco.com/en/US/prod/collateral/voicesw/ ps6788 /phones/ps7193/ps8486/product_data_sheet0900aecd8069cc65.html

[PW41] HP. *Teléfono IP HP 3500B (JC505A)especificaciones,* 16 de Junio del 2012, [En línea]. Disponible en: http://h10010.www1.hp.com/wwpc/ec/ es/sm/WF06b/12883-12883-4172263-4172269-4172269-4276977-4276983.html?dnr=1

[PW42] Cisco. *Cisco Video Surveillance 2520 Series,* 3 de Julio del 2012, [En línea]. Disponible en: http://www.cisco.com/en/US/prod/collateral/ps6712/ps9692/ps10304/data_sheet_c78-527843.pdf

[PW43] D-Link. *DCS-6111 - US Revision A,* 3 de Julio del 2012, [En línea]. Disponible en: http://www.dlink.com/-/media/Business_Products/ DCS/DCS%206111/Datasheet/DCS%206111_Datasheet_EN_US.pdf

[PW44] Cisco. *Cisco Video Surveillance 2900 Series Standard Definition IP PTZ Cameras,* 3 de Julio del 2012, [En línea]. Disponible en: http://www.cisco.com/en/US/prod/collateral/ps6712/ps9692/ps11252/datasheet_c78-624214.pdf

[PW45] D-Link. *DCS-6818 - Revision A,* 3 de Julio del 2012, [En línea]. Disponible en: http://www.dlink.com/-/media/Business_Products/DCS/DCS%206818/Datasheet/DCS%206818_Datasheet_EN_US.pdf

[PW46] Internet Systems Consortium. *BIND 9 Administrator Reference Manual,* 8 de Septiembre del 2012, [En línea]. Disponible en: http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.pdf

[PW47] Sin Autor. *djbdns: Domain Name System tools,* 8 de Septiembre del 2012, [En línea]. Disponible en: http://cr.yp.to/djbdns.html

[PW48] PowerDNS BV. *PowerDNS manual,* 8 de Septiembre del 2012, [En línea]. Disponible en: http://doc.powerdns.com/html/index.html

[PW49] Internet Systems Consortium.*DHCP,* 10 de Septiembre del 2012, [En línea]. Disponible en: http://www.isc.org/downloads/dhcp/

[PW50] E. Allman, C. Assmann, G. Neil. *Sendmail Installation And Operation Guide,* 10 de Septiembre del 2012, [En línea]. Disponible en: http://www.sendmail.com/pdfs/open_source/installation_and_op_guide.pdf

[PW51] Sin Autor. *Postfix Documentation,* 10 de Septiembre del 2012, [En línea]. Disponible en: http://www.postfix.org/documentation.html

[PW52] Sin Autor. *OpenLdap Documentation,* 13 de Septiembre del 2012, [En línea]. Disponible en: http://www.openldap.org/doc/admin24/

[PW53] Sin Autor. *389 Directory Server Documentation,* 13 de Septiembre del 2012, [En línea]. Disponible en: http://directory.fedoraproject.org/ wiki/ Documentation

[PW54] Sin Autor. *Basic User Guide Apache DS,* 13 de Septiembre del 2012, [En línea]. Disponible en: http://directory.apache.org/apacheds/basic-user-guide.html

[PW55] Sin Autor. *Documentation,* 21 de Septiembre del 2012, [En línea]. Disponible en: http://www.pureftpd.org/project/pure-ftpd/doc

[PW56] Sin Autor. *vsftpd, 2*1 de Septiembre del 2012, [En línea]. Disponible en: https://security.appspot.com/vsftpd.html

[PW57] Sin Autor. *ProFTPD Highly configurable GPL-licensed FTP server software, 2*1 de Septiembre del 2012, [En línea]. Disponible en: http://www.proftpd.org/docs/

[PW58] Sin Autor. *squid : Optimising Web Delivery, 2*5 de Septiembre del 2012, [En línea]. Disponible en: http://www.squid-cache.org/Doc/config/

[PW59] Sin Autor. *Privoxy 3.0.21 User Manual, 2*5 de Septiembre del 2012, [En línea]. Disponible en: http://www.privoxy.org/user-manual/index.html

[PW60] Sin Autor. *Resource Manager Administration, 10* de Octubre del 2012, [En línea]. Disponible en: http://community.zenoss.org/community/ documentation/servicedynamics/resource_manager_administration/4.1-v01

[PW61] Sin Autor. *Nagios Documentation, 10* de Octubre del 2012, [En línea]. Disponible en: http://www.nagios.org/documentation

[PW62] Sin Autor. *Instructor Handbook, 12* de Octubre del 2012, [En línea]. Disponible en: http://help.atutor.ca/common/print.php?instructor

[PW63] Sin Autor. *Manual completo Administrador y Profesor, 12* de Octubre del 2012, [En línea]. Disponible en: chamilo.googlecode.com/files/Chamilo-1.8.8.4-Guia-Admin-Docente-es.pdf

[PW64] Sin Autor. *Página Principal Documentación Moodle, 12* de Octubre del 2012, [En línea]. Disponible en: http://docs.moodle.org/all/es/P%C3% A1gin a_Principal

[PW65] Sin Autor. D*ocumentación del Servidor de HTTP Apache, 12* de Octubre del 2012, [En línea]. Disponible en: http://httpd.apache.org/docs/2.4/

[PW66] Sin Autor. *Documentation Index,* 14 de Octubre del 2012, [En línea]. Disponible en: http://tomcat.apache.org/tomcat-8.0-doc/index.html

[PW67] Sin Autor. *Cherokee 1.2 documentation,* 14 de Octubre del 2012, [En línea]. Disponible en: http://cherokee-project.com/doc/

GLOSARIO

[1]**FTP**: protocolo de red para la transferencia de archivos entre sistemas conectados a una red, basado en el modelo cliente-servidor.

