UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO

CARRERA: INGENIERÍA ELECTRÓNICA

Trabajo de titulación previo a la obtención del título de: INGENIERA ELECTRÓNICA E INGENIERO ELECTRÓNICO

TEMA: DISEÑO DE LA RED DE CAMPUS PARA LA ESCUELA SUPERIOR DE POLICÍA "GRAL. ALBERTO ENRÍQUEZ GALLO".

AUTORES: ALPUSIG ENDARA GLORIA ESTEFANY GRANDA VELASTEGUI JORGE RICARDO

TUTOR:
JUAN CARLOS DOMÍNGUEZ AYALA

Quito, agosto del 2018

CESIÓN DE DERECHOS DE AUTOR

Nosotros Gloria Estefany Alpusig Endara y Jorge Ricardo Granda Velastegui, con los documentos de identificación N° 1725356263 y N° 1718011644, respectivamente manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación intitulado: DISEÑO DE LA RED DE CAMPUS PARA LA ESCUELA SUPERIOR DE POLICÍA "GRAL. ALBERTO ENRÍQUEZ GALLO", mismo que ha sido desarrollado para optar por el título de: Ingeniera Electrónica e Ingeniero Electrónico, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

Alpusig Endara Gloria Estefany 1725356263 Granda Velastegui Jorge Ricardo 1718011644

Quito, agosto del 2018

DECLARATORIA DE COAUTORÍA DEL DOCENTE TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el Proyecto Técnico, DISEÑO DE LA RED DE CAMPUS PARA LA ESCUELA SUPERIOR DE POLICÍA "GRAL. ALBERTO ENRÍQUEZ GALLO" realizado por Alpusig Endara Gloria Estefany y Granda Velastegui Jorge Ricardo, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, agosto del 2018

Juan Carlos Dominguez Ayala

CI: 1713195590

ÍNDICE DE CONTENIDO

CESIÓN D	E DERECHOS DE AUTORii
DECLARA	TORIA DE COAUTORÍA DEL DOCENTE TUTORiii
ÍNDICE DI	E CONTENIDOiv
CAPÍTULO	011
ANTECED	ENTES 1
1.1. PL	ANTEAMIENTO DEL PROBLEMA1
1.2. JU	STIFICACIÓN1
1.3. OB	JETIVOS2
1.3.1.	Objetivo General
1.3.2.	Objetivos Específicos
CAPÍTULO	2
LEVANTA	MIENTO DE LA LÍNEA BASE 3
1.4. Mo	odelo OSI3
1.4.1.	Capa física3
1.4.2.	Capa de Enlace
1.4.3.	Capa de Red9
1.4.4.	Capa de Presentación y Aplicación
1.5. Rec	querimientos de seguridad de red11
1.6. TS	S11
1.6.1.	Mapa de calor11
CAPÍTULO	O 3
DISEÑO D	E LA RED
3.1. Me	etodología de diseño PPDIOO14
3.1.1.	Preparación14
3.1.2.	Planeación

3.1.3.	Diseño
3.2. Mo	odelo de arquitectura empresarial de cisco15
3.3. Dis	seño de la Red de campus15
3.3.1.	Modelo de núcleo colapsado
3.4. Dis	seño Lógico de la red LAN17
3.4.1.	Direccionamiento
3.4.2.	Diseño de VLAN
3.4.3.	Plan de Implementación de la red LAN19
3.4.4.	Alimentación redundante
3.5. Dis	seño físico de la red LAN24
3.5.1.	Análisis de los equipos para la red LAN24
3.5.2.	Esquema físico de la red
3.6. Dis	seño lógico de la red WLAN28
3.6.1.	Áreas de cobertura
3.6.2.	Densidad de usuarios
3.6.3.	Segmentación y direccionamiento Ipv4 de la WLAN
3.7. Dis	seño físico de la red WLAN
3.7.1.	Ubicación de las Access Point
3.7.2.	Configuración del AP cisco 1602i32
3.7.3.	Configuración del access point ubiquiti ac pro34
3.7.4.	Análisis de los equipos para la red WLAN
3.8. Ce	ntro de datos y granja de servidores
CAPÍTULO	38
SIMULAC	ION DE LA RED
4.1. Sir	nulación en Packet Tracer

		rueba de la configuración basica y VIP en el switch de nucleo colapsado y de acceso
	4.4.	Prueba de la configuración de las interfaces en el switch de núcleo colapsado 40
	4.5. y del s	Prueba de la configuración de la redundancia en el switch de núcleo colapsado switch de acceso
	4.6.	Prueba de la configuración de los puntos de acceso con su dirección IP y su etivo SSID
	4.7. en el s	Prueba de la configuración de las listas de acceso y control de ancho de banda switch de núcleo colapsado
	4.8.	Prueba de comunicación de datos
	4.9.	Prueba de la configuración SSH43
	4.10.	Prueba de la configuración de las listas de acceso
	4.11.	Prueba de la configuración del servidor de la escuela de la policía44
	4.12.	Prueba de la configuración de QoS
	4.13.	Prueba de asociación de la WLAN por interfaz de radio
C	CAPÍT	ULO 5
A	NÁLI	SIS DE COSTOS
	5.1.	Introducción
	5.2.	Costos de equipos
	5.3.	Costo de implementación
	5.4.	Costo total del proyecto
	5.5.	Valor actual neto (VAN)
	5.5.	1. Tasa de descuento
	5.5.	2. Cálculo del VAN
	5.6.	Tasa interna de retorno (TIR)
	5.7.	Periodo de recuperación del capital (PRC)

CONCLUSIONES	51
RECOMENDACIONES	52
BIBLIOGRAFÍA	53
ANEXOS	54

ÍNDICE DE FIGURAS

Figura 2.1 Descripción de la topología actual de la Escuela Superior de Policía	4
Figura 2.2 Diseño de la red de fibra óptica de la ESP	5
Figura 2.3 Diseño de Rack de Dirección de 36U y 48 U	7
Figura 2.4 Diseño Rack de 6U, SWITCH Super Stack 4228G 24P, patch panel	8
Figura 2.5 Diseño Rack de 6U, Switch Catalyst 2960 24P, patch panel	8
Figura 2.6 Trafico de la WAN utilizando el software WINBOX	10
Figura 2.7 Tráfico de la LAN utilizando el software WINBOX	10
Figura 2.8 Estudio del Sitio en el casino	12
Figura 2.9 Estudio del Sitio de la dirección	13
Figura 3.1 Modelo de arquitectura Empresarial de Cisco.	15
Figura 3.2 Esquema lógico utilizando el modelo de tres capas para la Escuela Sup	erior
de Policía	16
Figura 3.3 Redundancia en la capa de núcleo colapsado y acceso	21
Figura 3.4 Ejemplo de la configuración dhcp snooping	22
Figura 3.5 Cuadrante de Gartner para infraestructuras de redes LAN cableac	las e
inalámbricas	24
Figura 3.6 Esquema físico de la Escuela de Policía	26
Figura 3.7 Diagrama lógico de la red inalámbrica	30
Figura 3.8 Área de cobertura en las aulas nuevas	31
Figura 3.9 Configuración del sw conectado al AP	32
Figura 3.10 Configuración del al AP	32
Figura 3.11 Configuración de vlan en el AP	33
Figura 3.12 Configuración del SSID en el AP	33
Figura 3.13 Ventana principal del sofware Unifi Controller de Ubiquiti	34
Figura 3.14 Configuración IP de los AP's Ubiquiti	35
Figura 3.15 Creación de SSID	35
Figura 3.16 Parámetros de configuración de un grupo de WLAN	36
Figura 4.1 Esquema lógico realizado en el software de simulación	38
Figura 4.2 Configuración básica y vtp	39
Figura 4.3 Configuración de las vlan's	39
Figura 4.4 Configuración de las interfaces	40
Figura 4.5 Configuración de redundancia	40
Figura 4.6 Configuración de los puntos de acceso	41

