PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

SEDE AMBATO

DEPARTAMENTO DE INVESTIGACIÓN, POSGRADOS Y AUTOEVALUACIÓN

Tema:

"REDISEÑO DE LA RED DE CAMPUS CON CALIDAD DE SERVICIOS DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO"

Tesis de grado previo a la obtención del título de Magíster en Gerencia Informática con mención en redes y desarrollo de software

Autor:

ING. VERÓNICA MARIBEL PAILIACHO MENA

Director:

ING. MSC. DIEGO ÁVILA PESÁNTEZ

Ambato – Ecuador

Julio, 2008

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

DEPARTAMENTO DE INVESTIGACIÓN, POSGRADOS Y AUTOEVALUACIÓN

HOJA DE APROBACIÓN

Tema:

"REDISEÑO DE LA RED DE CAMPUS CON CALIDAD DE SERVICIOS DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO"

Autor:

ING. VERÓNICA MARIBEL PAILIACHO MENA

Ing. Msc. Diego Ávila DIRECTOR DE TESIS.	f. _____
Ing. Msc. Patricio Medina CALIFICADOR.	f. _____
Ing. Msc. Andrés López CALIFICADOR.	f. _____
Ing. Telmo Viteri JEFE DEL D.I.P.A.	f. _____
Dr. Pablo Poveda SECRETARIO GENERAL PUCESA.	f. _____

DECLARACIÓN DE AUTENTICIDAD

Y RESPONSABILIDAD

Yo, Verónica Maribel Pailiacho Mena portadora de la cédula de ciudadanía No. 060297023-8 declaro que los resultados obtenidos en la investigación que presento como informe final, previo la obtención del título de Magíster en Gerencia Informática con mención en Redes y Desarrollo de Software son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola y exclusiva responsabilidad legal y académica.

Ing. Verónica Pailiacho

AGRADECIMIENTO

A Dios todo poderoso que me dio la vida y la sabiduría, para alcanzar esta nueva meta.

A mis padres que me dieron el ser y me formaron con amor y espíritu de responsabilidad, persistencia y dedicación.

A mi esposo por su comprensión, paciencia y apoyo incondicional. A mi hermana y amigos que con sus palabras de aliento y motivación, me llenaron de coraje para continuar en la lucha del día a día

A la universidad y por ende a los maestros que compartieron sus conocimientos, experiencia y sobre todo su amistad.

Para todos ustedes gracias.

DEDICATORIA

El presente trabajo de investigación esta dedicado a mis padres por todo el sacrificio realizado durante toda su vida para darme la educación y formación de vida, a mi esposo Dennis por su optimismo, lealtad, comprensión y amor, a mi hermana por su apoyo incondicional en los momentos precisos.

Para ustedes con gratitud eterna.

RESUMEN

La infraestructura de la red LAN de la Pontificia Universidad Católica del Ecuador Sede Ambato juega un papel importante para una exitosa gestión al aplicar servicios de telecomunicaciones, por este motivo se decidió realizar un análisis sobre su funcionamiento real, tomando en cuenta los elementos activos y pasivos que conforman actualmente la red, así como el cumplimiento de las normas de Cableado Estructurado y niveles de satisfacción de los usuarios. Los principales problemas detectados fueron: red plana por consecuencia existencia de un solo dominio de broadcast, red poco escalable, falta de mecanismos de seguridad y monitoreo en la infraestructura de red, poco cumplimiento de las normas de cableado estructurado. La propuesta de rediseño de la red de campus con Calidad de Servicio para la PUCESA resuelve los problemas detectados permitiendo obtener una red apta para implementar nuevos servicios a futuro como son: videoconferencia, VoIP, sistemas de seguridad IP y por supuesto mejorar la transferencia, disponibilidad y seguridad de la red LAN. El desarrollo de la presente propuesta se basa en dos fases: Análisis y Diseño, primero se realizó el análisis de requerimientos y de flujos de datos, para luego pasar al diseño que incluye selección de tecnología, diseño lógico, diseño de VLAN´s y el diseño físico. Sin dejar de lado las políticas de seguridad para la administración y monitoreo de la red.

ABSTRACT

The LAN network infrastructure at the Catholic University of Ecuador in Ambato plays an important role for a successful administration when applying telecommunications services. For this reason, an analysis on its real operation was carried out, taking into account the active and passive elements that make up the network at the moment, as well as the execution of the norms of having structured wire and levels of the users' satisfaction. The main detected problems were: a flat net due to the existence of a single broadcast domain, a little scalable network, lack of security mechanisms and monitoring in the net infrastructure, and little execution of the norms of structured wire. The proposal to redesign the campus network with Quality of Service for Catholic University of Ecuador in Ambato solves the detected problems by allowing the user to obtain a capable network to implement new services for the future such as: videoconferences, VoIP, security systems IP and of course to improve the transfer, accessibility and security of the LAN network. The development of this proposal is based on two phases: Analysis and Design. First, the analysis of requirements and flow of data were carried out, then, the design was considered. It includes technology selection, logical design, design of VLAN´s and the physical design, without leaving aside security policies for the network administration and monitoring.

TABLA DE CONTENIDO

TABLA DE GRÁFICOS

TABLAS

CAPÍTULO I

1. PROYECTO DE INVESTIGACIÓN

1.1. Antecedentes

Actualmente, el manejo de la información de modo eficiente constituye una de las principales preocupaciones dentro de cualquier organización, sea esta de origen público o privado, por lo que se hace necesario manejarla y emplearla con mucho criterio, ya que de ello podría depender, en gran medida, el éxito o fracaso de las mismas.

Para compartir información se usan las redes de campus que consisten en un medio de transmisión compartido y un conjunto de software y hardware que sirve de interfaz entre dispositivos y el medio, para regular el orden de acceso al mismo y lograr con estas redes, velocidades de transmisión de datos altas en distancias relativamente cortas.

Al implementar una red de campus, varios conceptos claves se presentan por si mismos. Uno es la elección del medio de transmisión que puede ser par trenzado, coaxial, fibra óptica o medios inalámbricos. Otro problema es cómo realizar el control de acceso a un medio compartido pues resulta

necesario algún mecanismo para regular el acceso al medio de forma eficiente y rápida. Además se debe escoger la topología de red a implementarse, todas estas claves deben basarse en los estándares de cableado estructurado.

La Pontificia Universidad Católica del Ecuador Sede Ambato, cuenta con una red de campus implementada en el edificio principal, la misma que fue creciendo con el tiempo y fue desarrollada para cubrir los requerimientos de momento sin tomar en cuenta las normas y estándares de diseño de redes de campus. En la actualidad existen demoras en el rendimiento de la misma, excesiva cantidad de hubs y switches no administrables, entre otras cosas, por lo que es necesario rediseñarla tomando en cuenta requerimientos, normas y estándares.

1.2. Planteamiento Del Problema

Esta investigación plantea como base: El incumplimiento de estándares de cableado estructurado en la red de campus de la PUCESA lo que está generando deficiencias en su rendimiento, por lo que se requiere del Rediseño de la misma para así mejorar su administración y ofrecer calidad de servicios.

1.3. Problematización

- Falta de un estudio de los requerimientos de la red de campus.
- Crecimiento desmedido y problemático de dispositivos pasivos y activos. Dando como consecuencia una excesiva cantidad de Switches no administrables y Hubs.
- La red de campus actual no ofrece calidad de servicios en su infraestructura.
- Necesidad de usar herramientas de administración de redes que permitan conocer las verdaderas causas de fallas en el rendimiento de la red.

1.4. Delimitación

El presente proyecto será realizado en la Pontificia Universidad Católica del Ecuador, ubicada en la Provincia de Tungurahua, en el cantón Ambato. Esta solución se desarrollará para el edificio principal de la Universidad y está previsto realizarlo en el periodo de Marzo del 2007 a Julio del 2007.

Esta investigación consta de los siguientes aspectos: Análisis del diseño actual de la red de campus (Diagnóstico), Análisis de requerimientos actuales y Propuesta del rediseño de la red de campus del Edificio Principal de la PUCESA.

1.5. Justificación

La Pontificia Universidad Católica del Ecuador Sede Ambato ha pasado por procesos de modernización tanto en su estructura organizacional como en el soporte tecnológico, en tal sentido en los últimos 9 años las plataformas tecnológicas han sufrido permanentes cambios, con el propósito de alinearse a las nuevas tendencias tecnológicas, en lo que a redes se refiere.

Sin embargo no existe un estudio en el que se detalle el análisis de requerimientos realizado, el diseño planteado y las normas utilizadas en la implementación de la red de campus, lo que indica que la misma fue implementada por diferentes personas para resolver problemas de momento.

En el departamento de sistemas (Laboratorios) de la PUCESA, trabajan 3 personas, las mismas que han sabido manifestar la existencia de ciertos problemas de rendimiento, transmisión de datos, excesiva cantidad de hubs y switches no administrables, poca utilización de normas y estándares de cableado estructurado.

Por lo que se presenta la oportunidad de proponer un Rediseño de la red de campus del edificio principal de la Pontificia Universidad Católica del Ecuador Sede Ambato, la misma que estará basada en los estándares de cableado estructurado para mejorar su administración y ofrecer calidad de servicios. Con esta investigación se pretende proporcionar una guía de trabajo para que en el futuro se proceda con su implementación.

1.6. Objetivos

1.6.1. Objetivo General

- Rediseñar la red de campus del edificio principal de la Pontificia Universidad Católica del Ecuador Sede Ambato basado en los estándares de cableado estructurado, para mejorar su administración y ofrecer calidad de servicios.

1.6.2. Objetivos Específicos

- Analizar los requerimientos actuales de usuarios, aplicaciones, host y red para rediseñar la red de campus basada en estos.
- Rediseñar la red de campus tomando en cuenta el crecimiento de puntos de red a futuro.
- Ofrecer calidad de servicios en la infraestructura propuesta.
- Establecer políticas de administración y gestión de la red de campus, que involucren el uso de herramientas de administración de redes.

1.7. Hipótesis

Partiendo de los estándares de cableado estructurado será posible rediseñar la red de campus de la Pontificia Universidad Católica del Ecuador Sede Ambato para así mejorar su administración y ofrecer calidad de servicios.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Tecnología LAN

Una red LAN consiste en un medio de transmisión compartido y un conjunto de software y hardware para servir de interfaz entre dispositivos y el medio y regular el orden de acceso al mismo, lo que se desea lograr con estas redes es velocidades de transmisión de datos altas en distancias relativamente cortas.

Al implementar una red LAN, varios conceptos claves se presentan por si mismos. Uno es la elección del medio de transmisión, el cual pueden ser par trenzado, coaxial, fibra óptica o medios inalámbricos. Otro problema de diseño es como realizar el control de acceso, con un medio compartido resulta necesario algún mecanismo para regular el acceso al medio de forma eficiente y rápida. Los dos esquemas más comunes son CSMA/CD tipo Ethernet y anillo con paso de testigo.

El control de acceso al medio a su vez está relacionado con la topología que adopte la red. De esta manera podemos decir que los aspectos tecnológicos principales que determinan la naturaleza de una red LAN son:

- Topología
- Medio de transmisión
- Técnica de control de acceso al medio

2.1.1. Topologías

Las topologías usuales en LAN son bus, anillo y estrella.

Topología en bus

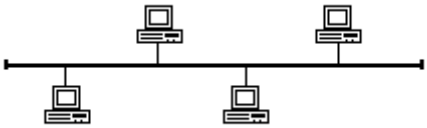


Gráfico 2.1: Topología en bus

Todas las estaciones se encuentran directamente conectadas, a través de interfaces físicas apropiadas conocidas como tomas de conexión, a un medio de transmisión lineal o bus.

Topología en anillo

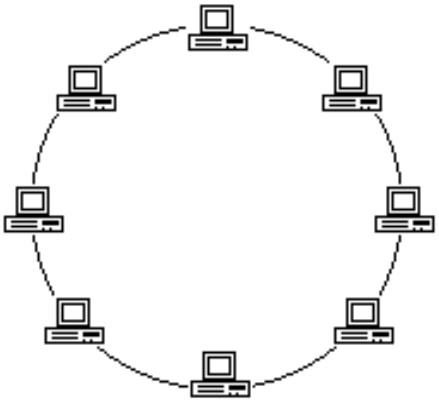


Gráfico 2.2: Topología en anillo

En esta topología, la red consta de un conjunto de repetidores unidos por enlaces punto a punto formando un bucle cerrado. Los enlaces son unidireccionales, es decir, los datos se transmiten solo en un sentido de las agujas del reloj o en el contrario. Como en el resto de las topologías los datos se transmiten en tramas. Una trama que circula por el anillo pasa por las demás estaciones de modo que la estación destino reconoce su dirección y copia la trama, mientras esta la atraviesa, en una memoria temporal local. La trama continua circulando hasta que alcanza de nuevo la estación origen donde es eliminada del nodo.

Topología en estrella

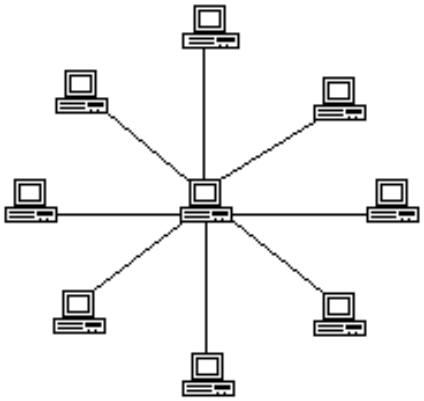


Gráfico 2.3: Topología en estrella

En redes LAN con topología en estrella cada estación esta directamente conectada a un nodo central, generalmente a través de dos enlaces punto a punto, uno para transmisión y otro para recepción. Aunque la disposición física es una estrella, lógicamente funciona como un bus; una transmisión desde cualquier estación es recibida por el resto de las estaciones y solo puede transmitir una estación en un instante de tiempo dado.

Otra aproximación es el funcionamiento del nodo central como dispositivo de conmutación de tramas. Una trama entrante se almacena en el nodo y se retransmite sobre un enlace de salida hacia la estación de destino.

2.1.2. Medios de Transmisión

2.1.2.1. Transmisión guiada

En medios guiados, el ancho de banda o velocidad de transmisión dependen de la distancia y de si el enlace es punto a punto o multipunto.

Par trenzado

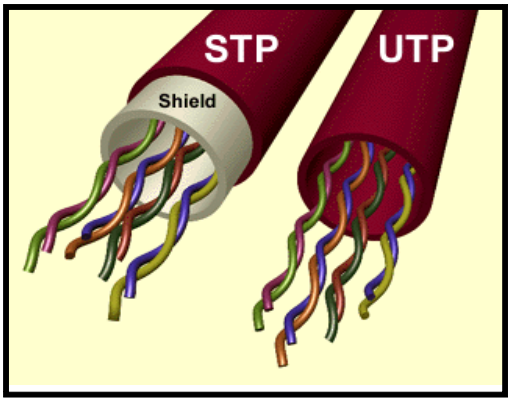


Gráfico 2.4: Par trenzado

Existe el par trenzado sin blindar conocido como UTP y el blindado conocido como STP. El primero es el soporte físico más utilizado en las redes LAN, pues instalación es barata y sencilla. Por él se pueden efectuar transmisiones digitales (datos) o analógicas (voz). Consiste en un mazo de conductores de cobre (protegido cada conductor por un dieléctrico), que están trenzados de dos en dos para evitar al máximo la Diafonía. Un cable de par trenzado puede tener pocos o muchos pares; en aplicaciones de

datos lo normal es que tengan 4 pares. Uno de sus inconvenientes es la alta sensibilidad que presenta ante interferencias electromagnéticas.

Fibra óptica

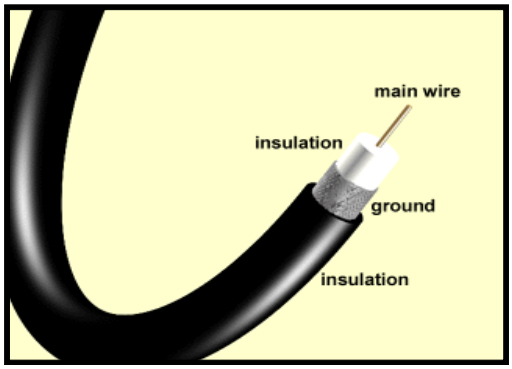


Gráfico 2.5: Fibra Óptica

Se trata de un medio muy flexible y muy fino que conduce energía de naturaleza óptica. Su forma es cilíndrica con tres secciones radiales: núcleo, revestimiento y cubierta.

El núcleo está formado por una o varias fibras muy finas de cristal o plástico. Cada fibra está rodeada por su propio revestimiento que es un cristal o plástico con diferentes propiedades ópticas distintas a las del núcleo. Alrededor de este conglomerado está la cubierta (constituida de material plástico o similar) que se encarga de aislar el contenido de aplastamientos, abrasiones, humedad, etc. Es un medio muy apropiado para largas distancias e incluso para LAN's.

Sus beneficios frente al par trenzado son:

- Permite mayor ancho de banda.
- Menor tamaño y peso.
- Menor atenuación.
- Aislamiento electromagnético.
- Mayor separación entre repetidores.

Su rango de frecuencias es todo el espectro visible y parte del infrarrojo. Su método de transmisión son los rayos de luz que inciden con una gama de ángulos diferentes en el núcleo del cable, los mismos que van rebotando a lo largo del cable hasta llegar a su destino. A este tipo de propagación se le llama multimodal. Si se reduce el radio del núcleo, el rango de ángulos disminuye hasta que sólo sea posible la transmisión de un rayo, el rayo axial, y a este método de transmisión se le llama monomodal.

Hay un tercer modo de transmisión que es un paso intermedio entre los anteriormente comentados y que consiste en cambiar el índice de refracción del núcleo. A este modo se le llama multimodo de índice gradual. Los emisores de luz utilizados son: LED (de bajo coste, con utilización en un amplio rango de temperaturas y con larga vida media) y ILD (más caro, pero más eficaz y permite una mayor velocidad de transmisión).

Distancias recomendadas de medios guiados

Medio de transmisión	Distancia entre		
	HCC y MCC	HCC e ICC	ICC y MCC
62.5 / 125 Cable de fibra óptica multimodo	2000 metros	500 metros	1500 metros
Fibra óptica monomodo	3000 metros	500 metros	2500 metros
UTP (voz)	800 metros	500 metros	300 metros
UTP (datos)	Limitado a un total de 90 metros		

Tabla 2.1: Distancias de medios guiados

MCC: main cross connect… cableado del armario principal

ICC: intermediate cross connect… cableado del armario de interconexión

HCC: horizontal cross connect… cableado del armario de planta

2.1.2.2. Transmisión inalámbrica

Se utilizan medios no guiados, principalmente el aire. Se radia energía electromagnética por medio de una antena y luego se recibe esta energía con otra antena.

Hay dos configuraciones para la emisión y recepción de esta energía: direccional y omnidireccional. En la direccional, toda la energía se concentra en un haz que es emitido en una cierta dirección, por lo que tanto el emisor como el receptor deben estar alineados. En el método omnidireccional, la energía es dispersada en múltiples direcciones, por lo que varias antenas

pueden captarla. Cuanto mayor es la frecuencia de la señal a transmitir, más factible es la transmisión unidireccional.

Por tanto, para enlaces punto a punto se suelen utilizar microondas (altas frecuencias). Para enlaces con varios receptores posibles se utilizan las ondas de radio (bajas frecuencias). Los infrarrojos se utilizan para transmisiones a muy corta distancia (en una misma habitación).

Microondas terrestres

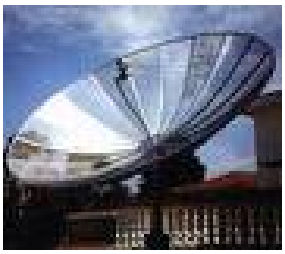


Gráfico 2.6: Microondas terrestres

Suelen utilizarse antenas parabólicas. Para conexiones a larga distancia, se utilizan conexiones intermedias punto a punto entre antenas parabólicas. Se suelen utilizar en sustitución del cable coaxial o las fibras ópticas ya que se necesitan menos repetidores y amplificadores, aunque se necesitan antenas alineadas. Se usan para transmisión de televisión y voz.

La principal causa de pérdidas es la atenuación debido a que las pérdidas aumentan con el cuadrado de la distancia y también aumenta con las lluvias.

Las interferencias es otro inconveniente de las microondas ya que al proliferar estos sistemas, puede haber más solapamientos de señales.

Microondas por satélite

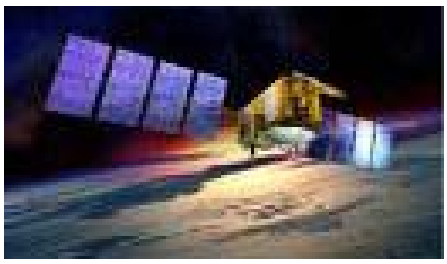


Gráfico 2.7: Microondas por satélite

El satélite recibe las señales y las amplifica o retransmite en la dirección adecuada. Para mantener la alineación del satélite con los receptores y emisores de la tierra, el satélite debe ser geoestacionario.

Se suele utilizar este sistema para:

- Difusión de televisión.
- Transmisión telefónica a larga distancia.
- Redes privadas.

El rango de frecuencias para la recepción del satélite debe ser diferente del rango al que este emite, para que no haya interferencias entre las señales que ascienden y las que descienden. Debido a que la señal tarda un pequeño intervalo de tiempo desde que sale del emisor en la Tierra hasta

que es devuelta al receptor o receptores, ha de tenerse cuidado con el control de errores y de flujo de la señal.

Las diferencias entre las ondas de radio y las microondas son:

- Las microondas son unidireccionales y las ondas de radio omnidireccionales.
- Las microondas son más sensibles a la atenuación producida por la lluvia.
- En las ondas de radio, al poder reflejarse estas ondas en el mar u otros objetos, pueden aparecer múltiples señales "hermanas".

Infrarrojos

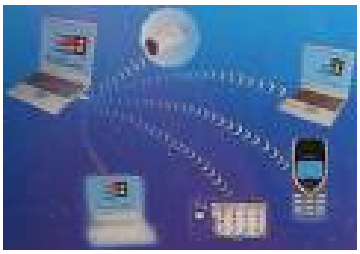


Gráfico 2.8: Infrarrojo

Los emisores y receptores de infrarrojos deben estar alineados o bien estar en línea tras la posible reflexión de rayo en superficies como las paredes. En infrarrojos no existen problemas de seguridad ni de interferencias ya que estos rayos no pueden atravesar los objetos (paredes por ejemplo).

Tampoco es necesario permiso para su utilización (en microondas y ondas de radio si es necesario un permiso para asignar una frecuencia de uso).

2.1.3. Ethernet y ethernet de alta velocidad (CSMA / CD)

Estas redes utilizan banda base sensible a la portadora y detección de colisiones. Algunas utilizan banda ancha. El estándar más utilizado es el IEEE 802.3.

2.1.3.1. Control de acceso al medio en IEEE 802.3

En estas redes, no hay un tiempo preestablecido de acceso al medio sino que cualquier estación puede acceder a él de forma aleatoria. Los accesos son de tipo competitivo.

La técnica más antigua utilizada es la ALOHA, que consiste en que si una estación quiere transmitir una trama, lo hace y espera el tiempo suficiente para que la estación de destino le de tiempo para confirmar la llegada de la trama . Si no llega la confirmación en ese tiempo, la estación vuelve a enviar la trama. Este proceso lo repite hasta que o bien recibe la confirmación o bien lo ha intentado una serie determinada de veces sin conseguir la confirmación. La estación receptora recibe la trama y si detecta que no hay error (mediante unos códigos) envía una confirmación. Puede ocurrir que dos tramas se interfieran (colisión) y entonces las dos son rechazadas, es decir que el receptor no envía confirmación.

El sistema ALOHA, aunque es muy sencillo, permite pocas cargas en la red ya que si hay muchas tramas circulando a la vez, la probabilidad de que interfieran (y sean erróneas) es muy grande.

La eficiencia de ALOHA es grande cuando las distancias entre estaciones es corta, ya que podría implementarse un mecanismo para que todas las estaciones dejaran de transmitir cuando una trama circulara por la red (ya que la espera sería muy pequeña al ser la distancia poca). A esta técnica más sofisticada se le llama CSMA. Es decir, con CSMA, la estación que desee transmitir escucha el medio para ver si hay ya una trama en él, y si no la hay emite su trama y espera confirmación para cerciorarse de que ha llegado a su destino correctamente. Las colisiones sólo se producirán si dos estaciones emiten tramas casi en el mismo instante.

Para evitar esta última ineficiencia, CSMA hace:

1. El emisor transmite si la línea está libre y si no, se aplica 2.
2. En caso de que el medio esté ocupado, se espera hasta que esté libre.
3. Si se detecta una colisión, el emisor que la ha detectado envía una señal de interferencia para que todas las estaciones sepan de la colisión y dejen de transmitir (para dejar de colisionar).
4. Después de emitir la interferencia, se espera un poco y se vuelve a emitir la trama.

De esta forma, CSMA sólo desaprovecha el tiempo en que se tarda en detectar una colisión. Dependiendo de la técnica de transmisión, la detección de colisión cambia.

2.1.3.2. Estándares de medios de transmisión

Estándar	Acceso al medio	Medio Físico	Distancia máxima	Observaciones
10Base 5	802.3	Cable coaxial de 50 ohms. N-Style. Utiliza interfaces AUI.	500 m	Soporta hasta 208 usuarios, conectores AUI. Utilizando repetidores la distancia máxima entre host en un mismo dominio de colisión es de 2500m.
10Base2	802.3	Cable coaxial de 50 ohms. RG-58 con conetor BNC	185 m	Soporta hasta 30 terminales conectadas en un mismo segmento. Topología en bus serial.
10BaseF	802.3	Denominación genérica para referirse a tecnologías Ethernet de 10 Mbps sobre cables de fibra óptica.		
10BaseT	802.3	Utp cat 3, 4. 5 o 5e de 100 Ohms, con conectores RJ45	100 m	Topologia estrella, utiliza 2 pares de cables de un cable de par trensado
100Base FX	802.3u	Dos hilos de fibra óptica multimodo de 62.5 / 125 micrones	412 m	Conectores ST o SC. Topologia en estrella
100Base TX	802.3u	Cable UTP cat 5, 5e, 6 o 7 o STP cat 1 de 100 Ohms., conectores RJ45 (EIA/TIA) 568	100 m	Fast Ethernet. Topologia estrella, utiliza 2 pares de cables
1000Base T	802.3ab	UTP cat 5e o 6 de 100 Ohms con conector RJ45	100 m	Utiliza 4 pares de cables para generar4 circuitos de transmisión full-duplex
1000Base CX	802.3z	Par trensado decbreblindado con conector RJ45	25 m	Diseñado para cubrir pequeñas distancias entre servidores, topologia en estrella
1000Base SX	802.3z	Fibra optica multimodo de 62.5 / 125 micrones con conectores SC	220 m	Utiliza un emisor de láser de 850nm. Opera como full-duplex
1000Base LX	802.3z	Fibra optica multimodo o monomodo de 9 /	Multimodo 550m. Monomono	Utiliza un emisor de láser de 1310nm. Topología en estrella

Estándar	Acceso al medio	Medio Físico	Distancia máxima	Observaciones
		125 micrones	5000m	
10GbE	802.3ae	Denominación general para redes Ethertnet de 10Gb sobre fibra optica. Prestan servicios como LAN, MAN o WAN. Operan solamente como full-duplex.		
10GBase-SR	802.3ae	Fibra multimodo de 62.5/125micrones 50/125 micrones	26 a 33m 66 a 300m	Utilizan un emisor de 850 nm
10GBase-LX4	802.3ae	Fibra multimodo de 62.5/125micrones 50/125 micrones	300m 240m	Utiliza multiplexación por división de longitud de onda.
		Fibra monomodo de 10 micrones	10 Km.	
10GBase-LR	802.3ae	Fibra monomodo de 10 micrones	10 Km.	Utiliza un emisor de 1310 nm.
10GBase-ER	802.3ae	Fibra monomodo de 10 micrones	30 Km.	Utiliza un emisor de 1550 nm.
10GBase-SW 10GBase-LW 10GBase-EW	802.3ae			Opera con equipamiento WAN para transporte sincrono

Tabla 2.2: Estándares de medios de transmisión

2.1.4. Qué es el Cableado Estructurado?

Por definición significa que todos los servicios en el edificio para las transmisiones de voz y datos se hacen conducir a través de un sistema de cableado en común.

Un sistema de cableado estructurado es la infraestructura de cable destinada a transportar, a lo largo y ancho de un edificio, las señales que emite un emisor de algún tipo de señal hasta el correspondiente receptor. Un sistema de cableado estructurado es físicamente una red de cable única y

completa. Permite la administración sencilla y sistemática de las mudanzas y cambios de ubicación de personas y equipos.

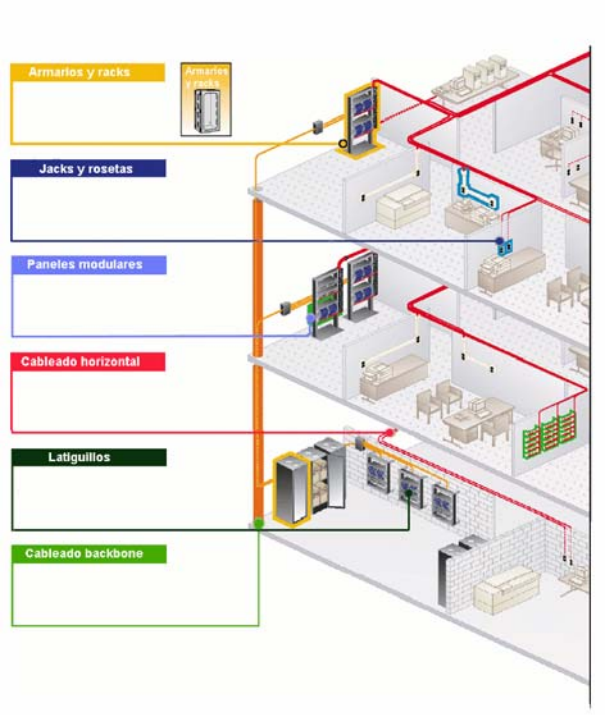


Gráfico 2.9: Cableado Estructurado

2.1.5. Normas y Estándares de Cableado Estructurado

- **ANSI/EIA/TIA-568-B:** Las topologías, la distancia máxima de los cables, el rendimiento de los componentes, las tomas y los conectores de telecomunicaciones.
- **EIA/TIA 569** - Rutas y espacios para cables de telecomunicaciones en una edificación.
- **EIA/TIA 606** - Administración de la infraestructura de telecomunicaciones para edificios comerciales.

- **EIA/TIA 607** - Tierra y junturas
- **EIA/TIA TSB 67** – Regula especificaciones de equipos de prueba, medición y certificación de cableado estructurado
- **EIA/TIA TSB 72** – Regula las especificaciones de sistemas centralizados de Fibra Óptica.
- **EIA/TIA TSB 75** – Regula lo referente a los espacios de las oficinas.
- **EIA/TIA TSB 95** – Equipos de prueba de nivel II mejorado. Certificación en la instalación de canales de categoría 5 para uso con 100Base T.
- Otra Norma es la **EIA/TIA 570** – Regula el cableado de telecomunicaciones residencial.

2.1.6. Elementos

A continuación se detallan los elementos más usuales:

KEYSTONE.- Se trata de un dispositivo modular de conexion monolinea, hembra, apto para conectar plug RJ45, que permite su inserción en rosetas y frentes de patch panels especiales mediante un sistema de encastre. Permite la colocación de la cantidad exacta de conexiones necesarias.

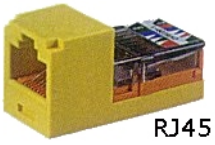


Gráfico 2.10: Keystone

ROSETA P/KEYSTONE.- Se trata de una pieza plástica de soporte que se amura a la pared y permite encastrar hasta 4 keystone, formando una roseta de hasta 4 bocas.

Gráfico 2.11: Roseta

FRENTE PARA KEYSTONE o FACEPLATE.- Se trata de una pieza plástica plana de soporte que es tapa de una caja estandard de electricidad embutida de 5x10 cm y permite encastrar hasta 4 keystone.

Gráfico 2.12: Faceplate

PATCH PANEL.- Están formados por un soporte, usualmente metálico y de medidas compatibles con rack de 19", que sostiene placas de circuito impreso sobre la que se montan: de un lado los conectores RJ45 y del otro los conectores IDC para block tipo 110. Se proveen en capacidades de 12 a 96 puertos (múltiplos de 12) y se pueden apilar para formar capacidades mayores.

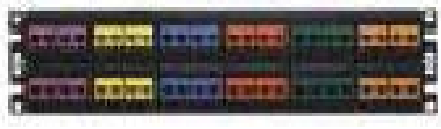


Gráfico 2.13: Patch Panel

PATCH CORD.- Están construidos con cable UTP de 4 pares flexible terminado en un plug 8P8C en cada punta de modo de permitir la conexión de los 4 pares en un conector RJ45. A menudo se proveen de distintos colores y con un dispositivo plástico que impide que se curven en la zona donde el cable se aplana al acometer al plug.

Gráfico 2.14: Patch cord

HERRAMIENTAS:

HERRAMIENTA DE IMPACTO.- Es la misma que se utiliza con block de tipo 110 de la ATT, la herramienta es de doble acción: inserta y corta el cable.

Gráfico 2.15: Herramienta de Impacto

HERRAMIENTA DE CRIMPEAR.- Es muy similar a la crimpeadora de los plugs americanos RJ11 pero permite plugs de mayor tamaño (8 posiciones). Permite: cortar el cable, pelarlo y apretar el conector para fijar los hilos flexibles del cable a los contactos.

Gráfico 2.16: Herramienta de Crimpear

PROBADOR RAPIDO DE CABLEADO.- Ideal para controlar los cableados por parte del técnico instalador. Permite detectar fácilmente: cables cortados o en cortocircuito, cables corridos de posición, piernas invertidas, etc.

Gráfico 2.17: Tester

2.1.7. Cableado Horizontal

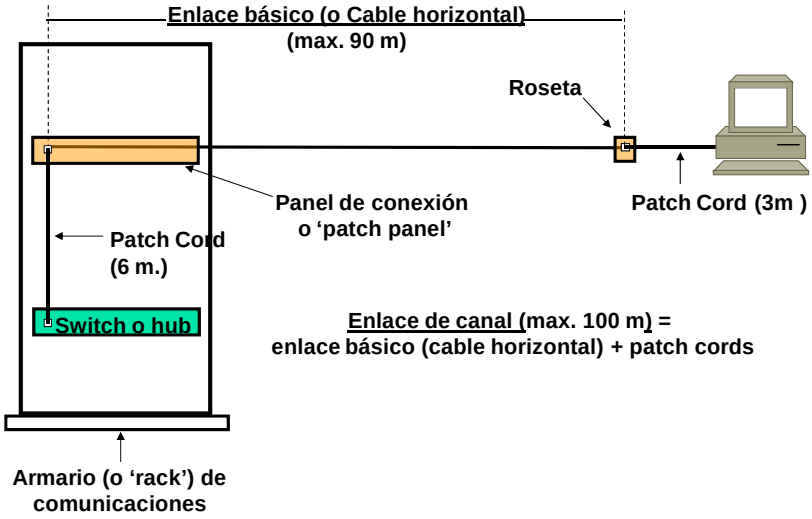


Gráfico 2.18: Cableado Horizontal

El término horizontal es utilizado debido a que típicamente el sistema de cableado se instala horizontalmente a través del piso o del techo del edificio. La norma EIA/TIA 568A define el cableado horizontal de la siguiente forma: "El sistema de cableado horizontal es la porción del sistema de cableado de telecomunicaciones que se extiende del área de trabajo al cuarto de telecomunicaciones (rack)".

El cableado horizontal consta de cable par trenzado, aunque si se requiere un alto rendimiento se puede utilizar fibra óptica. El cableado horizontal se debe implementar en una topología de estrella. Cada punto terminal de conexión de Datos y/o Voz debe estar conectado al Patch Panel.

Se debe tener en cuenta que no se permiten empates (múltiples apariciones del mismo par de cables en diversos puntos de distribución) en cableados de distribución horizontal. Se establece una conexión adicional entre el Patch Panel y el Switch, para que el equipo quede conectado a la red.

Consideraciones para el cableado horizontal:

Distancias Horizontales.- La máxima distancia horizontal permitida es de 90 metros (295 ft) independiente del tipo de medio. Esta es la distancia máxima entre el Patch Panel y el Terminal de conexión. La longitud máxima del punto terminal hasta la estación de trabajo es de 3 metros (9.8 ft).

Tipos de Cables.- Existen tres tipos de cables que pueden ser utilizados en los sistemas de cableado horizontal:

- Cable UTP (Unshielded Twisted Pair) de 4 pares a 100 W.
- Cable STP (Shielded Twisted Pair) de 2 pares a 150 W.
- Fibra Óptica 62.5/125 mm de 2 pares.

El cable a utilizar por excelencia es el par trenzado sin blindaje UTP de cuatro pares categoría 5.

Salidas de Área de Trabajo.- Los ductos a las salidas de área de trabajo (work area outlet, WAO) deben preveer la capacidad de manejar varios cables. Uno de los conectores debe ser del tipo RJ-45 bajo el código de colores de cableado T568A (recomendado) o T568B.

Manejo del cable.- El destrenzado de pares individuales en los conectores y paneles de empate debe ser menor a 1.25 cm. para cables UTP categoría 5. El radio de doblado del cable no debe ser menor a cuatro veces el diámetro del cable. Para par trenzado de cuatro pares categoría 5 el radio mínimo de doblado es de 2.5 cm.

Evitado de Interferencia Electromagnética.- A la hora de establecer la ruta del cableado de los closets de alambrado a los nodos es una consideración primordial evitar el paso del cable por los siguientes dispositivos:

- Motores eléctricos grandes o transformadores (mínimo 1.2 metros).
- Cables de corriente alterna
  - Mínimo 13 cm. para cables con 2KVA o menos
  - Mínimo 30 cm. para cables de 2KVA a 5KVA
  - Mínimo 91cm. para cables con mas de 5KVA
- Luces fluorescentes y balastros (mínimo 12 centímetros).
- El ducto debe ir perpendicular a las luces fluorescentes y cables o ductos

eléctricos.

- Intercomunicadores (mínimo 12 cms.)
- Equipo de soldadura
- Aires acondicionados, ventiladores, calentadores (mínimo 1.2 metros).
- Otras fuentes de interferencia electromagnética y de radio frecuencia.

2.1.8. Cableado Vertical

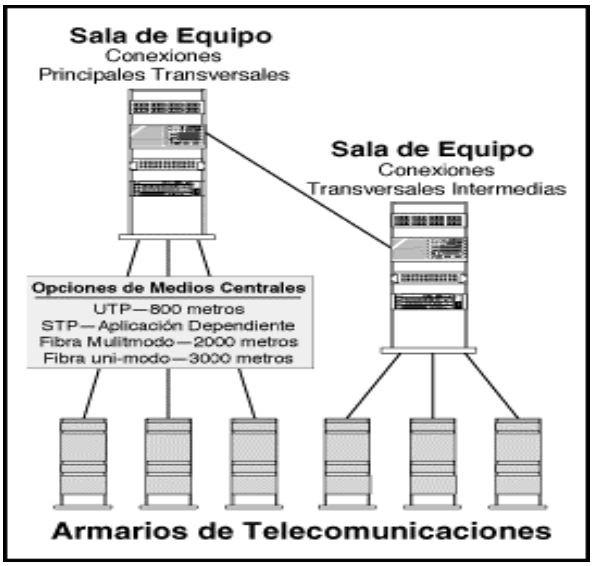


Gráfico 2.19: Cableado Vertical

Conocido tambien como backbone. El propósito del cableado del backbone es proporcionar interconexiones entre cuartos de entrada de servicios de edificio, cuartos de equipo y cuartos de telecomunicaciones. El cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos.

Para definir el backbone de datos es necesario tener en cuenta cuál será la disposición física del equipamiento. Normalmente, el tendido físico del

backbone se realiza en forma de estrella, es decir, se interconectan los gabinetes con uno que se define como centro de la estrella, en donde se ubica el equipamiento electrónico más complejo.

El backbone de datos se puede implementar con cables UTP o con fibra óptica. Actualmente, se utiliza fibra óptica por la mayor flexibilidad y posibilidad de crecimiento que brinda este medio. Se construye el backbone llevando un cable de fibra desde cada gabinete al gabinete centro de la estrella. Si bien para una configuración mínima ethernet basta con utilizar cable de 2 fibras, resulta conveniente utilizar cable con mayor cantidad de fibra (6 a 12) ya que la diferencia de costos no es importante y se posibilita por una parte disponer de conductores de reserva para el caso de falla de algunos.

La norma EIA/TIA 568 prevé la ubicación de la transmisión de cableado vertical a horizontal, y la ubicación de los dispositivos necesarios para lograrla, en habitaciones independientes con puerta destinada a tal fin, ubicadas por lo menos una por piso, denominadas armarios de telecomunicaciones. Se utilizan habitualmente gabinetes estándar de 19 pulgadas de ancho, con puertas, de aproximadamente 50 cm de profundidad y de una altura entre 1.5 y 2 metros. En dichos gabinetes se dispone generalmente de las siguientes secciones: Acometida de los puestos de trabajo: 2 cables UTP llegan desde cada puesto de trabajo. Acometida del backbone telefónico: cable multipar que puede determinar en regletas de conexión o en “patch panels”. Acometida del backbone de datos: cables de

fibra óptica que se llevan a una bandeja de conexión adecuada. Electrónica de la red de datos: Hubs, Switches, Bridges y otros dispositivos necesarios. Alimentación eléctrica para dichos dispositivos. Iluminación interna para facilitar la realización de trabajos en el gabinete. Ventilación a fin de mantener la temperatura interna dentro de límites aceptables.

Sistema de puesta a tierra y puenteado._ El sistema de puesta a tierra y puenteo establecido en estándar ANSI/TIA/EIA-607 es un componente importante de cualquier sistema de cableado estructurado moderno. El gabinete deberá disponer de una toma de tierra, conectada a la tierra general de la instalación eléctrica, para efectuar las conexiones de todo equipamiento. El conducto de tierra no siempre se halla indicado en planos y puede ser único para ramales o circuitos que pasen por las mismas cajas de pase, conductos ó bandejas. Los cables de tierra de seguridad serán puestos a tierra en el subsuelo.

2.2. Diseño

El Diseño toma como entrada el entendimiento de los requerimientos actuales y futuros de la red, la comprensión de la estructura y uso de la red existente, y determinar las funciones que debe cumplir el rediseño de la red o el diseño de la nueva red.