[2]**HTTP**: protocolo utilizado por las páginas web, que funciona de modo cliente servidor. Éste protocolo se ubica en la capa de Aplicación de modelo OSI.

[3]**DNS**: base de datos distribuida que almacena información de nombres de dominio en redes como Internet, cuya función más importante, es traducir estos nombres de dominio en direcciones IP asociadas con los equipos conectados a la red.

[4]**Nodo**: es cualquier estación de trabajo, terminal, ordenador personal, impresora o cualquier otro dispositivo conectado a la red.

[5]**IEEE**: son las siglas de Institute of Electrical and Electronic Engineers (Instituto de Ingenieros Eléctricos y Electrónicos), una asociación técnico-profesional mundial dedicada a la estandarización e investigación.

[6]**Switch** es un dispositivo digital de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI y sus características principales son: tantos dominios de colisión como puertos tenga el switch, cada estación puede utilizar todo el tiempo el canal de transmisión, y usa el aprendizaje de direcciones MAC para conmutar el tráfico por el puerto de salida correcto.

[7]**Half-Duplex**: término que indica que se puede enviar y recibir información por la red pero no de forma simultánea.

[8]**Full-Duplex**: término que indica que se puede enviar y recibir información por la red de forma simultánea.

[9]**Mbps**: M es un prefijo que representa un factor de multiplicación de 10^6 que afectará a la cifra numérica delante de esta expresión; y bps es la unidad en la que se mide la velocidad de transmisión de datos (1 [bps] =1 [bit]/1 [segundo]. Bit es la unidad básica de la información digital).

[10]**Access Point**: es un dispositivo de conectividad que cumple funciones como la autenticación y desautenticación de estaciones de trabajo, envío y recepción de datos y proporciona privacidad a la red inalámbrica.

[11]**U-NII**: Unlicensed National Information Infraestructure.

[12]**Indoor**: significa que el ambiente donde trabajan los dispositivos de red está en el interior de una oficina o edificio.

[13]**Outdoor**: significa que el ambiente donde trabajan los dispositivos de red está en exteriores.

[14]**Host**: término usado para referirse a dispositivos conectados en red.

[15]**Mulicast**: transmisión de una trama de datos hacia un grupo determinado de hosts que tienen configurado la misma dirección IP de multicast.

[16]**Loopback**: dirección IP utilizada para que el tráfico dirigido hacia esa dirección sea redirigido devuelta hacia host emisor. Esto es utilizado para pruebas de conectividad.

[17]**Broadcast:** transmisión de una trama hacia todos los dispositivos presentes en la red.

[18]**Patch Cord**: cable UTP o STP utilizado para conectar un dispositivo de red con otro

[19]**Softphone**: software que hace una simulación de un teléfono convencional y que permite usar una computadora para hacer llamadas a otros softphones o a otros teléfonos.

[20]**PSTN** (Public Switched Telephone Network): Red Telefónica Pública Conmutada. Red utilizada principalmente para la telefonía analógica pública.

[21]**Unicast**: transmisión de una trama de datos entre un host emisor y un host receptor pertenecientes a una red.

[22]**Bit rate**: indica la cantidad de información que se manda por segundo.

[23]**H.324**: estándar de videoconferencia y video telefonía en redes de conmutación de circuitos.

[24]**H.320**: recomendación para transmitir datos multimedia sobre la Red Digital de Servicios Integrados.

[25]**RTSP** (Real Time Streaming Protocol): protocolo de control diseñado para sistemas que envían flujos información multimedia.

[26]**Código Fuente**: es el núcleo del programa junto con sus librerías presentadas en un formato legible por un programador.

[27]**Código Binario**: nombre que se le da al código del programa que es ejecutado por el ordenador.

[28]**Faceplate**: es una placa en la que se instalan puntos de red para que los usuarios accedan a la red local.

[29]**U (Unidad de Rack):** unidad de medida que indica la dimensión de un equipo que va a ser montado sobre un rack.

[30]**Uplink**: es una conexión de alta velocidad entre los equipos de conectividad que trabajan en el mismo nivel del modelo OSI.

[31]**Peering:** acuerdo bilateral para la interconexión entre dos redes en internet administrativamente independientes con el propósito de intercambiar tráfico entre usuarios de cada una de las redes.

[32]**NAP Ecuador**: es la infraestructura de red que permite intercambiar localmente tráfico de Internet originado y terminado en el Ecuador.

[33]**PoE**: tecnología que incorpora la alimentación eléctrica para un dispositivo de red, a través del mismo cable Ethernet que se utiliza para la conexión a la red.

[34]**SFP (Small Form-factor Pluggable):** es una interfaz para la conexión de cables de fibra o de cobre que soporta velocidades de hasta 1 Gbps.

[35]**SFP+ (Enhaced Small Form-factor Pluggable):** es una interfaz para la conexión de cables de fibra o de cobre que soporta velocidades de 10 Gigabit Ethernet.

[36]**Site Survey Pasivo**: es el escaneo de una área o edificación para determinar si existen redes inalámbricas que puedan causar interferencia, identificar las zonas y canales de frecuencia más adecuados, para que ésta interferencia sea mínima o nula con la red inalámbrica que se desea instalar.