Figura 4.7 Configuración de las listas de acceso y QoS	41
Figura 4.8 Comunicación de datos entre la sala de instructores y jefatura de in	nstrucción
	42
Figura 4.9 Comunicación de datos entre Jefatura de instrucción a un d	lispositivo
inalámbrico de la jefatura financiera.	42
Figura 4.10 Funcionamiento de acceso al switch mediante SSH.	43
Figura 4.11 Prueba de funcionamiento de las listas de acceso	43
Figura 4.12 Funcionamiento del servidor dns y http	44
Figura 4.13 Funcionamiento de Qos en la interfaz fa0/1	45
Figura 4.14 Comprobación del BSSID por interfaz de radio	45
Figura 4.15 Conexión de la red wlan con su respectivo SSID	45

ÍNDICE DE TABLAS

Tabla 2.1 Disponibilidad de Access Point en ESP	6
Tabla 2.2 Puertos Activos del Router 1200 Mikrotik	9
Tabla 2.3 Dirección IP de la ESP	9
Tabla 2.4 Orden de intensidad en el software Acrylic heatmaps	12
Tabla 3.1 Distribución de Vlan's	18
Tabla 3.2 Valores para las prioridades de paquetes	23
Tabla 3.3 Tabla comparativa de los equipos de la capa distribución	25
Tabla 3.4 Equipos a utilizar para el diseño de la red LAN en la Escuela de Policía	27
Tabla 3.5 Cantidad de dispositivos conectados en WLAN	29
Tabla 3.6 Direccionamiento IPv4	29
Tabla 3.7 Grupos de usuarios con SSID	30
Tabla 3.8 Atenuaciones de acuerdo con los materiales de construcción	31
Tabla 3.9 Tabla comparativa de los equipos de Access Point	37
Tabla 5.1 Costo de equipos para la ESP	47
Tabla 5.2 Costo de ingeniería de proyecto	48
Tabla 5.3 Costo total del proyecto para la ESP	48
Tabla 5.4 flujo de caja aproximado	49

ANEXOS

Anexo 1 Tendido de Fibra Óptica en la ESP	54
Anexo 2 Datos obtenidos de los usuarios y número de puntos en la ESP	55
Anexo 3 Disponibilidad de equipos en ESP	56
Anexo 4 Vlan's de gestión y de acceso para cada departamento	56
Anexo 5 Configuración Básica	56
Anexo 6 Configuración SSH	56
Anexo 7 Configuración VTP en el switch de núcleo colapsado	57
Anexo 8 Configuración del nombre de las VLAN en el switch de núcleo colapsado	o 57
Anexo 9 Configuración de las interfaces de las vlan's en el switch de núcleo cola	apsado
	57
Anexo 10 Configuración DHCP en el switch de núcleo colapsado	57
Anexo 11 Configuración del protocolo de enrutamiento en el switch de	núcleo
colapsado	58
Anexo 12 Configuración de las ACL's para restringir acceso entre vlan's en el sw	itch de
núcleo colapsado	58
Anexo 13 Configuración de las ACL's para restringir servicios en el switch de	núcleo
colapsado	58
Anexo 14 Grupo de listas de acceso	59
Anexo 15 Configuración de LACP en el switch de núcleo colapsado	59
Anexo 16 Configuración VTP en el switch de acceso	59
Anexo 17 Configuración de LACP en el switch de acceso	59
Anexo 18 Configuración de las interfaces en el switch de núcleo colapsado	59
Anexo 19 Configuración de la interfaz de gestión y del acceso a las vlan's	60
Anexo 20 Configuración de QoS con CoS de 0.	60
Anexo 21 Configuración de QoS estándar	60
Anexo 22 Listas de acceso que van a hacer aplicadas en CoS y políticas	60
Anexo 23 Clases de servicio y políticas utilizando las listas de acceso	61
Anexo 24 Configuración de LACP en el switch de núcleo colapsado	61
Anexo 25 Configuración de LACP en el router frontera	61
Anexo 26 Especificaciones técnicas de las fuentes de alimentación	62
Anexo 27 Especificaciones técnicas de los switch de distribución	
Anexo 28 Especificaciones técnicas del switch de acceso	64
Anexo 29 Access Point distribuidos en toda la institución	

Anexo 30 Diagrama lógico de la wlan en la ESPN	. 66
Anexo 31 Mapa de cobertura de las aulas antiguas	. 67
Anexo 32 Mapa de cobertura de sala de instructores y comedor	. 67
Anexo 33 Mapa de cobertura de tribuna y auditorio	. 67
Anexo 34 Mapa de cobertura de la jefatura financiera	. 68
Anexo 35 Mapa de cobertura de la jefatura de instrucción	. 68
Anexo 36 Mapa de cobertura de dirección	. 68
Anexo 37 Diagrama físico de la red WLAN en la ESPN	. 69
Anexo 38 Especificaciones técnicas de los AP	70

RESUMEN

En el presente proyecto titulado: "Diseño de la red de campus para la Escuela Superior de Policía Gral. Alberto Enríquez Gallo", tiene como objetivo diseñar la red de campus para mejorar la gestión de la red y brindar una buena experiencia a los usuarios.

La Escuela Superior de Policía "Gral. Alberto Enríquez Gallo" se encuentra ubicado en la Av. Manuel Córdova Galarza S/N, vía a Pomasqui km 5 ½, en la ciudad de Quito.

Debido al crecimiento desorganizado y no planificado de la red, no se ha podido identificar los diferentes flujos de tráfico, la aplicación de políticas de seguridad, así como la definición de calidad de servicio se han vuelto muy difíciles de gestionar.

El diseño de la red actual no ha seguido un conjunto de buenas prácticas o un modelo de red para su diseño e implementación. El personal técnico y administrativo de la institución tampoco ha definido políticas que eviten el mal uso de los recursos informáticos.

Por tal motivo se realizó el diseño lógico y físico de la red LAN y WLAN cubriendo las necesidades previstas, dando una mejor solución en la estructura jerárquica, direccionamiento IP, y algunos aspectos técnicos como: la cobertura inalámbrica, ubicación de los APs, cantidad de usuarios y configuración de los equipos para que la red sea escalable, segura y confidencial.

ABSTRACT

In the present project entitled: "Design of the campus network for the Escuela Superior de Policía "Gral. Alberto Enríquez Gallo", aims to design the campus network to improve the management of the network and provide a good experience to users.

The Escuela Superior de Policía "Gral. Alberto Enríquez Gallo" is located on Av. Manuel Córdova Galarza S / N, via Pomasqui km 5 ½, in the city of Quito.

Due to the disorganized and unplanned growth of the network, it has not been possible to identify the different traffic flows, the application of security policies, as well as the definition of the quality of service have become very difficult to manage.

The design of the real network has not followed a set of good practices or a red model for its design and implementation. The technical and administrative staff of the institution has not defined policies that avoid the misuse of computer resources.