Cisco ha desarrollado el ciclo de vida de la red PDIOO que describe múltiples fases por las cuales pasa una red, como se ve en el gráfico 2.20

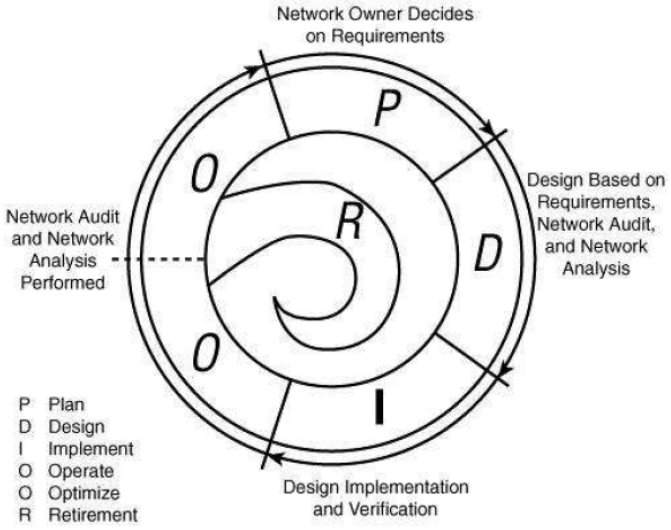


Gráfico 2.20: PDIOO

Plan.- consiste en identificar los requerimientos de la red y en observar la red existente (si existe).

Diseño.- La red es diseñada de acuerdo a los requerimientos iniciales y a los datos recolectados durante el análisis de la red existente. El diseño es refinado con el cliente.

Implementación.- La red es construida de acuerdo al diseño aprobado.

Operación.- La red es funcional y comienza a ser monitoreada. (Esta es la última prueba del diseño).

Optimización.- durante esta fase los problemas son detectados y corregidos

El Diseño de la red puede involucrar las siguientes tareas, como se muestran en el siguiente gráfico:

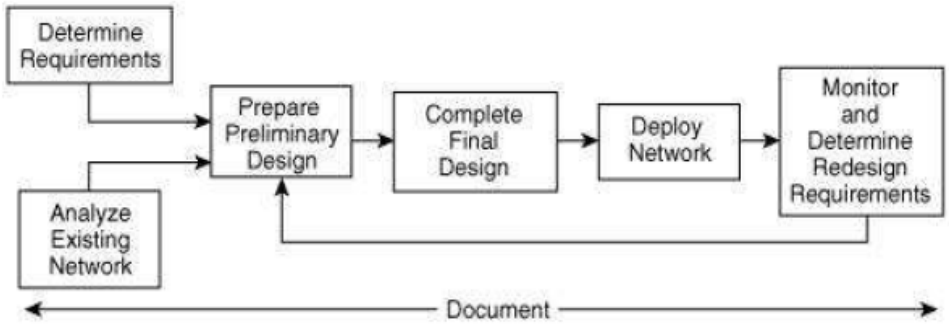


Gráfico 2.21: Diseño de red

1. Determinar los requerimientos
2. Analizar la red existente (si existe)
3. Preparar el diseño preeliminar
4. Desarrollar el diseño final
5. Implemetar la red
6. Monitorear y rediseñar si es necesario
7. Mantener actualizada la documentación

2.2.1. Determinar Requerimientos

Determinar los requerimientos de la red es parte del ciclo de vida de la red PDIOO. Muchos tipos de requerimientos deben ser considerados, incluyendo los técnicos y los del negocio, cualquier factor que pueda restringir el diseño debe ser identificado.

Los requerimientos técnicos y restricciones pueden ser:

- Aplicaciones que están funcionando en la red
- Conexión a Internet
- Restricciones en el uso de direcciones IP
- Soporte para direcciones IPv6
- Otros protocolos que estén corriendo en la red (Por ejemplo: router protocol)
- Requerimientos de cableado
- Requerimientos de redundancia
- Uso y existencia de equipos
- Servicios de Red (QoS, wireless)
- Seguridad integrada en la red
- Mantenimiento de la red
- Soporte para nuevas aplicaciones
- Disponibilidad de banda ancha

Los requerimientos y restricciones del negocio pueden ser:

- Presupuesto para los nuevos equipos y la implementación
- Planificación del tiempo
- Personal, incluye quien operará y administrará la red, la capacitación que estos requieran
- Revisión de contratos y asuntos legales
- Examinar la estructura de la red existente y determinar si cualquier

persona o grupo impedirá los cambios a realizarse

- Considerar las políticas de la organización para restringir el diseño de la red

2.2.2. Análisis de la red existente

Si se trata de un rediseño la red actual debe ser analizada y entendida, pues la existencia de la red es de alguna manera la restricción del diseño de la red. Por lo que se debe determinar qué esta bien y qué se debe cambiar.

Se recomienda que mientras se revisa la documentación de la red existente y se entrevista con los usuarios, administradores de la red, se puede ir realizando una auditoria de la red y así identificar items tales como los protocolos que están corriendo, dispositivos instalados, sus configuraciones y utilización de los mismos. Así se puede conocer el funcionamiento y distribución de los elementos actuales de la red.

Existen algunas herramientas de monitoreo de red que permiten conocer la información hardware y software de los dispositivos, analizar y diagnosticar los problemas de red, análisis de protocolos. Entre las herramientas que se pueden usar tenemos: Ethereal Network Analyzer y Observer.

2.2.3. Preparar el diseño preeliminar

El diseño preeliminar incluye los requerimientos técnicos y de negocio, así como las restricciones y determinar alternativas viables de solución. Entonces el administrador de la red es consultado y juntos escogen la mejor solución y esta solución es después desarrollada en el diseño final.

2.2.4. Desarollar el diseño final

El diseño final contiene dibujos detallados, especificación de configuraciones, plan de direccionamiento y cualquier otra información requerida para la implementación.

Se puede verificar el diseño implementando un prototipo de red, separado de la red existente y así verificar la consistencia del diseño.

2.2.5. Implementar la red

Para implementar la red se debe tomar en cuenta una planificación de actividades con sus respectivo tiempo de realización, es necesario desarrollar un Plan de Implementación en donde se detalla cómo y cuándo se realiza la implementación, así también se debería desarrollar un plan de contingencia en donde se defina los problemas que puedan ocurrir durante la implementación y cuál sería la mejor solución en caso de que este ocurra.

Si los administradores de la red requieren de alguna capacitación o entrenamiento este debe planearse en esta fase.

Cualquier problema de diseño encontrado en esta fase debe ser corregido y documentado.

2.2.6. Monitoreo y rediseño

Después de que la red este en funcionamiento, es necesario monitorearla para detectar anomalías y problemas. Si los problemas ocurridos requieren de un rediseño o si los requerimientos cambian o se incrementan se debe realizar el proceso de diseño entero para la segmento de red a cambiar o a toda la red si es necesario.

Por lo tanto la documentación del diseño debe contener:

- Todos los requerimientos y restricciones acordadas
- El estado de la red actual si existe
- Las alternativas del diseño preliminar y una breve descripción del porque fue escogida una de las alternativas.
- Detalles del diseño final
- Resultados del prototipo (si se realizó)
- Desarrollo de planes, planificación y otros detalles de la implementación
- Monitoreo de los requerimientos

2.3. Switching

Los switch´s pueden asegurar el rendimiento, flexibilidad y funcionalidad de una red. Las primeras redes fueron LAN, donde se habilitaban a múltiples usuarios en una pequeña área geográfica a intercambiar archivos, mensajes, a compartir recursos como impresoras y almacenamiento.

Un dispositivo de interconexión entre pc´s y servidores es el Hub. Dentro del modelo OSI este dispositivo es de capa 1 (Capa Física) básicamente extiende la funcionalidad de la red (LAN) para que el cableado pueda ser extendido a mayor distancia, es por esto que un "Hub" puede ser considerado como una repetidora. El problema es que el "Hub" transmite estos "Broadcasts" a todos los puertos que contenga, esto es, si el "Hub" contiene 8 puertos ("ports"), todas las computadoras que estén conectadas al "Hub" recibirán la misma información, y la mayoría de veces resulta innecesaria y excesiva, dando como resultado una red poco eficiente debido al dominio de Colisión existente.

Para mejorar el rendimiento de la red se utilizan switch´s que son dispositivos de capa 2, un switch es considerado un Hub inteligente, cuando es inicializado el switch, éste empieza a reconocer las direcciones MAC que generalmente son enviadas por cada puerto, en otras palabras, cuando llega información al switch éste tiene mayor conocimiento sobre que puerto de salida es el más apropiado, como se pude observar en el gráfico 11, y por lo tanto ahorra una carga (bandwidth) a los demás puertos del switch,

dividiendo los dominios de colisión de la red, esta es una de la principales razones por la cual en redes por donde viaja Vídeo o CAD, se procura utilizar switch´s para de esta forma garantizar que el cable no sea sobrecargado con información que eventualmente sería descartada por las computadoras finales en el proceso, otorgando el mayor ancho de banda posible a los Vídeos o aplicaciones CAD.

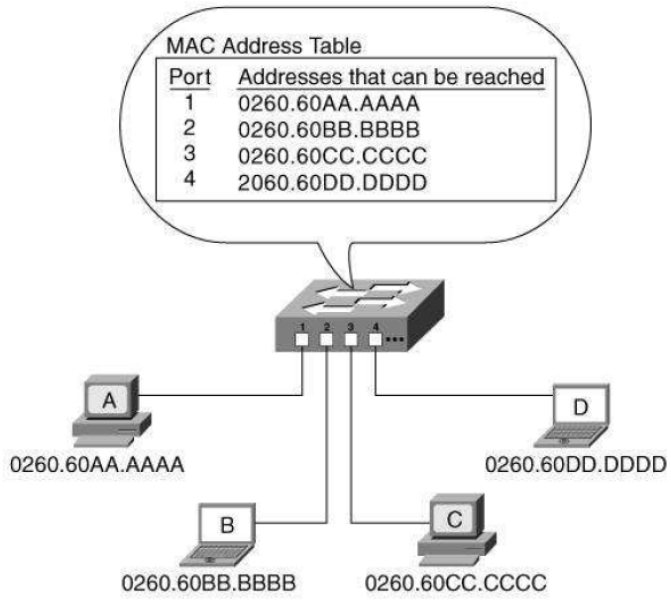


Gráfico 2.22: Switching

Hoy en día los switch’s soportan las VLAN’s, que permiten que dispositivos físicamente remotos puedan aparecer en la misma LAN. Cada VLAN tiene su propio dominio de broadcast. El trafico sin VLAN’s puede ser manejado por switch capa 2, sin embargo el trafico entre VLAN’s solo puede ser manejado por un dispositivo de capa 3 en el modelo OSI, tradicionalmente un dispositivo de capa 3 es el router, pero hoy en día existen switch´s de capa 3 con la misma funcionalidad de un router.

2.3.1. Comparación entre Switch de capa 2 y capa 3

Control de tráfico	Switch de capa 2	Switch de capa 3
Control de tráfico	Solo puede contener colisiones, pero **no hay un control de tráfico** de paquetes Broadcast o Multicast. En cuanto se presente una ráfaga de este tipo de tráfico la red se puede colapsar.	Existe un control de tráfico eficiente y de manera nativa. Este tipo de Switch's previenen el colapso de la red, ante la presencia de tormentas de Broadcast y manejan eficientemente el tráfico multicast.
Escalabilidad para el soporte de nuevas aplicaciones	Prácticamente no hay escalabilidad en un Switch de Capa 2, pues no cuenta con la inteligencia para "detectar" los tipos de tráfico que se presentan en las redes.	Aplicaciones que hoy en día se instalan en las redes actuales como Voz sobre IP, Multimedia para videoconferencia en PC's conectadas en red. Calidad de Servicio y Manejo de los Recursos de Red, demandan mayor capacidad e inteligencia en las redes switcheadas. Un switch de Capa 3 viene preparado para el manejo de este tipo de ambientes.
Rendimiento en el manejo del tráfico de la red	Un Switch de Capa 2 conectado a un Switch Central de Backbone, no puede discriminar cuando una conexión de Capa 3 tiene lugar localmente en el mismo switch, pues cuando se presente esta situación, el Switch de Capa 2 transfiere todos los paquetes hacia el Switch de Backbone, consumiendo innecesariamente recursos y tiempo en el backbone.	Un Switch de Capa 3 es capaz de identificar si el tráfico que arriba a sus puertos tiene que ser switcheado en Capa 2 o Capa 3, y si éste debe de tratarse de manera local, o switchearlo al backbone. De esta manera este equipo toma la decisión de manejarlo con sus propios recursos, sin consumir ancho de banda ni generar tráfico innecesario en el backbone.
Manejo de redes virtuales	Un switch de Capa 2 solo puede manejar Redes Virtuales a nivel de Capa 2, por lo tanto, cuando se configuren VLANs en este switch, este switch no puede pasar tráfico de una VLAN a otra en el mismo switch.	Un switch de Capa 3, puede switchear o rutear tráfico entre cualquier VLAN que haya sido definida en el Switch.
Seguridad	Un Switch de Capa 2 no cuenta con mecanismos de seguridad en la red. Cualquiera puede conectarse a sus puertos y generar cualquier tipo de tráfico, e inclusive puede "escuchar" información sensible que este viajando por la red, como passwords y/o claves de seguridad, así como información confidencial, o simplemente "saturar" la red, provocando el colapso de la misma.	Un Switch de Capa 3 tiene todos los niveles de control y seguridad con los que un ruteador normalmente cuenta. Existen mecanismos de seguridad para prevenir que un usuario indeseado se conecte a la red, incluso a nivel físico. Estos switches pueden filtrar información no deseada incluso de los usuarios que tienen permitido el acceso a la red, para prevenir ataques a servidores, bases de datos, o proteger aplicaciones con

Control de tráfico	Switch de capa 2	Switch de capa 3
		ciertos niveles de seguridad. También cuentan con mecanismos de protección para evitar que un usuario no deseado pueda infiltrarse a la configuración del switch.
Tendencias tecnológicas	Todos los fabricantes de tecnologías de información, así como de productos de comunicaciones para redes, están de acuerdo que mientras más "inteligente" es un dispositivo de red, funciona y se controla mejor, y la tecnología viene avanzando que este tipo de switches no solo son inteligentes sino muy rápidos. Los switches de capa 2 cada vez más están en desuso dado que no están preparados para las demandas de aplicaciones del tipo Intranet o de interacción con la Internet.	Un Switch de Capa 3 cuenta con la suficiente "inteligencia" para interactuar con el tráfico que va o viene de la Internet, y participa con ella en el manejo eficiente de los diferentes tipos de tráfico como Voz sobre IP por ejemplo, que ya es una realidad. Además, un Switch de Capa 3 tiene la capacidad para distinguir cuando los puertos donde se conectan los servidores de la empresa están, ocupados, saturados o caídos, de tal manera que puede reenviar eficientemente el tráfico y las peticiones de los usuarios de la red, hacia aquellos puertos que puedan responder. Una empresa que requiera de nuevas aplicaciones o que demande comunicación hacia y de la Internet, y que requiera de altos mecanismos de seguridad, debe usar switch de Capa 3.

Tabla 2.3: Comparación entre Switch capa 2 y capa 3

2.3.2. Spanning Tree Protocol

Spanning-Tree es un protocolo que se utiliza para evitar ciclos en la topología de red (es decir, que haya dos caminos distintos entre dos mismos dispositivos). El protocolo Spanning-Tree evita que se formen loops cuando los switches o los puentes están interconectados por múltiples caminos. STP implementa el algoritmo 802.1D IEEE intercambiando mensajes de configuración BDPU (Brigde Protocol Data Unit) entre switches para detectar

loops. Entonces elimina el loop cerrando las interfaces del puente seleccionado.

Este algoritmo garantiza que hay sólo un camino activo entre dos dispositivos de red. Y para ello, lo que hace es crear un árbol a partir de la topología de red, donde aparecen todos los nodos, y donde se evitan todos los posibles ciclos.

STP Permite comunicar el coste del camino entre dispositivos e información de identificación para que cada dispositivo pueda bloquear los caminos de mayor coste redundantes. Así, permite la implementación de caminos paralelos para el tráfico de red y asegura que:

- Los caminos redundantes son bloqueados (o deshabilitados) cuando los caminos principales (los de menor coste) son operacionales.
- Los caminos redundantes son habilitados si el camino principal falla.

El coste del camino es usado para calcular la distancia desde cada puerto de un switch hasta el switch raíz. Cada switch se identifica por un Switch ID y cada puerto (interfaz) en un switch se identifica por un Port ID.

2.3.3. Virtual LAN´s

Los grupos de trabajo en una red, hasta ahora, han sido creados por la asociación física de los usuarios en un mismo segmento de la red, o en un

mismo concentrador. Como consecuencia directa, estos grupos de trabajo comparten el ancho de banda disponible y los dominios de "broadcast", y con la dificultad de gestión cuando se producen cambios en los miembros del grupo. Más aún, la limitación geográfica que supone que los miembros de un determinado grupo deben de estar situados adyacentemente, por su conexión al mismo concentrador o segmento de la red.

Los esquemas VLAN (Virtual LAN o red virtual), nos proporcionan los medios adecuados para solucionar esta problemática, por medio de la agrupación realizada de una forma lógica en lugar de física. Sin embargo, las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios tienen conectividad entre ellos y comparten sus dominios de "broadcast".

Los usuarios pueden, así, "moverse" a través de la red, manteniendo su pertenencia al grupo de trabajo lógico. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios.

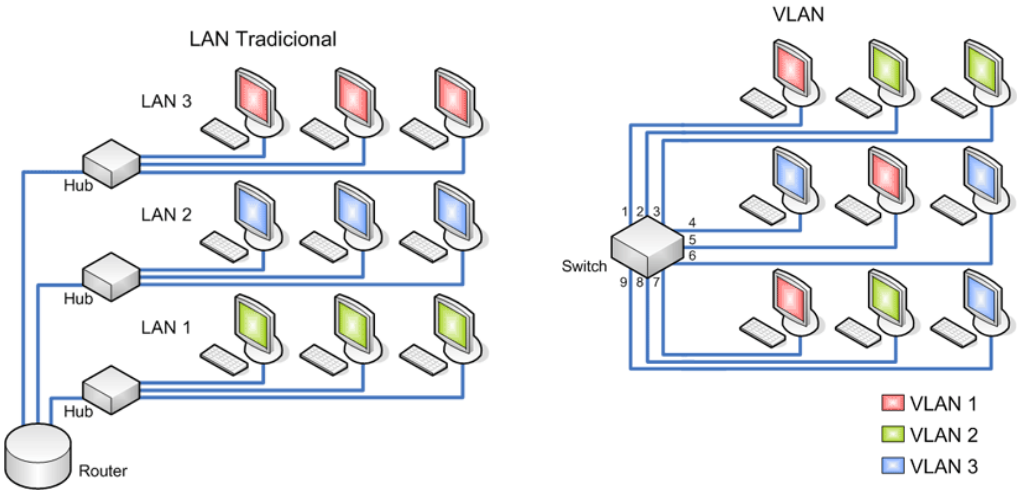


Gráfico 2.23: VLAN

2.3.4. Ruteo

Enrutamiento, ruteo o “routing”, es el proceso de enviar información a un destino concreto que puede ser otro ordenador o un sistema informático. El router es el dispositivo hardware que realiza ese envío y lo consigue utilizando diferentes protocolos de routing.

Router quiere decir enrutador, es decir, "buscador" del camino o ruta, por esta razon su principal funcion es determinar el mejor camino que cada paquete debe tomar para llegar a su destino, y para esto debe conocer dónde está el destino del paquete en la red, para determinarlo, el router utiliza la "máscara de subred" y determina a qué grupo de ordenadores pertenece uno en concreto. Si la máscara de subred de un paquete de información enviado no se corresponde a la red de ordenadores, el router

determinará, lógicamente que el destino de ese paquete está en alguna otra red.

El protocolo de enrutamiento más simple que existe es el enrutamiento estático, esto requiere que cada dirección de destino sea introducida individualmente en la memoria del router, con la dirección del siguiente router en la cadena. Este router destino es llamado “next hop” o siguiente salto.

Este método se utiliza en redes más bien pequeñas y poco complejas. Según las redes van creciendo con cientos de Routers y ordenadores, seguir un control ruta por ruta para direccionar datos de un lado a otro se hace bastante difícil. Por ello, existen los llamados protocolos de enrutamiento dinámico que encuentran los destinos de redes remotas de forma automática y con muy poca configuración manual, asi se tiene: RIP ("Routing Information Protocol"), OSPF ("Open Shortest Path First"), EIGRP ("Enhanced Internet Gateway Routing Protocol").

2.4. Diseño Wireless LAN

Una WLAN es una LAN que usa radio frecuencia para la comunicación en vez de cable, como se observa en el siguiente gráfico.

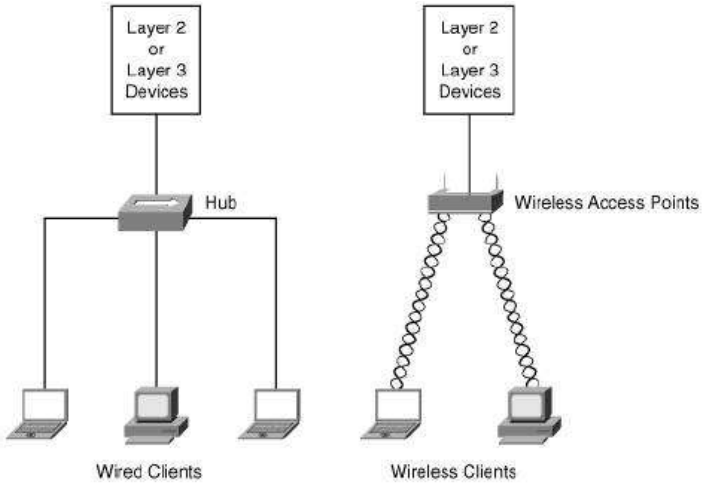


Gráfico 2.24: Acceso Wireless

El rendimiento (velocidad) de estas redes es inversamente proporcional a la distancia entre el transmisor y el receptor

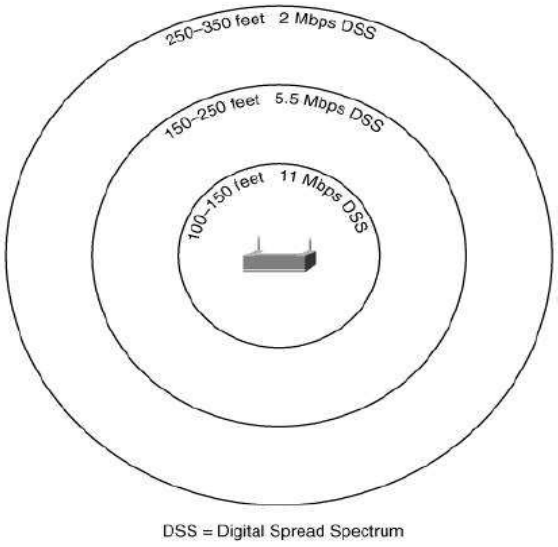


Gráfico 2.25: Digital Spread Spectrum

Los estándares que se manejan en la WLAN son:

Estándar	Velocidad (Mbps)	Frecuencia (Ghz)
802.11b	11	2.4
802.11a	54	5
802.11g	54	2.4
802.11n	>100	2.4

Tabla 2.4: Estándares WLAN

Los principales componentes de una red wireless son:

1. Access Point.- provee la conectividad estre los dispositivos de cliente wireless y la red inalambrica
2. Dispositivos de cliente wireless.- tienen una tarjeta wireless pueden ser una computadora, una portatil, PDA's o IP phones.

La calidad de señal que se tiene en una zona de cobertura wireless viene determinada por la relación entre la potencia de la señal recibida y el nivel de ruido existente, incluyendo posibles señales interferentes. A dicha diferencia de potencias se le conoce como la relación señal-ruido, o SNR. Se ha considerado que por encima de 15db de señal SNR la calidad de la señal recibida es aceptable. Así pues dicho umbral de señal SNR al moverse alrededor de un punto de acceso nos determinará un área de cobertura determinada.

Sin embargo dicha área de cobertura varia considerablemente según el entorno en que se encuentre ubicado dicho punto de acceso, por lo que no es posible extrapolar resultados obtenidos en un entorno abierto, hacia un

entorno cerrado o semicerrado de oficinas. De este modo en un entorno de oficinas con paredes y muros de hormigón armado el área de cobertura se reduce considerablemente en comparación con un entorno de oficinas donde las separaciones entre despachos esté realizada a base de ladrillos, madera o vidrio. Sin embargo dicha desventaja puede convertirse en un aliado cuando se desea limitar el área de cobertura a un determinado recinto por ejemplo por motivos de seguridad o bien para preservar el ancho de banda disponible.

En cuanto al emplazamiento de los puntos de acceso, hay un conjunto de recomendaciones que hay que tener en cuenta. Entre ellas que dicha banda de 2,4 Ghz es también utilizada por otras tecnologías sin hilos que pueden interferir con el servicio de wireless LAN. Por ejemplo: Microondas y otros dispositivos comerciales con tecnología Bluetooh que trabajan utilizando la misma banda. Sin embargo los teléfonos con tecnología inalámbrica DECT que operan a 1900Mhz no interfieren.

Así mismo el movimiento de personas también puede reducir el nivel de señal por lo que se recomienda no poner los puntos de acceso a alturas próximas al nivel de las personas sino algo más alto sobretodo en zonas de tránsito. También es bueno evitar las reflexiones de la señal por efecto de obstáculos ubicando dichos dispositivos a una cierta altura en un espacio abierto.

Hay también que tener en cuenta que dicho punto de acceso inalámbrico debe conectarse a un punto de red alámbrica así como a una toma de red eléctrica lo que limita a veces la ubicación de dicho punto. En este sentido la inyección de la señal eléctrica a través de los pares libres del cableado UTP han supuesto un significativo avance.

Es por todo ello que una vez determinadas las áreas a cubrir la opción más prudente consiste en analizar “in situ” el nivel de SNR detectado tras ubicar un punto de acceso en las proximidades e ir desplazando o reorientando este punto hasta conseguir cubrir el área deseada con los niveles deseados.

2.5. Diseño de Calidad de Servicio (QoS)

Es un conjunto de requisitos de servicio que la red debe cumplir para asegurar un nivel de servicio adecuado para la transmisión de los datos. Estos requisitos de servicio se basan en estándares de funcionalidad QoS.

QoS permite que los programas en tiempo real optimicen el uso del ancho de banda de la red. Como QoS asegura cierto nivel de garantía de recursos de red suficientes, ofrece a una red compartida un nivel de servicio similar al de una red dedicada.

Una garantía de QoS indica un nivel de servicio que permite que un programa transmita datos a una velocidad especificada y los entregue en un periodo de tiempo dado.

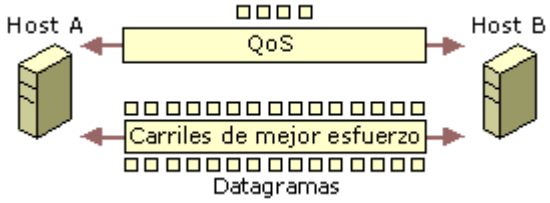


Gráfico 2.26: QoS

El objetivo de QoS es conseguir un sistema de entrega garantizada a través de un conjunto de estándares y mecanismos que aseguran la calidad en la transmisión de los datos en programas habilitados para QoS.

La implementación de QoS permite controlar y predecir el servicio que provee la red para una variedad de aplicaciones, controla los recursos de la red como el ancho de banda, asegura que las aplicaciones de misión critica sean atendidas mas pronto que las otras aplicaciones.

Una red sin una estrategia QoS envía todos los paquetes a la vez por el mismo canal y comparten el ancho de banda, si una empresa tuviera una llamada a través del Internet con un importante cliente y unos empleados se encuentran descargando unos videos por diversión, la red trata a ambos tipos de trafico igualmente y no considera la importancia del tráfico de voz, a este tipo de redes se les llama Convergentes, al existir mucha congestión en la red suelen perderse los paquetes que se están transmitiendo, al tratarse de voz no puede llegar tarde los paquetes porque no se entendería el mensaje, por esta razón es necesario priorizar el tráfico de las redes de la organización. Se debe hacer la priorización del tráfico por políticas que se

adecuen a los objetivos de la organización, asegurándose que las aplicaciones y recursos críticos reciban una cantidad garantizada del ancho de banda disponible.

Por ejemplo, es necesario asegurarse que el personal navegando en la red no este reduciendo los recursos para aplicaciones críticas como ERP, comercio electrónico, aplicaciones estratégicas y servidores de información clasificada. Esto es especialmente crítico en oficinas externas en donde el ancho de banda es un recurso costoso y limitado.

La priorización de servicios es indispensable. El acceso a las aplicaciones críticas puede ser menoscabado o inclusive totalmente inhabilitado por aplicaciones no críticas; personal bajando o subiendo grandes archivos vía www o ftp u observando aplicaciones multimedia vía Internet.

Ciertos servicios de uso regular, pero de menos prioridad o jerarquía, como correos con pesados anexos, largas colas de impresión, tráfico para efectuar respaldos, y la copia, movimiento o transferencia de archivos, sustraen el ancho de banda disponible y causan retraso y congestión en las redes provocando el colapso o inhabilitación de aplicaciones críticas, como el acceso a los datos en la base de datos SQL de la organización.

El tráfico puede ser marcado utilizando diferentes criterios (por sub-red, puerto de servicio, departamento, por usuario, grupo de trabajo, hora del día, tipo de servicio, dirección de origen, dirección de destino, puerto de origen,

puerto de destino, protocolo de comunicación, etc.). Una vez marcado se prioriza de acuerdo a su criticidad y se asignan rutas de recorrido y recursos de ancho de banda por cada tipo de servicio. Priorizando el tráfico a las aplicaciones de misión crítica se garantiza el acceso de estos a un ancho de banda mínimo, sin necesidad de afectar otros servicios menos prioritarios.

A los representantes, nómina mayor o gerencial y personal estratégico móvil en localidades remotas, debería garantizársele el ancho de banda mínimo requerido para efectuar sus transacciones sin perturbaciones ni tiempos innecesarios de espera.

En organizaciones pequeñas o medianas que cuentan con un acceso único a Internet de 256, 512 o 1.024kb a través de modem de línea telefónica a ethernet, de modem de antena exterior a ethernet o de modem CATV a ethernet presentan serios problemas de rendimiento de los servicios interactivos cuando se suben o se bajan archivos pesados (demos, napster, etc.) via www o ftp. Esto ocurre porque se forman largas colas de paquetes ip en los "buffers" de bajada y subida en los modems utilizados.

Mediante el servicio QoS se eliminan las colas de los modem y se trasladan al enrutador de administración de ancho de banda; una vez aquí se jerarquizan y administran adecuadamente, colocando delante los paquetes aleatorios de los servicios interactivos, sin obligarlos a esperar turno detrás de los paquetes generados por el tráfico de subida y bajada de archivos.

Simultáneamente se define el ancho de banda máximo del total disponible que cada servicio debe consumir.

2.5.1. Requerimientos de QoS para Voz, Datos y Video.

El tráfico de voz es muy sensible a los retardos, variación de tiempo entre retardos y los paquetes perdidos. Por lo que los requerimientos de la calidad del servicio de voz son:

- El retardo no puede ser mas de 150 milisegundos
- La variación de tiempo entre retardos no puede ser más de 30 milisegundos.
- No puede perderse más de un porcentaje de paquetes perdidos

El ancho de banda requerido por el tráfico de voz varía según el algoritmo de compresión y encapsulamiento utilizado en la capa 2.

El video interactivo o la video conferencia tienen los mismos requerimientos de calidad respecto a la voz, la diferencia está en el ancho de banda el requerimiento para paquetes de voz es pequeño mientras que el tamaño de los paquetes de video conferencia pueden variar. Por lo que es necesario proveer un 20% adicional del ancho de banda al utilizado por los datos.

Con respecto a los datos es importante priorizar las aplicaciones y sus datos, por ejemplo un email interno no es sensible al retardo, pero una aplicación

que trabaje con base de datos en arquitectura cliente / servidor si tiene una alta sensibilidad al retardo. Por lo que es necesario clasificar los datos de acuerdo a los objetivos corporativos de la empresa.

2.5.2. Modelos de QoS.

Existen dos modelos de desarrollo de QoS, IntServ y DiffServ los cuales se explican a continuación:

INTSERV.- Usa un explicito mecanismo de señalización desde las aplicaciones a los dispositivos de red. Las aplicaciones requieren de un determinado nivel de servicio incluyendo el ancho de banda y los requerimientos de retardo. Después de que los dispositivos de red confirman que esas aplicaciones pueden usar esos requerimientos, las aplicaciones envían solo los datos necesarios para hacer uso del servicio.

Las aplicaciones que trabajan en este ambiente usan el protocolo Resource Reservation Protocol (RSVP) para indicar sus requerimientos a los dispositivos de red. Estos dispositivos guardan información sobre el flujo de paquetes y se asegura que este flujo obtenga los recursos necesarios según su prioridad y políticas.

Los servicios que ofrece IntServ son:

- Garantía en el Servicio.- este servicio permite reservar ancho de banda

para satisfacer sus requerimientos a través de una cola del protocolo RSVP.

- Controla la carga.- este servicio permite disminuir el retardo y hacer el envió rápidamente incluso durante momentos de congestión.

Para hacer uso de este método todos los dispositivos requieren hacer uso de RSVP.

DIFFSERV.- La red intenta entregar a un nivel especifico el servicio con QoS especificado en la cabecera de cada paquete. Los dispositivos de red ubicados en la frontera de la red, estan configurados para clasificar a los paquetes dependiendo de su fuente, destino o tipo de tráfico. Cisco proporciona caracteristicas QoS con su sistema operativo IOS.

2.6. Seguridad de redes

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco

deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas. “Hackers”, “crakers”, entre otros, han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes.

Además de las técnicas y herramientas criptográficas, es importante recalcar que un componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red.

A la hora de plantearse en que elementos del sistema se deben de ubicar los servicios de seguridad podrían distinguirse dos tendencias principales:

Protección de los sistemas de transferencia o transporte.- En este caso, el administrador de un servicio asume la responsabilidad de garantizar la transferencia segura al usuario final de la información de forma lo más transparente posible. Ejemplos de este tipo de planteamientos serían el establecimiento de un nivel de transporte seguro, de un servicio de mensajería con MTAs (Mail Transport Agents) seguras, o la instalación de un firewall, que defiende el acceso a una parte protegida de una red.

Aplicaciones seguras extremo a extremo.- Si se piensa, por ejemplo, en el correo electrónico, consistiría en construir un mensaje en el cual el contenido ha sido asegurado mediante un procedimiento de encapsulado previo al envío. De esta forma, el mensaje puede atravesar sistemas heterogéneos y poco fiables sin por ello perder la validez de los servicios de seguridad provistos. Esta misma operatoria, puede usarse para abordar el problema de la seguridad en otras aplicaciones tales como videoconferencia, acceso a bases de datos, etc.

Otro problema de capital importancia es la gestión de passwords, que es inherente al uso de la criptografía y debe estar resuelto antes de que el usuario esté en condiciones de enviar un solo bit seguro.

2.6.1. Políticas

Una política de seguridad informática (PSI) es una forma de comunicarse con los usuarios y los gerentes. Las PSI establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización. No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que deseamos proteger y el por qué de ello.

Cada PSI es consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

2.6.1.1. Elementos de una Política de Seguridad Informática

Las PSI deben considerar entre otros, los siguientes elementos:

Alcance de las políticas.- incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.

Objetivos de la política y descripción.- clara de los elementos involucrados en su definición.

Responsabilidades .- por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.

Requerimientos mínimos.- para configuración de la seguridad de los sistemas que cobija el alcance de la política.

Definición de violaciones y de las consecuencias del no cumplimiento de la política.

Responsabilidades de los usuarios.- con respecto a la información a la que ella tiene acceso.

Las PSI deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios.

Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios entre otros.

No se debe dar por hecho algo que es obvio. Es necesario hacer explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI trazadas.

2.6.1.2. Niveles de Trabajo

Confidencialidad.- Consiste en proteger la información contra la lectura no autorizada explícitamente. Incluye no sólo la protección de la información en su totalidad, sino también las piezas individuales que pueden ser utilizadas para inferir otros elementos de información confidencial.

Integridad.- Es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida incluye no sólo la que está almacenada directamente en los sistemas de cómputo sino que también

se deben considerar elementos menos obvios como respaldos, documentación, registros de contabilidad del sistema, tránsito en una red, etc. Esto comprende cualquier tipo de modificaciones:

- Causadas por errores de hardware y/o software.
- Causadas de forma intencional.
- Causadas de forma accidental

Cuando se trabaja con una red, se debe comprobar que los datos no fueron modificados durante su transferencia.

Autenticidad.- En cuanto a telecomunicaciones se refiere, la autenticidad garantiza que quien dice ser "X" es realmente "X". Es decir, se deben implementar mecanismos para verificar quién está enviando la información.

No – repudio.- Ni el origen ni el destino en un mensaje deben poder negar la transmisión. Quien envía el mensaje puede probar que, en efecto, el mensaje fue enviado y viceversa.

Disponibilidad de los recursos y de la información.- De nada sirve la información si se encuentra intacta en el sistema pero los usuarios no pueden acceder a ella. Por tanto, se deben proteger los servicios de cómputo de manera que no se degraden o dejen de estar disponibles a los usuarios de forma no autorizada. La disponibilidad también se entiende

como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema.

Consistencia.- Se trata de asegurar que el sistema siempre se comporte de la forma esperada, de tal manera que los usuarios no encuentren variantes inesperadas.

Control de acceso a los recursos.- Consiste en controlar quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace.

Auditoría.- Consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno de los usuarios y los tiempos y fechas de dichas acciones.

En cuanto a los dos últimos puntos resulta de extrema importancia, cuando se trata de los derechos de los usuarios, diferenciar entre “espiar” y “monitorear” a los mismos. La ética es algo que todo buen administrador debe conocer y poseer. Finalmente, todos estos servicios de seguridad deben ser tomados en cuenta en el momento de elaborar las políticas y procedimientos de una organización para evitar pasar por alto cuestiones importantes como las que señalan dichos servicios. De esta manera, es posible sentar de forma concreta y clara los derechos y límites de usuarios y administradores. Sin embargo antes de realizar cualquier acción para lograr garantizar estos servicios, es necesario asegurarnos de que los usuarios

conozcan sus derechos y obligaciones (es decir, las políticas), de tal forma que no se sientan agredidos por los procedimientos organizacionales.

2.6.2. Seguridad en LAN inalámbricas

La tecnología de red de área local inalámbrica (WLAN) constituye un tema controvertido. Las organizaciones que han implementado WLAN están preocupadas acerca de si son o no seguras; a las que no las han implementado aún les preocupa desaprovechar la oportunidad de aumentar la productividad del usuario y reducir costes de propiedad. Existe todavía una gran confusión en relación con la seguridad de una WLAN en el entorno informático corporativo.

Desde que se detectaron los puntos débiles en la seguridad de WLAN de primera generación, analistas y empresas dedicadas a la seguridad en las redes han procurado resolver estos problemas. Algunos de estos esfuerzos han contribuido de manera significativa a la causa de la seguridad inalámbrica. Otros han participado de los defectos: algunos introducen un conjunto distinto de vulnerabilidades de seguridad; otros precisan hardware propietario costoso; y otros evitan la cuestión de la seguridad de WLAN por completo protegiéndose con otra tecnología de seguridad potencialmente compleja como es la de las redes privadas virtuales (VPN).

Paralelamente, la IEEE junto con otros organismos normativos y consorcios, han vuelto a definir y han mejorado con diligencia los estándares de

seguridad inalámbrica para permitir que las WLAN hagan frente al entorno de seguridad hostil de principios del siglo veintiuno. A continuación se detallan las principales amenazas a las que se enfrentan las redes WLAN.

Amenaza	Descripción de la amenaza
Interceptación (revelación de datos)	La interceptación de transmisiones de la red puede dar lugar a la revelación de datos confidenciales y de credenciales de usuario sin protección, además de a una posible usurpación de la identidad. Permite también que intrusos expertos recopilen información sobre los entornos de TI y la utilicen para atacar otros sistemas o datos que, de otra forma, no serían vulnerables.
Interceptación y modificación de los datos transmitidos	Si un atacante logra obtener acceso a la red, puede introducir un equipo falso que intercepte y modifique los datos comunicados entre dos usuarios autorizados.
Imitación	El acceso directo a la red interna permite que el intruso falsifique datos que parecen legítimos de manera que no sería posible desde fuera de la red, por ejemplo, un mensaje de correo electrónico de un usuario imitado. Los usuarios, incluso los administradores de sistemas, suelen confiar en los elementos originados dentro de la red mucho más que en los que proceden del exterior de la red corporativa.
Denegación del servicio (DoS)	Un agresor determinado puede activar un ataque de DoS de diversas maneras. Por ejemplo, la interrupción de las señales de radio se puede activar mediante algo tan simple como un microondas. Existen ataques más complejos cuyo objetivo son los protocolos inalámbricos de bajo nivel, y otros menos complejos cuyo objetivo son las redes mediante un gran incremento del tráfico aleatorio en la WLAN.
Carga libre (o robo de recursos)	Es posible que los intrusos sólo deseen utilizar su red como punto de libre acceso a Internet. Si bien esto no es tan grave como las demás amenazas, hará que, como mínimo, no sólo empeore el nivel de servicio prestado a los usuarios autorizados sino también que puedan introducirse virus y otras amenazas.
Amenazas accidentales	Algunas características de las WLAN facilitan la aparición de amenazas no intencionadas. Por ejemplo, un visitante

Amenaza	Descripción de la amenaza
	autorizado podría iniciar el equipo portátil sin la intención de conectarse a la red, pero se conecta a su WLAN automáticamente. Así, el equipo portátil del visitante se convierte en un punto de entrada de virus en la red. Este tipo de amenaza sólo se da en WLAN desprotegidas.

Tabla 2.5: Principales amenazas de WLAN

2.6.2.1. Protección real de la WLAN

Desde el descubrimiento de las vulnerabilidades de seguridad de las WLAN que se han descrito hasta el momento, los principales proveedores de redes, los organismos reguladores y los analistas han centrado gran parte de sus esfuerzos en encontrar soluciones para hacer frente a estos problemas. De esta forma, se han generado una serie de respuestas a las preocupaciones sobre la seguridad de las WLAN. Las principales opciones son:

No implementar tecnología de WLAN.- Quizás la manera más evidente de lidiar con las amenazas de la seguridad en las WLAN sea evitarlas por completo al no implementar ninguna WLAN. Las organizaciones que siguen este enfoque asumen el "precio de la demora", que no es más que el coste de la oportunidad y con el tiempo este precio puede ser demasiado alto.

Utilizar seguridad básica mediante 802.11 (WEP estática).- La seguridad 802.11 básica (WEP estática) emplea una clave compartida para controlar el acceso a la red y usa la misma clave para cifrar el tráfico inalámbrico. Este modelo de autorización simple se complementa a menudo con el uso del

filtrado de puertos basado en direcciones de hardware de tarjeta de WLAN, aunque no forma parte de la seguridad de 802.11 como tal. El principal atractivo de este enfoque es su sencillez. Si bien ofrece un nivel de seguridad algo mejor que las WLAN sin proteger, cuenta con grandes inconvenientes de administración y seguridad, sobre todo en organizaciones de gran tamaño.