For this reason, the logical and physical design of the LAN and WLAN network covering the anticipated needs was performed, giving a better solution in the hierarchical structure, IP addressing, and some technical aspects such as: wireless coverage, location of the APs, number of users and configuration of the equipment so that the network is scalable, secure and confidential.

INTRODUCCIÓN

El desarrollo del presente proyecto está dividido en función de los siguientes capítulos:

En el primer capítulo se detalla los objetivos generales y específicos y la respectiva justificación del proyecto.

En el segundo capítulo se definen la línea base de la red actual de la Escuela Superior de Policía identificando las necesidades a ser cubiertas. Esto corresponde a como se encuentra actualmente distribuido el cable estructurado en cada uno de los departamentos que posee esta institución.

En el tercer capítulo se diseña la red de campus LAN y WLAN para mejorar la seguridad, calidad de servicio, escalabilidad y disponibilidad, con los datos obtenidos en la línea base mediante el modelo jerárquico de Cisco. A su vez el diseño de la red inalámbrica permitirá tener mayores oportunidades en movilidad, productividad y servicio a diferencia de una red cableada.

En el cuarto capítulo se simula la red propuesta para analizar la viabilidad técnica, y así poder demostrar su factibilidad de implementación cumpliendo con los requisitos planteados que son el de comprobar que la red sea eficiente, flexible y escalable, haciendo que la experiencia del usuario sea satisfactoria.

El quinto capítulo se analiza la viabilidad de costos del proyecto mediante TIR y VAN para evaluar la factibilidad económica del proyecto.

CAPÍTULO 1

ANTECEDENTES

1.1. PLANTEAMIENTO DEL PROBLEMA

La Escuela Superior de Policía ha tenido un crecimiento no planificado debido a que el diseño de la red actual no ha adoptado un conjunto de buenas prácticas o un modelo de red que permita una comunicación viable, motivo por el cual la experiencia de los usuarios no ha sido satisfactoria en cuanto a la navegación a internet.

Además, no se han establecido lineamientos generales que definan el uso de los recursos y servicios informáticos de la Institución. La ausencia de estas políticas genera la posibilidad de que los usuarios hagan un mal uso de los recursos y servicios, afectando la seguridad y funcionalidad de la red.

La red actual no posee políticas de seguridad, calidad de servicio y una organización jerárquica, por consiguiente, la información de cada área es transportada sin ningún tipo de prioridad por el mismo medio, provocando congestionamiento y saturación en la red local, razón por la cual esta infraestructura se ha limitado en brindar solo acceso a internet.

1.2. JUSTIFICACIÓN

El presente proyecto tiene como finalidad la contribución al fortalecimiento y la organización de las Redes de Área Local en la Escuela Superior de Policía "Gral. Alberto Enríquez Gallo" para mejorar mediante un modelo jerárquico de la red para lo cual se definirá la topología LAN, distribución de direcciones IP y configuración adecuada para su funcionamiento. A su vez se realiza un análisis comparativo de los dispositivos de las diferentes marcas con la finalidad de seleccionar el equipo adecuado que cubra las necesidades de la Institución.

Debido a que los grupos de trabajo han sido distribuidos equitativamente por segmento de la red ha provocado que los usuarios compartan los mismos servicios como la confidencialidad de la información que ha ocasionado múltiples ataques de personas mal intencionadas que buscan borrar, manipular, espiar y dañar archivos importantes, así como obtener contraseñas y usarlas a su beneficio; para lo cual es necesario facilitar

la organización, la identificación y creación de políticas, que permitirán mejorar el rendimiento y eficiencia de la red.

Al no existir una red de campus debidamente planificada es necesario un diseño fundamentado en un modelo jerárquico empresarial que ayudará con la organización de la infraestructura de red actual, basados en la metodología PPDIOO de Cisco, el mismo que establece el ciclo de vida en la red por etapas, se aportará al análisis de los requerimientos y la organización, para satisfacer el correcto funcionamiento de la red.

1.3. OBJETIVOS

1.3.1. Objetivo General

Diseñar la red de campus para la Escuela Superior de Policía "Gral. Alberto Enríquez Gallo" para mejorar la gestión de la red y brindar una buena experiencia a los usuarios.

1.3.2. Objetivos Específicos

- Definir la línea base de la red actual de la Escuela Superior de Policía para la identificación de las necesidades a ser cubiertas.
- Diseñar la red de campus LAN y WLAN para mejorar seguridad, calidad de servicio, escalabilidad y disponibilidad.
- Simular la red diseñada para comprobar con la red actual y analizar la factibilidad técnica.
- Analizar la viabilidad de costos del proyecto mediante TIR y VAN para evaluar la factibilidad del proyecto.

CAPÏTULO 2

LEVANTAMIENTO DE LA LÍNEA BASE

La Escuela Superior de Policía "General Alberto Enríquez Gallo", es una institución pública que permite la formación de oficiales profesionales para que cumplan eficientemente las leyes de la constitución del Ecuador, por lo cual tienen varios departamentos ubicados por todo el campus, de los cuales se detallan a continuación:

- Dirección
- Auditorio
- Jefatura Financiera
- Jefatura de Instrucción
- Tribuna
- Aulas antiguas
- Aulas nuevas
- Sala de instructores
- P5
- Garita o prevención

1.4. Modelo OSI

Para el levantamiento base de la línea en la Escuela Superior de Policía se utilizó el modelo de referencia OSI que consiste en 7 capas que son: física, enlace de datos, red, transporte sesión, presentación y aplicación.

1.4.1. Capa física

En la actualidad la Escuela Superior de Policía cuenta con una red alámbrica con topología estrella y con equipos informáticos que tienen acceso a la red entre laptops o computadoras del personal administrativo y cadetes, estos son aproximadamente 300 equipos, con un ancho de banda de la red LAN de tipo asimétrica debido a que su velocidad varía entre 100Mbps a 1Gbps, además cuenta con un ancho de banda del servicio de internet por parte del proveedor CNT de 18 Mbps para el departamento de dirección, 5 Mbps en el comedor nuevo y 5 Mbps para las Aulas Nuevas, dando un total de 28 Mbps para todo el Campus. A continuación, se muestra en la figura 2.1 la topología física del campus.

Primer Año Sale Instituctores CNT CNT (5 Dormitorio Mujeres (5Mbps) Mbps) Dermitorio Tercer Afvo 0100 Jefature de Instrucción CNT (18 Mbps) Switch D-Link Switch-Cisco 2960 Restrito 2-Pcs Bodega Yusco Tribuna onono AP Carco

Figura 0.1 Descripción de la topología actual de la Escuela Superior de Policía

Elaborado por: Alpusig Estefany, Granda Ricardo

1.4.1.1. Cableado De Fibra Óptica

El acceso a la red de la Escuela Superior de Policía (ESP) se realiza a través de fibra óptica monomodo implementados en un inicio por la empresa Telconet y posteriormente por la empresa Akros que implemento el nuevo tendido.

La red de fibra óptica provista por la empresa Telconet se encuentra conectada a través de cajas de distribución ODF aéreas ubicada en postes, la cual es de tipo monomodo con diferentes cantidades de hilos como de 24, 48, y 96 hilos, los cuales son utilizados para dar conectividad a equipamiento activo de frontera que es un transceiver de marca TP-LINK MC 112CS. Mientras que la conexión del switch con los computadores de las áreas y los access point se realiza usando cable UTP categoría 6A. (Anexo 1)

La red de fibra óptica posee puntos de red en los diferentes edificios y se observan a continuación en la figura 2.2.

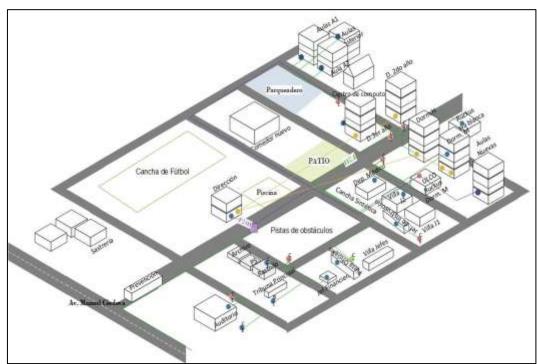


Figura 0.2 Diseño de la red de fibra óptica de la ESP

Elaborado por: Alpusig Estefany, Granda Ricardo

1.4.1.2. Distribución de usuarios en la ESP

En base a una inspección física en la Institución juntamente con la colaboración del departamento de TIC, se recopiló la información de la distribución del espacio y el número de usuarios por cada edificio. La Escuela Superior de Policía tiene diferentes

áreas de cobertura alrededor del campus tal como se muestra en el anexo 2, sin embargo, el número de puntos de datos existente no son suficientes para la cantidad de usuarios, por lo que ha sido necesario la instalación de un switch D-Link DCS-110 con la finalidad de brindar conectividad a todos los trabajadores.

1.4.2. Capa de Enlace

1.4.2.1. Distribución de los Access Point

Hay 17 dispositivos de red inalámbrica o Access Point marca Cisco Aironet 1602i y 2 Ruckus ZoneFlex 7762-AC que han sido adquiridos para la institución, sin embargo, no se encuentran en uso ya que no están ubicados estratégicamente.

En la tabla 2.1 se puede observar que de todos los puntos de acceso instalados solamente 2 se encuentran activos y en funcionamiento para todo el campus. Existen, 8 AP's no están operando debido a que se encuentran en los dormitorios de los cadetes y solo pueden acceder al internet desde las aulas de laboratorio. Adicionalmente cabe señalar que existen 9 AP's en buen estado que se mantienen almacenados en el centro de datos.

Tabla 0.1 Disponibilidad de Access Point en ESP

	Identificación en la inspección				
# Área		Cantidad	Observación		
1	Casino de oficiales	1	Activo-Interior		
2	Villas de Oficiales	1	Inactivo-Exterior		
3	Villas J1	1	Inactivo-Interior		
4	Dormitorio 1er año	1	Inactivo-Exterior		
5	Dormitorio 2do año	1	Inactivo-Exterior		
6	Dormitorio 3ero año	1	Inactivo-Exterior		
7	Comedor	1	Inactivo-Exterior		
8	Jefatura de Instrucción	1	Inactivo-Interior		
9	Auditorio	1	Inactivo-Interior		
10	Dirección	1	Activo-Interior		
11 TICS 9 Desconectados		Desconectados			
TOTAL 19					

Elaborado por: Alpusig Estefany, Granda Ricardo

Según las políticas de estándar de los equipos de Cisco, el access point Aironet 1602i se encuentra fuera de venta y su vida útil a finalizado en el 2016, por lo que sería un limitante para el diseño de la red inalámbrica.

1.4.2.2. Distribución de los Rack

1.4.2.2.1. Rack de Dirección

En este departamento se encuentra el centro de datos que tiene un rack de 36 U y 48 U, en donde se observa que los cables se encuentran conectados de forma desorganizada y sin apilar, no obstante, funcionan normalmente, como se muestra en la figura 2.3.



Figura 0.3 Diseño de Rack de Dirección de 36U y 48 U

Elaborado por: Alpusig Estefany, Granda Ricardo

En el rack de 36 U se encuentra el switch Cisco de capa 3 catalyst 3750 de 12 puertos de los cuales 7 están conectados. Por recomendación del fabricante Cisco, el switch terminó su vida útil en el año 2012, fecha en la que fue retirado del mercado y por tanto las actualizaciones y el soporte ya no se encuentran disponibles.

A su vez está conectado a un switch cisco catalyst 2960 de 48 puertos de los cuales 36 están conectados y 12 desconectados.

En el rack de 48 U están ubicados los transeiver, fuentes de poder.

1.4.2.2.2. Rack de Jefatura Financiera

En este departamento se encuentra un switch super stack 3COM 4228G 24P (10 puertos conectados) que brinda servicio de acceso a la red y la conectividad a los usuarios a través de enlaces UTP con velocidades de hasta 100 Mbps, como se muestra en la figura 2.4

Figura 0.4 Diseño Rack de 6U, SWITCH Super Stack 4228G 24P, patch panel



Elaborado por: Alpusig Estefany, Granda Ricardo

Las conexiones dentro del rack de 6U son: un patch panel que no se encuentra en uso y un switch super stack 3COM 4228G, que brinda acceso de Internet a la Jefatura Financiera.

1.4.2.2.3. Rack de Jefatura de Instrucción

En este departamento se utiliza un switch Cisco Catalyst 2960-24 puertos (8 conectados, 16 desconectados) que brinda servicio de acceso a la red y conectividad a los usuarios a través de enlaces UTP con velocidades de hasta 100 Mbps, como se muestra en la figura 2.5

Figura 0.5 Diseño Rack de 6U, Switch Catalyst 2960 24P, patch panel



Elaborado por: Alpusig Estefany, Granda Ricardo

1.4.2.2.4. Rack de Dormitorio Tercer Año

En el dormitorio de tercer año dispone de un switch Cisco Catalyst 2960-12 puertos de los cuales 7 están conectados y 5 desconectados que brinda acceso a la red.

Adicionalmente se usa un switch D-Link de 18 puertos, con 4 usados, también un switch Cisco Catalyst 2960 de 48 puertos, del cual solo se usan 6 puertos, específicamente para las cámaras de vigilancia.

1.4.3. Capa de Red

Para la gestión del tráfico en la capa 3 se utiliza un router de la marca MIKROTIK 1200 de 10 puertos, de los cuales 8 se encuentran en uso, como se muestra en la tabla 2.2.

Este router se encuentra ubicado en el edificio de Dirección, desde donde se usa como punto central del backbone.

Tabla 0.2 Puertos Activos del Router 1200 Mikrotik

ROUTERBOARD 1200 MIKROTIK				
<u>№</u> Puertos	Nombre	Observación		
1	WAN CNT	Activo		
2	Libre WAN CNT Respaldo	Inactivo		
3	TICS	Activo		
4	Libre	Inactivo		
5	Dirección/ Aulas/ Auditorio	Activo		
6	Servidor Antivirus NOD32	Activo		
7	Bodega Yusca	Activo		
8	Jefatura de instrucción	Activo		
9	Aulas Sala Instructores	Activo		
10	Jefatura financiera	Activo		

Elaborado por: Alpusig Estefany, Granda Ricardo

Según la topología física, desde el router se despliega un cable UTP categoría 6A hacia un switch Cisco Catalyst 2960 de 48 puertos de la capa de borde (36 activos y 12 inactivos). Este enlace, brinda acceso a la red a los equipos del edifico de dirección.

1.4.3.1. Direccionamiento

Debido a la necesidad de tener acceso a internet en otras áreas la Escuela Superior de Policía cuenta con diferentes rangos de direcciones IP en todo el campus, por lo tanto, el proveedor de servicios de internet ha asignado una subred de 2048 direcciones IP públicas con 2046 hosts válidos para las aulas nuevas, antiguas y dirección, mencionado en la tabla 2.3.