Entre los inconvenientes de utilizar WEP se incluyen los siguientes:

- Las claves WEP estáticas se pueden averiguar en cuestión de horas en una red con bastante tráfico si se utiliza un equipo con un adaptador de WLAN y herramientas de pirateo, como Airsnort o WEPCrack.
- El punto débil más grave de WEP es que no existe ningún mecanismo para asignar o actualizar dinámicamente la clave de cifrado de la red.
- Las claves estáticas se pueden cambiar, pero el proceso para hacerlo en los puntos de acceso y los clientes inalámbricos es, por lo general, manual y laborioso. Para empeorar la situación, las actualizaciones de clave se deben efectuar en los clientes y los puntos de acceso simultáneamente con el fin de evitar que se interrumpa la conexión de los clientes.
- La clave estática precisa que se comparta entre todos los usuarios de la WLAN y todos los puntos de acceso inalámbrico. Un secreto compartido entre un gran número de personas y dispositivos es poco probable que permanezca a salvo durante mucho tiempo.

WEP proporciona a las WLAN un mecanismo de control del acceso muy limitado, basado en el conocimiento de la clave WEP. Si se descubre el nombre de la red (algo muy sencillo) y la clave WEP, es posible conectarse a la red.

Una manera de intentar mejorar esta situación es configurar los puntos de acceso inalámbrico de forma que sólo admitan un conjunto predefinido de direcciones de adaptadores de red cliente. Esto suele conocerse como filtrado de direcciones de control de acceso de medios (MAC). La capa MAC hace referencia al firmware de bajo nivel del adaptador de red.

Redes privadas virtuales.- Las VPN son probablemente la manera más popular de cifrado de red; mucha gente confía en las tecnologías VPN probadas y de confianza para proteger la confidencialidad de los datos enviados a través de Internet. Cuando se detectaron las vulnerabilidades de la WEP estática, VPN se propuso rápidamente como la manera de proteger los datos que viajan a través de una WLAN.

VPN es una solución excelente para atravesar una red hostil como Internet (aunque la calidad de las implementaciones de VPN varíe). Sin embargo, no es necesariamente la mejor solución para asegurar las WLAN internas. Para este tipo de aplicaciones, una VPN ofrece poca o ninguna seguridad adicional en comparación con las soluciones 802.1X; al mismo tiempo que incrementan de manera significativa la complejidad y los costes, reducen el

aprovechamiento y hacen que partes importantes de las funciones no estén operativas.

Entre las ventajas de utilizar VPN para proteger las WLAN se incluyen:

- La protección de los datos de la VPN suele emplear el cifrado de software que permite que los algoritmos se modifiquen y se actualicen con mayor facilidad que el cifrado basado en el hardware.
- Es posible utilizar hardware relativamente menos costoso porque la protección de VPN es independiente del hardware de WLAN (aunque el aumento de precio que conlleva el hardware de red apto para 802.1X no ha desaparecido en absoluto).

Entre los inconvenientes de utilizar VPN en lugar de la seguridad de WLAN nativa se incluyen:

- Las VPN carecen de transparencia para el usuario. Por regla general, los clientes VPN precisan que el usuario inicie manualmente una conexión con el servidor de VPN; por lo tanto, la conexión nunca será tan transparente como una conexión LAN con cable.
- Dado que la conexión de VPN solo la puede iniciar el usuario, un equipo inactivo o desconectado no se conectará a la VPN (y por lo tanto, tampoco a la LAN corporativa). En consecuencia, un equipo no se puede administrar o supervisar remotamente a menos que un usuario inicie la sesión. Determinadas configuraciones de objeto de directiva de grupo de

equipos (GPO), tales como las secuencias de comandos de inicio y el software asignado al equipo, no se aplicarán nunca.

- Si se reanuda desde un estado de espera o hibernación, la conexión de VPN no se volverá a establecer de forma automática, sino que el usuario deberá hacerlo manualmente.
- Aunque los datos del interior del túnel VPN están protegidos, la VPN no ofrece protección para la propia WLAN. Un intruso podría seguir conectado a la WLAN e intentar sondear o atacar dispositivos conectados a la WLAN.
- Los servidores de la VPN se pueden convertir en un cuello de botella. Todo el acceso de clientes WLAN a la LAN corporativa se realiza a través del servidor. Los dispositivos VPN suelen prestar servicio a una gran cantidad de clientes remotos con velocidades relativamente bajas; de ahí, que la mayoría de las puertas de enlace VPN no puedan hacer frente a las decenas o cientos de clientes que se ejecutan con toda la velocidad de una LAN.

VPN se adapta de manera ideal para asegurar el paso del tráfico a través de redes hostiles, tanto si el usuario se ha conectado a través de una conexión de banda ancha doméstica o desde una zona interactiva inalámbrica. No obstante, las VPN nunca se diseñaron para proteger el tráfico de la red en las redes internas. Para la mayoría de las organizaciones, las VPN con este papel serían demasiado voluminosas y estarían limitadas en cuanto a las funciones para el usuario; además de ser demasiado costosas y complejas para el departamento de TI encargado de mantenerlas.

Seguridad IP.- IPSec permite que dos partes de una red se autentiquen la una a la otra de forma segura y autentiquen o cifren paquetes de red individuales. IPSec se puede utilizar tanto para abrir un túnel seguro de una red a otra, como para simplemente proteger los paquetes IP que se transmiten entre dos equipos.

Los túneles IPSec se suelen utilizar en el acceso de cliente o las conexiones de VPN de sitio a sitio. El modo de túnel IPSec es una forma de VPN y funciona con la encapsulación de un paquete de IP completo dentro de un paquete protegido mediante IPSec. Esto agrega una carga a la comunicación, al igual que otras soluciones de VPN, que no es realmente necesaria para la comunicación entre sistemas de la misma red.

IPSec también puede asegurar el tráfico de un extremo a otro entre dos equipos (sin túnel) mediante el modo de transporte IPSec. Al igual que VPN, IPSec es una solución excelente en muchas circunstancias, pero no puede sustituir directamente a la protección de WLAN nativa que se distribuye en la capa de hardware de red.

Algunas de las ventajas de la protección del modo de transporte IPSec son:

- Es transparente para los usuarios. Al contrario de las VPN, no se precisa ningún procedimiento de inicio de sesión especial.
- La protección de IPSec es independiente del hardware de WLAN. Sólo precisa una WLAN abierta y sin autenticar. A diferencia de las VPN, no

se necesitan servidores ni dispositivos adicionales porque la seguridad se negocia entre los equipos en cada extremo de la comunicación.

- La utilización de algoritmos de cifrado no se encuentra limitada por el hardware de WLAN.

Entre los inconvenientes de utilizar IPSec en lugar de la seguridad de WLAN nativa se incluyen:

- IPSec utiliza sólo la autenticación de nivel de equipo y no existe manera de implementar a la vez un esquema de autenticación basado en el usuario. Para muchas organizaciones, esto no supondrá ningún problema pero permite que los usuarios no autorizados se conecten a otros equipos protegidos con IPSec de la red si inician la sesión en un equipo autorizado.
- La administración de directivas IPSec puede ser muy complicada en grandes organizaciones. Si se trata de imponer la protección general del tráfico IP, se podrían poner en peligro otros usos más especializados de IPSec, donde la protección de un extremo a otro es necesaria.
- La seguridad completa exige el cifrado de todo el tráfico de un extremo a otro, pero algunos dispositivos pueden ser incompatibles con IPSec. De este modo, se obligaría a que el tráfico hacia estos dispositivos se transmita sin cifrar. IPSec no ofrecerá protección para estos dispositivos, que quedarán expuestos a todos los usuarios que se conecten a la WLAN.
- IPSec de un extremo a otro no puede proteger el tráfico de difusión o

multidifusión porque IPSec depende de dos partes que se autentican e intercambian claves mutuamente.

Protección de la WLAN mediante la autenticación 802.1X y el cifrado de datos.- Las ventajas clave de una solución 802.1X se resumen en la siguiente lista:

- *Nivel de seguridad alto*: se trata de un esquema de autenticación de seguridad elevado porque puede emplear certificados de cliente o nombres de usuario y contraseñas.
- *Cifrado más seguro*: permite un cifrado muy seguro de los datos de la red.
- *Transparencia*: proporciona una autenticación y una conexión a la WLAN transparentes.
- *Autenticación de usuarios y de equipos*: permite la autenticación por separado de usuario y de equipo. La autenticación por separado de un equipo permite administrarlo incluso cuando ningún usuario ha iniciado la sesión.
- *Bajo coste*: bajo coste del hardware de red.
- *Alto rendimiento*: dado que el cifrado se lleva a cabo en el hardware de WLAN y no en la CPU del equipo cliente, el cifrado de WLAN no influirá en el nivel de rendimiento del equipo cliente.

La solución 802.1X también cuenta con algunas advertencias.

- Aunque 802.1X disfruta de una aceptación casi universal, el uso de distintos métodos de EAP (protocolo de autenticación extensible) implica que la interoperabilidad no siempre está garantizada.
- WPA está todavía en las primeras fases de adopción así que es posible que no se encuentre disponible en hardware más antiguo.
- La RSN (802.11i) de próxima generación está todavía pendiente de ratificación y precisará la implantación de actualizaciones de hardware y software (por lo general, el hardware de red necesitará una actualización de firmware).

Estas estrategias se detallan en orden de menor a mayor grado de satisfacción, basándose en una combinación de seguridad, funcionalidad y aprovechamiento; aunque, hasta cierto punto, se trata de un juicio subjetivo.

2.6.2.2. Comparación de los enfoque se seguridad WLAN

Característica	WLAN 802.1X	WEP estática	VPN	IPSec
Autenticación segura	Sí	No	Sí, pero no las VPN que utilicen autenticación de clave compartida.	Sí, si se emplea autenticación de certificados o Kerberos.
Cifrado de datos de alta seguridad	Sí	No	Sí	Sí
Conexión transparente y reconexión a la WLAN	Sí	Sí	No	Sí
Autenticación de usuario	Sí	No	Sí	Sí

Característica	WLAN 802.1X	WEP estática	VPN	IPSec
Autenticación de equipo	Sí	Sí	No	Sí
Difusión y tráfico de multidifusión protegidos	Sí	Sí	Sí	No
Se requieren dispositivos de red adicionales	Servidores RADIUS	No	Servidores VPN, servidores RADIUS	No
Acceso seguro a la propia WLAN	Sí	Sí	No	No

Tabla 2.6: Comparación de los enfoques de seguridad de WLAN

CAPÍTULO III

3. REDISEÑO DE LA RED DE CAMPUS DE LA PUCESA

3.1. Diagnóstico de la red de campus actual

Esta sección tiene por objetivo conocer el estado actual de la red LAN

3.1.1. Diseño de la red actual

Actualmente la Pontificia Universidad Católica del Ecuador Sede Ambato tiene un área de 10.010 m^2 está conformada por dos edificios: El Edificio Principal que cuenta con 4 pisos distribuidos en el área administrativa, Biblioteca, en las Escuelas de: Sistemas, Sicología, Optometría, Diseño Industrial, Departamento de Investigación, Posgrados y Autoevaluación y el Centro de Cómputo todas están interconectadas a través una red LAN, y el Edificio nuevo en el cual trabajan la Escuela de Administración y de Lenguas. Independientemente en el campus están el área de pastoral y el bar que también están interconectados a la red. El campus universitario cuenta con una red Wireless que permite conectar equipos inalámbricos.

3.1.2. Distribución de equipos activos y pasivos de la red actual

Campus de la Universidad

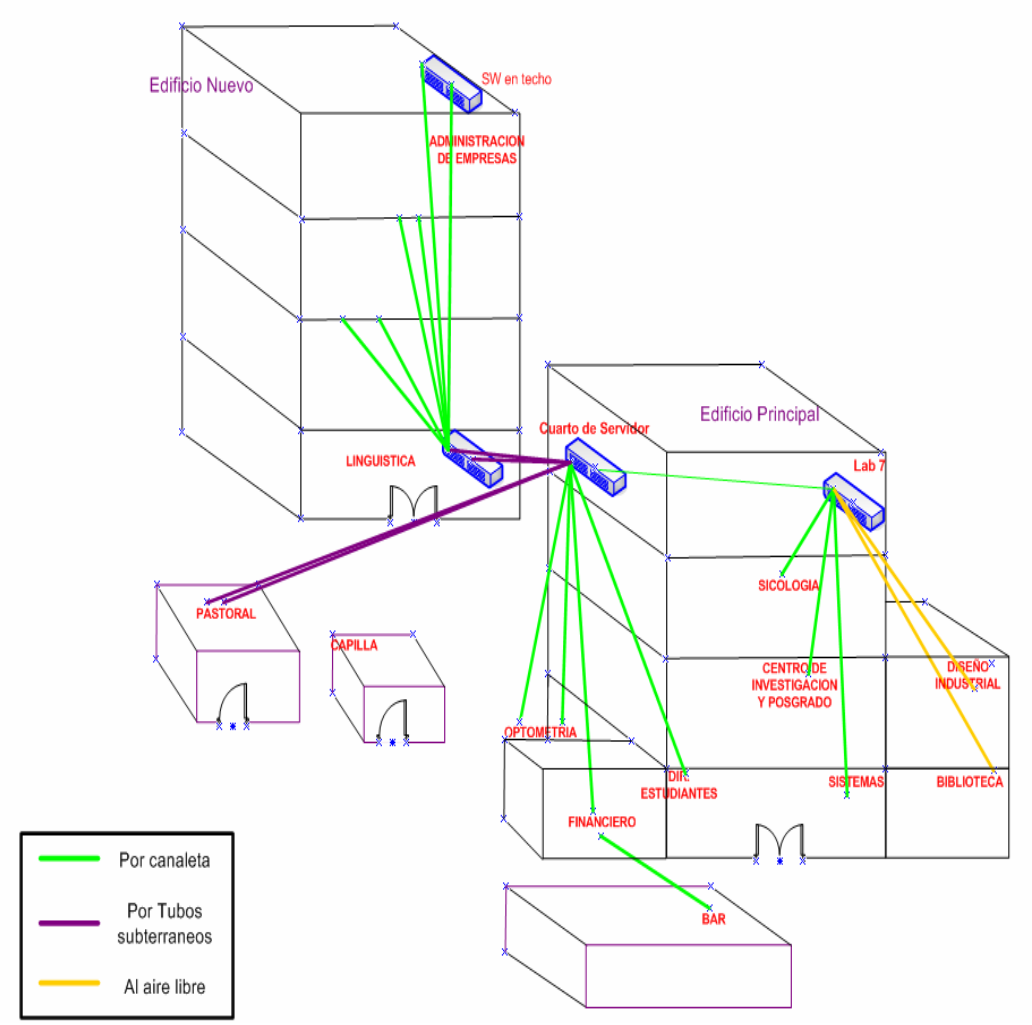


Gráfico 3.1: Interconexión del Campus de la Universidad

En el campus de la PUCESA existen un total de 21 switch´s, 136 Pc´s y 10 AP´s que se encuentran distribuidos como se observa en los gráficos siguientes.

En el cuarto piso al lado izquierdo del edificio principal se encuentra el cuarto de servidores y los 2 switch principales desde donde se administra y distribuye la red.

De estos bajan por canaleta 4 cables UTP Cat 5e:

- Dos cables al Primer Piso uno a la Dirección de Estudiantes y otro al Departamento Financiero. Desde el departamento Financiero se conecta el Access Point del bar por canaleta.
- Dos cables a la Escuela de Optometría.

Por tubería subterránea viajan 5 cables UTP Cat 5e:

- Dos cables a pastoral, de los cuales 1 esta libre
- Dos cables van al edificio nuevo primer piso.

En el lado derecho del cuarto piso está ubicado el laboratorio 7 del cual bajan 5 cables UTP Cat 5e en total, por canaleta van 3 cables a:

- Escuela de Sicología,
- Departamento de Investigación, Posgrado y Autoevaluación (DIPA)
- Escuela de Sistema

Los otros 2 cables están sueltos a la intemperie, estos llegan a:

- Diseño Industrial
- Biblioteca.

Edificio Principal

Primer Piso

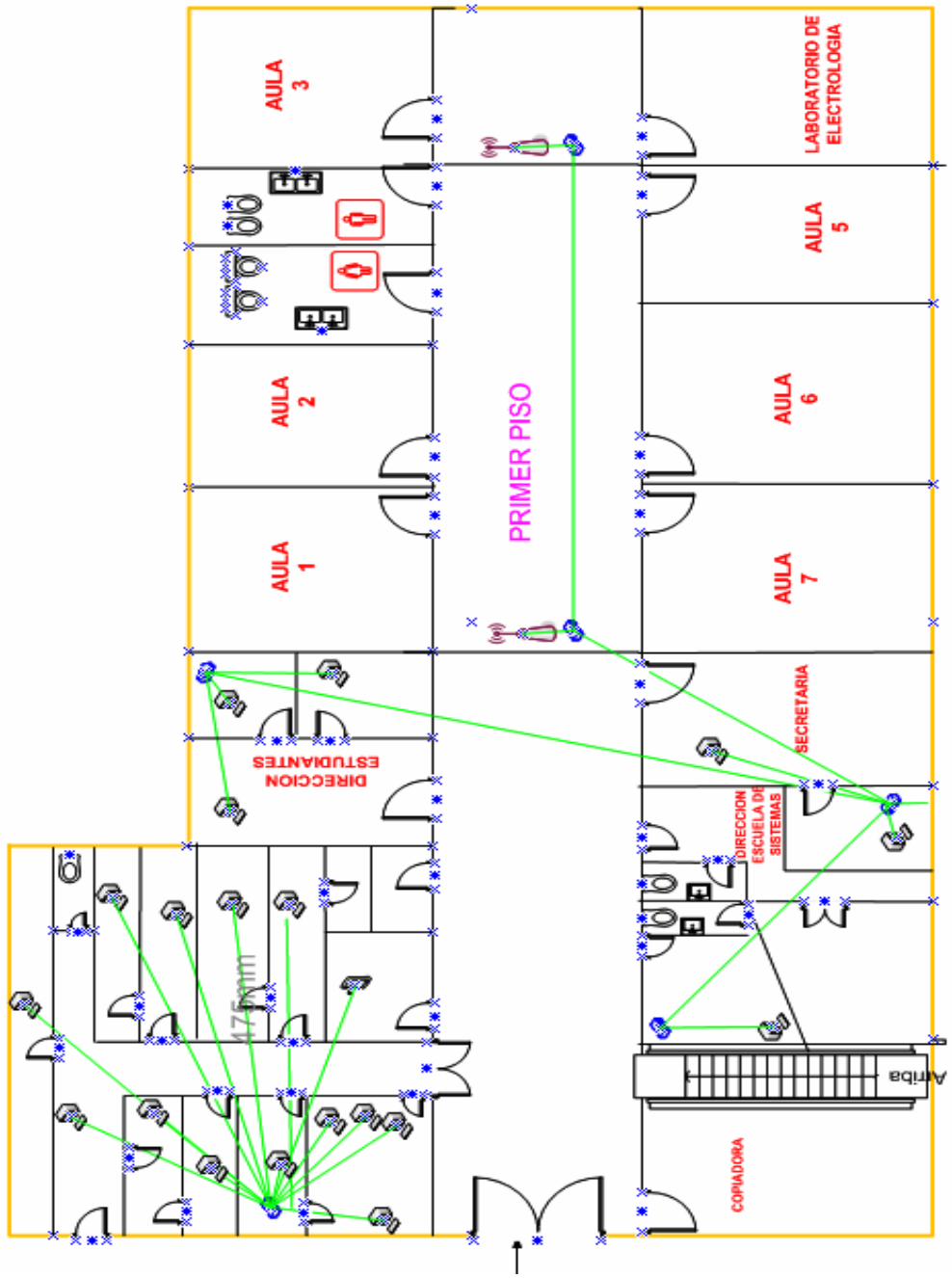


Gráfico 3.2: Interconexión del Primer Piso

En el primer piso se encuentra el Área Administrativa y la Escuela de Sistemas:

- En el Departamento financiero existen 1 MINI HUB de 16 puertos, de los cuales 10 están ocupados y también existe un Switch Advanced Network 10/100 de 8 puertos de los cuales 7 están usados, la mayoría de cables están etiquetados, de aquí se distribuye la red para toda el área administrativa, que cuenta con 13 pc´s, 1 touch hand y también sale por canaleta la conexión al bar. Estos equipos están en el suelo de este departamento como se puede observar en el siguiente gráfico.

Gráfico 3.3: Equipos en la Dirección Financiera

- En la Dirección de Estudiantes se encuentra otro Switch Advanced Network 10/100 de 8 puertos de los cuales 4 están usados, se conectan 3 pc´s

Gráfico 3.4: Switch de la Dirección de Estudiantes

- La Escuela de Sistemas poseen 2 Switch´s. El primero está ubicado en la Dirección de la Escuela es un Switch NEXXT 10/100 de 16 puertos y están ocupados 11, los cuales están distribuidos de la siguiente manera:
  - El punto de red que llega desde el Laboratorio 7
  - Un punto a Secretaria de la Escuela
  - Dos puntos de red en la Dirección de la Escuela
  - Un punto de red a 1 Switch de 8 puertos en cual a la vez se conecta con los 2 Access Point existentes en este piso.
  - Un punto de red a la Dirección de Estudiantes.

- Un punto de red al Switch número 2, es CNET de 8 puertos de los cuales están ocupados 3, a este se conecta el Servidor del Sistema Escolástico y la pc para los docentes.

No hay etiquetas en los cables por lo que no se conoce cual es el destino del resto de cables pues no están a la vista. Estos Switch´s están ubicados el primero en el piso y el otro sobre el escritorio del servidor.

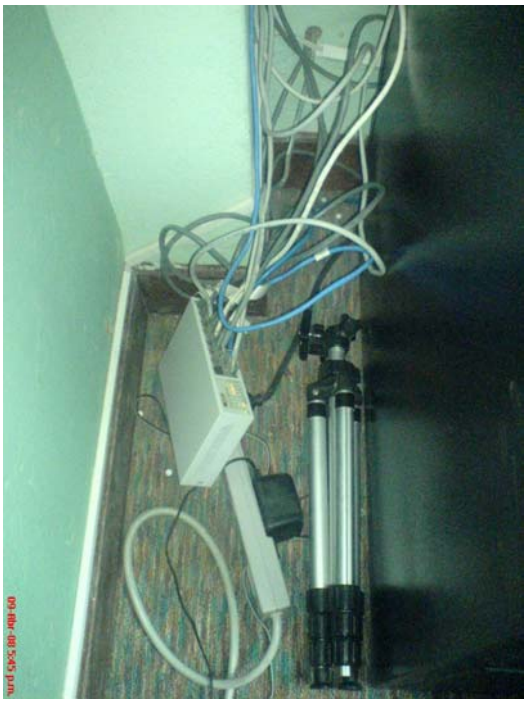


Gráfico 3.5: Switch de la Dirección de Sistemas

Biblioteca y Auditorio

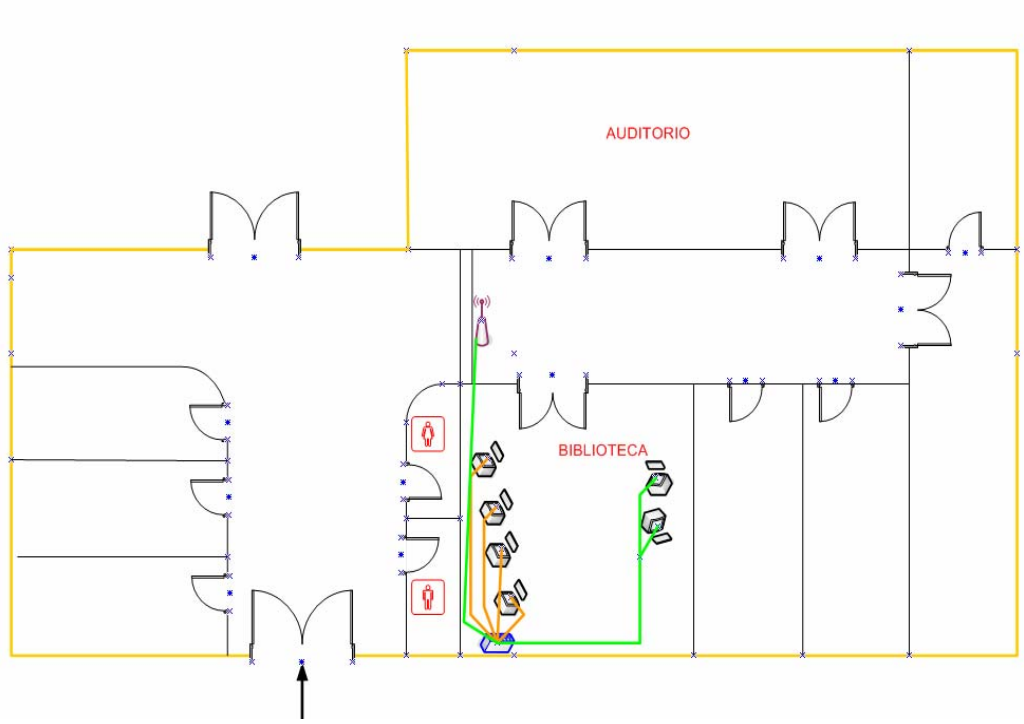


Gráfico 3.6: Interconexión de la Biblioteca

Aquí se puede encontrar 1 Switch CNET de 16 puertos al cual se conectan, 1 Access Point el cable pasa por canaleta y 6 Pc´s de las cuales los cables de 2 van por canaleta y las otras 4 presentan cables vistos.

Este SWITCH esta ubicado en el piso entre el escritorio de la pc que usan los estudiantes como se puede observar en la siguiente imagen.

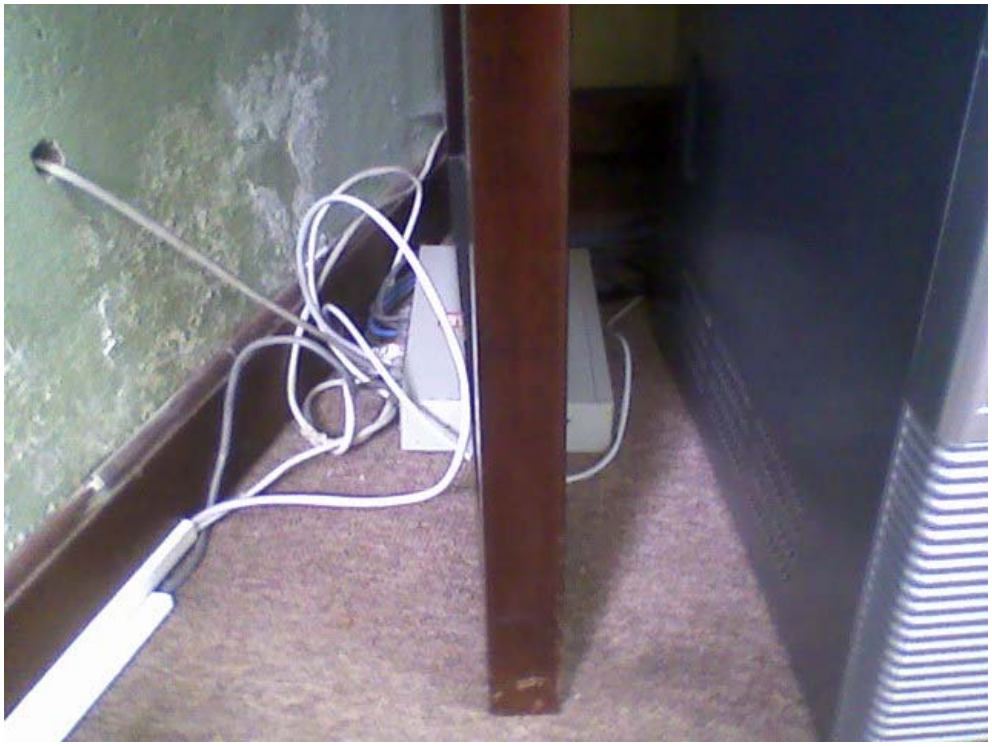


Gráfico 3.7: Switch en la Biblioteca

Escuela de Optometría

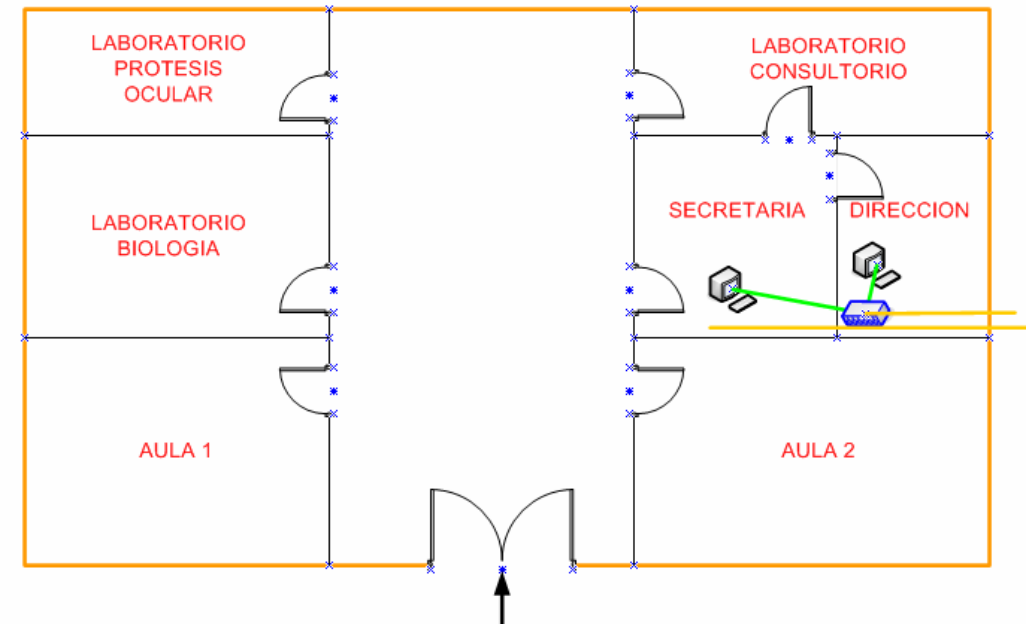


Gráfico 3.8: Interconexión de la Escuela de Optometría

A esta escuela le llegan 2 cables desde el rack central, el uno se conecta a un Switch Advantek Networks de 8 puertos y el otro cable esta suelto. Al Switch se conectan las 2 pc´s existentes en esta escuela.

Aquí el Switch esta en el piso debajo del escritorio de la Dirección de Escuela, ocultado por el CPU como se puede observar en la siguiente imagen.

Gráfico 3.9: Switch en la Escuela de Optometría

Segundo Piso

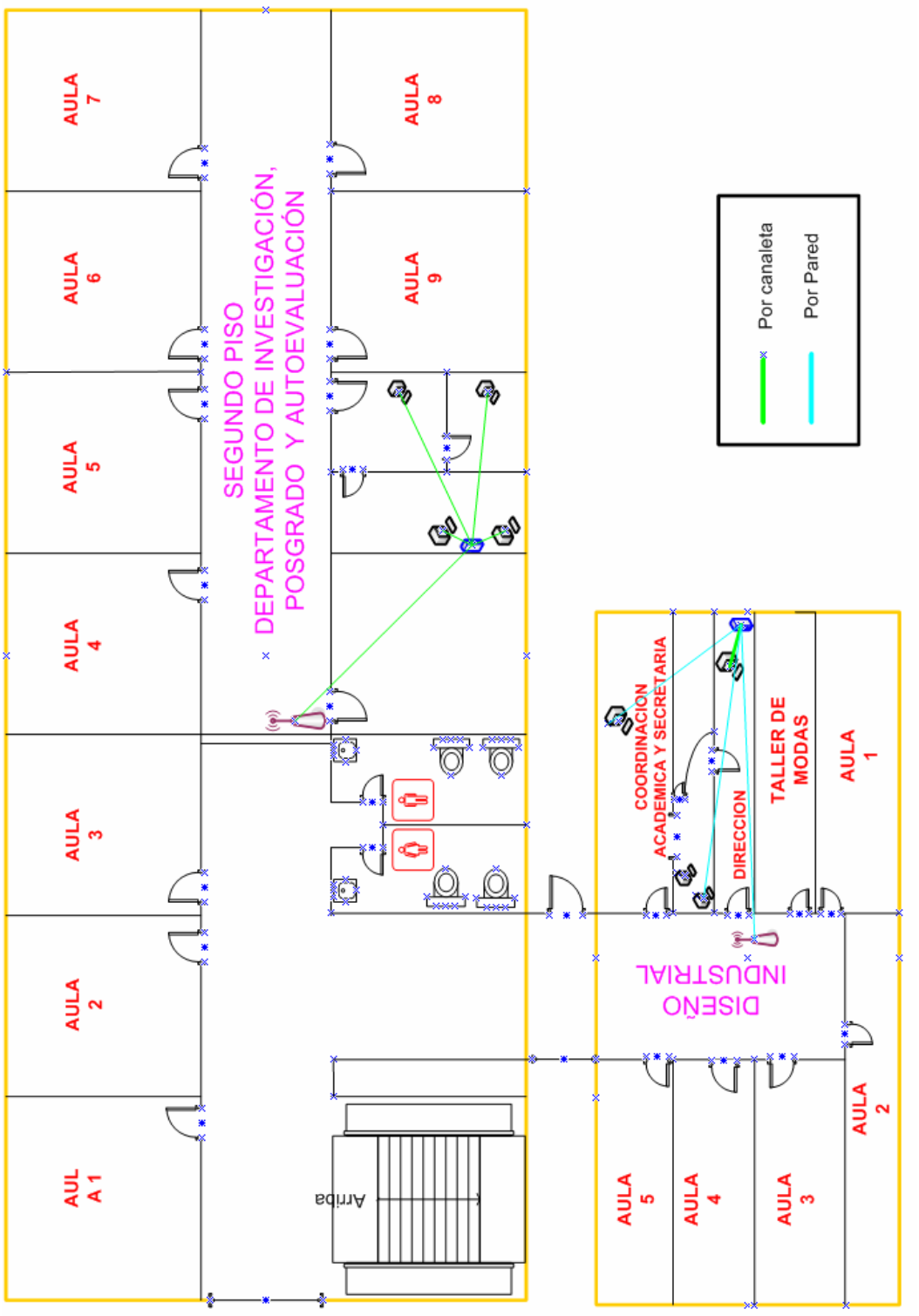


Gráfico 3.10: Interconexión del Segundo Piso

En el segundo piso se encuentra:

- Departamento de Investigación, Posgrado y Autoevaluación. Aquí existe un Switch CISCO 10/100 de 8 puertos al que se conectan: 4 Pc´s, un Access Point y 2 cables UTP que están libres para la conexión de cualquier Pc. Esta SWITCH esta pegado contra la pared tras de las computadores utilizadas por los profesores dedicados a la Investigación, como se puede observar en la siguiente imagen.

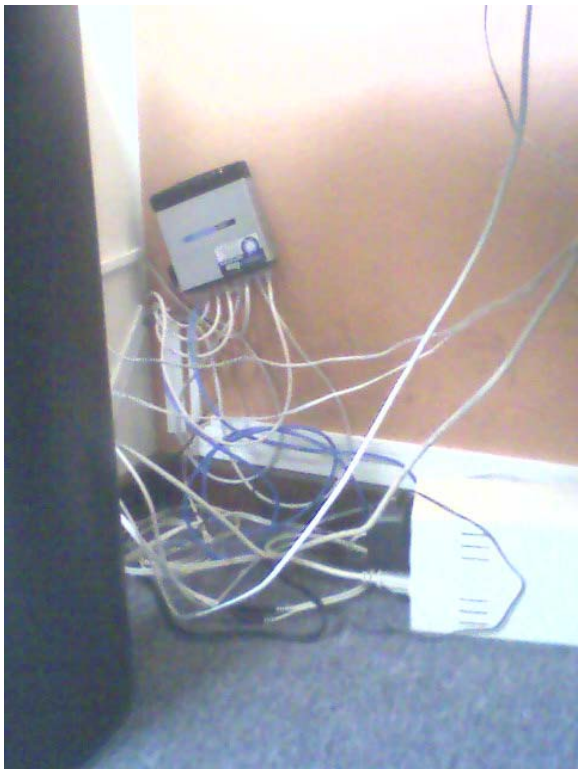


Gráfico 3.11: Switch en el Dpto. de Investigacion y Posgrado

- La Escuela de Diseño Industrial que posee 1 HUB ASANTE 10T de 8 puertos, al cual se conectan 1 Access Point y 3 Pc´s. Aunque existe una pc mas pero esta no está conectada a la red. Este HUB está en el piso

en la Dirección de la Escuela como se puede observar en la siguiente imagen.

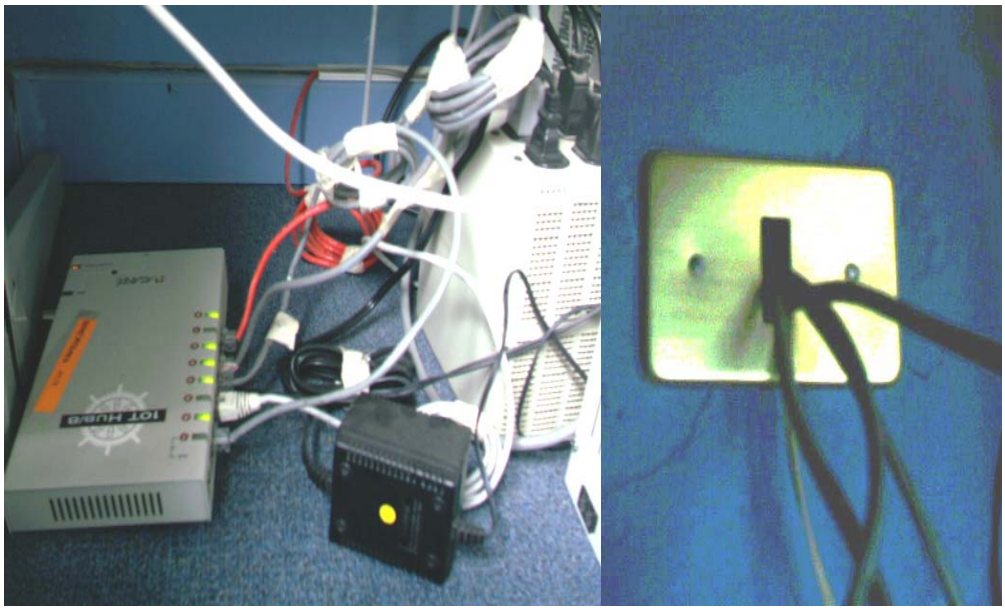


Gráfico 3.12: HUB de la Escuela de Diseño Industrial

Tercer Piso

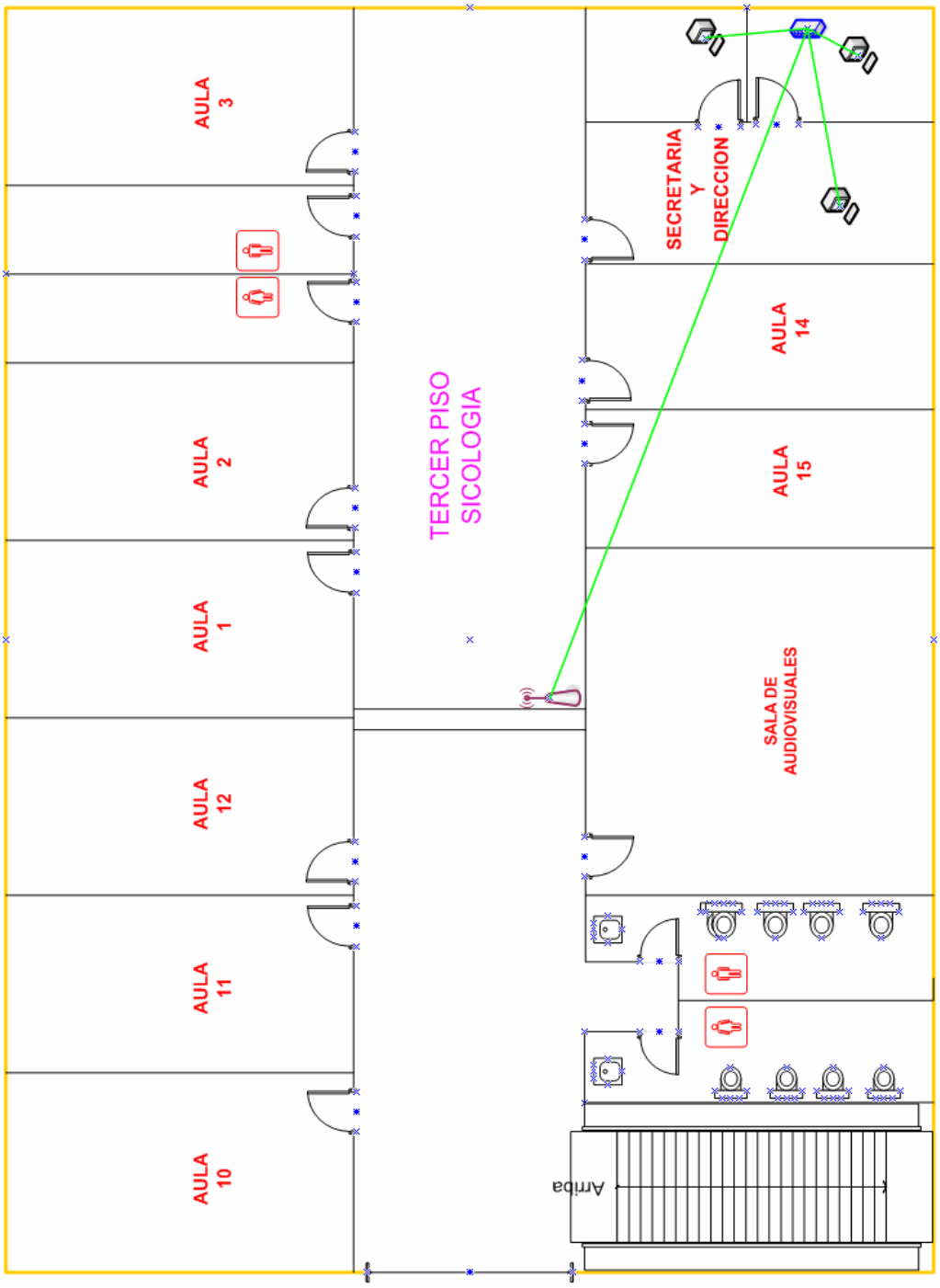


Gráfico 3.13: Interconexión del Tercer Piso

En el tercer piso trabaja la Escuela de Sicología. Aquí se encuentra 1 Switch Advantek Networks de 8 puertos al que se conectan 3 PC´s y 1 Access Point. Este Switch esta en el piso de la Dirección de la Escuela, bajo el escritorio del director como se puede observar en la siguiente imagen.