Tabla 0.3 Dirección IP de la ESP

	Aulas antiguas	Aulas Nuevas	Dirección
Dirección IP	186.46. 164.XX	200.125. 235.XX	192.168.0. XX
Máscara	255.255.248.0	255.255.248.0	255.255.248.0
Gateway	186.46.164.161	200.125.235.73	192.168.0.1
DNS preferido	200.107.10.100	200.107.10.100	200.107.10.100
DNS preferido	200.107.10.105	200.107.10.105	200.107.10.105

Elaborado por: Alpusig Estefany, Granda Ricardo

1.4.3.2. Análisis del tráfico de la red

Para analizar y monitorear el tráfico que atraviesa el router Mikrotic se usó el software WINBOX, durante un mes. Los resultados obtenidos indican que en la interfaz WAN el ancho de banda alcanza a 17.72 Mb, mientras que a la salida es de 4.07 Mb, como se muestra en la figura 2.6

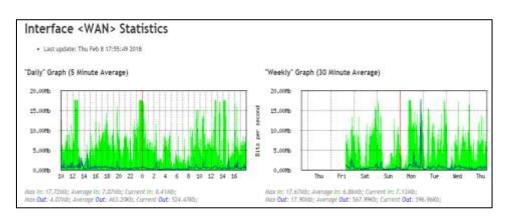


Figura 0.6 Trafico de la WAN utilizando el software WINBOX.

Elaborado por: Alpusig Estefany, Granda Ricardo

En la figura 2.7, se muestra la interfaz de la LAN alcanza picos de 6.19 Mbps, en cambio en la salida los picos son de 18.14Mbps, lo que significa que esta herramienta nos permite observar el tráfico dentro de la WAN y la LAN.

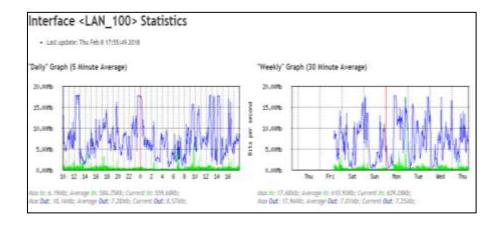


Figura 0.7 Tráfico de la LAN utilizando el software WINBOX.

Elaborado por: Alpusig Estefany, Granda Ricardo

1.4.4. Capa de Presentación y Aplicación

En esta capa se encuentra instalado un servidor virtual remoto con el software ESET NOD 32 versión 7.3.1611 con dirección IP 192.168.100.8, con un sistema operativo

CentOS de 64 bits, que brinda servicios de antivirus a los dispositivos finales desde diciembre del 2017.

1.5. Requerimientos de seguridad de red.

La institución requiere establecer reglas de seguridad particularmente en el área administrativa que es la más vulnerable y en donde se hallan los datos más críticos, como son el historial académico y financiero. También se deben establecer políticas de seguridad para los accesos a la red pública (Internet).

Es necesario establecer dos tipos de redes, una red administrativa y otra para los estudiantes, mediante el uso de un switch que permitan la administración del tráfico de la red, tanto de entrada como de salida.

1.6. TSS

Technical Site Survey (TSS) por sus siglas en inglés es un estudio técnico del sitio en donde nos proporciona una información detallada de la infraestructura de la red que se encuentra actualmente.

Para llevar a cabo un Site Survey de los sistemas inalámbricos, se debe tener un esquema físico del sitio que se va a analizar, identificación de usuarios y ubicación de los Access point para finalmente documentar los resultados.

1.6.1. Mapa de calor

Los mapas de calor son estudios completos de la red inalámbrica, que permite determinar los valores de la señal, el ruido de los puntos de acceso wifi, las interferencias entre otras características.

El software que se empleó para este estudio es Acrylic heatmaps que permite analizar de un modo sencillo la cobertura y la propagación de la señal de los puntos de acceso en donde los valores del RSSI "Received Signal Strength Indication" varían desde 0 dBm (mejor señal), hasta -100 dBm (peor señal).

A continuación, se muestra la tabla 2.4 con los valores y colores del rango de intensidad de la señal.

Tabla 0.4 Orden de intensidad en el software Acrylic heatmaps

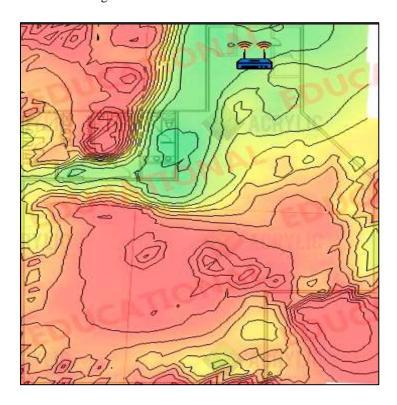
Rango de intensidad	Color		Valores
-30dBM -40dbm			Alta
-40 dBM -70dBm			Media alta
-70dBM -80dBm			Media
-80dBM -90dBm			Media baja
-90dBM -100 dBm			Baja

Elaborado por: Alpusig Estefany, Granda Ricardo

En la Escuela Superior de Policía se encuentran dos access point activos que están localizados en el Departamento de Dirección, el primero en primera planta llamado casino y segundo piso (dirección), mostrado en la tabla 2.2.

En la figura 2.8 se muestra el RSSI del AP que se encuentra ubicado en el casino, en donde se observa que no abarca toda el área de cobertura en el primer piso, para lo cual no es óptima su ubicación.

Figura 0.8 Estudio del Sitio en el casino



Elaborado por: Alpusig Estefany, Granda Ricardo

La figura 2.9 muestra un plano de la infraestructura de la red, la intensidad de la señal y la cobertura, en donde se puede observar que el AP no abarca todo el departamento, esto

también se debe al tipo de material que tienen las paredes produciendo pérdidas de la señal por obstrucción de obstáculos.

Figura 0.9 Estudio del Sitio de la dirección

Elaborado por: Alpusig Estefany, Granda Ricardo

CAPÍTULO 3

DISEÑO DE LA RED

El diseño que se planteará a continuación permitirá a la red del campus de la institución llegar a tener una red resistente a fallos, flexible, escalable y segura con el fin de obtener resultados significativos para esto se va a diseñar LAN y WLAN.

3.1. Metodología de diseño PPDIOO

La metodología PPDIOO permite formalizar el ciclo de vida de una red en seis fases: Preparación, Planificación, Diseño, Implementación, Operación y Optimización. En este proyecto, se emplean las tres primeras fases que son:

3.1.1. Preparación

Esta fase permitió definir las características técnicas de la red en la Escuela Superior de Policía, a través de la documentación de la red.

Es importante hacer el análisis del rendimiento de la red ya que se necesita saber si el modelo lógico que se va a proponer va a ser compatible o tendrá suficiente funcionalidad en los enlaces cableados e inalámbricos actuales. Esta fase se encuentra descrita en el capítulo 2, que es el estado actual de la red en el que se encuentra la Escuela de la Policía.

Como parte de esta etapa también se proponen los posibles equipos activos a utilizar para el diseño y posterior implementación de la red LAN.

3.1.2. Planeación

En esta fase se definen los requerimientos de los servicios de red, los cuales se obtuvieron como producto del análisis de la situación actual y de varias técnicas empleadas en la recolección de datos y de la forma como está distribuido estratégicamente el ancho de banda en cada departamento de la Escuela Superior de Policía. El desarrollo de esta fase se describe en la línea base. Se usa un modelo jerárquico de red que facilita la identificación de los puntos de interacción de la red, el mismo que cumplirá con los requerimientos básicos de red como son seguridad, calidad de servicio, escalabilidad y disponibilidad.

3.1.3. **Diseño**

En esta fase se propone el diseño de la red de campus LAN y WLAN en la Escuela Superior de Policía. El diseño se desarrollará en base al análisis realizado y los requerimientos obtenidos del capítulo 2, el cual permitirá a los usuarios tener una mejor experiencia de la red debido a que se realizará una red segura, confiable y rápida.

3.2. Modelo de arquitectura empresarial de cisco

Este modelo desarrollado por Cisco facilita el diseño de redes corporativas, aportando beneficios tales como la escalabilidad, flexibilidad y facilidad en la implementación. Los módulos más funcionales se muestran en la figura 3.1.

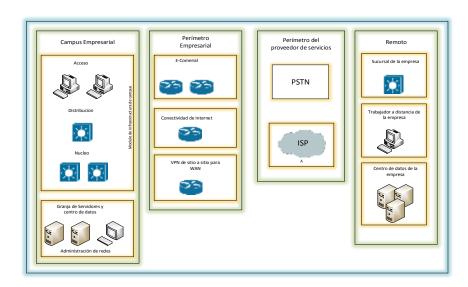


Figura 0.1 Modelo de arquitectura Empresarial de Cisco.

Fuente: (Walton, 2018)

3.3. Diseño de la Red de campus

La jerarquía utilizada por el modelo empresarial de Cisco permite definir funciones dentro de cada capa con la finalidad de que se pueda aplicar una configuración de una manera más apropiada. Este modelo puede proporcionar un diseño e implementación más sencillo, además de escalabilidad en la red como tener una red más confiable y a un mejor costo, si tomamos en cuenta los beneficios que se pueden obtener con este tipo de modelo que utiliza las capas acceso, distribución y núcleo. A continuación, se muestra la topología que se desea emplear en la Escuela de Policía, señalando cada una de las capas en la figura 3.3.

CNT NUCLEO/ DISTRIBUCION **ACCESO**

Figura 0.2 Esquema lógico utilizando el modelo de tres capas para la Escuela Superior de Policía.

Elaborado por: Alpusig Estefany, Granda Ricardo

3.3.1. Modelo de núcleo colapsado

3.3.1.1. Capa de núcleo colapsado

Un modelo de núcleo colapsado se utiliza para redes empresariales, este tipo de modelo en la que la capa núcleo y distribución se combinan en una misma capa y las funciones de ambas capas se implementan en un mismo dispositivo de red. Con esto se puede reducir el nivel de costos para la red LAN del campus de la institución y sin perder las ventajas que puede ofrecer el modelo de tres capas planteadas anteriormente.

Se utilizará el switch Cisco 3850, el mismo que cumple con las funciones de un switch de núcleo colapsado que permita realizar entre otros, filtrado de paquetes, seguridad basado en políticas, enrutamiento entre VLAN's, redundancia entre el dispositivo de la capa núcleo colapsado, por lo que este dispositivo estará concentrado en el centro de datos de la institución.

El modelo de núcleo colapsado permitirá utilizar un único dispositivo como núcleo y distribución, mientras que los demás dispositivos funcionan como dispositivos de acceso.

3.3.1.2. Capa de acceso

La capa de acceso es el primer punto de entrada a la red que proporciona conectividad alámbrica e inalámbrica garantizando la seguridad y flexibilidad. En esta capa se encuentran los dispositivos finales que están controlados por los usuarios.

Para el diseño de la institución se utiliza un switch Catalyst 2960 para los diferentes departamentos existentes en el campus y estos se enlazarán a otro dispositivo de las mismas características que estará ubicado en el centro de datos, para lo cual este equipo deberá tener al menos dos puertos de 1 Gbps para la conexión hacia la capa de núcleo colapsado que serán configurados como puertos troncales.

3.4. Diseño Lógico de la red LAN

3.4.1. Direccionamiento

Una dirección IP se utiliza para identificar un dispositivo en una red. El direccionamiento se compone de 32 bits binarios, tal dirección puede dividirse tanto en

una porción de red como en una porción de host mediante la máscara de subred. Los 32 bits binarios se dividen en cuatro octetos, es decir que cada octeto estará compuesto por ocho bits por lo que cada octeto se convierte a decimal y se separa con un punto. (Cisco, 2016)

Se comenzará realizando el direccionamiento IP, el cual va a estar basado en clase B debido a que esta clase se recomienda para empresas medianas por el número de usuarios con el que se va a estar realizando el diseño.

El siguiente punto es el diseño de las VLAN´s, mismo que se muestra en la tabla 3.1 y que detalla las direcciones IP para cada uno de los departamentos. Se usarán subredes en caso de que cada departamento lo requiera, y de cada rango de direcciones IP se dejarán direcciones disponibles en caso de que la red tenga un crecimiento en el futuro.

3.4.2. Diseño de VLAN

Las redes de Área Local Virtuales permiten filtrar broadcast, definiendo subgrupos lógicos o segmentos dentro de una LAN con lo cual reduce el tráfico y la congestión en la red, por lo que permite tener un mayor control de la red y realizar una distribución de los usuarios para cada uno de los departamentos que se requiera, proporcionando así una mayor seguridad, control de tráfico y flexibilidad. (Tajamar, 2018)

Para el diseño de las VLAN's en la Escuela Superior de Policía se tomará en cuenta la definición dada anteriormente, y el direccionamiento se ha escogido una red de clase B (/16) pero con una máscara variable 255.255.248.0 debido a que esta máscara de subred cubre con el rango de direcciones requeridas para la Escuela de Policía como se indica en la tabla 3.1.

Tabla 0.1 Distribución de Vlan's

VLAN	Características	Host	Dirección	Gateway
2-5	Inalámbricas	600	172.20.0.0	255.255.252.0
6	Administrativo	80	172.20.4.0	255.255.255.0
7	Cadetes	90	172.20.5.0	255.255.255.0
8	Instructores	50	172.20.6.0	255.255.255.0
9	Servidores	4	172.20.7.0	255.255.255.240
99	Gestión	16	172.20.7.16	255.255.255.240

Elaborado por: Alpusig Estefany, Granda Ricardo

Una vez definidas las VLAN's para cada uno de los departamentos con su respectiva dirección IP, se procede a realizar la configuración en los dispositivos mencionados en

la tabla 3.4 y en la topología lógica en la figura 3.2. En el anexo 4 se muestra la VLAN's de gestión y de acceso para cada departamento.

3.4.3. Plan de Implementación de la red LAN

3.4.3.1. Configuración del switch de Core

A continuación, se va a realizar la configuración del switch 3850 (capa 3), el cual representa al switch de núcleo colapsado como se muestra a continuación en los siguientes puntos.