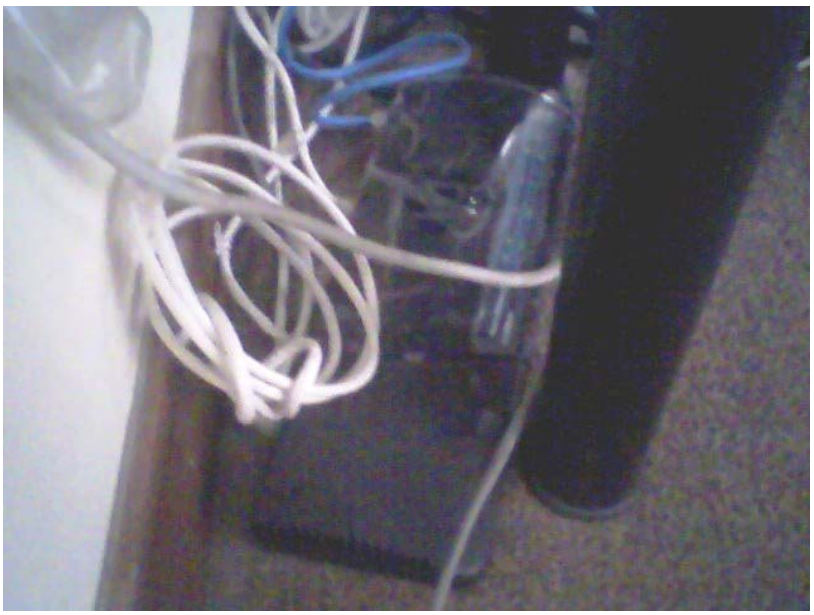


Gráfico 3.14: Switch de la Escuela de Sicología

Cuarto Piso

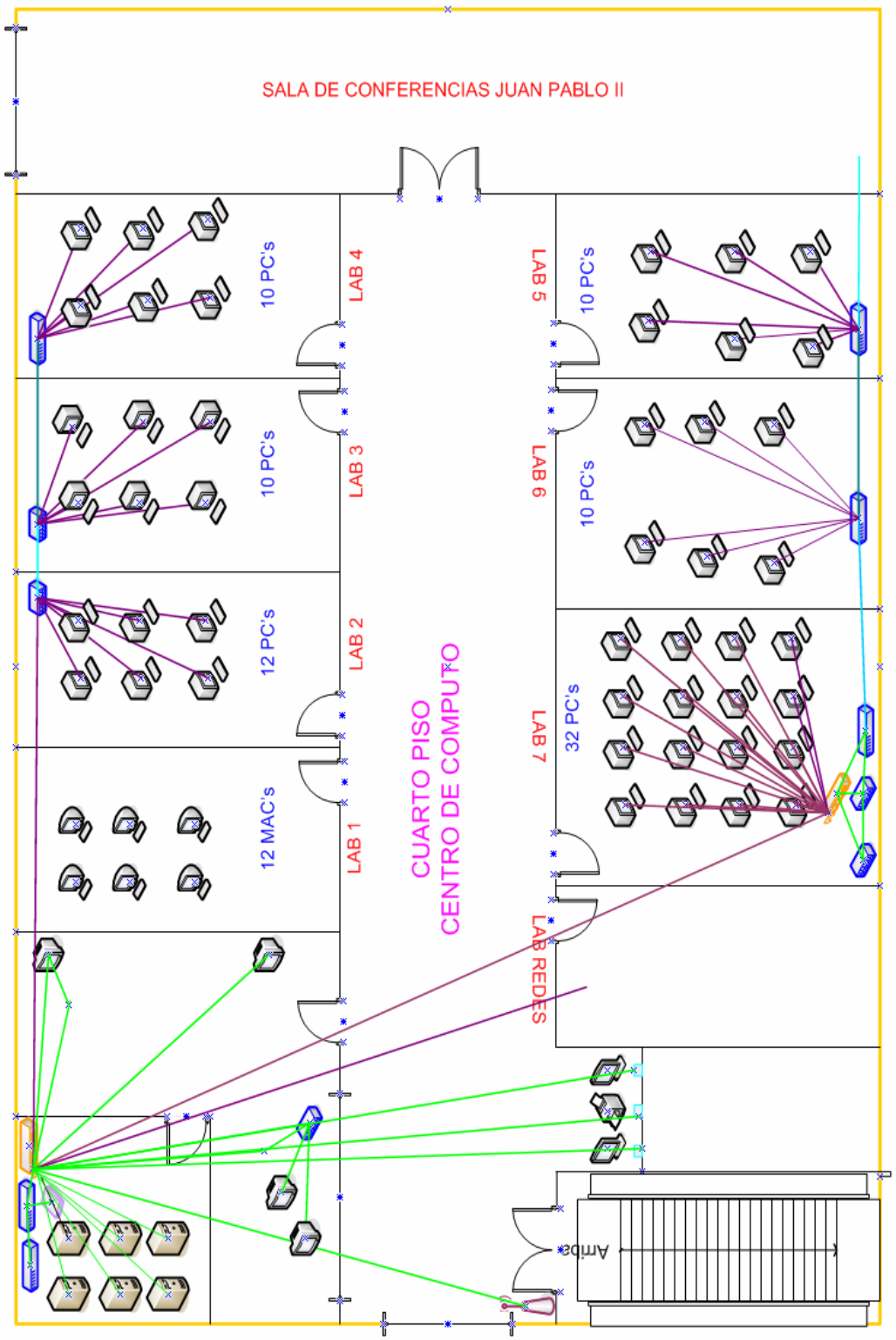


Gráfico 3.15: Interconexión del Cuarto Piso

En el cuarto piso existen 8 laboratorios, un cuarto de telecomunicaciones y un área donde se encuentra al kiosco de impresión y registro. En total existen 90 pc´s conectadas a la red, 12 MAC´s, 6 Servidores. Para su interconexión existen en este piso 11 Switch´s.

Cabe recalcar que las conexiones dentro de los laboratorios son subterráneas a través de mangueras y salen del piso, como se observa en la figura

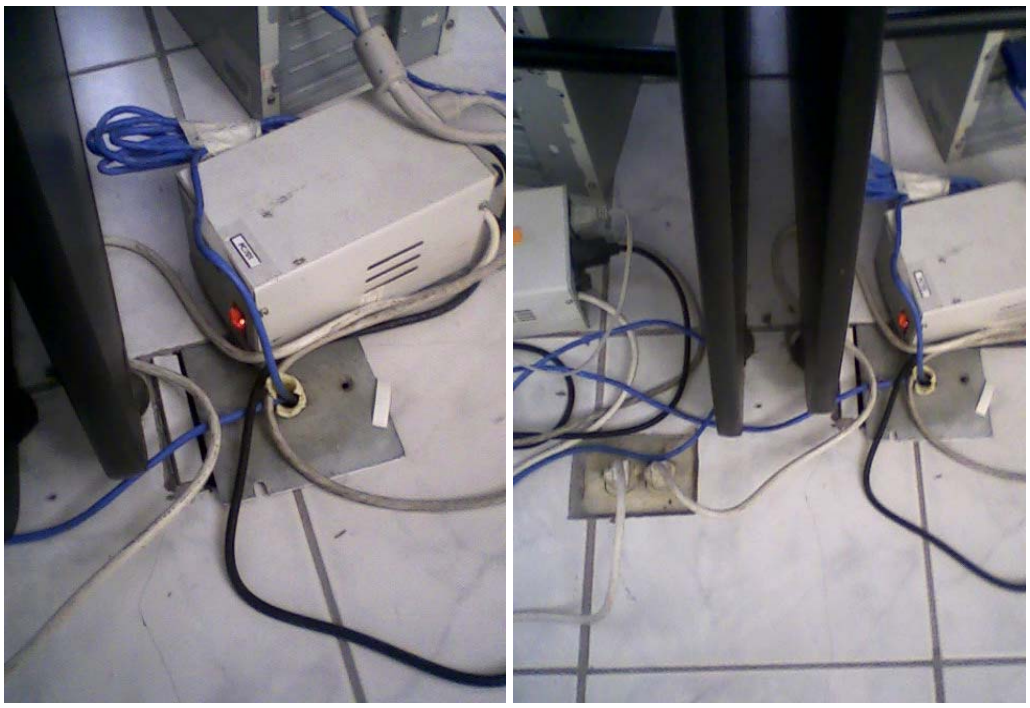


Gráfico 3.16: Conexiones subterráneas

- Laboratorio 1. Aquí existe 12 MAC´s que no están conectadas a la red.

Gráfico 3.17: Laboratorio 1

- Laboratorio 2. En este existen 12 Pc´s conectadas al Switch NEXXT 10/100 de 16 puertos, este laboratorio se conecta directamente con el cuarto de telecomunicaciones. Todos los puertos del Switch están ocupados, no se conoce por que. Como se observa en la figura el Switch esta en el piso.

Gráfico 3.18: Laboratorio 2

- Laboratorio 3 esta conformado por 10 Pc´s interconectadas a través de un Switch CNET 10/100 de 16 puertos, este laboratorio se interconecta con el laboratorio 2. Catorce puertos del Switch están ocupados. Este Switch esta empotrado en la pared.

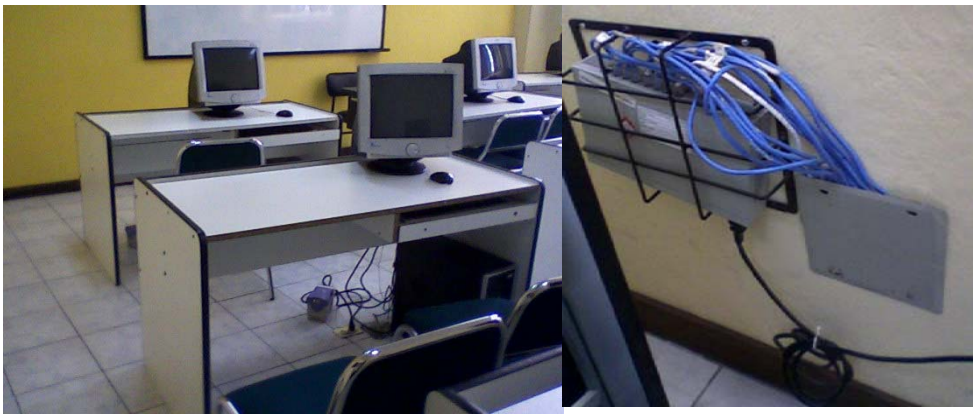


Gráfico 3.19: Laboratorio 3

- Laboratorio 4 formado por 10 Pc´s interconectadas a través de un Switch DIMAX Fast Ethernet de 16 puertos, este laboratorio se interconecta con el laboratorio 3. El SWITCH esta empotrado en la pared y 13 puertos están ocupados.

Gráfico 3.20: Laboratorio 4

- Laboratorio 7 aquí encontramos 32 pc´s interconectadas en un rack cerrado empotrado en la pared donde se tiene 3 SWITCH´S interconectados entre sí:

  - Un Switch CNET 100BaseTX / 10BaseT de 24 puertos, de los cuales 2 puertos están libres.
  - NEXXT 10/100 de 16 puertos, de los cuales 6 están libres.
  - DIMAX Fast Ethernet 10/100 de 16 puertos, de los cuales 4 puertos están libres.
  - También en el rack se encuentran 2 pacth panel de 24 puertos cada uno.

Gráfico 3.21: Laboratorio 7

Gráfico 3.22: Rack Abierto en Laboratorio 7

- Laboratorio 6 formado por 10 Pc´s interconectados a través de un Switch DIMAX Fast Ethernet de 16 puertos empotrado en la pared, están ocupados 13 puertos, este laboratorio se interconecta con el laboratorio 7. En este laboratorio existe UTP Cat 5e.

Gráfico 3.23: Laboratorio 6

- Laboratorio 5 está formado por 10 Pc´s interconectadas a través de un Switch DIMAX Fast Ethernet de 16 puertos y están ocupados 12, que a la vez se conecta con el laboratorio 6. Y desde este sale un punto de red a la Sala de Conferencias Juan Pablo II.

Gráfico 3.24: Laboratorio 5

- Laboratorio de redes a este laboratorio llega un punto de red pero ninguna PC se conecta a la red por ser un laboratorio de práctica.

Gráfico 3.25: Laboratorio de Redes

- Centro de Cómputo aquí existen 4 Pc´s, un Switch CNET de 16 puertos estan 4 ocupados y esta ubicado en el piso. En el Cuarto de Telecomunicaciones están ubicados: un rack abierto que cuenta con un patch panel, 2 Switch´s 3COM serie 4500, un modem SMARTAX MT 840 para conexión del Internet, 2 armarios de servidores en los cuales se alojan 6 Servidores: Dominio. Manager Server, Internet, Correo, Biblioteca, Antivirus.

Gráfico 3.26: Armarios de Servidores

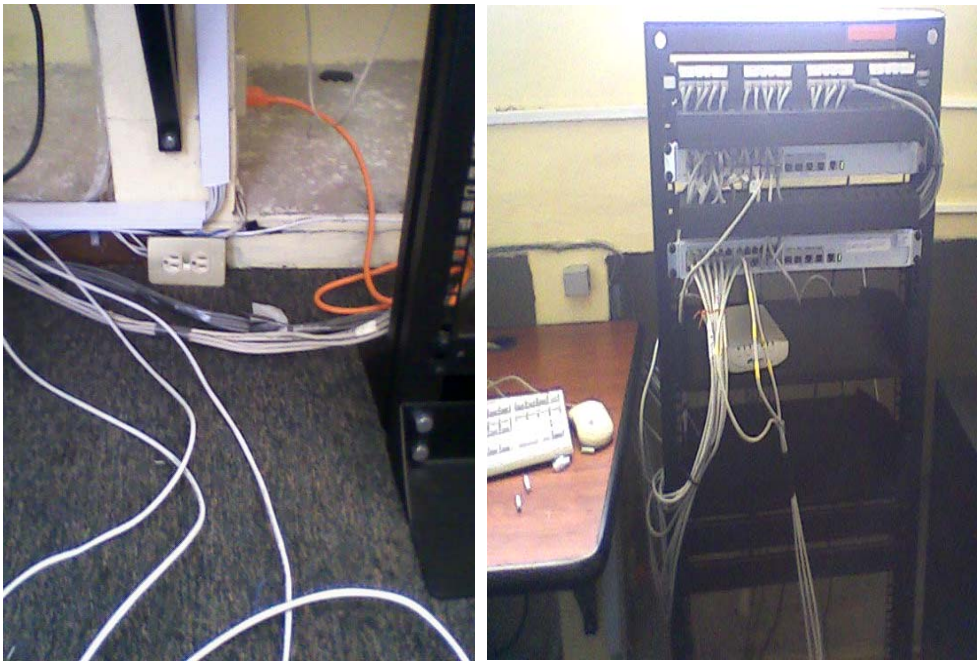


Gráfico 3.27: Rack Abierto

- Kiosko de Registro e Impresión, aquí llegan dos puntos de red. Desde el Switch Principal, a través de canaletas. Aquí existen 2 rosetas y los patch cord utilizan UTP Cat 5e.

Gráfico 3.28: Kiosko de Registro e Impresión

Edificio Nuevo

En este edificio los cables de distribución al primer, segundo, tercer y cuarto piso llegan al cielo raso y desde ahí bajan los cables por pared.

Primer Piso

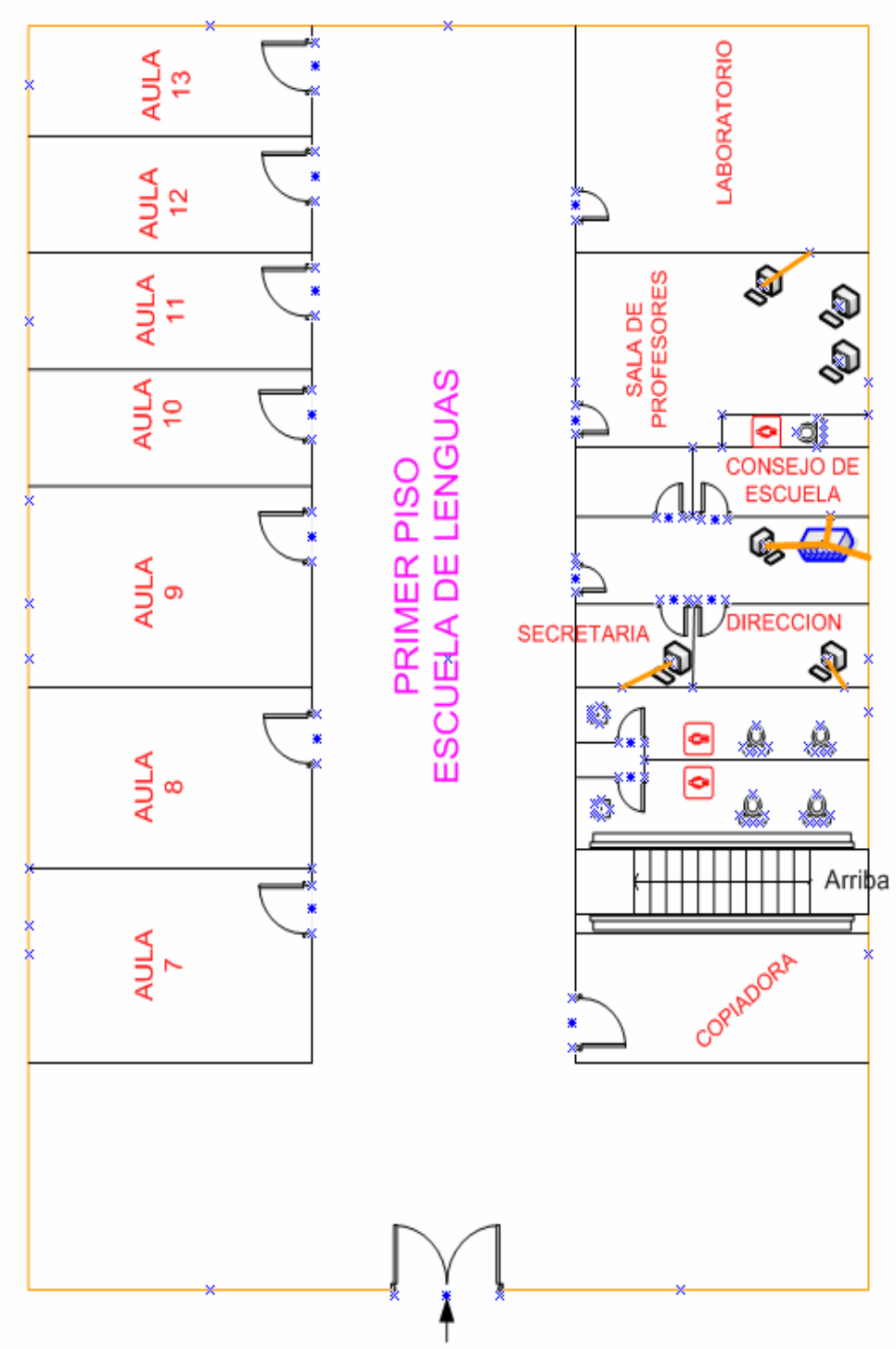


Gráfico 3.29: Interconexión del Primer Piso

En el primer piso funciona la Escuela de Lenguas. Aquí se encuentra 1 Rack abierto qué contiene un patch panel y un Switch 3COM 10100/BaseX/T y 1000BaseX/T de 24 puertos, de los cuales 12 están ocupados. A este edificio desde el rack principal le llegan dos puntos de red que se conectan a este Switch por redundancia, también en este piso encontramos 6 pc's, de las cuales 4 están conectadas a la red.

Gráfico 3.30: Rack Abierto del Edificio nuevo

Segundo Piso

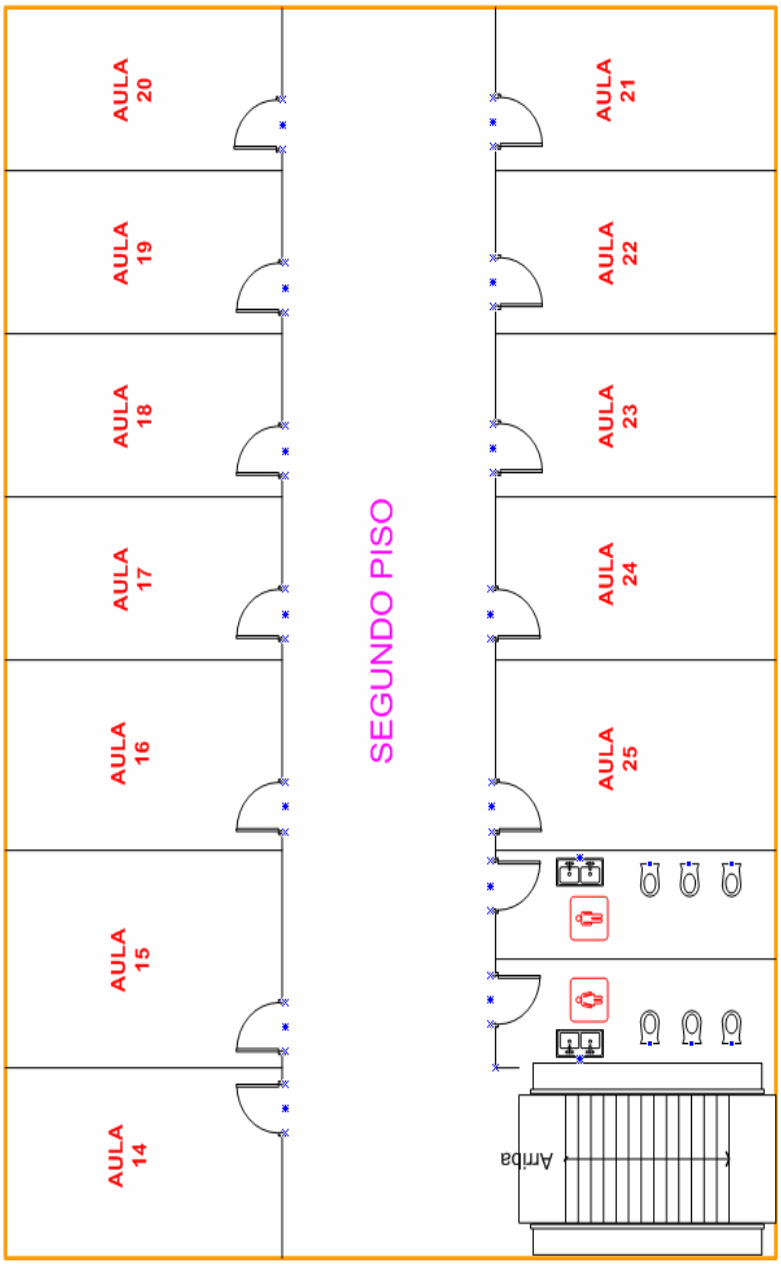


Gráfico 3.31: Interconexión del Segundo Piso

Al segundo piso desde el rack de este edificio le llegan 2 cables para futuras conexiones. Porque en este piso solo existen aulas.

Tercer Piso

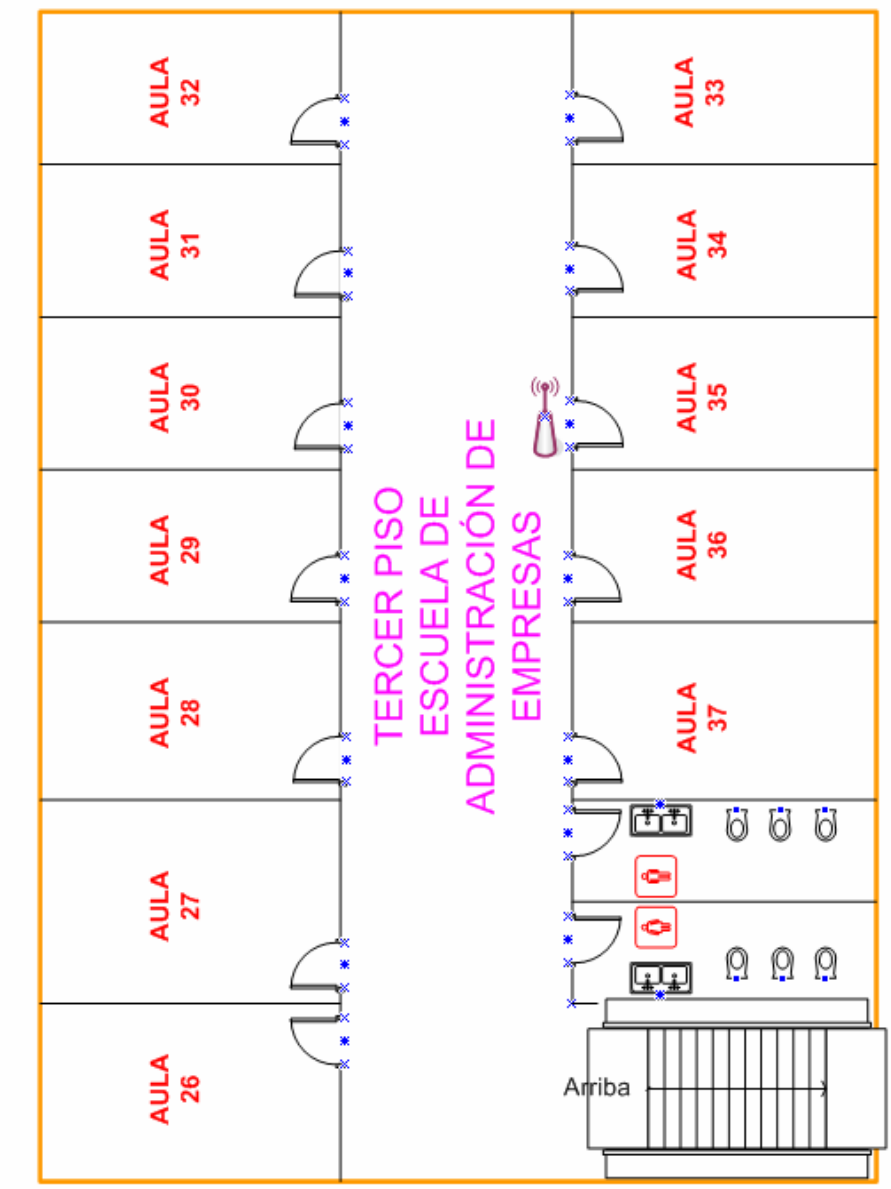


Gráfico 3.32: Interconexión del Tercer Piso

Al tercer piso desde el rack de este edificio le llegan 2 cables, uno de los cuales se conecta a un Switch 3COM 10100/BaseX/T y 1000BaseX/T de 24 puertos, a este se conecta un Access Point y el otro es para futuras conexiones.

Cuarto Piso

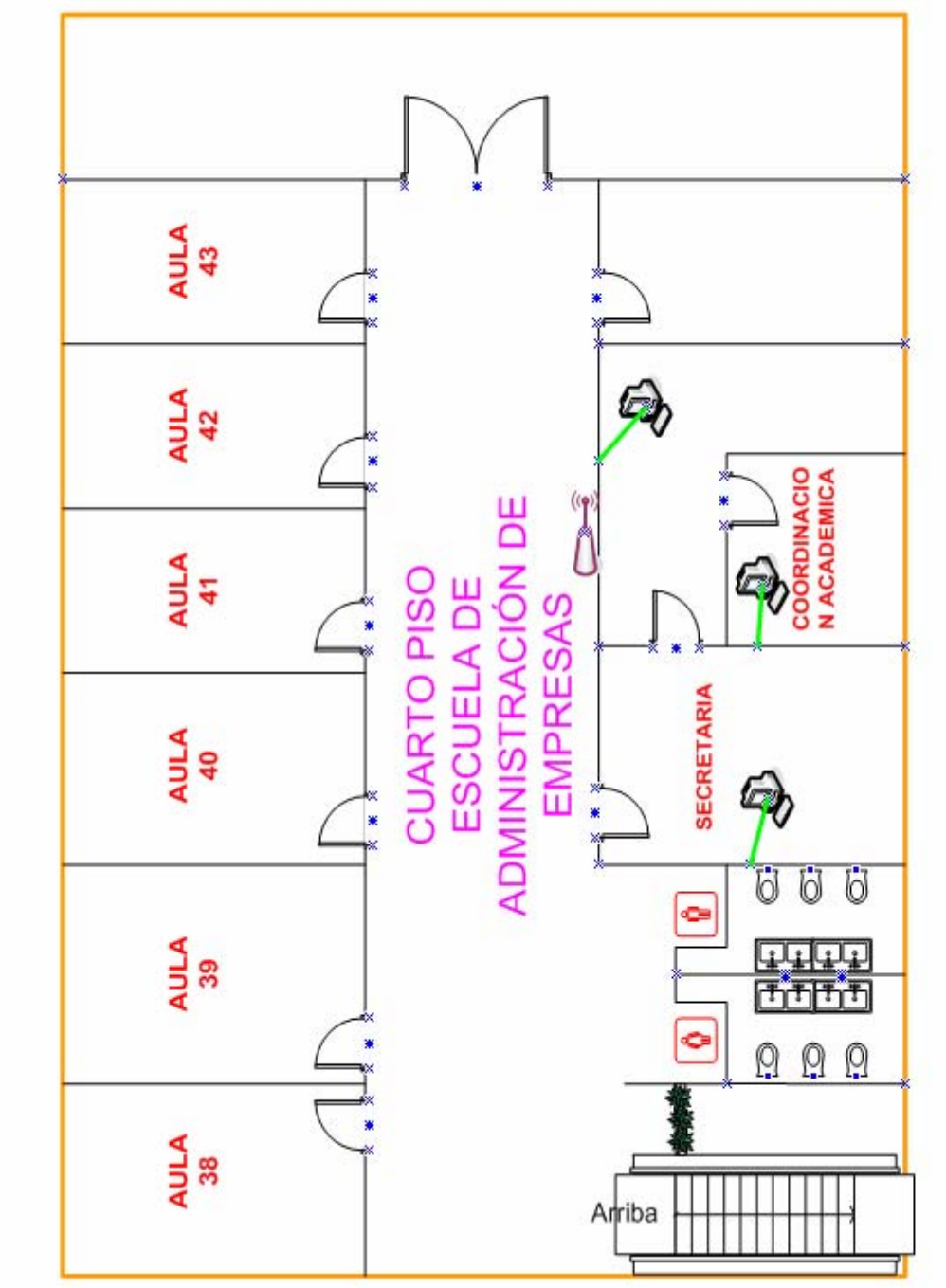


Gráfico 3.33: Interconexión del Cuarto Piso

En el cuarto piso funciona la Escuela de Administración de Empresas, a este piso desde el rack de este edificio le llegan 2 cables, uno de los cuales se

conecta al un Switch 3COM 10100/BaseX/T y 1000BaseX/T de 24 puertos, que está ubicado en el cielo raso y el otro es por redundancia. De este Switch se distribuye la conexión a 3 pc's ubicados en la dirección, secretaría, y en la sala de profesores.

Pastoral

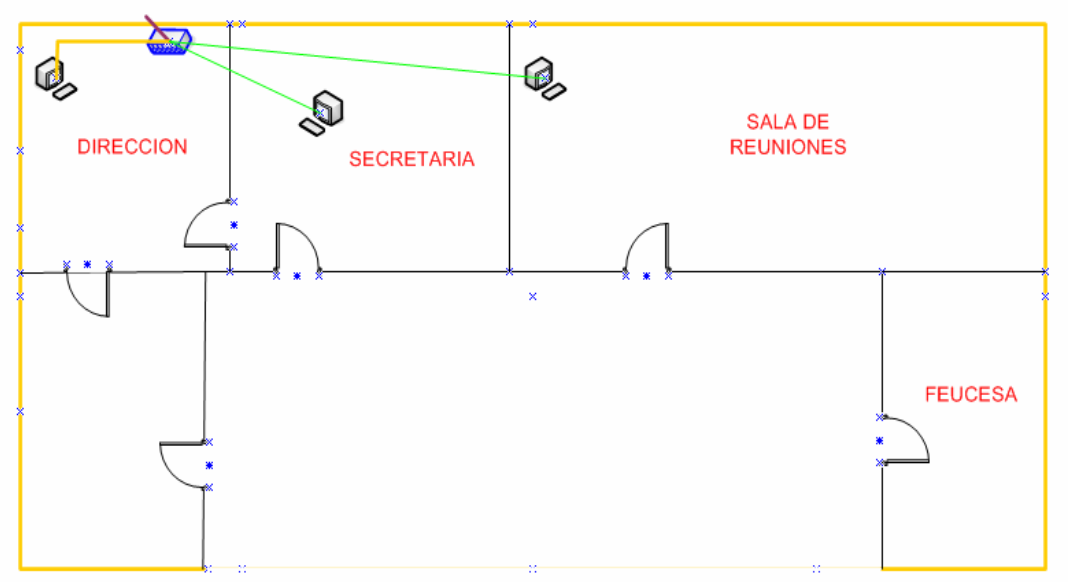


Gráfico 3.34: Interconexión de Pastoral

Pastoral es un área independiente de los edificios. Desde el rack principal le llega un punto de red que se conecta con el Switch existente en la Dirección. El Ing. Milton Jerez supo manifestar que llega 1 punto de red más, que está libre. El Switch es D-Link de 8 puertos 10/100 Fast Ethernet, de los cuales 4 están ocupados, pues desde el Switch que esta empotrado en la pared se conectan las tres pc's existentes, una en dirección, en secretaria y en la sala de reuniones.

Bar

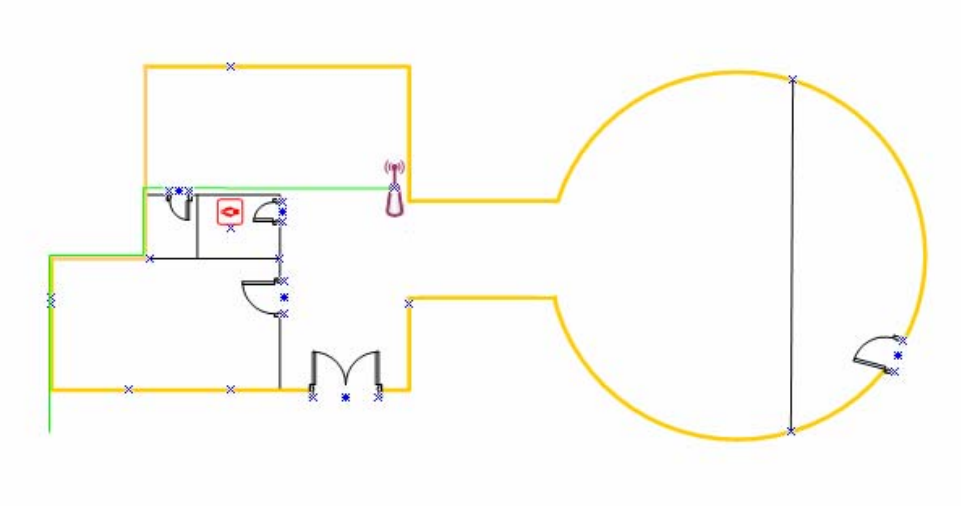


Gráfico 3.35: Interconexión del Bar

En el área del bar solo existe un Access Point cuya conexión viene desde el área administrativa.

3.1.3. Resumen de dispositivos en la red actual

Dispositivo	Modelo	No de Puertos	No de puertos ocupados	Ubicación	PC conectadas
MINI HUB		16	10	Dpto. Financiero	13 Conectadas, un Touch Hand, AP del Bar
Switch Advanced Network 10/100		8	7		
Switch Advanced Network 10/100		8	4	Dir. de Estudiantes	3 Pc´s
Switch NEXXT 10/100		16	11	Escuela de Sistemas	3 Pc´s Conexión a los 2 otros Switch´s
Switch CNET		8	3		2 AP´s
Switch CNET		8	3		1 Pc y 1 Servidor
Switch CNET		16	8	Biblioteca	6 Pc´s, 1 AP
Switch Advantek Networks 10/100		8	3	Escuela de Optometría	2 Pc´s
Switch CISCO 10/100		8	8	DIPA	4 Pc´s, un AP, y 2 cables sueltos

Dispositivo	Modelo	No de Puertos	No de puertos ocupados	Ubicación	PC conectadas
HUB ASANTE 10T		8	5	Escuela de Diseño Industrial	3 Pc´s y 1 AP
Switch Advantek Networks 10/100		8	5	Escuela de Sicología	3 PC´s y 1 AP
Switch NEXXT 10/100		16	16	Laboratorio 2	12 PC´s
Switch CNET 10/100		16	14	Laboratorio 3	10 PC´s
Switch DIMAX Fast Ethernet		16	13	Laboratorio 4	10 PC´s
Switch DIMAX Fast Ethernet		16	12	Laboratorio 5	10 PC´s
Switch DIMAX Fast Ethernet		16	13	Laboratorio 6	10 PC´s
Switch CNET 100BaseTX / 10BaseT		24	22	Laboratorio 7	32 PC´s
Switch NEXXT 10/100		16	10		
Switch DIMAX Fast Ethernet 10/100		16	12		
Switch CNET		16	4	Centro de Cómputo	4 Pc´s, 1 AP
2 Switch´s 3COM 1000BaseX/T	serie 4500 3CR175 61-91	24	44	Cuarto de Telecomu-nicaciones	A 21 puntos, 6 servidores, kiosco de impresión y registro
Modem SMARTAX	MT 840				Para conexión a Internet
Switch 3COM 1000BaseX/T	serie 4500 3CR175 61-91	24	12	Escuela de Lingüística	6 pc´s en el primer piso, 2 cables al segundo piso, tercer piso y cuarto piso
Switch 3COM 1000BaseX/T	serie 4500 3CR175 61-91	24	2	Piso 3	1AP
Switch 3COM 1000BaseX/T	serie 4500 3CR175 61-91	24	5	Escuela de Administra-ción	3 pc´s y 1 AP
Switch D-Link		8	4	Pastoral	3 pc´s

Tabla 3.1: Resumen de dispositivos en la red LAN actual

Dispositivo	Número
HUB	2
Switch DIMAX Fast Ethernet	4
Switch NEXXT 10/100	3
Switch CNET 10/100	6
Switch Advantek Networks 10/100	4
Switch CISCO 10/100	1
Switch´s 3COM serie 4500 3CR17561-91	5
Access Point (AP)	10
Computadores	136
kiosco de registro e impresión	2
Servidores	7

Tabla 3.2: Total de dispositivos en la red LAN actual

La mayoría de cables en la red de campus son UTP Cat 5e, existiendo algunos UTP Cat 5.

3.1.4. Análisis de la Red

3.1.4.1. Análisis de Encuestas y Entrevistas

Para determinar el estado de la red es necesario conocer la percepción de los usuarios con el servicio brindado, por lo que se realizaron encuestas en la universidad tanto al personal administrativo, docentes y estudiantes (ver encuestas en anexo 1), de estas se obtuvieron los siguientes resultados:

1. Cuántas horas promedio al día, usted utiliza la red de la PUCESA?

Respuestas	Ocurrencias
Menos de 2 horas	12
De 2 a 5 horas	16
Más de 5 horas	2
Total	30

Tabla 3.3: Resultados pregunta 1

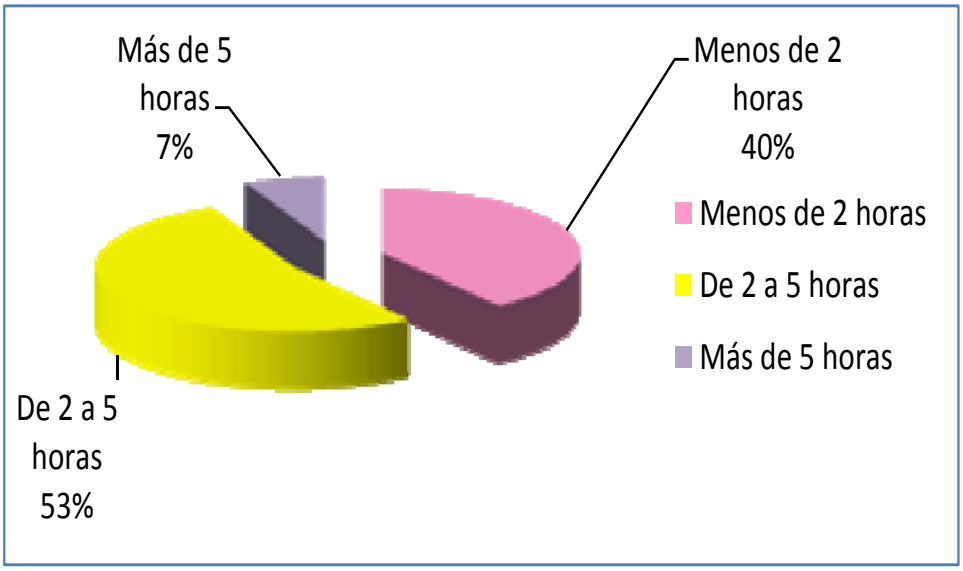


Gráfico 3.36: Tabulación Pregunta 1

Conclusión: De las 30 personas encuestadas 12 utilizan la red de la PUCESA menos de 2 horas diarias, 16 personas de 2 a 5 horas diarias y solo 2 personas la utilizan más de 5 horas al día. Por lo que se deduce que la red es más usada entre 2 y 5 horas diarias por cada usuario.

2. Cuáles son las aplicaciones que utiliza con mayor frecuencia?

Respuestas	Ocurrencias
Internet	28
Sistema Académico	14
Sistema Financiero	13
Biblioteca	11
Correo de la PUCESA	15
Pagina Web de la PUCESA	15
Compartir archivos entre computadoras de la red	21
Otras	0

Tabla 3.4: Resultados pregunta 2

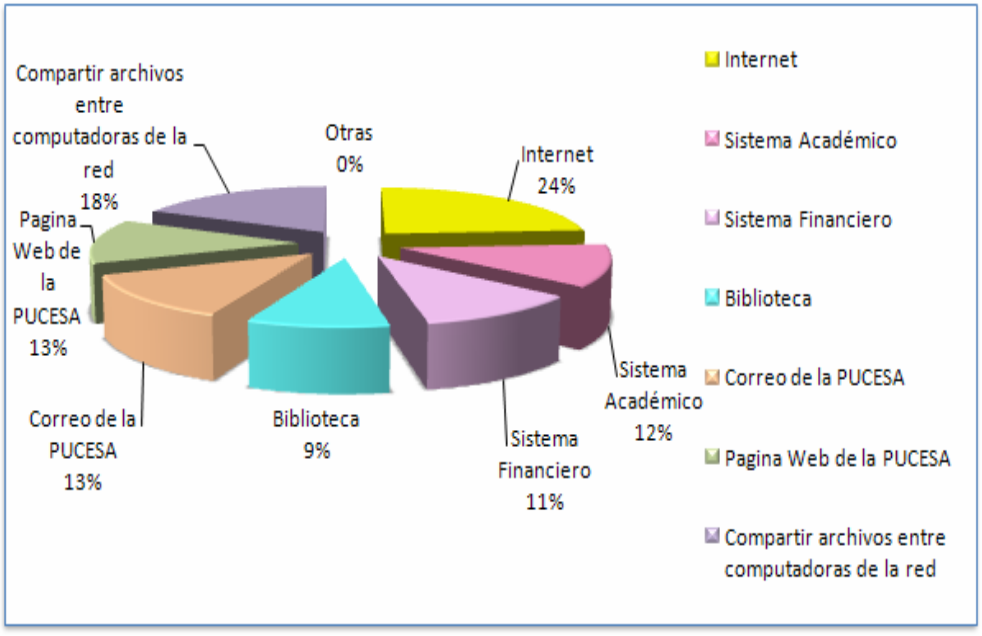


Gráfico 3.37: Tabulación Pregunta 2

Conclusión: La aplicación más utilizada por los usuarios de la red es el Internet, seguido del servicio de compartir y transmitir archivos. La mitad de los usuarios encuestados utilizan la página Web de la PUCESA y el correo electrónico, tomando en cuenta que la cantidad de alumnos triplica al número de personal administrativo, existe un gran número de usuarios que utilizan el Sistema Escolástico y Financiero. Dejando por último al sistema de Biblioteca debido a que no existe mucha bibliografía en la institución.