3.4.3.1.1. Configuración básica

Se realizó la configuración de un mensaje al establecer una sesión remota, el nombre del dispositivo, encriptar contraseñas, proteger los puertos de consola y el auxiliar. (anexo 5)

3.4.3.1.2. Configuración para la administración remota (SSH)

Se realiza la configuración para la administración remota de los equipos de la Escuela Superior de Policía mediante SSH, en la cual se va a utilizar el nombre de usuario, en este caso el administrador que va a tener el privilegio 15 y con su respectiva contraseña (anexo 6)

3.4.3.1.3. Configuración VTP

El protocolo VTP permitirá la administración de las VLAN's desde el switch de Core mismo que será configurado como servidor permitiendo que si en el servidor se modifica la configuración de las VLAN's, el switch de acceso configurado como cliente tomará los cambios realizados en el servidor, la configuración se muestra en el anexo 7

3.4.3.1.4. Nombre de las VLAN's

Como se muestra en la tabla 3.1, se realizará la configuración de cada VLAN con el respectivo nombre de cada departamento. (anexo 8)

3.4.3.1.5. Configurar las interfaces para cada VLAN

En cada interfaz de las Vlan's creadas en el punto anterior se va a colocar una dirección IP, la cual va a ser la primera dirección válida para las subredes de cada uno de los departamentos. (anexo 9)

3.4.3.1.6. Configuración del servidor DHCP

En la configuración dinámica DHCP para cada departamento, se ha colocado un tiempo de arrendamiento de un día para cada dirección IP debido a que pueden existir muchos equipos funcionando por lo es recomendable tiempos cortos de alquiler, ya que existe un límite de direcciones IP para cada VLAN, además se debe excluir las direcciones de gateway y las direcciones IP para usuarios específicos en cada departamento. (anexo 10)

3.4.3.1.7. Protocolo de enrutamiento

El enrutamiento de paquetes no será necesario debido a que el switch 3850 de capa 3 se encuentran conectadas las interfaces directamente de cada VLAN, por lo que el switch 3850 que funciona como núcleo colapsado conocerá las rutas de destino y origen por las que viajan los paquetes dentro de la LAN. Lo que se requiere es una ruta estática o por defecto para enrutar todo el tráfico desde el switch de núcleo colapsado hacia el router de frontera. (anexo 11)

3.4.3.1.8. Seguridad

Para la implementación de seguridad se configuran varias listas de acceso las cuales permitirán controlar el flujo del tráfico en un router. Las ACL's son una estrategia efectiva para determinar los permisos de acceso de los paquetes de una red o de un host en particular. La lista de acceso se debe configurar en cada SVI configurado en el punto 3.4.3.1.5.

En el apartado de anexos (12 y 13), para efectos de control de tráfico se describen las listas de acceso (anexo 14), clases y políticas necesarias para evitar una posible sobrecarga en la red de la Escuela de Policía. Estas configuraciones se deben realizar en el router frontera.

3.4.3.1.9. Redundancia

3.4.3.1.9.1. Capa de núcleo colapsado y acceso

Según las recomendaciones de modelo existe un elevado número de usuarios, es necesario diseñar redes redundantes, con la finalidad que garantice una buena disponibilidad, es por esta razón que se conectará un switch de distribución ubicado en el centro de datos con el switch de acceso como se muestra en la figura 3.3.

Capa Núcleo Colapsado

Capa de Acceso

Figura 0.3 Redundancia en la capa de núcleo colapsado y acceso

Elaborado por: Alpusig Estefany, Granda Ricardo

Se propone además utilizar la característica etherchannel debido a que es una tecnología de cisco que permite la agrupación lógica de varios enlaces físicos ethernet, y así poder tener múltiples enlaces como uno solo para lograr tener balanceo de carga, es decir que si un enlace falla el otro enlace sigue funcionando, además suma las velocidades de los puertos teniendo así un enlace troncal de alta velocidad. (anexo 15)

3.4.3.1.10. Configuración de las interfaces del switch

Determina los puertos de acceso a las vlan's que se requiera en cada departamento. Además, se utiliza una descripción para cada rango de interfaces, para identificar al departamento que están conectados los puertos.

3.4.3.2. Configuración de switch de acceso

3.4.3.2.1. Configuración VTP

Se debe configurar el modo cliente en cada switch que se encuentren en los departamentos. (anexo 16)

3.4.3.2.2. Configuración de las interfaces

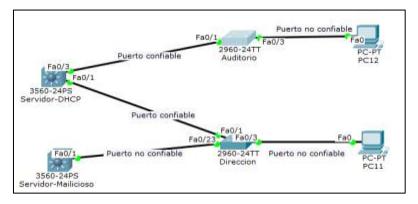
Se realiza la configuración para el acceso a la VLAN's correspondientes en cada switch. Se configura desde la interfaz 3 debido a que la interfaz 1 y 2 están ocupadas para el protocolo de redundancia LACP como se muestra en el anexo 17. En el anexo 4, se observa la IP de la VLAN de gestión y que VLAN's tendrán acceso para uno de los switch de los departamentos, para la seguridad de los puertos del switch se utiliza el comando port-security para evitar el acceso a usuarios no deseados o intrusos. La configuración se muestra en el anexo 18.

Además, para tener una mayor seguridad en los switches se ha incluido DHCP SNOOPING para prevenir que un servidor DHCP que no corresponda a la configurada en el switch de core puede ser conectado en la red del campus de la policía, por lo que se definió los puertos que van a ser confiables y no confiables, utilizando "trust" y "untrust" respectivamente, como en los puertos trunk y acceso del switch de capa 2.

A continuación, se detalla la configuración para prevenir ataques de DHCP.

- Habilitar en modo global el comando IP DHCP SNOOPING en cada switch 2960.
- Ingresar a las interfaces que se encuentran en modo trunk o troncalizadas (interface range Fa0/1-2) y colocar el comando ip dhcp snooping trust que van a ser las únicas interfaces confiables para recibir solicitudes y acuses de recibo del servidor DHCP. Hay que considerar que el switch tiene vlan's por lo que se debe agregar al comando anterior las VLAN's a las que se les va a asociar como se muestra en la figura 3.4.
- Las interfaces restantes no se deben colocar ningún comando debido a que al momento de ingresar el comando IP DHCP SNOOPING todos los puertos se vuelven no confiables. Así, se asegura que ningún puerto del switch puede dar lugar a un ataque de DHCP malicioso.

Figura 0.4 Ejemplo de la configuración dhcp snooping



3.4.3.2.3. Calidad de Servicio

Se debe priorizar cierto tráfico que puede generar la capa de acceso para que no ocasione algún cuello de botella o latencia, y así mantener una mejor gestión del ancho de banda de la red.

Por lo que, se va a configurar QoS estándar en cada una de las interfaces fastethernet del switch, una vez realizada la configuración, el tráfico de la red se va a clasificar con sus valores por defecto, es decir con el valor de CoS igual a 0 y un estado de confianza.

El valor de CoS se puede basar en la tabla 3.3, la cual muestra los valores para diferentes prioridades según la clase de servicio que se requiera. Por ejemplo, por defecto, la PC realiza él envió de datos sin etiquetar y el teléfono IP realiza él envió con la etiqueta dot1q asociado a su VLAN de voz. Si se coloca un valor de cos en 3 en el puerto, el CoS de los datos enviados por la PC tendrán el valor de 3 pero no cambia el valor del CoS del teléfono IP, lo que se recomienda es usar un valor de CoS 5 para voz, por lo que en este caso se colocaría un valor de 5 al CoS para voz y aplicar el comando priority extend cos 2 para cambiar el valor del cos de la PC en 3.