3. Cómo calificaría el servicio de Internet?

Respuestas	Ocurrencias
Excelente	1
Bueno	11
Medio	12
Regular	4
Malo	2
Total	30

Tabla 3.5: Resultados pregunta 3

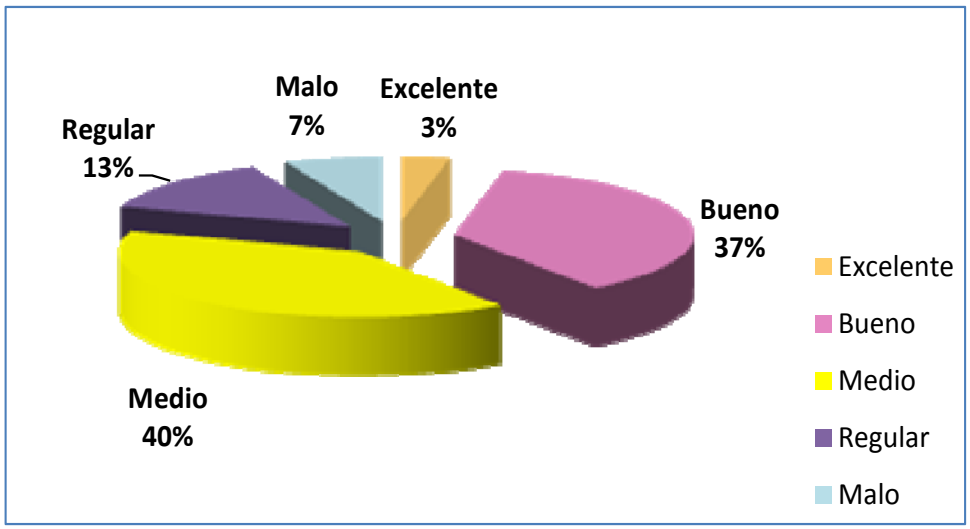


Gráfico 3.38: Tabulación Pregunta 3

Conclusión: La mayoría de personas opinan que el servicio de Internet tiene una calidad de media a buena.

4. Cómo calificaría el servicio de red de la PUCESA (transferencia de archivos, uso de aplicaciones en red)?

Respuestas	Ocurrencias
Excelente	1
Bueno	11
Medio	15
Regular	3
Malo	0
Total	30

Tabla 3.6: Resultados pregunta 4

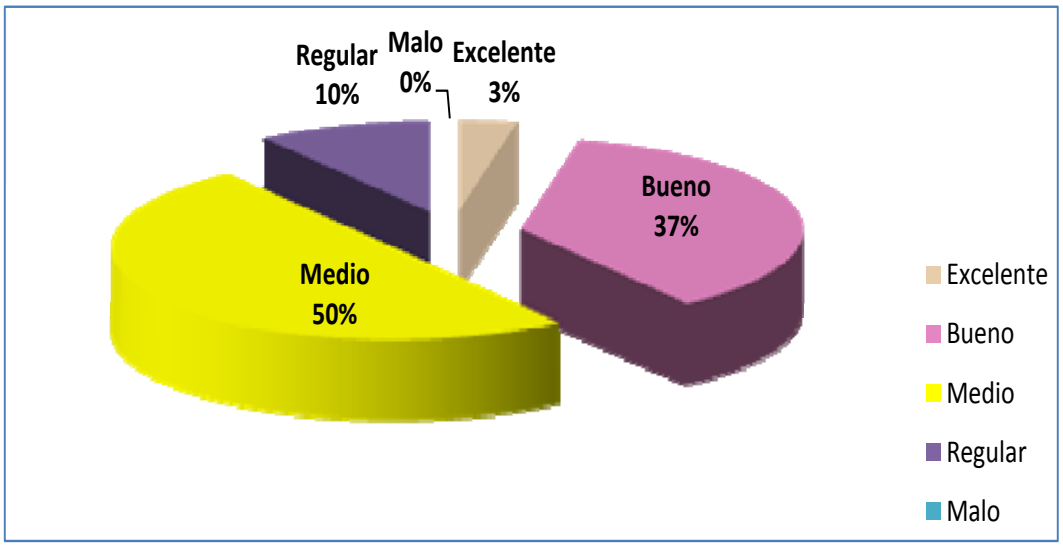


Gráfico 3.39: Tabulación Pregunta 4

Conclusión: De acuerdo a las respuestas obtenidas se determina que la calidad de servicio de la red de la PUCESA es media.

5. En qué horario tiene mayor dificultad con la calidad del servicio de la red?

Respuestas	Ocurrencias
Mañana	5
Tarde	7
Noche	11
Todo el día	7
Total	30

Tabla 3.7: Resultados pregunta 5

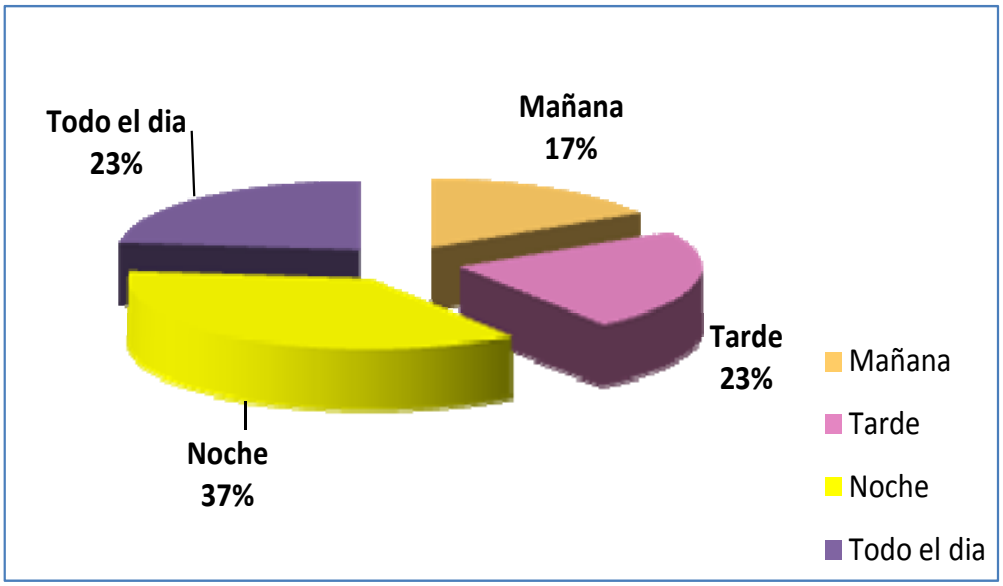


Gráfico 3.40: Tabulación Pregunta 5

Conclusión: En el horario que más ocurrencias tiene es el de la noche debido a que los estudiantes asisten más a la universidad en este horario.

6. Seleccione las características de la red actual de la PUCESA

RAPIDEZ

Respuestas	Ocurrencias
Alta	4
Media	22
Baja	4
Total	30

Tabla 3.8: Resultados pregunta 6

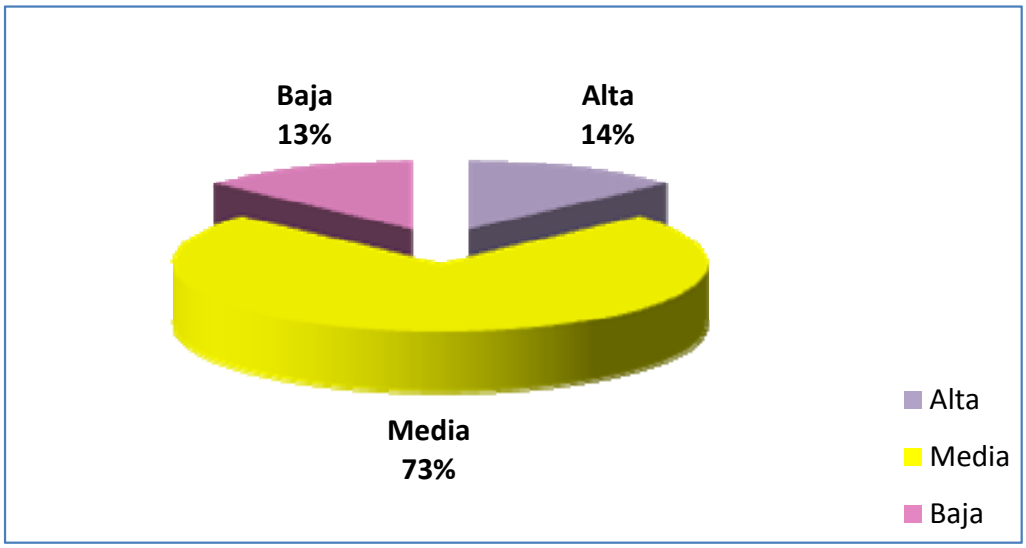


Gráfico 3.41: Tabulación Pregunta 6

Conclusión: Los usuarios catalogan qué la rapidez de la red en la universidad es de nivel media.

DISPONIBILIDAD

Respuestas	Ocurrencias
Alta	4
Media	21
Baja	5
Total	30

Tabla 3.9: Resultados pregunta 6

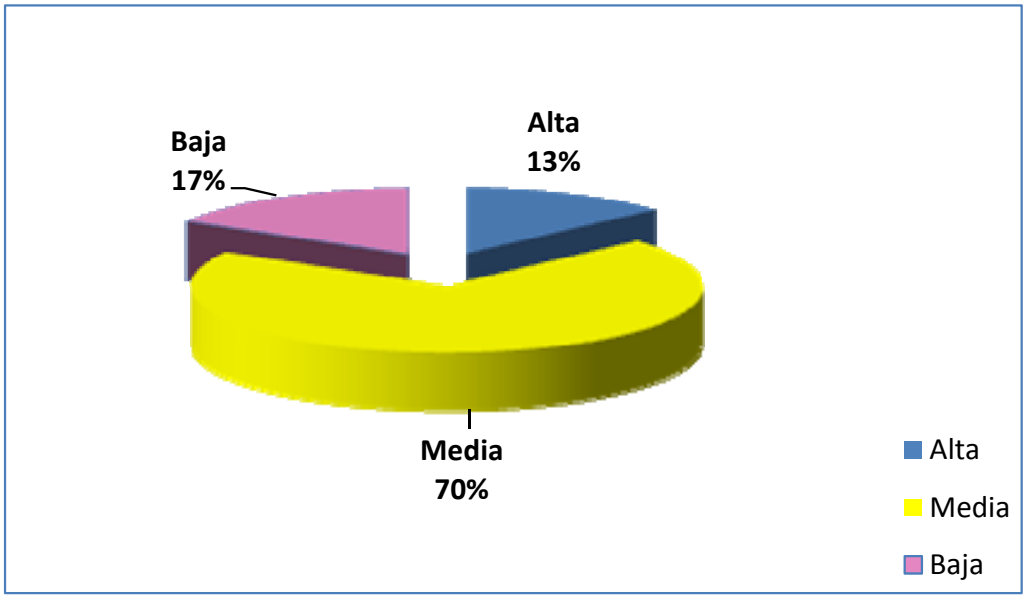


Gráfico 3.42: Tabulación Pregunta 6

Conclusión: La red tiene una disponibilidad catalogada por los usuarios de nivel medio.

SEGURIDAD

Respuestas	Ocurrencias
Alta	5
Media	19
Baja	6
Total	30

Tabla 3.10: Resultados pregunta 6

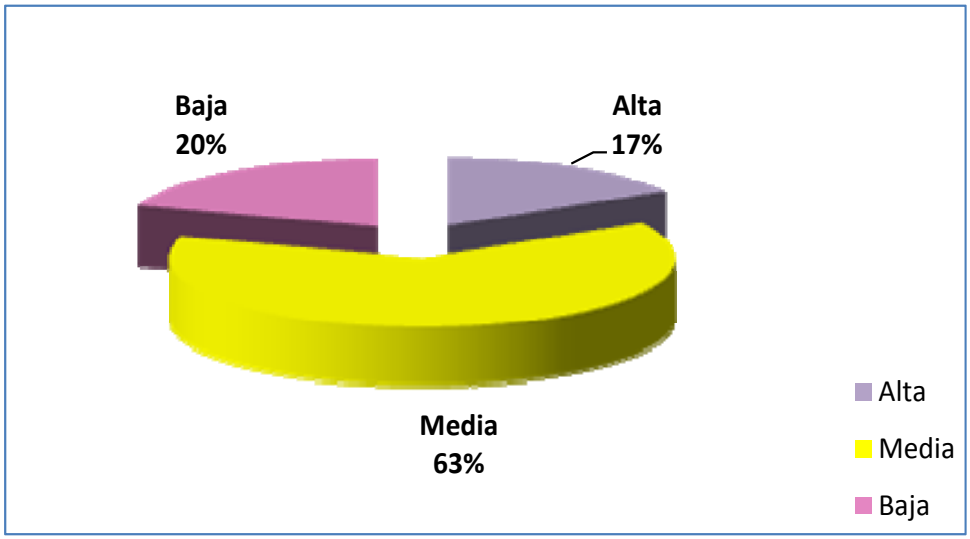


Gráfico 3.43: Tabulación Pregunta 6

Conclusión: Los usuarios opinan que los datos existentes en la universidad no están seguros, pues le catalogan como media al nivel de seguridad.

7. Qué servicios le gustaría utilizar en la red de la PUCESA?

Respuestas	Ocurrencias
Intranet	23
Correo electrónico interno	17
Video Conferencia	23
Voz sobre IP	9
Otros	6

Tabla 3.11: Resultados pregunta 7

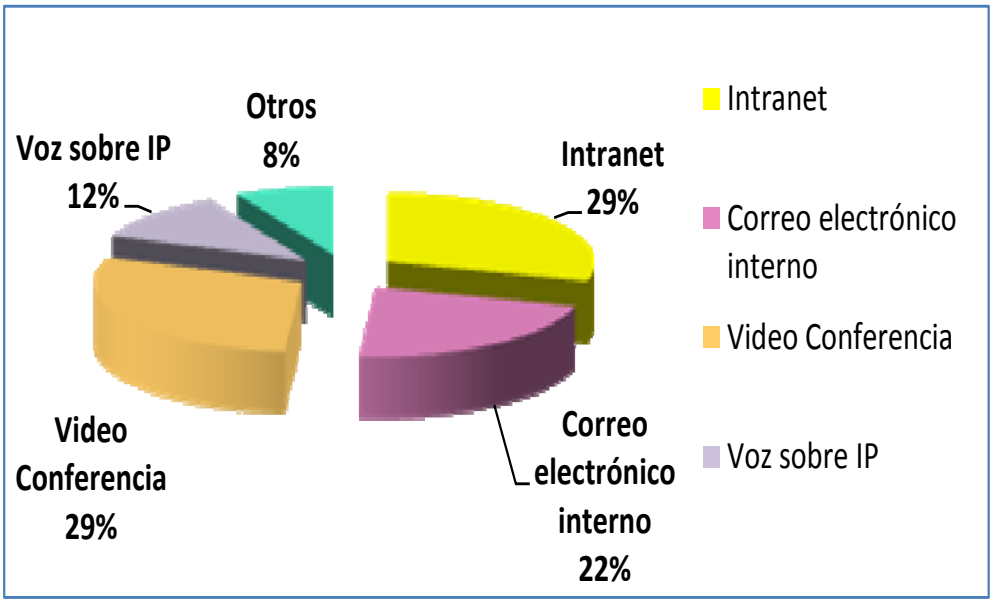


Gráfico 3.44: Tabulación Pregunta 7

Conclusión: A la mayoría de usuarios les gustaría contar con servicios como una Intranet, Video Conferencia y correo electrónico interno.

Entrevistas

Fue necesario también realizar dos entrevistas, para conocer las preguntas ver anexo 2, las mismas que se aplicaron al Ing. Diego Santacruz Director del Centro de Cómputo de las cuales se obtuvieron los siguientes resultados:

Las aplicaciones que están funcionando en la actualidad son:

- Aplicación Web (www.pucesa.edu.ec)
  - Control de entrada salida RRHH
  - Informativos de monitores (Touch Screen)
  - Auto evaluación
  - Evaluacion Docente
  - Control de Egresados
  - Bolsa de empleo
  - Extensión universitaria
  - Control de matriculas para procuraduría
  - Manejo de resolución de consejos
  - Documentación de contratos
  - Webmail
- Servidor de Antivirus
- Controlador de Dominio
- Sistema Académico - Escosoft
- Sistema Financiero - Safi
- Generación de solicitudes de estudiantes

Se está pensando a futuro utilizar dos aplicaciones proporcionadas por la PUCE Quito, las cuales son: Baank para el área financiera y Adam para el personal administrativo.

La red tiene un acceso de un 80% a sus recursos, tiene una alta disponibilidad, el problema se da con los recursos externos, especialmente con el servicio de Internet, actualmente se esta realizando pruebas con un nuevo proveedor Telconet es un canal ADSL de 1 a 1 con una velocidad de 1Mbps

Se requiere controlar el ancho de banda interno, proporcionándolo en el siguiente orden: laboratorios, financiero y personal administrativo. Así como también restringir el acceso a personas no autorizadas.

En la actualidad no se tienen registradas las fallas existentes en la red, sin embargo en el registro de los estudiantes a los laboratorios existe un casillero para observaciones donde se registran las fallas en las pc´s. No se registran las fallas pues son corregidas de inmediato y se conocen los equipos con que se cuenta en la red.

Con el anterior proveedor de Internet que era Andinanet muy esporádicamente no se tenía el servicio y las veces que ocurrieron no duraron más de una hora. En la actualidad se está realizando las pruebas con TELECOM.

3.1.4.2. Análisis con Ethereal Network Analyzer

Luego de realizadas las encuestas y entrevistas se empleo la herramienta ETHEREAL NETWORK ANALYZER que es un proyecto de software open source, liberado bajo la Licencia Pública GNU (GPL), es quizá uno de los mejores sniffers disponibles hoy en día, pues captura los paquetes de la red para posteriormente ser analizados.

Algunas de las características de Ethereal son:

- Disponible para UNIX y para Windows.
- Captura y muestra paquetes desde cualquier interface.
- Muestra paquetes capturados
- Guarda las capturas en varios formatos
- Filtra paquetes por muchos criterios.
- Busca paquetes usando filtros.
- Colorea paquetes basándose en filtros

Actualmente existen 3 redes: la 192.168.1 destinada al área administrativa, la 192.168.2 utilizada para los laboratorios y la 192.168.3 destinada a la red inalámbrica.

Ethereal fue utilizado para analizar la red 2, La dirección ip utilizada fue la 19.168.2.79 del laboratorio 7.

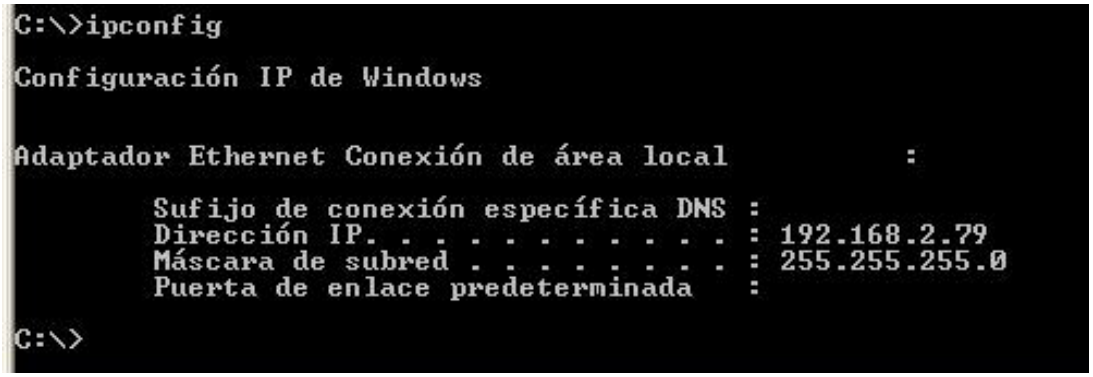


Gráfico 3.45: Ipconfig

El Software capturó los paquetes de la red en un tiempo aproximado de 1 hora 20minutos.

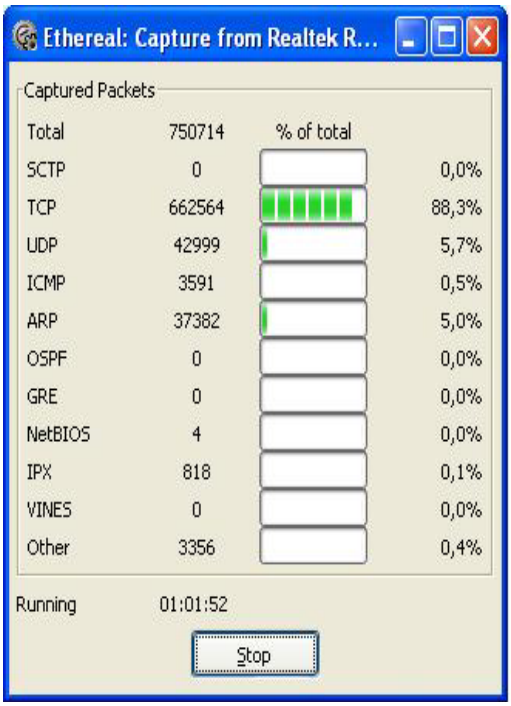


Gráfico 3.46: Captura de paquetes

Los resultados obtenidos fueron:

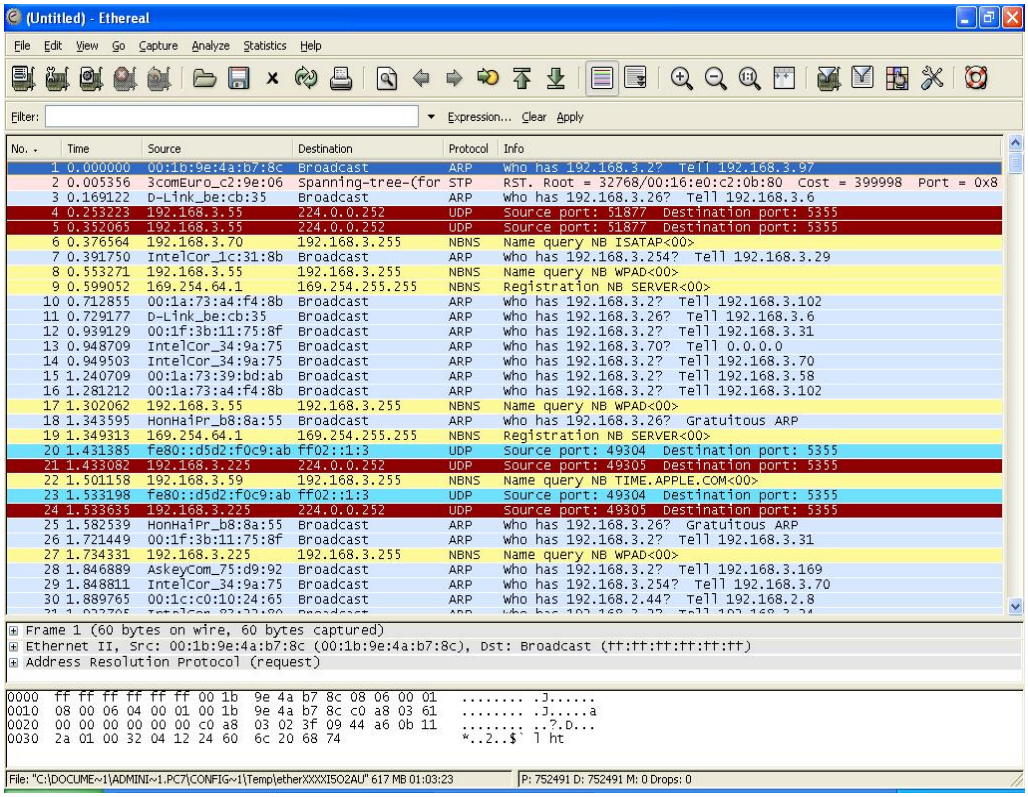


Gráfico 3.47: Resultados de paquetes capturados

Para observar mejor los resultados se hizo uso de las estadísticas graficas que proporciona la herramienta Ethereal.

A los protocolos se los visualiza con los siguientes colores

- ARP: Negro
- TCP color: Rojo
- UDP color: Verde
- HTTP color: Azul

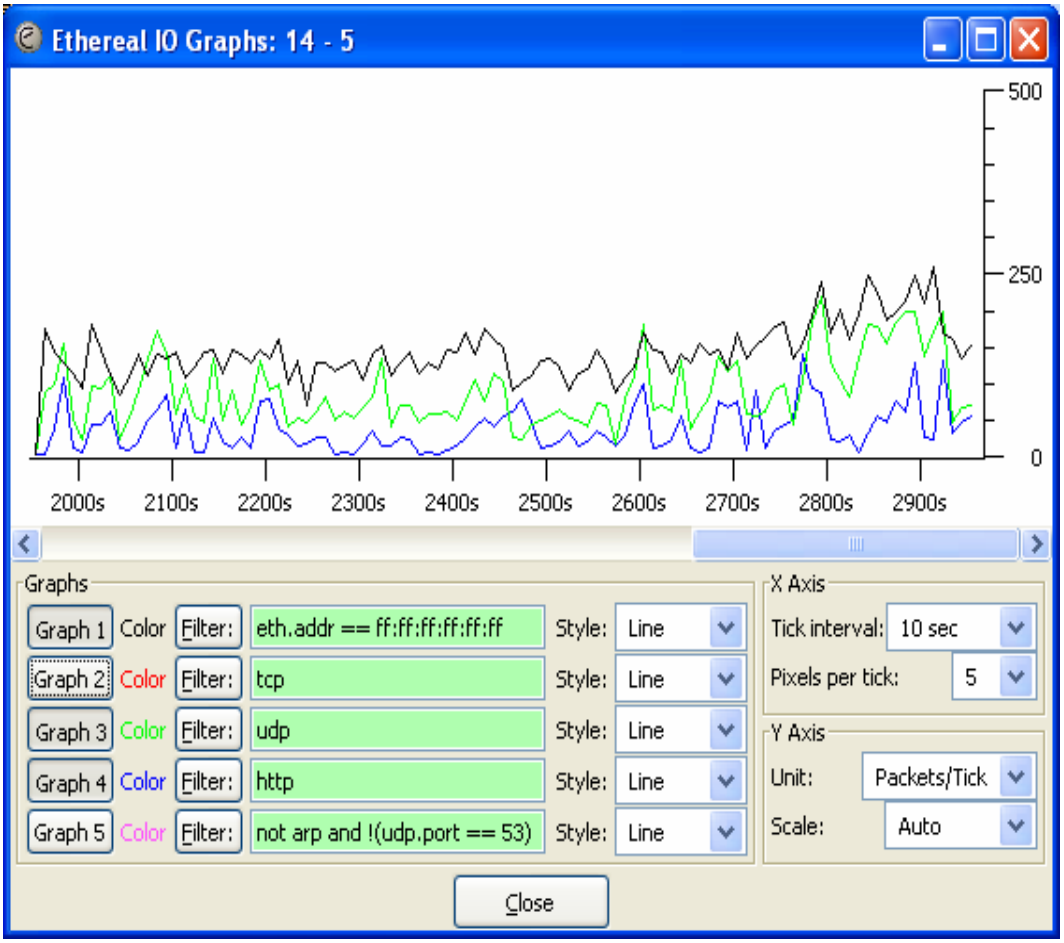


Gráfico 3.48: ARP comparado con HTTP y UDP

Como se puede observar el Broacast (ARP) es el recurso que mas ancho de banda consume en la red, comparado con UDP y HTTP, lo que implica un desperdicio de recursos al ser una red plana.

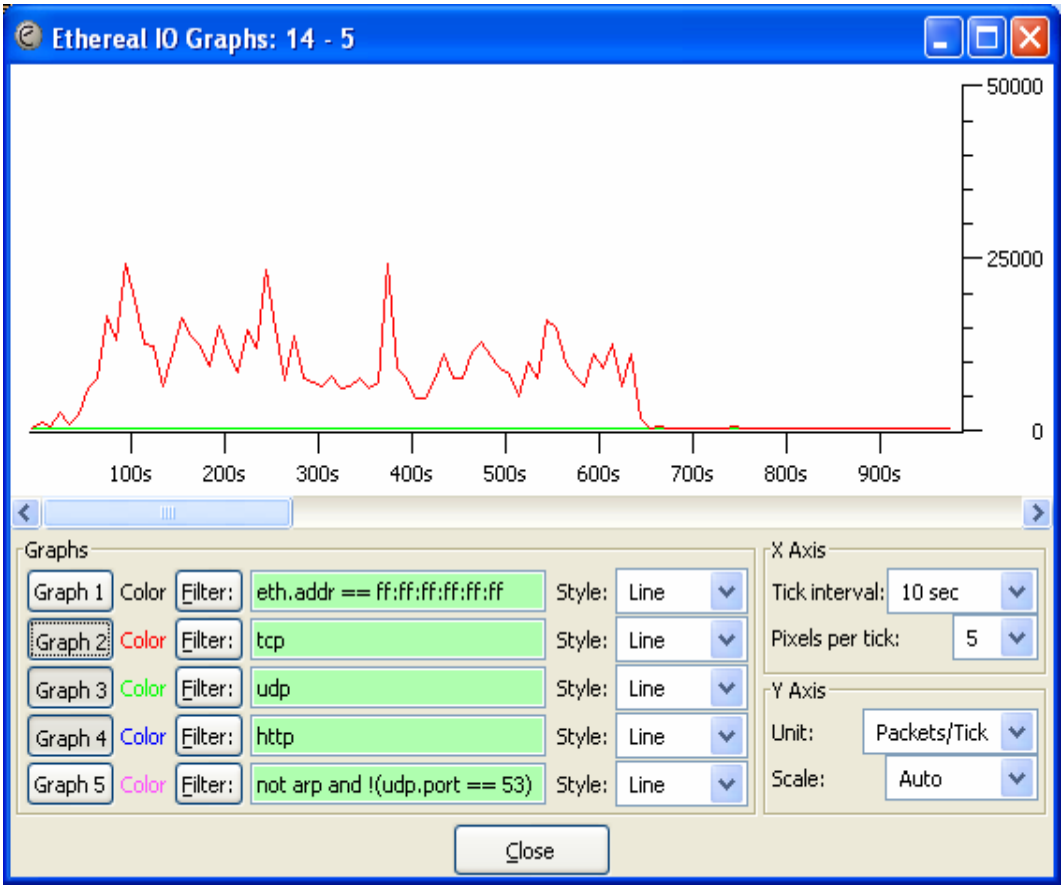
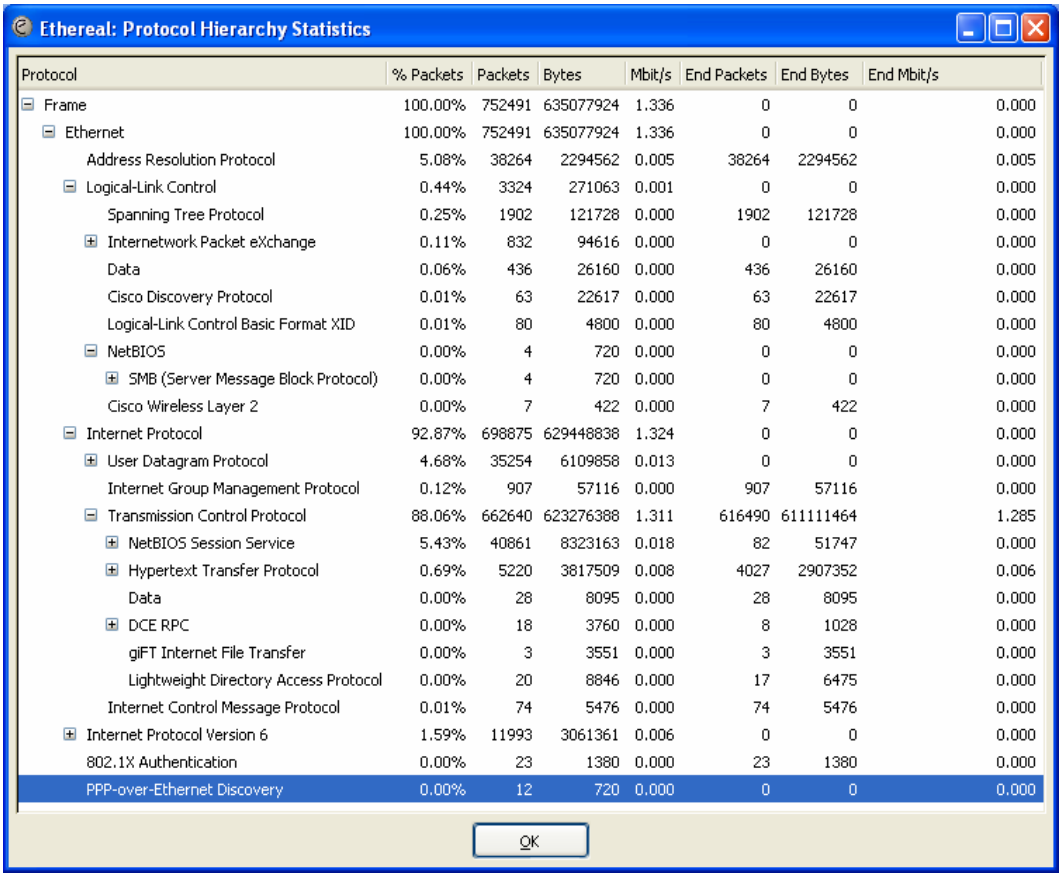


Gráfico 3.49: TCP comparado con UDP y HPTT

Pero el protocolo mas difundido es el TCP como se puede observar en el gráfico anterior.

A continuación se detalla en resumen los paquetes capturados con su respectivo porcentaje.



Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00%	752491	635077924	1.336	0	0	0.000
Ethernet	100.00%	752491	635077924	1.336	0	0	0.000
Address Resolution Protocol	5.08%	38264	2294562	0.005	38264	2294562	0.005
Logical-Link Control	0.44%	3324	271063	0.001	0	0	0.000
Spanning Tree Protocol	0.25%	1902	121728	0.000	1902	121728	0.000
Internetwork Packet eXchange	0.11%	832	94616	0.000	0	0	0.000
Data	0.06%	436	26160	0.000	436	26160	0.000
Cisco Discovery Protocol	0.01%	63	22617	0.000	63	22617	0.000
Logical-Link Control Basic Format XID	0.01%	80	4800	0.000	80	4800	0.000
NetBIOS	0.00%	4	720	0.000	0	0	0.000
SMB (Server Message Block Protocol)	0.00%	4	720	0.000	0	0	0.000
Cisco Wireless Layer 2	0.00%	7	422	0.000	7	422	0.000
Internet Protocol	92.87%	698875	629448838	1.324	0	0	0.000
User Datagram Protocol	4.68%	35254	6109858	0.013	0	0	0.000
Internet Group Management Protocol	0.12%	907	57116	0.000	907	57116	0.000
Transmission Control Protocol	88.06%	662640	623276388	1.311	616490	611111464	1.285
NetBIOS Session Service	5.43%	40861	8323163	0.018	82	51747	0.000
Hypertext Transfer Protocol	0.69%	5220	3817509	0.008	4027	2907352	0.006
Data	0.00%	28	8095	0.000	28	8095	0.000
DCE RPC	0.00%	18	3760	0.000	8	1028	0.000
giFT Internet File Transfer	0.00%	3	3551	0.000	3	3551	0.000
Lightweight Directory Access Protocol	0.00%	20	8846	0.000	17	6475	0.000
Internet Control Message Protocol	0.01%	74	5476	0.000	74	5476	0.000
Internet Protocol Version 6	1.59%	11993	3061361	0.006	0	0	0.000
802.1X Authentication	0.00%	23	1380	0.000	23	1380	0.000
PPP-over-Ethernet Discovery	0.00%	12	720	0.000	0	0	0.000

Gráfico 3.50: Estadística de Jerarquía de Protocolos

Los mismos resultados se obtienen en las otras 2 redes pues la configuración es la misma.

3.1.5. Diagnóstico

3.1.5.1. Factores que debe cumplir la red LAN

- Funcionalidad: favorecer el nivel de aplicación entre usuarios y sus prestaciones (velocidad, seguridad, etc)
- Escalabilidad: permite el crecimiento sin grandes modificaciones
- Adaptabilidad: capaz de integrar nuevas tecnologías

- Manejabilidad: Que permita una fácil monitorización
- Disponibilidad: Respecto a la red, las prestaciones como tiempo de respuesta, productividad, continuidad y acceso de los recursos

3.1.5.2. Resultados Obtenidos

Luego del análisis realizado en base a la observación de la estructura de la red, del conocimiento del nivel de satisfacción de los usuarios sobre el estado de la red y del uso de Ethereal se han detectado los siguientes problemas:

- Red plana con un solo dominio de broadcast, es decir los paquetes se envían a toda la red, aunque vayan dirigidos a un único destinatario,
- Sobrecarga de tráfico en las Estaciones de Trabajo, ya que esta decide si acepta o rechaza una trama Ethernet.
- Falta de una plan de contingencias y planificación estratégica en el Departamento de Cómputo.
- Falta de mecanismos de Seguridad y Monitoreo en la infraestructura de la red de campus universitario.
- Presenta poca funcionalidad de acuerdo a los resultados de las encuestas realizadas.
- Es poco escalable por este motivo existe cascadeo en la interconexión y los puntos de red son desorganizados.
- En el semestre actual se incrementaron cámaras de seguridad qué están conectadas a una pc y debido a este incremento aumentaron las

canaletas, instalándose las conexiones en donde había espacio lo que representa que no es una red adaptable

- Los servidores en la actualidad no cuentan con UPS, lo que implica que cuando se va la luz estos se apagan, pudiendo producirse pérdidas de información y de equipos; la red wireless presenta una buena señal solo en determinados lugares, pues existe interferencia por las paredes del edificio.
- No cumple los estándares de cableado estructurado, la mayoría de equipos de interconexión están en el piso empolvados.
- Pocos son los cables etiquetados por lo que existe aglomeración de cables y desconocimiento de donde provienen o a dónde van los mismos.
- Existen 2 HUB´s en la PUCESA lo que limita a sus usuarios en la utilización ancho de banda y por ende incrementa el broadcast.

3.2. Solución Propuesta

3.2.1. Análisis

Primero se determinará los requerimientos existentes para el rediseño de la red LAN, los mismos que están divididos en:

- Requerimientos de usuarios
- Requerimientos de aplicaciones
- Requerimientos de Host

- Requerimientos de Red
- Análisis del flujo de datos

3.2.1.1. Requerimientos de usuarios

Requerimientos de usuario	Descripción	Total
Localización y número de usuarios	Área Administrativa con un total de 17 usuarios	151 usuarios
	Escuela de Sistemas con un total de 3 usuarios	
	Biblioteca con un total de 6 usuarios	
	Escuela de Optometría con un total de 3 usuarios	
	Departamento de Investigación, Posgrado y Autoevaluación con un total de 4 usuarios	
	Escuela de Diseño Industrial con un total de 4 usuarios	
	Escuela de Sicología con un total de 3 usuarios	
	Centro de Cómputo con un total de 3 usuarios	
	Laboratorio 1 con un total de 12 usuarios	
	Laboratorio 2 con un total de 12 usuarios	
	Laboratorio 3 con un total de 10 usuarios	
	Laboratorio 4 con un total de 10 usuarios	
	Laboratorio 5 con un total de 10 usuarios	
	Laboratorio 6 con un total de 10 usuarios	
	Laboratorio 7 con un total de 32 usuarios	
	Escuela de Lenguas con un total de 6 usuarios	
	Escuela de Administración de Empresas con un total de 3 usuarios	
	Pastoral con un total de 3 usuarios	
Localización y número de Router Wireless	Edificio Principal primer piso 2	15
	Edificio Principal segundo piso 2	
	Edificio Principal tercer piso 1	
	Edificio Principal cuarto piso 2	
	Biblioteca 1	
	Bar 1	
	Escuela de Optometría 1	
	Edificio Nuevo primer piso 1	
	Edificio Nuevo segundo piso 1	
	Edificio Nuevo tercer piso 1	

Requerimientos de usuario	Descripción	Total
	Edificio Nuevo cuarto piso 1	
	Pastoral 1	
Crecimiento esperado en el número de usuarios	En un año	7%
	En dos años	11%
Expectativas del usuario	Rapidez Disponibilidad Seguridad Confiabilidad	

Tabla 3.12: Requerimientos de Usuarios

3.2.1.2. Requerimientos de aplicaciones

De acuerdo a los resultados de las encuestas y entrevistas realizadas se determinó las aplicaciones existentes y con las que a futuro se podría contar, las mismas que se detallan a continuación:

Aplicaciones Existentes		
Código	**Nombre**	**Tamaño promedio de datos**
Aplicación A	Aplicaciones Web	2 Mbps
Aplicación B	Sistema Escolástico	40 Mbps
Aplicación C	Generación de solicitudes de estudiantes	1 Mbps
Aplicaciones Futuras		
Código	**Nombre**	**Tamaño promedio de datos**
Aplicación D	Sistema Financiero	40 Mbps
Aplicación E	Sistema Administrativo	40 Mbps
Aplicación F	Correo electrónico para toda la PUCESA	3.33 Mbps
Aplicación G	Intranet	2 Mbps
Aplicación H	Video Conferencia	8 Mbps

Tabla 3.13: Requerimientos de Aplicaciones

A las aplicaciones determinadas es necesario categorizarlas dependiendo de su función y del rendimiento que se espera de las mismas.

Aplicaciones	Misión Crítica	Tiempo Real	Best - Effort
Aplicación A			X
Aplicación B			X
Aplicación C			X
Aplicación D			X
Aplicación E			X
Aplicación F			X
Aplicación G			X
Aplicación H	X		

Tabla 3.14: Categorización de Aplicaciones

3.2.1.3. Requerimientos de host

Del estudio de campo realizado se determinó los siguientes requerimientos de host:

Tipo de Host o Equipo	Cantidad - Ubicación
Estaciones de Trabajo	138 – Escuelas, departamentos y unidades administrativas
MAC´s	12 – Laboratorio 1
Hand Punch	1 – Área Administrativa
Wireless Router	15 – En todos los pisos de los edificios de la universidad.
Servidor de Aplicación A y G	2 – Centro de cómputo
Servidor de Aplicación B y C	2 – Centro de cómputo
Servidor de Aplicación D	1 – Centro de cómputo
Servidor de Aplicación F	1 – Centro de cómputo
Servidor de Aplicación H	1 – Centro de cómputo

Tabla 3.15: Requerimientos de Host

3.2.1.4. Requerimientos de red

Tomando en cuenta el estudio realizado se ha determinado los siguientes requerimientos.

- Incrementar el ancho de banda disponible para cada usuario final dependiendo de las aplicaciones que utilice cada escuela, departamento y/o unidad administrativa.
- Diseño jerárquico de la red de campus.
- Aplicar las normas de cableado estructurado.
- Emplear el manejo de VLANs para organizar a los usuarios de la red en grupos de trabajo lógico que sean independientes de la topología física del armario de instalación.
- Reducir los costos de administración de las operaciones de la red, simplificándola y facilitando las reconfiguraciones.
- Proveer escalabilidad, control de tráfico, y mayor seguridad
- Proporcionar soporte integrado para agentes de monitoreo.
- Facilidad de configuración
- Proveer calidad de servicios (QoS).

3.2.1.5. Análisis del flujo de datos

En este diagrama se representa el flujo de información en la red tomando en cuenta que todas las aplicaciones estarán ubicadas en los servidores del Centro de Cómputo.

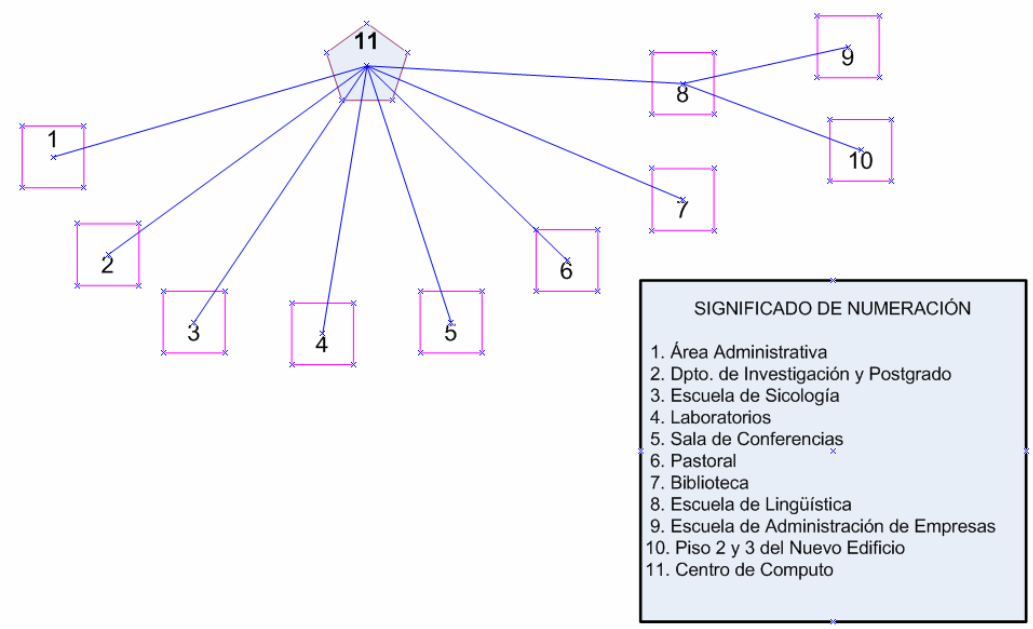


Gráfico 3.51: Distribución de flujo

Para completar el análisis es necesario establecer el modelo y la distribución del flujo de datos.

Aplicación	Id de flujo	Modelo	Distribución
A	Fa	Cliente - Servidor	80/20 (local/remoto)
B	Fb	Cliente - Servidor	80/20 (local/remoto)
C	Fc	Cliente - Servidor	20/80 (local/remoto)
D	Fd	Cliente - Servidor	80/20 (local/remoto)
E	Fe	Cliente - Servidor	80/20 (local/remoto)
F	Ff	Cliente - Servidor	80/20 (local/remoto)
G	Fg	Cliente - Servidor	80/20 (local/remoto)
H	Fh	Cliente - Servidor	80/20 (local/remoto)
I	Fi	Cliente - Servidor	20/80 (local/remoto)
J	Fj	Cliente - Servidor	20/80 (local/remoto)

Tabla 3.16: Modelo y distribución de datos

Los flujos individuales se representan en el siguiente gráfico:

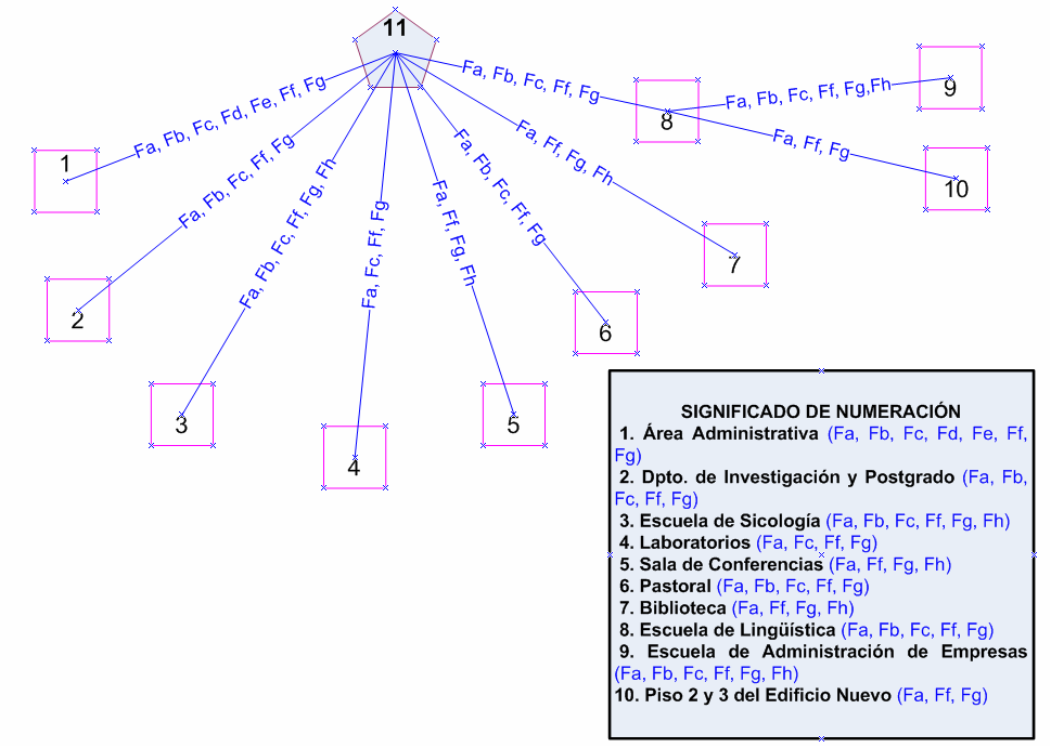


Gráfico 3.52: Distibución individual del flujo de datos

Los flujos compuestos se determinan haciendo una sumatoria de los flujos individuales para así determinar la cantidad de información que se transmite en las diferentes áreas de la red.

Área	Flujo individuales	Sumatoria (Mbps)	Total (Mbps)
1. Área Administrativa	Fa, Fb, Fc, Fd, Fe, Ff, Fg	2 + 40 + 1+ 40 + 40 + 3.33 + 2	128.33
2. Dpto. de Investigación, Posgrado y Autoevaluación	Fa, Fb, Fc, Ff, Fg	2 + 40 + 1 + 3.33 + 2	48.33
3. Escuela de Sicología	Fa, Fb, Fc, Ff, Fg, Fh	2 + 40 + 1 + 3.33 + 2 + 8	56.33
4. Laboratorios	Fa, Fc, Ff, Fg	2 + 1 + 3.33 + 2	8.33
5. Sala de Conferencia	Fa, Ff, Fg, Fh	2 + 3.33 + 2 + 8	15.33
6. Pastoral	Fa, Fb, Fc, Ff, Fg	2 + 40 + 1 + 3.33 + 2	48.33
7. Biblioteca	Fa, Ff, Fg, Fh	2 + 3.33 + 2 + 8	15.33
8. Escuela de Lenguas	Fa, Fb, Fc, Ff, Fg	2 + 40 + 1 + 3.33 + 2	48.33

Área	Flujo individuales	Sumatoria (Mbps)	Total (Mbps)
9. Escuela de Administración de Empresas	Fa, Fb, Fc, Ff, Fg, Fh	2 + 40 + 1 + 3.33 + 2 + 8	56.33
10. Piso 2 y 3 del Edificio Nuevo	Fa, Ff, Fg	2 + 3.33 + 2	7.33

Tabla 3.17: Flujos Compuestos

3.2.2. Diseño

En la fase de análisis están determinados los requerimientos que debe cumplir el rediseño de la red de campus LAN de la Pontificia Universidad Católica del Ecuador Sede Ambato.

3.2.2.1. Selección de tecnología

Para una mejor transmisión de datos se determinó que se debe usar Gigabit Ethernet en los nodos con mayor requerimiento de capacidad y en las subredes Fast Ethernet.

Cableado Vertical

Para el cableado vertical (backbone) se usara Fibra Óptica Multimodo pues se usan comúnmente en aplicaciones de corta distancia, menores a 2 Km; es simple de diseñar y económica. Además posee resistencia al agua, hongos, inmunidad al ruido e interferencia, y emisiones ultra violeta, proporcionando una alta velocidad al navegar por Internet.

Las características de la fibra multimodo a utilizarse se detalla a continuación:

Características	1000 Base - SX
Longitud de onda	850
Tipo de FO (núcleo)	62,5 / 125 μm
Ancho de banda (Mhz/Km.)	160-200
Distancia (m)	220-275
Perdida del link (dB)	3,2 - 3,2

Tabla 3.18: Características de la Fibra Óptica Multimodo

Con respecto a distancia y número de hilos se tiene:

Desde	Hasta	Número de hilos	Distancia Aproximada (m)	Tecnología
Centro de Cómputo	Dirección de Estudiantes	2	17	Giga Ethernet
Centro de Cómputo	Departamento de Investigación, Posgrado y Autoevaluación	2	25	Fast Ethernet
Centro de Cómputo	Escuela de Sicología	2	21	Fast Ethernet
Centro de Cómputo	Pastoral	2	55	Fast Ethernet
Centro de Cómputo	Biblioteca	2	53	Fast Ethernet
Centro de Cómputo	Escuela de Lingüística	12	110	GIga Ethernet
Escuela de Lingüística	Piso 2 del edificio nuevo	2	5	Fast Ethernet
Escuela de Lingüística	Escuela de Administración	2	16	Fast Ethernet

Tabla 3.19: Fibra Óptica para Cableado Vertical

Cableado Horizontal

En la siguiente tabla se detalla el tipo de cable y distancia utilizada para la interconexión horizontal.

Desde	Hasta	Cable	Número de cables	Cantidad Aproximada (m)
Dirección de Estudiantes	Estaciones de la misma área	UTP cat 5e	6	37
Dirección de Estudiantes	Dirección Financiera	UTP cat 5e	11	305
Dirección de Estudiantes	Dirección Administrativa	UTP cat 5e	2	29
Dirección de Estudiantes	Rectorado	UTP cat 5e	4	126
Dirección de Estudiantes	Dirección Académica	UTP cat 5e	3	51
Dirección de Estudiantes	Secretaría General	UTP cat 5e	3	39
Dirección de Estudiantes	Estación de registro	UTP cat 5e	2	19
Dirección de Estudiantes	Escuela de Sistemas	UTP cat 5e	12	281
Dirección de Estudiantes	Escuela de Optometría	UTP cat 5e	5	110
Dirección de Estudiantes	Bar	STP	1	40
Biblioteca	Estaciones de la misma área	UTP cat 5e	47	1048
Departamento de Investigación, Posgrado y Autoevaluación	Estaciones de la misma área y Escuela de Diseño Industrial	UTP cat 5e	21	315
Escuela de Sicología	Estaciones de la misma área	UTP cat 5e	40	1420
Centro de Cómputo	Servidores y estaciones de administración	UTP cat 5e	28	360
Laboratorio 2	Lab 1y 2	UTP cat 5e	48	560
Laboratorio 4	Lab 3 y 4	UTP cat 5e	48	560
Laboratorio 6	Lab 5 y 6	UTP cat 5e	51	590
Laboratorio 7	Lab 7	UTP cat 5e	48	896
Laboratorio de redes	Lab de redes	UTP cat 5e	27	182

Desde	Hasta	Cable	Número de cables	Cantidad Aproximada (m)
Sala de Conferencias J.P.II	Sala de Conferencias J.P.II	UTP cat 5e	42	480
Pastoral	Estaciones de la misma área	UTP cat 5e	12	114
Escuela de Lingüística	Estaciones de la misma área	UTP cat 5e	48	1428
Piso 2 del edificio nuevo	Router Wireless y Piso 3 del edificio nuevo	UTP cat 5e	2	16
Escuela de Administración	Estaciones de la misma área y Auditorio	UTP cat 5e	57	2070
Total:		UTP cat 5e	562	10926
		STP	1	40

Tabla 3.20: Cableado Horizontal

En el cuarto piso del Edificio Principal se utilizará fibra óptica multimodo de 2 hilos para interconectarlo, a continuación se detalla la cantidad aproximada:

Desde	Hasta	Número de cables	Cantidad Aproximada (m)	Tecnología
Centro de Cómputo	Laboratorio 2	1	14	Fast Ethernet
Centro de Cómputo	Laboratorio 4	1	26	Fast Ethernet
Centro de Cómputo	Laboratorio 6	1	66	Fast Ethernet
Centro de Cómputo	Laboratorio 7	1	82	Fast Ethernet
Centro de Cómputo	Laboratorio de Redes	1	90	Fast Ethernet
Centro de Cómputo	Sala de Conferencias Juan Pablo II	1	34	Fast Ethernet
	Total	6	312	

Tabla 3.21: Fibra Óptica en el cuarto piso

3.2.2.2. Mecanismos de interconexión

Se debe adquirir los siguientes dispositivos, para una correcta configuración y administración de la red:

Dispositivo	Número de puertos	Número	Área
SWITCH de capa 3	48	1	Cuarto de Telecomunicaciones
SWITCH de capa 2	48	1	Dirección de Estudiantes
		1	Biblioteca
		1	Departamento de Investigación, Posgrado y Autoevaluación
		1	Escuela de Sicología
		1	Laboratorio 2
		1	Laboratorio 4
		1	Laboratorio 6
		1	Laboratorio 7
		1	Laboratorio de Redes
		1	Sala de Conferencias Juan Pablo II
		1	Escuela de Lingüística
		1	Escuela de Administración
Total Switch de capa 2 de 48 puertos		**12**	
SWITCH de capa 2	24	1	Pastoral
		1	Piso 2 del Edificio nuevo
		1	Escuela de Administración
Total SWITCH de capa 2 de 24 puertos		**3**	
Patch Panel	24	3	Donde se ubiquen los Switch capa 2 de 24 puertos
	48	13	Donde se ubique los Switch´s capa 2 de 48 puertos y el Switch capa 3 de 48 puertos
Router Wireless		15	En cada piso de los edificios de la PUCESA Bar Pastoral Biblioteca

Tabla 3.22: Dispositivos de interconexión

Las características que deben cumplir los dispositivos mencionados se detallan a continuación:

- Switch de Capa 2:

Estándar	Función
802.1Q	Soporte para VLAN's
802.1P	QoS/CoS Protocol for Traffic Prioritization
802.1X	Autenticación
SNMP	Protocolo simple de administración de redes
Port Security	Seguridad en cada puerto del SW a través de las MACs

Tabla 3.23: Características del SW capa 2

- Switch de Capa 3:

Estándar	Función
802.1Q	Soporte para VLAN's
802.1P	QoS/CoS Protocol for Traffic Prioritization
802.1X	Autenticación
SNMP	Protocolo simple de administración de redes
RIP, OSPF,IGPR	Protocolos de ruteo

Tabla 3.24: Características del Switch capa 3

- Router de banda ancha Wireless-G para el servicio de Internet inalámbrico con las siguientes características.

Velocidad	Velocidad de datos de hasta 54 Mbps
Frecuencia	Banda de 2,4 GHz
Alcance	30-45 metros en interiores. Opción de ampliador de alcance disponible
Opciones de seguridad del router	WEP, WPA, WPA2

Tabla 3.25: Características del Router Wireless

3.2.2.3. Diseño Lógico

Para poder graficar el cableado estructurado en el que se basa esta propuesta se ha hecho uso de la siguiente simbología.

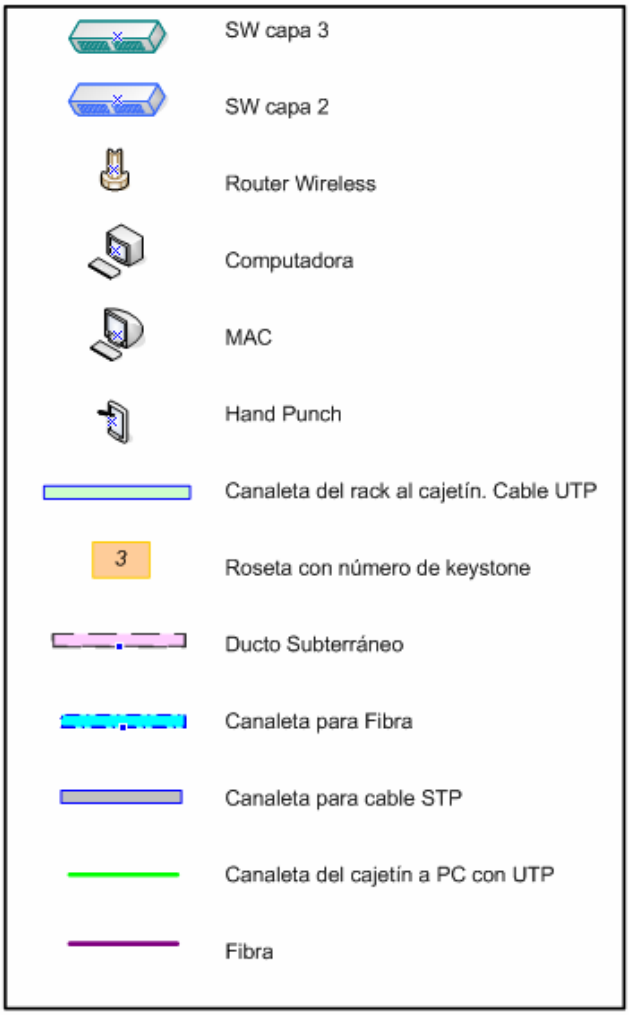


Gráfico 3.53: Simbología

Para comenzar a implantar las normas del cableado estructurado se iniciará por el cableado vertical, el mismo que partirá desde el Centro de Cómputo a través de un Switch capa 3 de 48 puertos que actuará como un router y desde este se repartirá fibra óptica multimodo a Switch de capa 2 ubicados en:

- Departamento de Investigación, Posgrado y Autoevaluación en el segundo piso del edificio principal
- Dirección de Estudiantes en el primer piso del edificio principal
- Escuela de Sicología
- Biblioteca
- Pastoral
- Escuela de Lingüística en el primer piso del edificio nuevo

Desde la Escuela de Lingüística se distribuye fibra óptica multimodo al resto del edificio nuevo, parten 2 fibras una al segundo piso y otra al cuarto piso.

A continuación se puede observar la distribución mencionada:

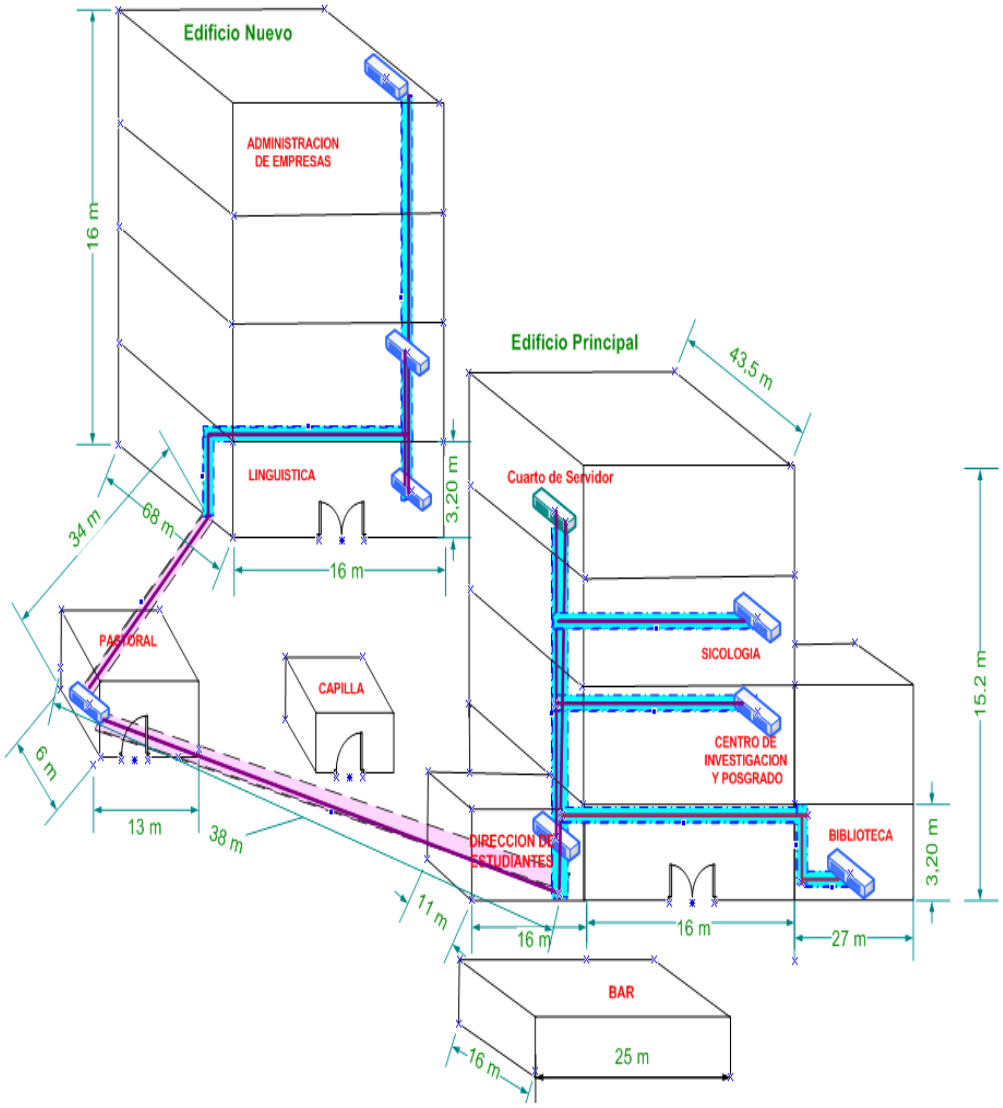


Gráfico 3.54: Cableado Vertical

EDIFICIO PRINCIPAL

PRIMER PISO

La fibra óptica multimodo llega a la Dirección de estudiantes, al rack compuesto de un Switch capa 2 de 48 puertos y un patch panel de 48

puertos, desde aquí se distribuye cable UTP Cat 5e a través de canaletas, como lo exigen las normas de cableado estructurado estos cables llegan a las rosetas con su respectivos face plate y keystone y desde estos se conectan las pc´s, a través de los patch cord.

Para cumplir con el diseño propuesto en el primer piso del edificio principal se requiere de:

Elemento	Número	Medidas aproximadas
Rack de pared	1	
Patch panel	1	
SWITCH de capa 2	1	
Patch Cord	74	350 m
Canaletas	-	120 m
Face plate	19	
Roseta	19	
Keystone	48	
Cable Horizontal UTP Cat 5e	52	9977 m
Cable Horizontal STP	1	40 m
Conectores RJ45	244	
Capuchones	244	

Tabla 3.26: Elementos del primer piso

Estos elementos están distribuidos como se puede observar en el gráfico siguiente:

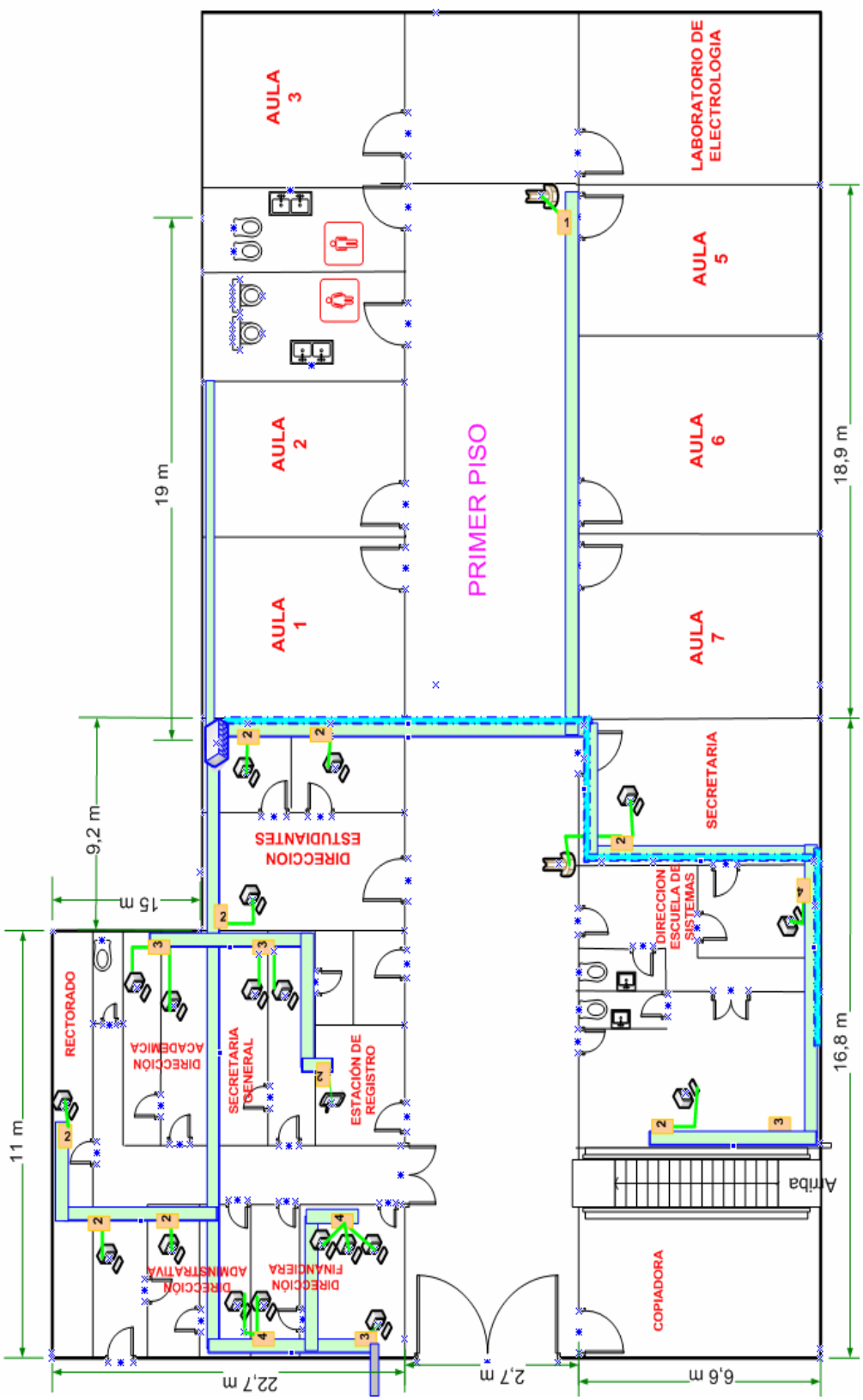


Gráfico 3.55: Primer Piso

Desde el rack de la Dirección de Estudiantes se interconectará a:

- Rectorado
- Dirección de Estudiantes
- Dirección Financiera
- Dirección Administrativa
- Dirección Académica
- Secretaría General
- Estación de registro
- Escuela de Sistemas
- Escuela de Optometría
- Bar

OPTOMETRÍA

La Escuela de Optometría está ubicada un piso más abajo de la Escuela de Sistemas por esta razón se ha decidido interconectar desde el rack de la Dirección de Estudiantes a esta escuela, a través de cable UTP Cat 5e.

La distribución de la red se puede observar en el gráfico siguiente:

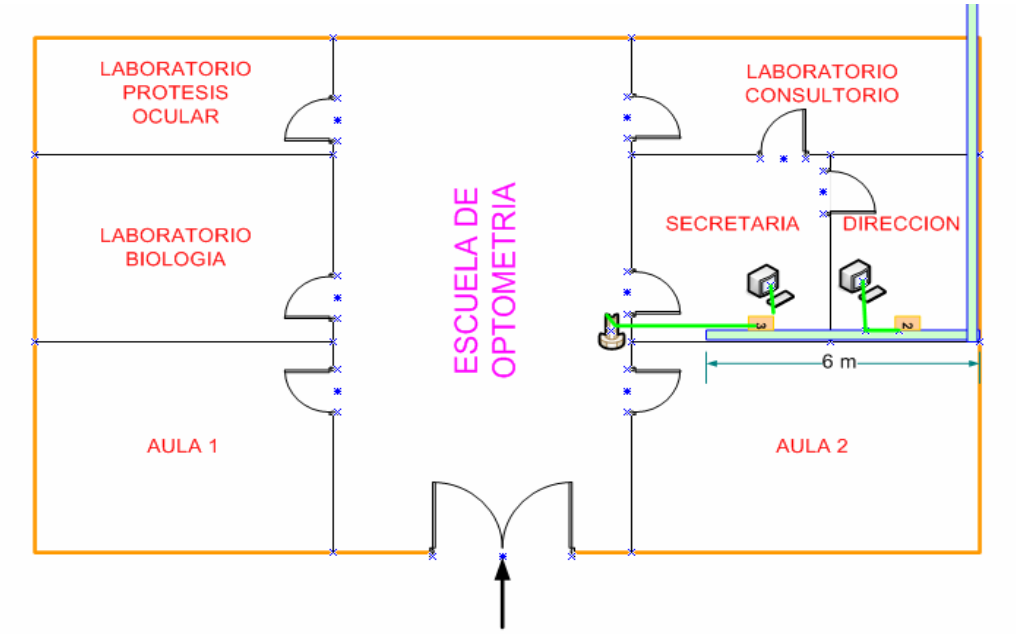


Gráfico 3.56: Optometría

BAR

En el bar se va a incluir un router wireless esta conexión viene desde la Dirección de Estudiantes, al igual que Optometría el cable va por fuera del bar y para ofrecer un buen servicio se deberá usar cable STP aproximadamente de 28m, como se puede observar en el gráfico siguiente:

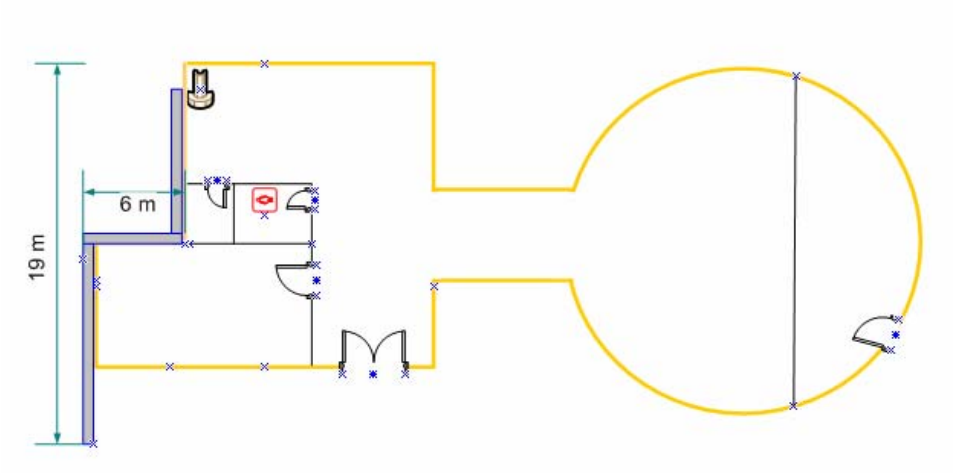


Gráfico 3.57: Bar

BIBLIOTECA

A la Biblioteca le llega un punto de fibra óptica desde el rack principal, pues a más de la biblioteca existe un auditorio en donde se da charlas y es necesario que se tenga acceso a la red, para ello son necesarios los siguientes elementos:

Elemento	Número	Medidas aproximadas
Rack de pared	1	
Patch panel	1	
SWITCH de capa 2	1	
Patch Cord	54	250 m
Canaletas	-	47 m
Face plate	18	
Roseta	18	
Keystone	47	
Cable Horizontal UTP Cat 5e	47	1048 m
Conectores RJ45	212	
Capuchones	212	

Tabla 3.27: Elementos de la Biblioteca

La distribución se puede observar en el gráfico siguiente:

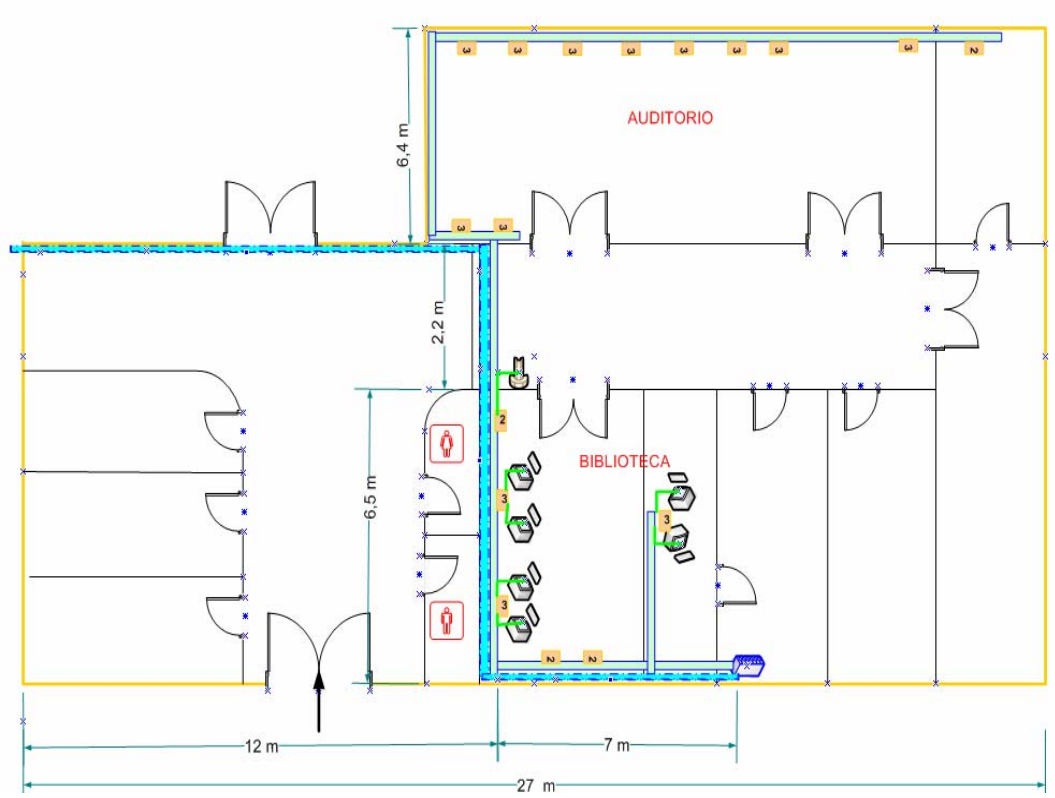


Gráfico 3.58: Biblioteca

SEGUNDO PISO

Desde el rack principal llega un punto de fibra al Departamento de Investigación, Posgrado y Autoevaluación al rack secundario, desde aquí se distribuye la red a las pc´s de esta área y a la Escuela de Diseño Gráfico.

Para ese piso se requiere:

Elemento	Número	Medidas aproximadas
Rack de pared	1	
Patch panel	1	
SWITCH de capa 2	1	
Patch Cord	52	250 m
Canaletas	-	120 m
Face plate	7	
Roseta	7	
Keystone	21	
Cable Horizontal UTP Cat 5e	21	315 m
Conectores RJ45	104	
Capuchones	104	

Tabla 3.28: Elementos del segundo piso

Los mismos que están distribuidos como se muestra a continuación:

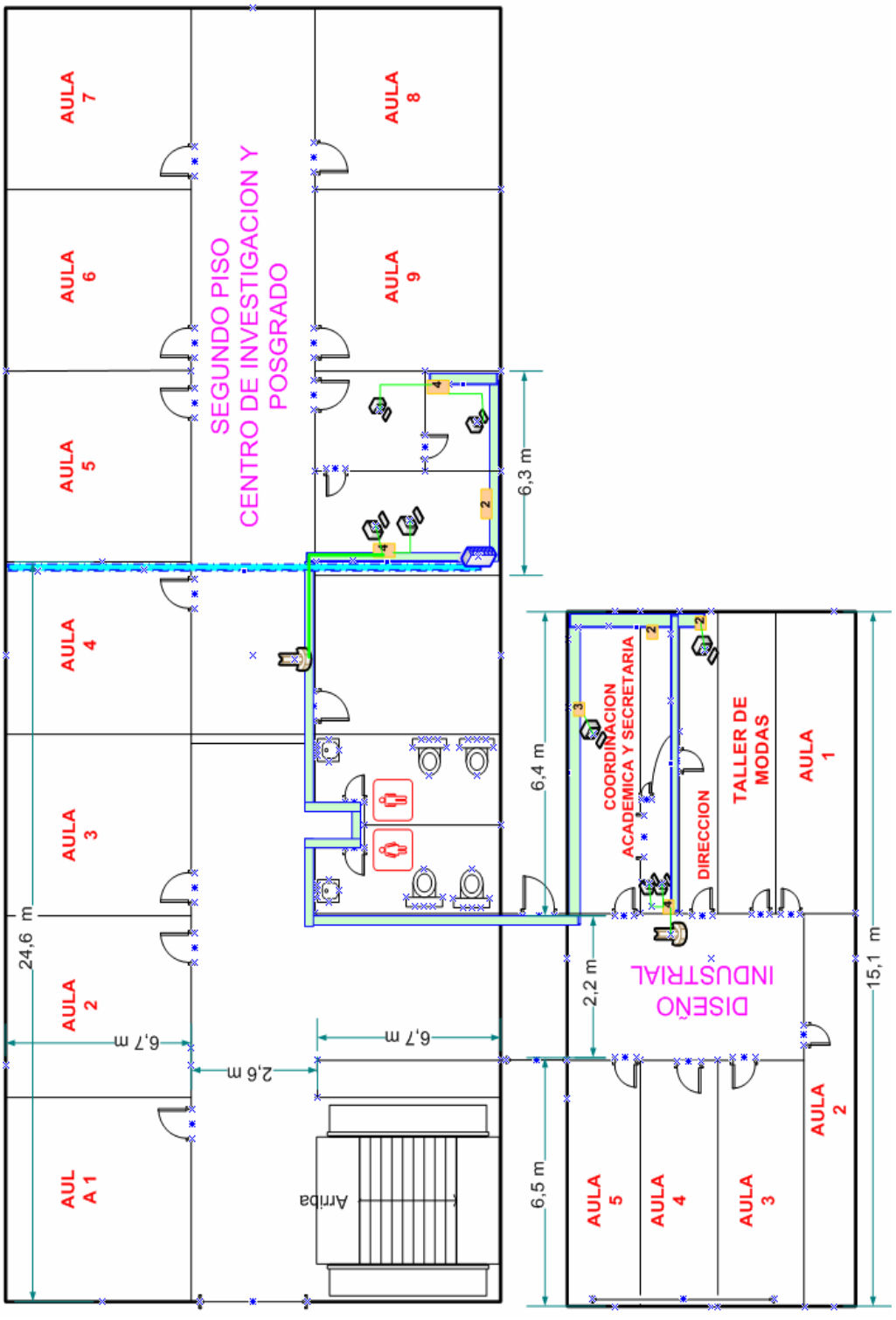


Gráfico 3.59: Segundo Piso

TERCER PISO

En el tercer piso se encuentra la Escuela de Sicología y una sala de conferencias que requiere tener puntos de red, por lo tanto en este piso existe un rack secundario cuya conexión de fibra llega desde el Centro de Cómputo. Para realizar la interconexión se requiere:

Elemento	Número	Medidas aproximadas
Rack de pared	1	
Patch panel	1	
SWITCH de capa 2	1	
Patch Cord	43	330 m
Canaletas	-	60 m
Face plate	14	
Roseta	14	
Keystone	40	
Cable Horizontal UTP Cat 5e	40	1420 m
Conectores RJ45	166	
Capuchones	166	

Tabla 3.29: Elementos del tercer piso

Estos elementos están distribuidos como se puede observar en el siguiente gráfico:

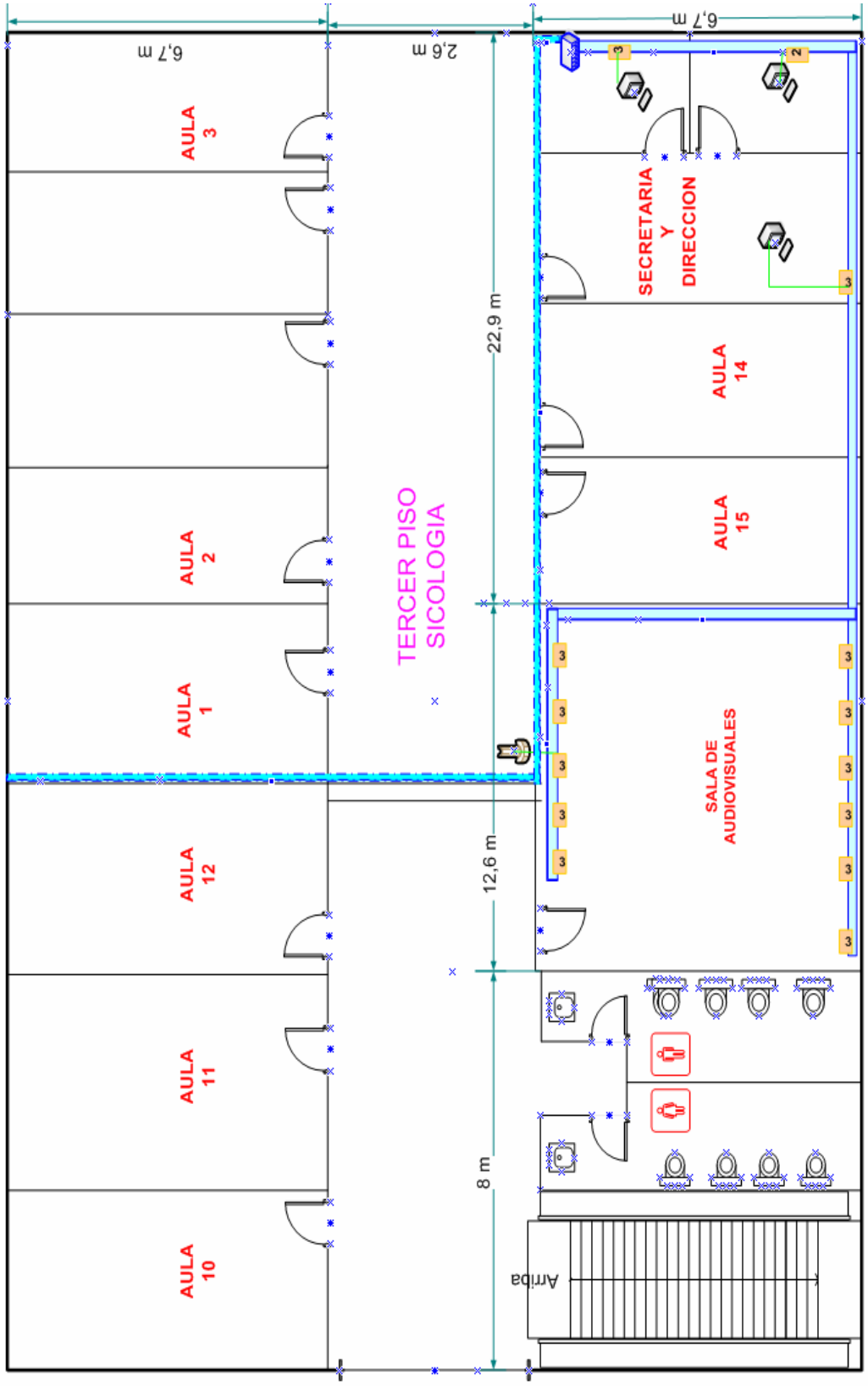


Gráfico 3.60: Tercer Piso

CUARTO PISO

En el cuarto piso existen 8 laboratorios y la Sala de Conferencias Juan Pablo II. Debido al número de computadoras y a la demanda del servicio existente en este piso, se ha determinado la necesidad de configurar la red incluyendo amas del rack principal, 6 racks secundarios con los siguientes elementos:

Cuarto de Telecomunicaciones:

Elemento	Número	Medidas aproximadas
Rack de piso	1	
Patch panel para UTP	1	
Patch panel para F.O.	1	
SWITCH de capa 3	1	
Patch Cord	38	200 m
Canaletas	-	40 m
Face plate	7	
Roseta	7	
Keystone	28	
Cable Horizontal UTP Cat 5e	28	887 m
Conectores RJ45	132	
Capuchones	132	

Tabla 3.30: Elementos del Cuarto de Telecomunicaciones

Laboratorio 2:

Elemento	Número	Medidas aproximadas
Rack de pared	1	
Patch panel	1	
SWITCH de capa 2	1	
Patch Cord	72	400 m
Canaletas	-	40 m

Elemento	Número	Medidas aproximadas
Face plate	12	
Roseta	12	
Keystone	48	
Cable Horizontal UTP Cat 5e	48	560 m
Conectores RJ45	250	
Capuchones	250	

Tabla 3.31: Elementos del Laboratorio 1 y 2

Laboratorio 4:

Elemento	Número	Medidas aproximadas
Rack de pared	1	
Patch panel	1	
SWITCH de capa 2	1	
Patch Cord	72	400 m
Canaletas	-	40 m
Face plate	12	
Roseta	12	
Keystone	48	
Cable Horizontal UTP Cat 5e	48	560 m
Conectores RJ45	250	
Capuchones	250	

Tabla 3.32: Elementos del Laboratorio 3 y 4

Laboratorio 6:

Elemento	Número	Medidas aproximadas
Rack de pared	1	
Patch panel	1	
SWITCH de capa 2	1	
Patch Cord	71	390 m
Canaletas	-	45 m
Face plate	13	

Elemento	Número	Medidas aproximadas
Roseta	13	
Keystone	51	
Cable Horizontal UTP Cat 5e	51	590 m
Conectores RJ45	244	
Capuchones	244	

Tabla 3.33: Elementos del Laboratorio 5 y 6

Laboratorio 7:

Elemento	Número	Medidas aproximadas
Rack de pared	1	
Patch panel	1	
SWITCH de capa 2	1	
Patch Cord	80	450 m
Canaletas	-	32 m
Face plate	16	
Roseta	16	
Keystone	48	
Cable Horizontal UTP Cat 5e	48	896 m
Conectores RJ45	352	
Capuchones	352	

Tabla 3.34: Elementos del Laboratorio 7

Laboratorio de redes:

Elemento	Número	Medidas aproximadas
Rack de pared	1	
Patch panel	1	
SWITCH de capa 2	1	
Patch Cord	54	220 m
Canaletas	-	21 m
Face plate	9	
Roseta	9	

Elemento	Número	Medidas aproximadas
Keystone	27	
Cable Horizontal UTP Cat 5e	27	182 m
Conectores RJ45	108	
Capuchones	108	

Tabla 3.35: Elementos del Laboratorio de redes

Sala de Conferencias Juan Pablo II:

Elemento	Número	Medidas aproximadas
Rack de pared	1	
Patch panel	1	
SWITCH de capa 2	1	
Patch Cord	42	200 m
Canaletas	-	43 m
Face plate	14	
Roseta	14	
Keystone	42	
Cable Horizontal UTP Cat 5e	42	480 m
Conectores RJ45	168	
Capuchones	168	

Tabla 3.36: Elementos del la Sala de Conferencia Juan Pablo II

Estos elementos se distribuyen como se muestra en el gráfico:

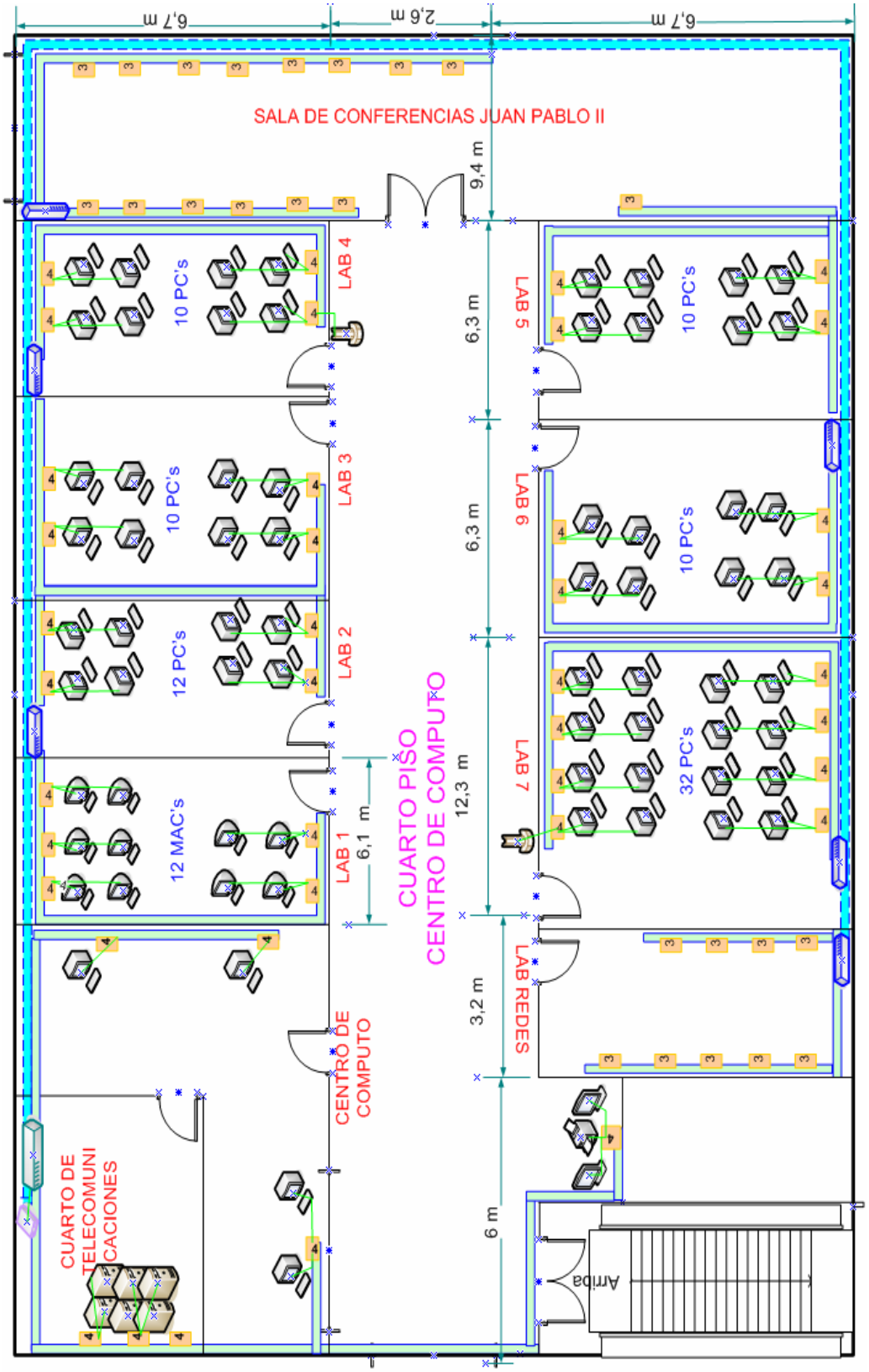


Gráfico 3.61: Cuarto Piso

PASTORAL

En la actualidad existe un ducto subterráneo por el cual se envía cable UTP, por este mismo ducto se ha planificado enviar fibra óptica a Pastoral e incrementar un router wireless que permita incluso acceso a la red en los jardines y canchas de la PUCESA, para esta conexión se requieren los siguientes elementos:

Elemento	Número	Medidas aproximadas
Rack de pared	1	
Patch panel	1	
SWITCH de capa 2	1	
Patch Cord	16	80 m
Canaletas	-	18 m
Face plate	4	
Roseta	4	
Keystone	12	
Cable Horizontal UTP Cat 5e	12	114 m
Conectores RJ45	56	
Capuchones	56	

Tabla 3.37: Elementos de Pastoral

Su distribución se indica en el siguiente gráfico:

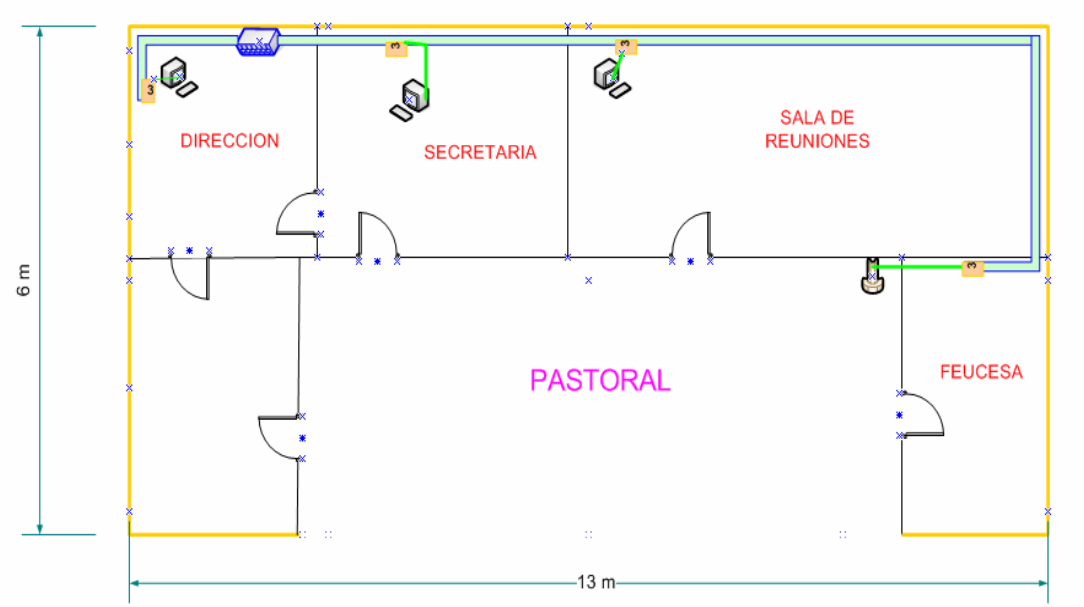


Gráfico 3.62: Pastoral

EDIFICIO NUEVO

PRIMER PISO

Al primer piso del nuevo edificio le llega a través del ducto subterráneo fibra óptica, en este piso trabaja la Escuela de Lingüística y el rack estará ubicado aquí y desde este se distribuirá la red a todo el edificio. Se debe tomar en cuenta que este edificio tiene techo falso lo que se aprovechara para pasar los cables por ahí.

Para la conexión en este piso se requieren los siguientes elementos:

Elemento	Número	Medidas aproximadas
Rack de piso	1	
Patch panel	1	
SWITCH de capa 2	1	
Patch Cord	66	300 m
Canaletas	-	57 m
Face plate	12	
Roseta	12	
Keystone	48	
Cable Horizontal UTP Cat 5e	48	1428 m
Conectores RJ45	228	
Capuchones	228	

Tabla 3.38: Elementos del primer piso del edificio nuevo

La distribución se la realizará como se muestra a continuación:

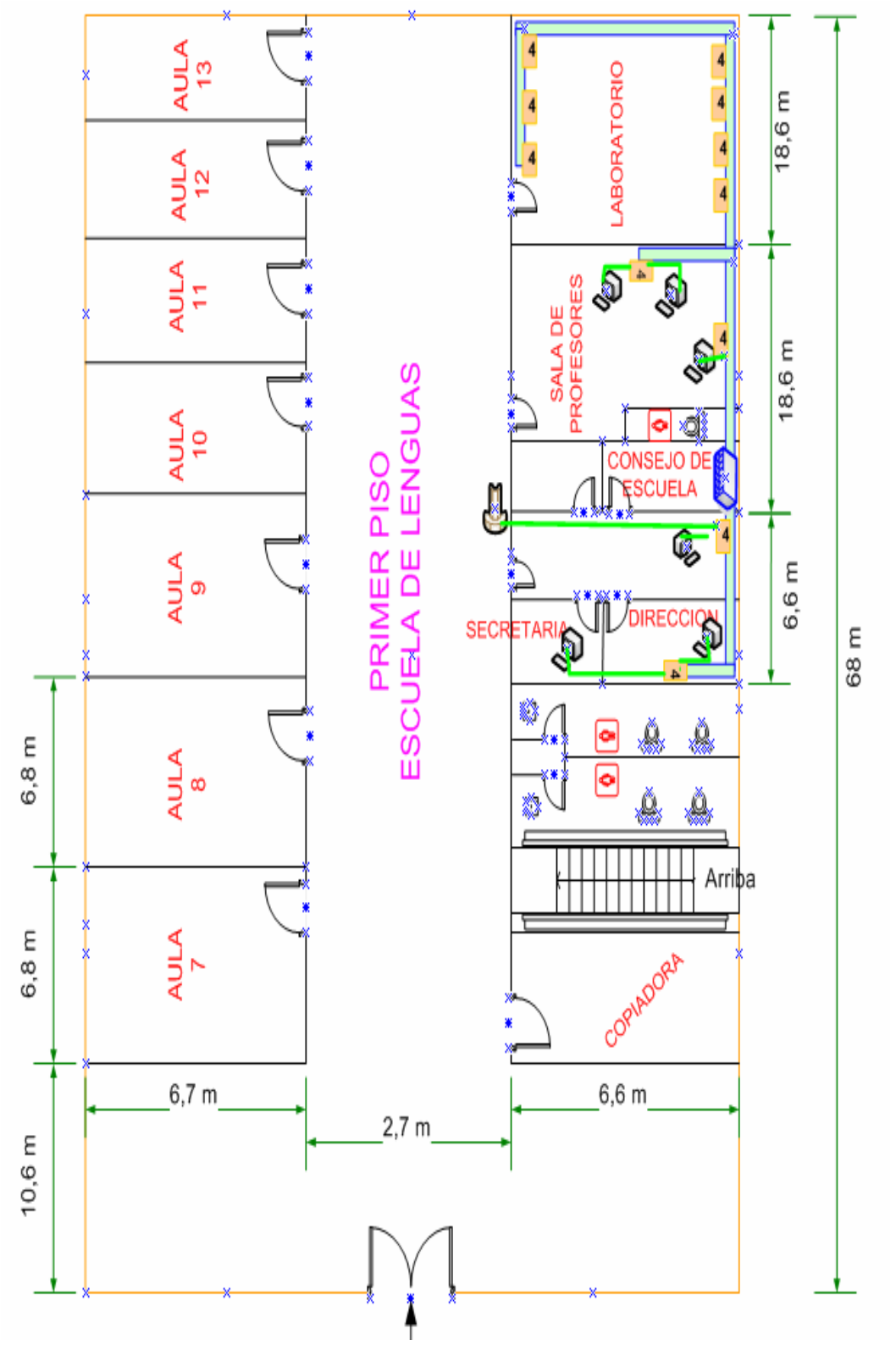


Gráfico 3.63: Primer Piso

SEGUNDO PISO

El segundo y tercer piso hasta la actualidad poseen solamente aulas pero para futuras conexiones se contará con un rack en este piso que a la vez servirá de conexión para el tercer piso. En estos dos pisos existirá un router wireless en cada uno.

Para realizar la interconexión se requieren los siguientes elementos:

Elemento	Número	Medidas aproximadas
Rack de pared	1	
Patch panel	1	
SWITCH de capa 2	1	
Patch Cord	4	10 m
Canaletas	-	20 m
Face plate	2	
Roseta	2	
Keystone	2	
Cable Horizontal UTP Cat 5e	2	16 m
Conectores RJ45	12	
Capuchones	12	

Tabla 3.39: Elementos del segundo piso del edificio nuevo

La distribución se la realizará como se muestra en los siguientes gráficos:

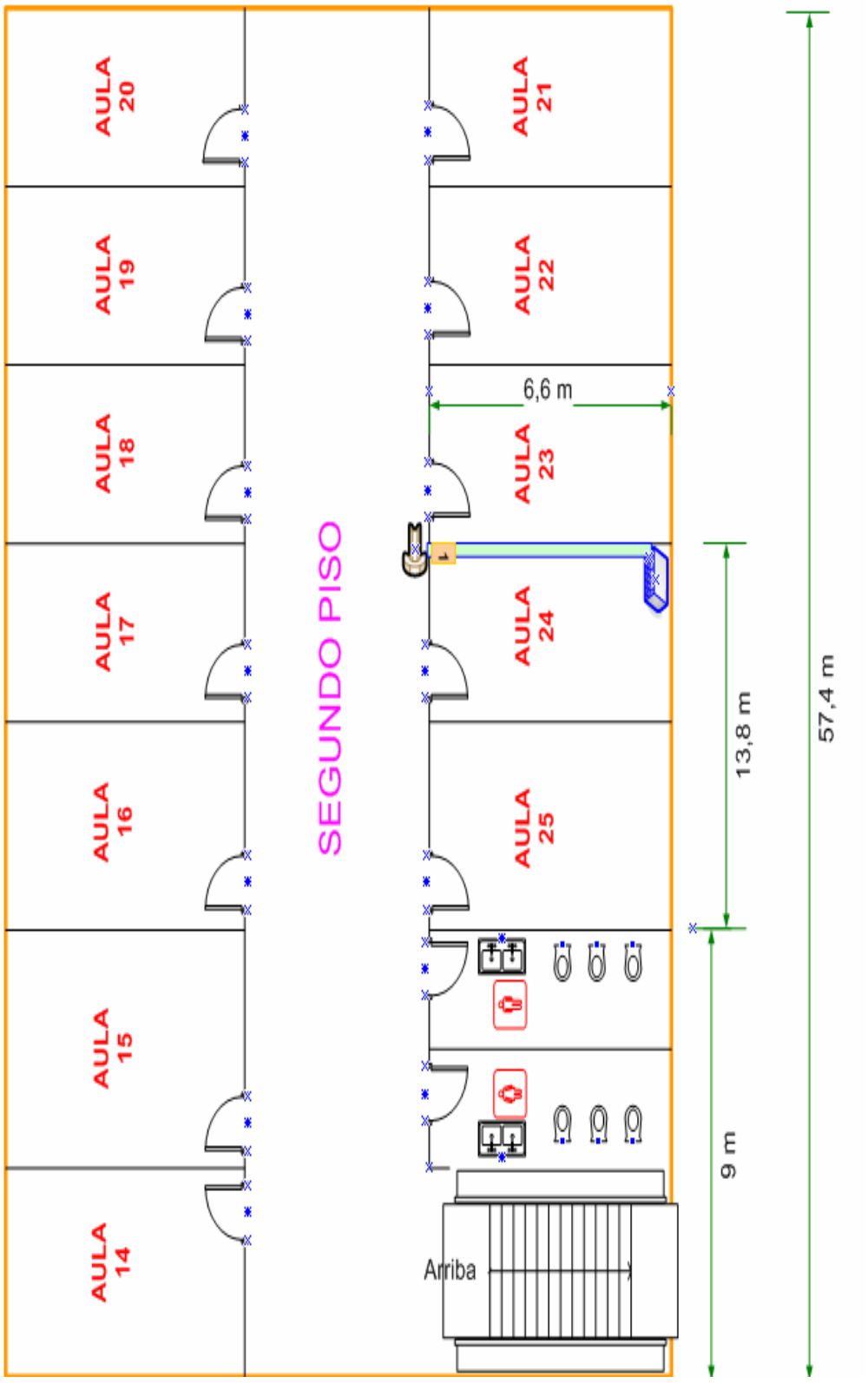


Gráfico 3.64: Segundo Piso

TERCER PISO

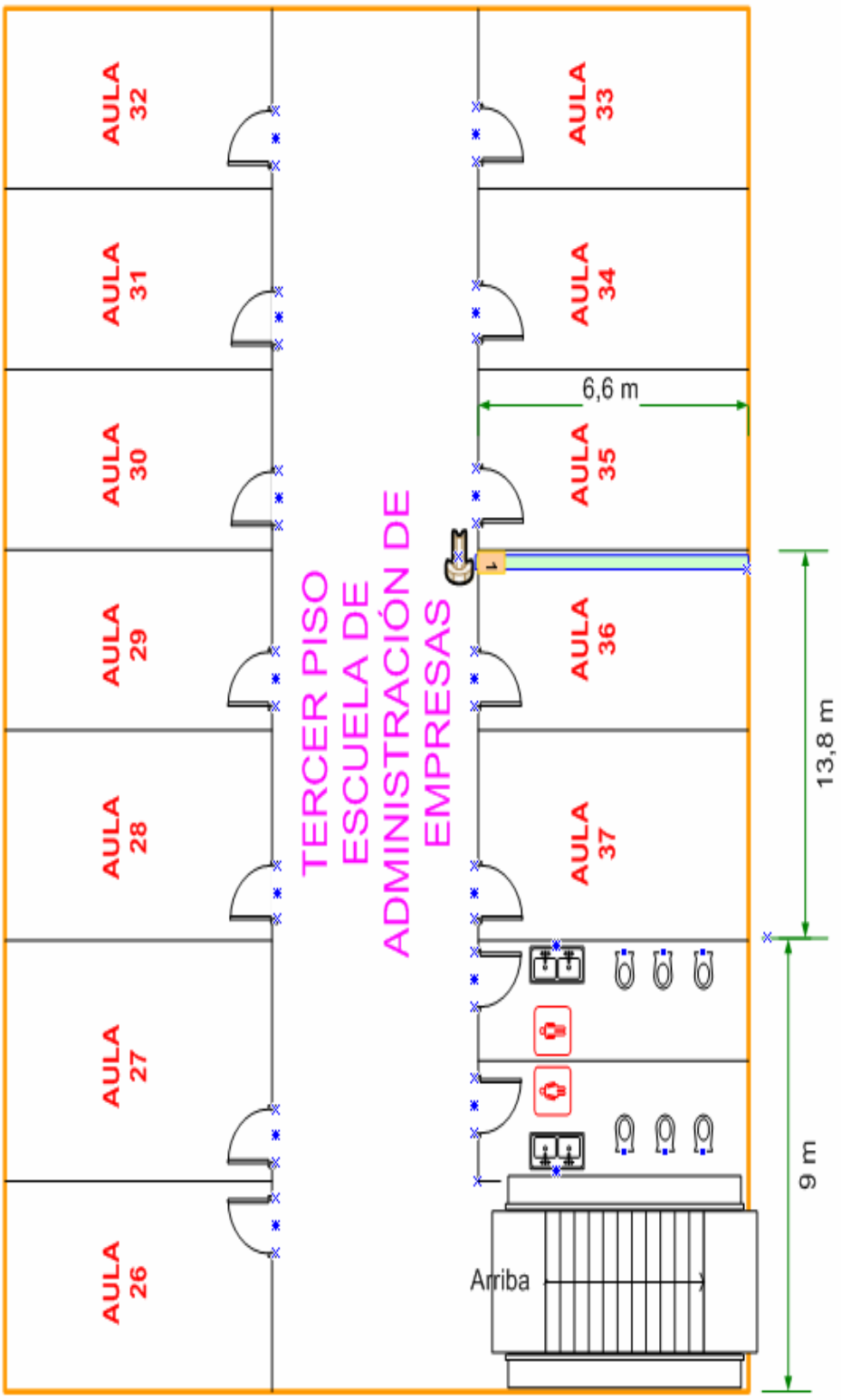


Gráfico 3.65: Tercer Piso

CUARTO PISO

En el cuarto piso trabaja la Escuela de Administración y su Auditorio, el rack estará ubicado en las oficinas administrativas, por crecimiento se instalarán varios puntos de red tanto en las oficinas como en el auditorio, para lo cual se requieren los siguientes elementos:

Elemento	Número	Medidas aproximadas
Rack de pared	1	
Patch panel	2	
SWITCH de capa 2	2	
Patch Cord	61	300 m
Canaletas	-	95 m
Face plate	14	
Roseta	14	
Keystone	57	
Cable Horizontal UTP Cat 5e	57	2069,6 m
Conectores RJ45	236	
Capuchones	236	

Tabla 3.40: Elementos del cuarto piso del edificio nuevo

La distribución se la realizará como se muestra en el siguiente gráfico:

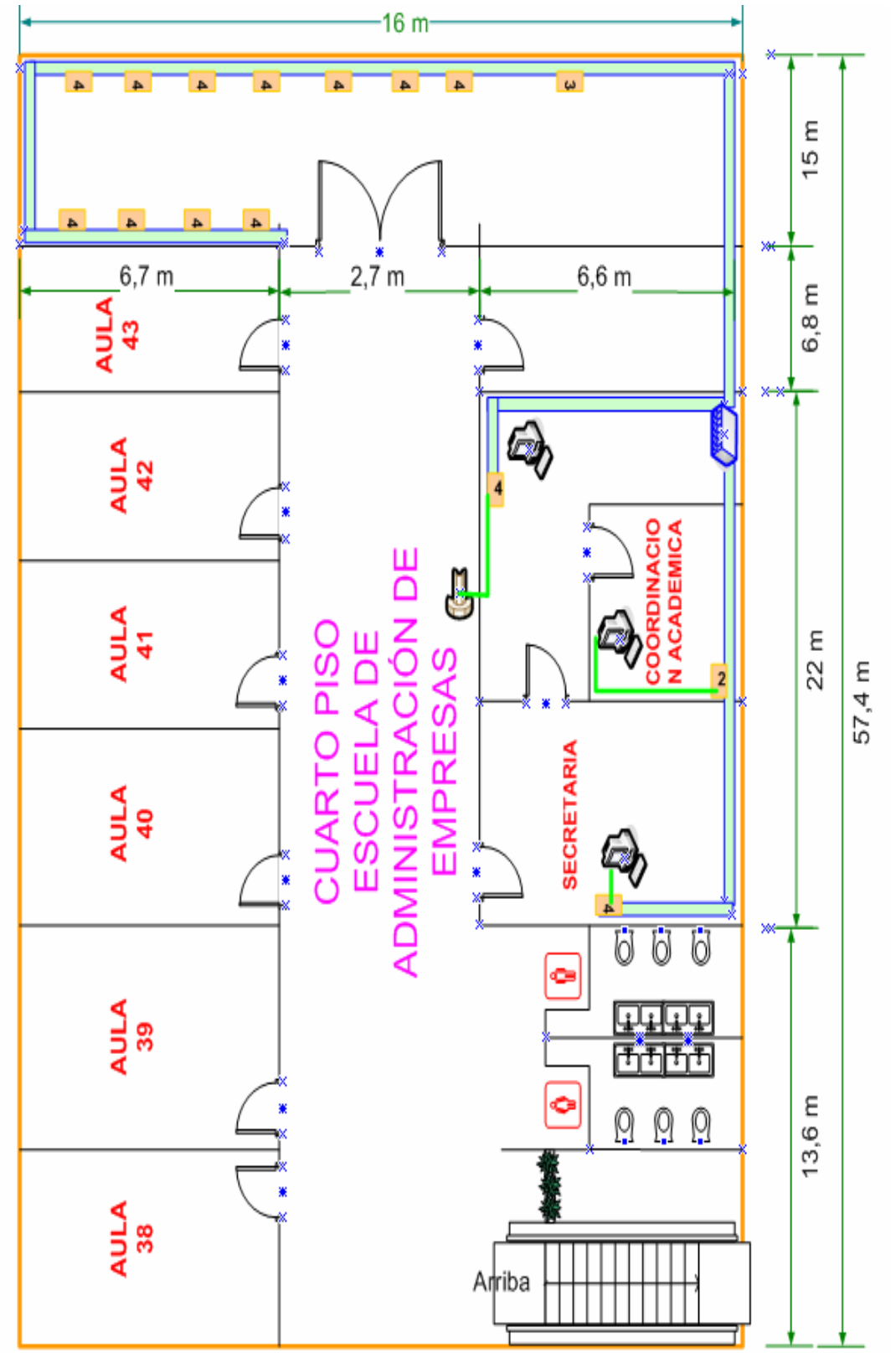


Gráfico 3.66: Cuarto Piso

3.2.2.4. Diseño de VLANs

Para evitar que exista un solo dominio de broadcast y consuma al ancho de banda de la red, es necesaria la segmentación de la misma, mediante la creación de VLANs, que como se mencionó anteriormente son redes de área local virtuales donde la conexión no es física sino lógica.

En la PUCESA se deberán crear 8 VLANs las cuales se detallan a continuación:

No	Nombre de VLAN	Áreas	Personal	Número de puertos
1	V_AREA_ADMIN	Rectorado	Prorrector Secretaria	17
		Dirección Académica	Director Académico Secretaria	
		Dirección Financiera	Directora Financiera 3 Cajeras 1 Contadora	
		Secretaria General	Secretario General Secretaria	
		Dirección de Recursos Humanos	Directora de RRHH Secretaria	
		Dirección de Estudiantes	Directora de D.E. Secretaria Asuntos Publicitarios	
		Control de Ingreso y Salida	Hand Punch	
2	V_AREA_ACAD	Escuela de Sistemas	Director Secretaria	18
		Escuela de Sicología	Director Secretaria	
		Escuela de Administración	Director Secretaria	
		Escuela de Lingüística	Director Secretaria Recepción	

No	Nombre de VLAN	Áreas	Personal	Número de puertos
		Escuela de Diseño Industrial	Director Secretaria	
		Escuela de Optometría	Director Secretaria	
		Pastoral	Director Secretaria	
		Departamento de Investigación, Posgrado y Autoevaluación	Director Secretaria	
3	V_DOC	Escuela de Sistemas	Pc_docentes	12
		Escuela de Sicología	Pc_docentes	
		Escuela de Administración	2 Pc_docentes	
		Escuela de Lingüística	3 Pc_docentes	
		Escuela de Diseño Industrial	2 Pc_docentes	
		Pastoral	Pc_docentes	
		Biblioteca	2 Bibliotecarios	
4	V_SER	Servidores	8 Servidores	14
		Centro de Cómputo	Director 2 Asistentes Kiosco de registro Kiosco de impresión Impresora de red	
5	V_WIR	Router Wireless	Estudiantes, Docentes	30
6	V_LAB1_2	Laboratorio 1	12 MAC’s	24
		Laboratorio 2	12 PC’s	
7	V_LAB3_4	Laboratorio 3	10 PC’s	20
		Laboratorio 4	10 PC’s	
8	V_LAB5_6	Laboratorio 5	10 PC’s	24
		Laboratorio 6	10 PC’s	
		Biblioteca	4 PC’s	
9	V_LAB7	Laboratorio 7	32 PC’s	32
10	V_VCSJ	Sala Juan Pablo II	45 PC’s	45
11	V_VCSA	Sala de Audiovisuales	33 PC’s	33
12	V_VCA	Auditorio	36 PC’s	36
13	V_VCSC	Sala de conferencias	47 PC’s	47

Tabla 3.41: VLAN’s

Estas VLAN’s serán creadas en los Switch de capa 2 y se permitirá la comunicación entre estas a través del Switch de capa 3.

3.2.2.5. Diseño Físico

3.2.2.5.1. Topología y Cableado

La topología a ser utilizada es Estrella, desde el Cuarto de Telecomunicaciones ubicado en el Centro de Cómputo se distribuye la red mediante fibra óptica multimodo a cada piso del edificio principal y al edificio nuevo como se observa en el gráfico 67, desde cada piso se vuelve a distribuir mediante cable UTP Cat 5e a cada estación de trabajo.

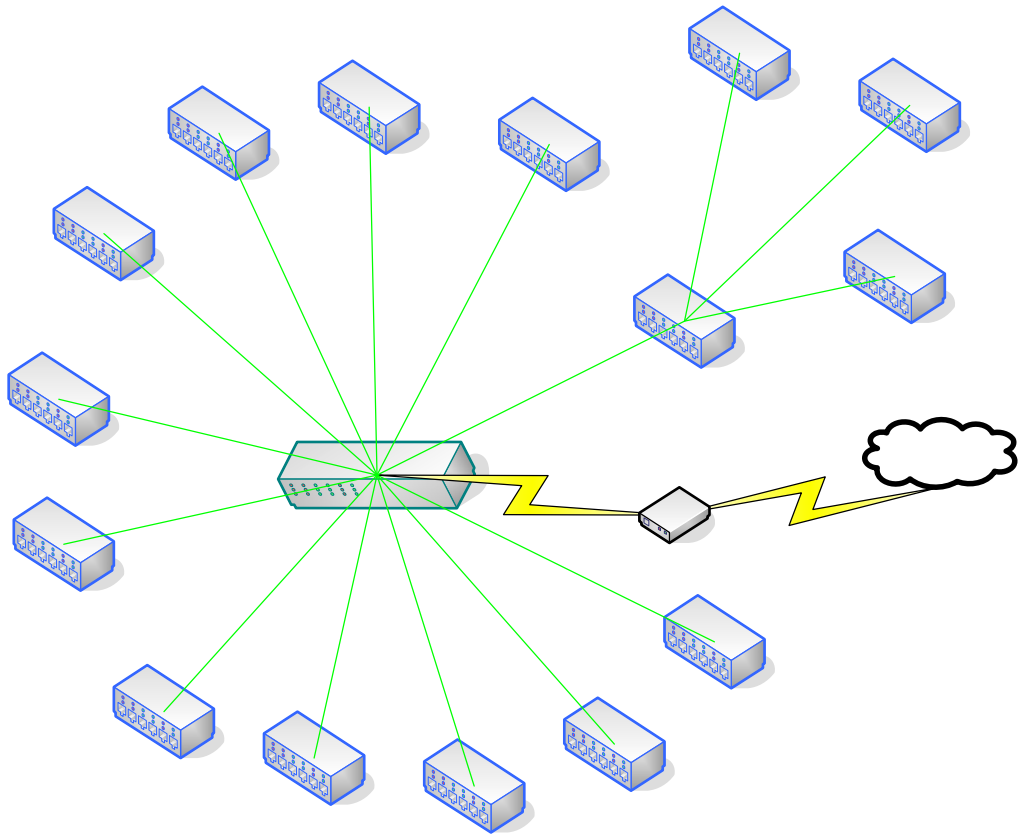


Gráfico 3.67: Modelo Jerárquico

3.2.2.5.2. Ubicación de dispositivos

El cuarto de telecomunicaciones está ubicado en el cuarto piso del edificio principal. Aquí se encontrarán:

- Los servidores en sus respectivos armarios
- Rack principal
- Patch Panel
- SWITCH de capa 3
- MODEM ADSL

En los edificios de la PUCESA, los computadores no sufrirán cambios físicos. Los racks secundarios (por pisos) si tendrán nuevas ubicaciones para una mejor distribución con respecto a las distancias.

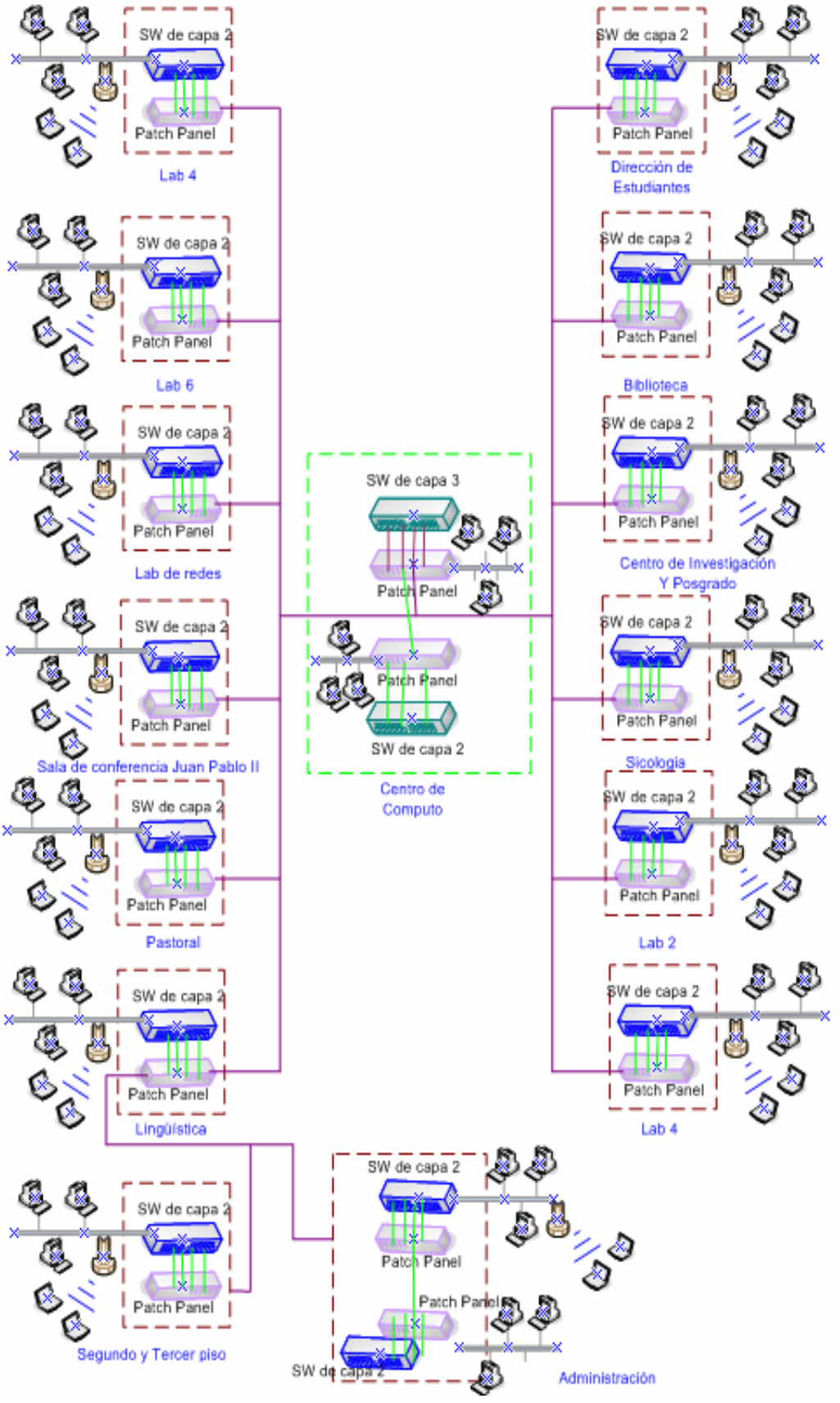


Gráfico 3.68: Diseño Lógico

3.2.2.5.3. Resumen de elementos necesarios

Elementos	Número		
Rack de piso	2 u		
Rack de pared	13 u		
SWITCH capa 3 de 48 puertos	1 u		
Switch capa 2 de 48 puertos	12 u		
SWITCH capa 2 de 24 puertos	3 u		
Patch Panel de 48 puertos para RJ 45	13 u		
Patch Panel de 24 puertos para F.O.	1 u		
Patch Panel de 24 puertos	3 u		
Router Wireless	15 u		
Patch Cord del SWITCH al Patch Panel Patch Cord del Keystone a Pc	797 u / total en metros 4130		
Cable UTP Cat 5e	571 u / total en metros 11036 m		
Cable STP	1 u / total en metros 40 m		
Pacth Cord de Fibra Óptica	14 u / total en metros 14 m		
Fibra Óptica multimodo de 62,5 / 125 μm	2 hilos	Color Azul	504 m
	12 hilos	Color Verde agua	110 m
Rosetas	173		
Face Plate de 4	173		
Keystone	567		
RJ45	2772		
Protectores para RJ45 (Capuchones)	2772		
Conectores de Fibra Óptica SC	56		
Canaletas	802 m para UTP		
	306m para Fibra Óptica		

Tabla 3.42: Total de elementos

NOTA: Todos los componentes de interconexión deben ser categoría 5e y deben cumplir con la norma 568-B y T569.

3.2.3. Seguridad de la red

Como se conoce la seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

Las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

Establecer el valor de los datos es algo totalmente relativo, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones. Además, las medidas de seguridad no influyen en la productividad del sistema por lo que las organizaciones son resistentes a dedicar recursos a esta tarea tan importante.

Siempre hay que tener en cuenta que la seguridad comienza y termina con personas.

3.2.3.1. Recursos a proteger

Para comenzar es necesario establecer tres tipos de recursos que se deben proteger:

- Los recursos físicos son las impresoras, los servidores de archivos, los routers, los switch´s.
- Los recursos lógicos son las bases de datos de las cuales se obtiene la información con que trabaja la organización (Sistema Financiero, Sistema Administrativo, Sistema Escolástico, Generación de solicitudes de estudiantes).
- Los servicios son Aplicación Web, Correo electrónico Controlador de dominio, Antivirus, Intranet, Video Conferencia

Las metas de seguridad se resumen a continuación en el siguiente gráfico:

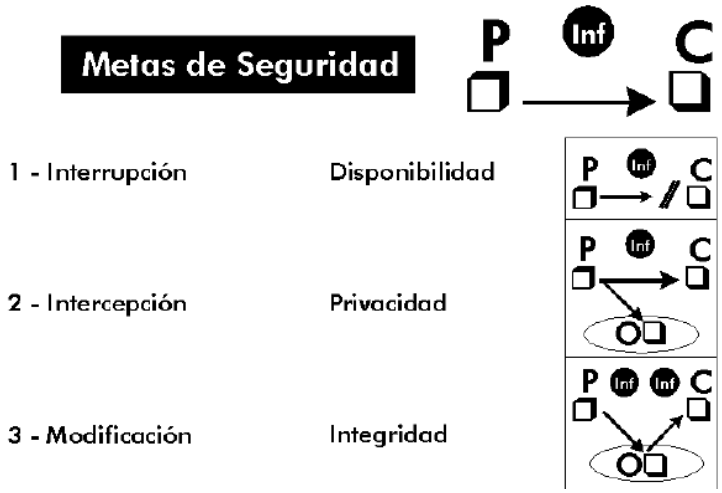


Gráfico 3.69: Metas de Seguridad

El caso número uno es el de INTERRUPCIÓN. Este caso afecta la disponibilidad del recurso. Como se detalla a continuación.

Recurso afectado	Nombre	Causa	Efecto
Servicio	Correo electrónico	Alguien dio de baja el servidor (por algún método)	No poder enviar mail
	Aplicación Web	Mantenimiento en el servidor	No se puede acceder a la página Web
	Controlador de dominio	Mantenimiento en el servidor	No se tiene acceso a la red
	Antivirus	Mantenimiento en el servidor	No se tiene acceso a las actualizaciones
	Intranet	Mantenimiento en el servidor	No se tiene acceso a la página Web interna
	Video Conferencia	Fallas en la conexión de Internet	Baja calidad de video conferencia
Físico	Impresora	Falta de alimentación eléctrica. Fallas físicas	No imprime
	Computadoras Personales	Falta de alimentación eléctrica. Fallas físicas y/o de software	No se encienden
	Servidores	Falta de alimentación eléctrica. Fallas físicas y/o de software	No permite trabajar con sus datos
	Switch	Falta de alimentación eléctrica. Fallas físicas	No se permite acceso a la red
	Router	Falta de alimentación eléctrica. Fallas físicas	No permite acceso a la red
	Touch Screen	Falta de alimentación eléctrica. Fallas físicas	No se enciende
Lógico	Sistema Financiero	Fallas en el servidor Fallas en la red	No se pueden realizar las funciones del sistema
	Sistema Administrativo	Fallas en el servidor Fallas en la red	No se pueden realizar las funciones del sistema
	Sistema Escolástico	Fallas en el servidor Fallas en la red	No se pueden realizar las funciones del sistema
	Generación de solicitudes de estudiantes	Fallas en el servidor Fallas en la red	No se pueden realizar las funciones del sistema

Tabla 3.43: Interrupción

El segundo caso es el de INTERCEPCIÓN, en el cual se pone en riesgo la privacidad de los datos.

Recurso afectado	Nombre	Causa	Efecto
Servicio	Correo electrónico	Programa que duplica los mensajes (mails) que salen de una sección y los envía a una dirección.	Leer información
	Intranet	Uso de sniffer	Capturar información y / o contraseñas
Lógico	Sistema Financiero	Uso de sniffer	Capturar información y / o contraseñas
	Sistema Administrativo	Uso de sniffer	Capturar información y / o contraseñas
	Sistema Escolástico	Uso de sniffer	Capturar información y / o contraseñas

Tabla 3.44: Intercepción

El tercer caso, Modificación afecta directamente la INTEGRIDAD de los datos que le llegan al consumidor.

Recurso afectado	Nombre	Causa	Efecto
Servicio	Aplicación Web	Alguien logró ingresar como WEBMASTER y ha cambiado los contenidos de la página	Los datos mostrados en la página no son los reales
	Intranet	Alguien logró ingresar como una cuenta de docente y ha cambiado las notas de la página	Los datos han sido alterados
Lógico	Sistema Financiero	Alguien logró ingresar al sistema	Datos monetarios alterados
	Sistema Administrativo	Alguien logró ingresar al sistema	Datos de consejos alterados
	Sistema Escolástico	Alguien logró ingresar al sistema	Datos de estudiantes alterados

Tabla 3.45: Integridad

3.2.3.2. Identificación de usuarios

Una vez identificados los recursos que se deben proteger. Es importante conocer de quién se deben proteger?, todos los estudios realizados demuestran que el 80% de los problemas proceden de los llamados “clientes internos” de la organización (los empleados o elementos que se desempeñan en la organización), y sólo el 20 % restante, proviene de elementos externos a la organización.

Una aproximación acerca de cómo proteger los recursos de los problemas originados por el cliente interno consiste en la identificación del uso correcto de los mismos por parte de éstos. Pero primero, se debe conocer quiénes son los que van a hacer uso de los recursos. Es decir se debe contar, previamente, con un conocimiento cabal de todos los usuarios del sistema. Esta lista no es obligatoriamente individual, sino que puede ser, en efecto, una lista por grupos de usuarios y sus necesidades en el sistema y así determinar los permisos que tendrán.

A continuación se detalla los usuarios, los recursos que utilizan, el tipo de acceso que tienen los usuarios frente al recurso y los permisos otorgados para trabajar con el recurso:

Servicios.- el tipo de acceso puede ser Local (ingresar dentro de la institución) y remoto (fuera de la institución).

Recurso del sistema		Identificación del usuario	Tipo de acceso	Permisos otorgados
Número	**Nombre**			
1	Correo electrónico	Personal administrativo, docente, y estudiantil	Local	Lectura y escritura
		Personal técnico	Local	Acceso Total
2	Aplicación Web	Personal administrativo, docente, estudiantil y comunidad	Local y remoto	Lectura
		Personal técnico	Local y remoto	Acceso Total
3	Controlador de dominio	Personal técnico	Local	Acceso Total
4	Antivirus	Personal administrativo, docente y estudiantil.	Local	Lectura
		Personal técnico	Local	Acceso Total
5	Intranet	Personal administrativo, docente,	Local	Lectura y escritura
		Personal técnico	Local	Acceso Total
		Estudiantes	Local	Lectura
6	Video Conferencia	Personal técnico	Local	Acceso Total
		Estudiantes	Local	Lectura

Tabla 3.46: Identificación de usuarios de Servicios

Recursos Físicos.- el tipo de acceso puede ser Local (manejo del recurso en el mismo lugar donde esta ubicado) y remoto (desde otro lugar dentro de la institución).

Recurso del sistema		Identificación del usuario	Tipo de acceso	Permisos otorgados
Número	**Nombre**			
1	Impresora	Personal administrativo, docente, y	Local y remoto	Lectura

Recurso del sistema		Identificación del usuario	Tipo de acceso	Permisos otorgados
Número	**Nombre**			
		estudiantil		
		Personal técnico	Local y remoto	Acceso total
2	Computadoras Personales	Personal administrativo, docente y estudiantil.	Local	Lectura
		Personal técnico	Local y remoto	Acceso total
3	Servidores	Personal administrativo, docente y estudiantil.	Remoto	Lectura y escritura
		Personal técnico	Local y remoto	Acceso total
4	Switch	Personal técnico	Local y remoto	Acceso total
5	Router	Personal técnico	Local y remoto	Acceso total
6	Touch Screen	Personal administrativo	Local	Lectura
		Personal técnico	Local	Acceso total

Tabla 3.47: Identificación de usuarios de Recursos Físicos

Recursos Lógicos.- el tipo de acceso puede ser Local (manejo del recurso en el mismo lugar donde está ubicado) y remoto (desde otro lugar dentro de la institución).

Recurso del sistema		Identificación del usuario	Tipo de acceso	Permisos otorgados
Número	**Nombre**			
1	Sistema Financiero	Área financiera	Remoto	Lectura y escritura
		Personal técnico	Local y remoto	Acceso remoto
2	Sistema Administrativo	Personal administrativo	Remoto	Lectura y escritura
		Personal técnico	Local y remoto	Acceso remoto
3	Sistema Escolástico	Áreas académicas	Remoto	Lectura y escritura
		Personal técnico	Local y	Acceso remoto

Recurso del sistema		Identificación del usuario	Tipo de acceso	Permisos otorgados
Número	Nombre			
			remoto	
4	Generación de solicitudes de estudiantes	Estudiantes	Remoto	Lectura y escritura
		Personal técnico	Local y remoto	Acceso remoto

Tabla 3.48: Identificación de usuarios de Recursos Lógicos

3.2.3.3. Procedimientos de Seguridad

¿Cómo aseguramos que no están ingresando a nuestro sistema por un puerto desprotegido o mal configurado?

¿Cómo nos aseguramos de que no se estén usando programas propios del sistema operativo o aplicaciones para ingresar al sistema en forma clandestina?

¿Cómo aseguramos de que, ante un corte de energía eléctrica, el sistema seguirá funcionando?

¿Cómo nos aseguramos de que los medios de transmisión de información no son susceptibles de ser monitoreados?

¿Cómo actúa la organización frente al alejamiento de uno de sus integrantes?

La respuesta a estos interrogantes reside en la posibilidad de conseguir dicha seguridad por medio de herramientas de control y seguimiento de accesos, utilizando check-lists para comprobar puntos importantes en la configuración y/o funcionamiento de los sistemas y por medio de procedimientos que hacen frente a las distintas situaciones.

Es muy aconsejable que se disponga de una agenda con las tareas que se deben llevar a cabo regularmente, a fin de que el seguimiento de los datos obtenidos sea efectivo y se puedan realizar comparaciones válidas al contar con datos secuenciales.

Procedimiento de alta de cuenta de usuario

Cuando un elemento de la organización requiere una cuenta de operación en el sistema, debe llenar un formulario que contenga, al menos los siguientes datos:

- Nombre y Apellido
- Puesto de trabajo
- Jefe inmediato superior que avale el pedido
- Descripción de los trabajos que debe realizar en el sistema
- Consentimiento de que sus actividades son susceptibles de ser auditadas en cualquier momento y de que conoce las normas de “buen uso de los recursos” (para lo cual, se le debe dar una copia de tales normas).
- Explicaciones breves, pero claras de cómo elegir su password.

Asimismo, este formulario debe tener otros elementos que conciernen a la parte de ejecución del área encargada de dar de alta la cuenta, datos como:

- Tipo de cuenta

- Fecha de caducidad
- Fecha de expiración
- Datos referentes a los permisos de acceso (por ejemplo, tipos de permisos a los diferentes directorios y/o archivos)
- Si tiene o no restricciones horarias para el uso de algunos recursos y/o para el ingreso al sistema.

Procedimiento de baja de cuenta de usuario

Este procedimiento es el que se lleva a cabo cuando se aleja un elemento de la organización o cuando alguien deja de trabajar por un determinado tiempo (licencia sin goce de sueldo, vacaciones, viajes prolongados, etc.). En base a la explicación anterior hay, entonces, dos tipos de alejamientos: permanente y parcial.

Aquí, es necesario definir un circuito administrativo a seguir, y que como todos los componentes de la política de seguridad, debe estar fuertemente apoyado por la parte gerencial de la organización.

Un ejemplo de este circuito, podría ser: ante el alejamiento de un elemento de la organización, la Administración de los RRHH debe informar en un formulario de “Alejamiento de personal”, todos los datos del individuo que ha dejado la organización, así como de la posición que éste ocupaba y el tipo de alejamiento (permanente o no). Una vez llegada la información al Centro de Cómputo se procede a dar de baja o inhabilitar la cuenta del usuario.

La definición de si se da de baja o se inhabilita es algo importante pues, si se da de baja, se deberían guardar y eliminar los archivos y directorios del usuario, mientras que si sólo se inhabilita, no pasa de esa acción. Si el alejamiento del individuo no era permanente, al volver a la organización, la sección que había informado anteriormente de la ausencia, debe comunicar su regreso, por medio de un formulario dando cuenta de tal hecho para volver a habilitar la cuenta al individuo.

Procedimiento para determinar passwords

Aunque no lo parezca, la verificación de palabras claves efectivas no es algo frecuente en casi ninguna organización. El procedimiento debe explicar las normas para elegir un password. Se debe explicitar:

- La cantidad de caracteres mínimo que debe tener,
- No debe que tener relación directa con las características del usuario.
- Debe constar de caracteres alfanuméricos, mayúsculas, minúsculas, números y símbolos de puntuación.

Para mayor seguridad una vez que el usuario ha elegido su password, se le debe correr un “programa crackeador” para tener idea de cuán segura es, en base al tiempo que tarda en romper la palabra.

Procedimientos de verificación de accesos

Se deben realizar auditorías de los archivos logísticos de ingresos a la red a fin de detectar actividades anómalas. Normalmente, este trabajo es realizado por programas a los que se les dan normativas de qué y cómo comparar. Escanean archivos de “log” con diferentes fechas tomando en cuenta las reglas que se le han dado. Ante la detección de un desvío, generan reportes informando el mismo.

Este procedimiento debe ser realizado por el personal del Centro de Cómputo sería recomendable realizarlo una vez al mes. Es necesario determinar el tiempo entre la auditoria y cómo actuar en caso de detectar desviaciones, esto será responsabilidad del área administrativa tanto en la determinación del tiempo como de las sanciones.

Procedimiento para el chequeo del tráfico de la red

Es necesario conocer el comportamiento del tráfico en la red, solo así se podrá determinar la calidad de servicio que se esta prestando, también permite detectar variaciones que pueden ser síntoma de mal uso de la red, para alcanzar este objetivo existen algunas herramientas gratuitas como es el Ethereal Network Fluke, Observer para determinar quien esta utilizando la red, entre otros.

Este trabajo es muy importante y necesita de personal capacitado para qué pueda interpretar, monitorear, analizar e informar los resultados, se recomienda realizar este monitoreo una vez al mes

Procedimiento para el monitoreo de los volúmenes de correo

Este procedimiento permite conocer los volúmenes del tráfico de correo o la cantidad de “mails” en tránsito. Dicho procedimiento se encuentra realizado por programas que analizan el tráfico en la red y llevan las estadísticas, generando reportes con la información pedida. El conocimiento de esta información permite conocer, entre otras cosas, el uso de los medios de comunicación. Al igual que el procedimiento anterior este es efectuado por el personal del Centro de Cómputo.

Procedimientos para el monitoreo de conexiones activas

Este procedimiento se efectúa con el objeto de prevenir que algún usuario deje su terminal abierta y sea posible que alguien use su cuenta. Es necesario determinar cierto tiempo de inactividad, trascurrido este se cierra la conexión y se genera un log con el acontecimiento.

Procedimiento de modificación de archivos

Este procedimiento sirve para detectar la modificación no autorizada y la integridad de los archivos. Para realizar este procedimiento existe software

que permite conocer accesos no autorizados, pero es necesario también establecer sanciones a estos actos que deberán ser designados por el área administrativa.

Procedimientos para el resguardo de copias de seguridad

Es necesario tener copias de seguridad de la información relevante para la Universidad, esta información deberá ser respaldada cada semana en horarios donde no exista mucha congestión de red por ejemplo los Sábados en la mañana, y guardada no solo en un servidor sino en un medio magnético. Mismos que deben estar ubicados en un armario cuyo acceso solo sea permitido al Director del Centro de Cómputo.

Es necesario determinar cuál es la información relevante para la universidad, misma que se detalla a continuación:

Sistema	Información
Controlador de dominio	Active Directory
Servidor de correo	Cuentas y bandejas de entrada
Sistema Escolástico	Base de datos, código fuente
Sistema Financiero	Base de datos, código fuente
Sistema Administrativo	Base de datos, código fuente
Aplicación Web e Intranet	Base de datos, código fuente
Computadores de Escuelas	La carpeta de documentos importantes
Computadores del Área Administrativa	La carpeta de documentos importantes

Tabla 3.49: Información a respaldar

Procedimientos para el monitoreo de los puertos en la red

Este procedimiento permite saber que puertos están habilitados en la red, y, en algunos casos, chequear la seguridad de los mismos.

Como se mencionó en el rediseño de la red es necesario la creación de Vlans una por cada área de trabajo y escuelas. La asignación de Vlans será por puerto y por MAC's para evitar que un intruso acceda a la red solo conectando su máquina al cable de red.

Para un mejor control es necesario documentar que VLans se crearán, qué puertos están asignados a las mismas; solo así se tendrá un control las conexiones y no habrá cables cuyo destino es desconocido.

Este procedimiento deberá ser realizado por el personal del Centro de Cómputo.

Procedimientos de cómo dar a publicidad las nuevas normas de seguridad

Este tipo de procedimiento no siempre es tenido en cuenta. Sin embargo, en una organización es muy importante conocer las últimas modificaciones realizadas a los procedimientos, de tal manera que nadie pueda poner como excusa "que no conocía las modificaciones". Ya que un porcentaje de los problemas de seguridad, según está demostrado en estudios de mercado,

proviene del desconocimiento de las normas y/o modificaciones a ellas por parte de los usuarios.

Toda modificación a un procedimiento será notificada al personal mediante un mailing y por notificación escrita en las carteleras y laboratorios de la institución, si una vez conocida la modificación el o los usuarios que incumplan o infrinjan las normas deberán recibir una sanción.

Procedimientos para recuperar información

Este procedimiento sirve para reconstruir todo el sistema o parte de él, a partir de las copias de seguridad. Es importante documentar los pasos a seguir para la restauración de cada aplicación y/o información respaldada, pues solo así en caso de emergencia cualquier integrante del Centro de Cómputo podrá dar solución al problema.

3.2.3.4. Check-Lists

Es un conjunto de ítems referentes a lo que habría que chequear y realizar para el buen funcionamiento de la red y por ende del sistema.

- Asegurar el entorno. ¿Qué es necesario proteger? ¿Cuáles son los riesgos?
- Determinar prioridades para la seguridad y el uso de los recursos.
- Crear planes avanzados sobre qué hacer en una emergencia.

- Trabajar para educar a los usuarios del sistema sobre las necesidades y las ventajas de la buena seguridad
- Asegurarse de que cada persona utilice su propia cuenta.
- ¿Están las copias de seguridad bien resguardadas?
- No almacenar las copias de seguridad en el mismo sitio donde se las realiza
- ¿Los permisos básicos son de sólo lectura?
- Tener sensores de humo y fuego en el cuarto de telecomunicaciones.
- Tener medios de extinción de fuego adecuados en el cuarto de telecomunicaciones.
- Entrenar a los usuarios sobre qué hacer cuando se disparan las alarmas.
- Instalar y limpiar regularmente filtros de aire en el cuarto de telecomunicaciones.
- Instalar UPS, protectores gaseosos al menos en el cuarto de telecomunicaciones.
- Tener planes de recuperación de desastres.
- Nunca usar teclas de función programables en una terminal para almacenar información de login o password.
- Concientizar a los usuarios de pulsar la tecla ESCAPE antes de ingresar su login y su password, a fin de prevenir los “Caballos de Troya”.
- Asegurarse de que cada cuenta tenga un password.
- No crear cuentas por defecto o “guest” para alguien que está temporariamente en la organización.
- Deshabilitar las cuentas de personas que se encuentren fuera de la organización por largo tiempo.

- Deshabilitar las cuentas “dormidas” por mucho tiempo.
- Limitar el acceso físico a cables de red, routers, switches.
- Cumplir los procedimiento de red

3.2.3.5. Implementación

La implementación de medidas de seguridad, es un proceso técnico administrativo. Como este proceso debe abarcar toda la organización, sin exclusión alguna, debe estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

Es fundamental no dejar de lado la notificación a todos los involucrados en las nuevas disposiciones y, darlas a conocer al resto de la organización con el fin de otorgar visibilidad a los actos de la administración y no causar un fuerte impacto dentro de la organización.

De lo expuesto anteriormente**,** resulta claro que proponer o identificar una política de seguridad requiere de un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea a la Universidad.

Todos los procedimientos deben ser registrados en una bitácora de datos que permita conocer al detalle todos los procedimientos realizados y así no

existan confusiones, repeticiones y se pueda llevar un control de los mismos. La manera más adecuada es llenando formularios mensuales de cada procedimiento. Por ejemplo:

Procedimiento: Alta de cuenta de usuario **Mes:……..**

Fecha	Nombre del usuario	Cuenta de usuario	Observación

Tabla 3.50: Registro de procedimiento de alta de cuenta de usuarrio

Procedimiento: Baja de cuenta de usuario **Mes:……..**

Fecha	Nombre del usuario	Cuenta de usuario	Observación

Tabla 3.51: Registro de procedimiento de baja de cuenta de usuario

CAPÍTULO IV

4. VALIDACIÓN

4.1. Demostración de la hipótesis

La hipótesis planteada al inicio de la investigación fue: Partiendo de los estándares de cableado estructurado será posible rediseñar la red de campus de la Pontificia Universidad Católica del Ecuador Sede Ambato para así mejorar su administración y ofrecer calidad de servicios.

Se ha visto necesario realizar una comparación para conocer el nivel de cumplimiento de los estándares o normas de cableado estructurado entre la red actual y la presente propuesta de rediseño de la red de campus. Estos valores están tomados de las encuestas, entrevistas y el análisis realizado en el capitulo anterior.

Para poder cuantificar los resultados se ha asignado los siguientes pesos a las diferentes respuestas.

Alto o bueno	3 puntos
Medio o regular	2 puntos
Bajo o malo	1 punto

Criterios de Evaluación	Actual			Propuesta		
	Alto 3	Medio 2	Bajo 1	Alto 3	Medio 2	Bajo 1
Los componentes de la red satisfacen las necesidades del usuario		X		X		
Se determinó las medidas del lugar sobre las cuales se ubica la red		X		X		
Se creó el mapa del diseño físico de una red			X	X		
Se creó el mapa del diseño lógico de una red			X	X		
Se estructuró una de red de área local con las medidas de seguridad e higiene según las especificaciones de cableado estructurado			X	X		
Los medios de transmisión están instalados de una manera correcta y bien distribuida (orden) todos en canaletas o tubos		X		X		
Todos los elementos activos de la red Switch o hub están ubicados en su respectivo gabinete con rack y pacth panel			X	X		
El área de trabajo cuenta con los elementos como rosetas, face plate, keystone y patch cord			X	X		
Los elementos de interconectividad están ubicados en áreas libres de interferencia electromagnética		X		X		
Los elementos de interconectividad están ubicados en lugares seguros fuera de la manipulación de los usuarios			X	X		
El cableado estructurado cumple con la norma TIA/EIA 568-B (impedancias, colores, cableado horizontal)			X	X		
El cableado estructurado cumple con la norma TIA 569-A (distribución de cableado, backbones, armario de cableado, terminales, canalizaciones).			X	X		
Existe una fácil identificación del destino de los cables en todo los puntos de red		X		X		
Existe congestión y carga en la red			X	X		
La red permite escalabilidad			X	X		
La red tiene una buena disponibilidad	X			X		
La red permite integración de servicios (teléfono, fax, LAN, sistemas de audio y video, seguridad, etc.)			X	X		
TOTAL:	24			51		

Tabla 4.1: Puntos de Evaluación del Cableado estructurado

Como se puede comprobar numéricamente la red actual cumple con un 50% de los puntos de evaluación o normas del cableado estructurado, debido a que a medida que aumentaban los requerimientos de los usuarios de interconexión a la red se fueron incrementando puntos de red para satisfacer de momento las necesidades del usuario, sin realizar un análisis previo de lo que podía pasar a futuro con la misma. Por esta razón existen grandes colisiones dentro del medio, pues al tener una red plana cuando un paquete es enviado por el usuario este se transmite por toda la red, por lo que es imposible implementar nuevas tecnologías que satisfagan las necesidades de los usuarios, pues la base para el buen funcionamiento de las mismas es una infraestructura de red con calidad de servicio.

La presente propuesta se fundamenta en el cumplimiento de normas de cableado estructurado y así satisfacer las necesidades actuales y futuras de los usuarios, diseñando una infraestructura de red adecuada que proporcione disponibilidad, escalabilidad, confiabilidad y seguridad. Para evitar que sigan existiendo colisiones es necesario segmentar la red y jerarquizarla, garantizando Calidad de Servicio, pero una vez implantada la red es necesario que ésta, sea fácil de administrar, de aquí la necesidad de centralizar la infraestructura y cumplir con políticas de seguridad a nivel organizacional.

Con este antecedente para la comprobación de la hipótesis se ha utilizado el Método Lógico.

Variable Independiente: Estándares de cableado estructurado

Variable Dependiente: Rediseñar la red de campus del edificio principal de la Pontificia Universidad Católica del Ecuador Sede Ambato para así mejorar su administración y ofrecer calidad de servicios.

Método Lógico (A $\rightarrow$ B):

El método Ponendo Ponens sostiene que “Afirmando Afirma”, es decir que, si se cumple A entonces se cumple B, por lo tanto se demuestra que:

Partiendo de los estándares de cableado estructurado será posible rediseñar la red de campus de la Pontificia Universidad Católica del Ecuador Sede Ambato para así mejorar su administración y ofrecer calidad de servicios.

4.2. Conclusiones

- La infraestructura de red en la Pontificia Universidad Católica del Ecuador Sede Ambato juega un papel importante para una exitosa gestión al aplicar servicios de telecomunicaciones, aptas para brindar servicios de datos, imagen, audio, telefonía, sistemas de seguridad. La toma de decisión para elegir la infraestructura óptima es de gran responsabilidad y no debe orientarse solamente al costo financiero de la inversión inicial, sino debería orientarse a su aplicación y buen funcionamiento por un prolongado tiempo de por lo menos para 10 años.

- Una vez realizado el análisis sobre la estructura y funcionamiento de la red LAN actual de la Pontificia Universidad Católica del Ecuador Sede Ambato se detectaron varias anomalías, entre las principales están: incumplimiento de las normas de cableado estructurado, equipos de interconexión en el piso, red plana por consecuencia existencia de un solo dominio de broadcast, red poco escalable, falta de mecanismos de seguridad y monitoreo en la infraestructura de red.

- Debido a los problemas detectados, el nivel de satisfacción de los usuarios y los requerimientos de aplicaciones futuras, se justifica el desarrollo de la presente propuesta del rediseño de la red LAN de campus de la PUCESA con calidad de servicio que se basa en el cumplimiento de las normas de cableado estructurado, toma en cuenta el crecimiento de los puntos de red a futuro, ofrece calidad de servicio y

establece políticas de administración y seguridad.

- La topología a implementarse será en estrella extendida. El cableado estructural consta de cableado vertical llamado también backbone, el cual se distribuye desde un Switch de capa 3 ubicado en el cuarto piso del edificio principal mediante fibra óptica multimodo a los demás puntos de concentración ubicados estratégicamente en el campus de la PUCESA y el cableado vertical que hace uso de concentradores de estaciones de trabajos switch´s de capa 2, Patch Panels (paneles de distribución), Cable UTP categoría 5e y los elementos qué conforman el Área de trabajo.

- La segmentación de la red es una característica importante en esta propuesta de rediseño, pues solo la creación de VLAN´s en los Switch permitirá disminuir considerablemente el broadcast y disponer eficientemente del ancho de banda. Para la creación, configuración e interconexión de VLAN´s, QoS y seguridad en los puertos es necesario la adquisición de equipos que cumplan determinados estándares como: 802.1Q, 802.1P, 802.1X, SNMP, Port Security, RIP, OSPF, IGPR.

- La infraestructura de red de la PUCESA debe ser fácilmente monitoreada y administrada constantemente, es una política de seguridad que no puede evadirse, pues así se puede controlar el funcionamiento de la red, los flujos de datos que se transmiten por la misma y esta tarea se puede realizar en base al uso de Software como es el caso de Ethereal o

Wireshark cuya licencia es GNU, todas estas acciones deben registrarse y así obtener un historial de la red que permita tomar decisiones a futuro.

- Por seguridad de los equipos de red es necesario la implementación de conexiones a tierra y el uso de UPS, pues de esta manera se garantiza el buen uso y funcionamiento de los mismos.

4.3. Recomendaciones

- La presenta propuesta de rediseño de la red de campus para la Pontificia Universidad Católica del Ecuador Sede Ambato permite que la red sea funcional, escalable, adaptable y fácil de monitorear, por lo que se recomienda implementar la misma y así contar con una infraestructura de red robusta, para que a futuro se pueda incorporar eventualmente otros servicios como: videoconferencia, cámaras IP, VoIP, sin necesidad de cambios drásticos o adiciones en el cableado del edificio reduciendo costos e inconvenientes.

- Si bien para la implementación de esta propuesta de rediseño de la red de campus de la PUCESA se requiere una importante inversión inicial en la adquisición de elementos activos y pasivos de la red, capacitación al personal encargado de la administración de la red; la misma se compensará con los ahorros en los costos de mantenimiento y de expansión o crecimiento de las redes soportadas.

- La implementación se la podría realizar por fases, para que la inversión se realice paulatinamente. La primera fase sería capacitar al personal y equipar el cuarto de telecomunicaciones y los laboratorios. La segunda fase contemplaría el primer piso y la escuela de optometría. La tercera fase sería el tercer y segundo piso del edificio principal. La cuarta fase alcanzaría la biblioteca, bar y pastoral. La quinta fase el primer y segundo piso del nuevo edificio. Y la sexta fase el tercer y cuarto piso del

mismo.

- La evaluación del comportamiento de la red es muy importante pues solo evaluando se puede mejorar, pero esta tarea debe documentarse, no puede pasarse por alto y más aún cuando las herramientas que se pueden utilizar, facilitan esta tarea, generando reportes de la red, filtrando los paquetes que se desea analizar y visualizando en forma gráfica su comportamiento. La administración y monitoreo de red no debe ser una tarea tediosa sino por el contrario fácil y confiable.

- Al emplear una topología estrella extendida, se facilita realizar cambios y modificaciones en la red de una manera rápida y sin complicaciones, es decir, los otros dispositivos en la red no se verán afectados por algún cambio en el patch panel.

BIBLIOGRAFÍA

Libros electrónicos

- Cisco Press Campus Network Design Fundamentals.pdf, Dec. 2005
- GEROMETA, Oscar. Principios Básicos de Networking, para redes CISCO IOS, Version 3.0, 2005
- Cisco Quality of Service Networking.pdf
- Cisco Internet Working Technology.pdf
- Cisco CCIE Fundamentals: Network Design.pdf
- Cisco Network Security.pdf
- Essential SNMP.pdf
- Redes inalámbricas en países en desarrollo.pdf
- Seguridad en redes.pdf
- Structured Cabling Supplement.pdf.
- Security & Privacy, IEEE Computer Magazine Supplement.pdf
- Manual de Ethereal.pdf

Internet

- http://www.mundopc.net/cursos/redes/redes11.php
- http://directorio.adfound.com/visitar.php?ID=1822&nombre=Redes%20de%20comunicación&url=http://serviger.8m.com
- http://www.pchardware.org/redes/intranet/red_local.php
- http://www.pchardware.org/redes/redes.php

- http://nti.educa.rcanaria.es/conocernos_mejor/apuntes/paginas/redes.htm
- http://www.disc.ua.es/asignaturas/rc/ingtecinf/trabajos/fastether/practica4.html
- http://webs.demasiado.com/inda/gigabit.htm
- http://www.alsurtecnologias.com.ar/fibra-optica.php
- http://www-es.linksys.com
- http://www.zonagratuita.com/servicios/seguridad/wireles.html
- http://www.saulo.net/pub/inv/SegWiFi-art.htm
- http://www.siemon.com/surveys/perseus6.js
- http://www.optral.es
- http://www.panduitemea.com

GLOSARIO

A

Administración

El método para etiquetado, identificación, documentación y uso necesario para implantar movimientos, adiciones y cambios al cableado estructurado de la red

Ancho de Banda

El ancho de banda describe la capacidad de frecuencia de un sistema de transmisión y es una función del tipo de fibra, distancia, y características del transmisor. El margen de ancho de banda maximiza la capacidad de un sistema para soportar aplicaciones avanzadas.

Anycast

Cuando se envía un paquete a un destinatario cualquiera de un conjunto de destinatarios posibles. Ejemplo: servicio de alta disponibilidad ofrecido por varios servidores simultáneamente; el cliente solicita una determinada información y espera recibir respuesta de uno cualquiera de ellos.

Área de trabajo

Espacio en el edificio, contenedor o taller donde los usuarios interactúan con el equipo terminal o computador.

Atenuación

Es una medida de la disminución de la intensidad de la señal a lo largo de la línea de transmisión. Asegurar una baja atenuación de señal es crítico porque la tecnología digital de procesamiento de señales no puede compensar por demasiada atenuación de señal.

ARP (Address Resolution Protocol – Protocolo de Resolución de Dirección)

Cada dispositivo en una red tiene al menos dos direcciones: una dirección de control de acceso al medio (Media Access Control – MAC), y una dirección de Protocolo Internet (IP). La dirección MAC es la dirección de la tarjeta de interface físico con la red, en el interior del dispositivo, y no cambia nunca para esa tarjeta. La dirección IP puede cambiar si la máquina es trasladada a otro lugar de la red o si la red utiliza DCHP. ARP, uno de los protocolos IP, se utiliza para asociar o resolver una dirección IP con su correspondiente dirección MAC (y viceversa). ARP trabaja enviando un paquete broadcast a todas las máquinas conectadas a una red Ethernet. El paquete contiene la dirección IP con la que el emisor quiere comunicarse. La mayoría de las máquinas lo ignoran. La máquina que reconoce la dirección IP contenida en el paquete como suya, devuelve una respuesta.

B

Broadcast

Los paquetes se envían a toda la red, aunque vayan dirigidos a un único destinatario. Ejemplo: para anunciar nuevos servicios en la red.

C

Cableado Estructurado

Es un medio de comunicación físico-pasivo para las redes LAN de cualquier empresa o edificio de oficinas. Con él se busca un medio de transmisión independiente de la aplicación, es decir que no dependa del tipo de red, formato o protocolo de transmisión que se utilice: Ethernet, Token Ring, Voz, RDSI, Control, Video, ATM sino que sea flexible a todas estas posibilidades.

Cableado Horizontal.

El cableado horizontal incorpora el sistema de cableado que se extiende desde la salida del área de trabajo hasta el cuarto de telecomunicaciones.

Cableado del Backbone (Cableado Vertical)

El cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos, medios de transmisión (cables), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas.

ConectorRJ-45

Se utiliza con el cable UTP. Está compuesto de 8 vías con 8 "muelas" que a la hora de colocar el conector pincharán el cable y harán posible la transmisión de datos. Por eso será muy importante que todos los hilos queden a ras del conector.

Conector de Fibra Óptica duplex Tipo SC

Dispositivo de terminación mecánica para un par de fibras ópticas. Tiene una alta precisión en cuanto a la dimensión del mecanismo y además tiene un alto desempeño.

Cuarto de Telecomunicaciones

Es el área en un edificio utilizada para el uso exclusivo de equipos asociados con el sistema de cableado de telecomunicaciones. El espacio de este cuarto no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. Además, debe ser capaz de albergar equipos de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. El diseño de los cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de telecomunicaciones. Todo edificio debe contar con al menos un cuarto de telecomunicaciones o cuarto de equipos. No hay un límite máximo en la cantidad de cuartos de telecomunicaciones que pueda haber en un edificio.

D

Dirección MAC (Media Access Control – Control de Acceso al Medio)

Es una de las dos direcciones que tiene cada ordenador conectado en red (siendo la otra la dirección IP). La dirección de Control de Acceso al Medio es un único identificador de 48-bits que se escribe normalmente como 12 caracteres hexadecimales agrupados en pares (e. g., 00-00-0c-34-11-4e). Normalmente está dirección es otorgada por el fabricante de la tarjeta de interfaz de red y no cambia nunca. Representa la dirección física de un dispositivo de datos, y se utiliza como una ayuda para los routers que tratan de identificar máquinas en grandes redes.

E

Elementos pasivos

Cables y accesorios de conexión.

Elementos activos

Switch, router, hub.

I

ICMP (Internet Control Message Protocol – Protocolo de Control de Mensajes de Internet)

Protocolo utilizado para enviar mensajes de control y de error en un sentido y en otro entre nodos de Internet. Quizá el comando más utilizado sea ping.

Interconexión

Conexión directa de un equipo a un bloque de conexión o panel de parcheo de la red de cableado estructurado, a través de un cordón de parcheo o puente.

L

LAN (local area network – Red de área local)

Una red de ordenadores que se extiende en un área relativamente pequeña, generalmente confinada a un único edificio o a un grupo de edificios.

M

Multicast

Si se envía a un grupo selecto de destinatarios de entre todos los que hay en la red. Ejemplo: emisión de videoconferencia.

N

NIC (Network Interface Card – Tarjeta de Interface de Red)

Dispositivo que envía y recibe datos entre el ordenador y el cable de red. Cada ordenador conectado a la red debe estar provisto de una de estas tarjetas.

P

Patch cords

Se pueden elegir variedad de colores y longitudes para asegurar el máximo de esmero en la instalación, especialmente en racks con gran cantidad de patch panels (se sugiere instalar distintos colores de patch cords) o en aquellos muy pequeños en los cuales los sobrantes de cable dificultan la administración (se sugiere utilizar patch cords de un largo acorde al tamaño del rack).

Patch panels (paneles de “pacheo”)

Los patch panels son dispositivos que sirven para interconectar diferentes puntos de una red. Los patch panels deben ser de primera calidad debido a que por sus puntos transitan señales de alta velocidad. Los patch panels pueden tener conectores tipo RJ45 o de fibra óptica, que pueden servir tanto para redes como para telefonía. Disponiendo de un patch panel, se puede, eventualmente, cambiar un punto de red por un punto de teléfono si así se

necesita. Un patch panel brinda enorme flexibilidad porque le permite intercambiar puntos de la red rápidamente.

Q

QoS

Un método de aplicación de QoS es utilizar algún tipo de algoritmo avanzado de colas. QoS entra en juego cuando el administrador de red quiere tratar algunos paquetes diferente a los demás. Por ejemplo: e-mail paquetes pueden retrasarse durante varios minutos sin que nadie lo note, mientras que los paquetes de VoIP no puede demorarse durante más de un décimo de un segundo pues los usuarios notaran el problema al no entenderse la comunicación

R

Racks de telecomunicaciones

Existen varios tipos de racks o anaqueles: de pie, abierto (open frame) y del tipo mural. Cada uno se utiliza en casos específicos según la disponibilidad de espacio, seguridad, capacidad a instalar, etc. Los frentes vienen preparados para soportar equipos de 19" de ancho y su profundidad dependerá del tipo de equipos que se deseen instalar. El caso más crítico es el de los del tipo mural, que son de tamaño reducido (hasta 18 HU). El espacio de rack en un rack estándar es medido en unidades de altura (HU, o

simplemente U). Un HU o altura útil es el espacio que ocuparía un ordenador estándar en el rack y equivale a 4.44 cm. De esta manera un dispositivo que tiene 8.88 cm de altura toma 2HU de espacio de rack. Los racks solucionan los problemas de organización en los sistemas de cableado y de cabecera.

S

Segmentación

Consiste en dividir a la red en pequeños dominios, llamados segmentos, conectando un pequeño hub de grupo de trabajo a un puerto de switch o bien se aplica micro segmentación la cual se realiza conectando cada estación de trabajo y cada servidor directamente a puertos de switch teniendo una conexión dedicada dentro de la red, con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario. El dispositivo que realiza la segmentación es el Switch que soporte creación de VLANs.

Sistema de Puesta a Tierra y Puenteado

El sistema de puesta a tierra y puenteado establecido en el estándar ANSI/TIA/EIA-607 es un componente importante de cualquier sistema de cableado estructurado moderno, no es mas que una conexión conductiva hacia tierra o hacia algún cuerpo conductivo que haga la función de tierra, ya sea intencional o accidental entre un circuito eléctrico (por ejemplo telecomunicaciones) o equipo.

SNMP (Simple Network Management Protocol)

Es el protocolo sencillo y fácil de implantar que permite la administración y monitoreo de la red, pues su único objetivo es descubrir los verdaderos problemas que tiene la red a través del envío de agentes.

T

Telecomunicaciones

Toda emisión, transmisión o recepción de signos, señales, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos (Ley de Telecomunicaciones).

Topología

Arreglo físico o lógico de un sistema de telecomunicaciones.

Topología estrella

Topología en la cual cada salida/conector de telecomunicaciones está directamente cableado a un punto de distribución, es decir que todos los puntos de red se concentren en un solo punto.

U

Unicast

Si se envía a un destinatario concreto. Es el más normal.

V

VLAN (Virtual Local Area Network – Red de área local Virtual)

Una VLAN se encuentra conformada por un conjunto de dispositivos de red interconectados, se define como una subred lógica y es considerada como un dominio de Broadcast que puede estar en el mismo medio físico o bien puede estar sus integrantes ubicados en distintos sectores de la corporación.

VPN (Virtual Private Network – Red Virtual Privada)

Un medio para tener los beneficios de seguridad de una red privada, dedicada, sin el coste de poseer realmente una red. VPN usa criptografía para desordenar los datos de manera que sean ilegibles mientras recorren Internet, proporcionando así privacidad en líneas públicas. Las compañías con sucursales utilizan generalmente VPNs para conectar múltiples lugares.

W

WEP (Wired Equivalent Privacy – Privacidad Equivalente a Cableada)

Aspectos de seguridad del estándar 802.11 que permite que dispositivos inalámbricos como PDAs y ordenadores laptop, accedan a una red de ordenadores a través de radiofrecuencia en vez de cableado físico. WEP cumple tres tareas: 1) Autenticar clientes en Puntos de Acceso; 2) Encriptar los datos entre los clientes y el Punto de Acceso; y 3) Incluir en cada paquete intercambiado un código de integridad. La realización inicial de WEP proporciona una seguridad débil. Aunque no completamente inútil, el

mejor uso que se le puede dar es como otra capa de seguridad complementaria a otras que establezcan medidas de seguridad más potentes.

ANEXOS

ANEXO 1. ENCUESTA A USUARIOS DE LA RED

OBJETIVO: Conocer el estado de la red actual de la Pontificia Universidad Católica del Ecuador Sede Ambato y medir su calidad de servicio.

La información proporcionada servirá como parámetros para la evaluación del estado de la red LAN actual, por lo que se solicita contestar de la manera más sincera posible.

Marque una X para indicar su respuesta

1. Cuántas horas promedio al día, usted utiliza la red de la PUCESA?

   Menos de 2 horas ( )

   De 2 a 5 horas ( )

   Más de 5 horas ( )

2. Cuáles son las aplicaciones que utiliza con mayor frecuencia?

   Internet ( )

   Sistema Académico ( )

   Sistema Financiero ( )

   Biblioteca ( )

   Correo de la PUCESA ( )

Pagina Web de la PUCESA ( )

Compartir archivos entre computadoras de la red ( )

Otras ( ) ……

3. Cómo calificaría el servicio de Internet?

   Excelente ( )

   Bueno ( )

   Medio ( )

   Regular ( )

   Malo ( )

4. Cómo calificaría el servicio de red de la PUCESA (transferencia de archivos, uso de aplicaciones en red)?

   Excelente ( )

   Bueno ( )

   Medio ( )

   Regular ( )

   Malo ( )

5. En qué horario tiene mayor dificultad con la calidad del servicio de la red?
6. Seleccione las características de la red actual de la PUCESA

   Rapidez

   Alta ( ) Media ( ) Baja ( )

Disponibilidad.- siempre que necesita usar la red funciona

Alta ( ) Media ( ) Baja ( )

Seguridad.- los datos en la red no pueden ser vistos o modificados por otras personas

Alta ( ) Media ( ) Baja ( )

7. Qué servicios le gustaría utilizar en la red de la PUCESA?

Intranet ( )

Correo electrónico interno ( )

Video Conferencia ( )

Voz sobre IP ( )

Otros ( ) ……..

Gracias por su colaboración

ANEXO 2. PREGUNTAS DE LA ENTREVISTA

ENTREVISTA

DIRIGIDA A:

- ING. Diego Santacruz, DIRECTOR DEL CENTRO DE CÓMPUTO
- ING. Santiago Acurio, DIRECTOR DE LA ESCUELA DE INGENIERIA EN SISTEMAS

1. ¿Cuáles son las aplicaciones que se implementarán?

2. ¿Cuáles son los criterios de éxito?

3. ¿Cuál es el nivel de seguridad, disponibilidad y rapidez que tiene la red?

4. ¿Cuáles son los segmentos de red más frágiles o críticos?

5. ¿Existe documentación acerca de los puntos más comunes de falla dentro de la red de campus?

6. ¿Cuál fue la causa de la falla en el segmento de la red?