Tabla 0.2 Valores para las prioridades de paquetes

Clase de servicio (CoS)	Características	DSCP		Cola
0	Rutina (IP 0)	Poe defecto	0-7	2
1	Prioridad y mejor esfuerzo (IP 1)	CS1 AF11 AF12 AF13	8-15	1
2	Inmediato y excelente esfuerzo (IP 2)	CS2 AF21 AF22 AF23	16-23	3
3	Flash y aplicación critica LVS (IP 3)	CS3 AF31 AF32 AF33	24-31	4
4	Flash-override y video (IP 4)	CS4 AF41 AF42 AF43	32-39	5
5	Crítico y voz IP (IP 5)	CS5 EF	40-47	6
6	Internet (IP 6)	CS6	48-55	7
7	Red (IP 7)	CS7	56-63	8

Los resultados se muestran en la figura 4.16 del capítulo de simulación y en el anexo 19

se muestra el resultado del ejemplo planteado en caso de existir VoIP en la Escuela de

Policía.

3.4.4. Alimentación redundante

No es necesario incluir un dispositivo redundante como el RPS debido a que el switch

3850 tiene disponibles fuentes de alimentación redundantes duales, en caso de que la

fuente por defecto tenga alguna falla, la segunda fuente entrara en funcionamiento, por

lo que es recomendable instalar ambas fuentes de alimentación para evitar puntos de

fallo en la red y sobre todo en el switch de core.

Para mantener a los servidores y sala de datos en ejecución se recomienda obtener un

respaldo de alimentación eléctrica para ello se debe utilizar una fuente de alimentación

redundante UPS (fuente de alimentación ininterrumpida) que mantiene encendidos los

equipos aproximadamente 15 minutos, tiempo necesario para asegurar la información

ante los posibles fallos que puedan surgir. Entre los equipos mencionados en el anexo

26 se tomó en cuenta el equipo Cyber Power CP900EPFCLCD ya sea por

características apropiadas para cumplir esta función y por el costo.

3.5. Diseño físico de la red LAN

Para realizar el diseño físico de la red LAN de la Escuela de Policía se tuvo que realizar

un análisis de los posibles equipos que se puedan utilizar para llevar acabo el diseño.

Dicho análisis se describe en el punto 3.5.1 y que se basó en las tablas de comparación y

tablas de decisión.

3.5.1. Análisis de los equipos para la red LAN

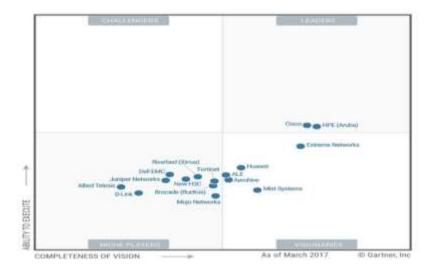
Para la decisión de las marcas de los dispositivos que se van a utilizar en este diseño usó

el cuadrante de Gartner, mismo que permite observar a los mejores proveedores en la

infraestructura de la red, que se muestra en la Figura 3.5.

Figura 0.5 Cuadrante de Gartner para infraestructuras de redes LAN cableadas e inalámbricas

24



Fuente: (Prashanth, 2017)

Para el análisis de los equipos se va a realizar una tabla de decisión para los dispositivos que van a ser utilizados en el diseño de la red como son switch capa 3 y switch capa 2, access point cada uno de los dispositivos van a ser comparadas por diferentes modelos o marcas como se muestran en los anexos 27 y 28.

Switch de Core

Para los switch de capa 3 que se van a utilizar para la capa de distribución de la red se lo realiza mediante una tabla comparativa, que se muestra en el anexo 27.

Al comparar los tres dispositivos se pueden obtener las siguientes características más importantes:

- Todos los dispositivos trabajan a 10/100/1000 -Tx, con fuente de alimentación de CA 120/230 V (50/60 Hz).
- El protocolo de más preeminencia es el STP (Spannig Tree Protocol), que nos proporciona redundancia sin bucles.
- La configuración de VLANS, control de acceso (ACLs), dhcp, calidad de servicio son esenciales para el diseño de este proyecto debido a que nos permite tener un mayor control sobre la red.

A continuación, en la tabla 3.3 se realiza una comparación de los equipos dando una ponderación numérica de: $1 \rightarrow \text{malo}$, $2 \rightarrow \text{regular}$, $3 \rightarrow \text{bueno}$.

Tabla 0.3 Tabla comparativa de los equipos de la capa distribución

Parámetros	Mikrotik Crs 125- 24g-1s-rm	Cisco Catalyst 3850	Aruba- 2930f
Estándar 802.3	3	3	3
Tamaño de la RAM	1	3	2
QoS, STP	3	3	3
Protocolos de gestión remota	3	3	3
Rendimiento	2	2	3
Consumo de energía	3	2	1
Soporte PoE	3	3	3
Rendimiento	2	3	2
Soporta VLAN	3	3	3
Soporte STP / TFTP	2	3	3
Soporte Telnet / SSH	1	3	3
SNMP	1	3	3
IGMP	3	3	3
Soporte Stacking	1	3	3
Ethernet Channel	1	3	3
Calidad de servicio	1	3	3
Soporte ACL	1	3	3
Enrutamiento estático y			
dinámico	1	3	3
Precio	3	1	1
Total	38	53	50

De acuerdo con las necesidades que la Institución presenta los factores más importantes son el precio, rendimiento y el consumo de energía siendo este último más relevante debido a que este dispositivo se va a encontrar conectado las 24 horas al día por lo que el equipo Cisco Catalyst 3850 sería el elegido para este proyecto.

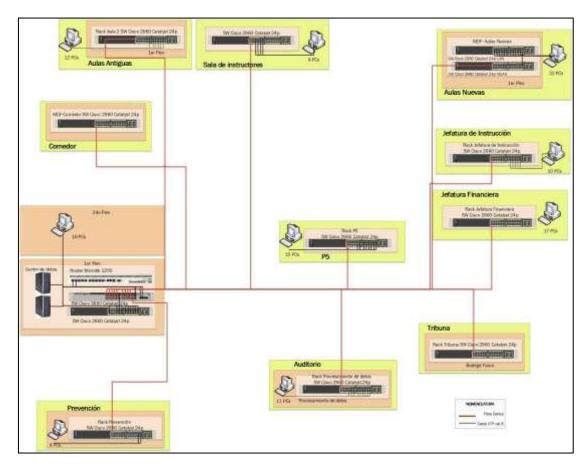
Switch de acceso.

Para los switch capa 2 que se van a utilizar para el acceso de la red son los equipos que se encuentran vigentes en la Escuela Superior de Policía, sin embargo, es necesario adicionar otros debido a que, en ciertos departamentos, existen switch que no se encuentran en capacidad de realizar las prestaciones para este proyecto. En el anexo 28 se muestra las características del equipo para la capa de acceso.

3.5.2. Esquema físico de la red

A continuación, se muestra en la figura 3.6, la distribución de los equipos a utilizar y sus conexiones en las diferentes áreas.

Figura 0.6 Esquema físico de la Escuela de Policía



El centro de datos de la Escuela de Policía se encuentra un router mikrotik RB1200 el cual se lo podría utilizar para la interconexión de la WAN, este router se va a conectar a un switch catalyst 3850 que va a funcionar como switch de núcleo colapsado, se utilizara para el acceso los switch 2960 los cuales servirán para conectar los diferentes departamentos.

Por otra parte, para la red inalámbrica se utilizarán los access point cisco 1602i, ubiquiti unifi y rukus, AP's que soportan hasta 100 dispositivos inalámbricos. A continuación, se muestra la tabla 3.4 donde se mencionan los equipos a utilizar el diseño de la red LAN.

Tabla 0.4 Equipos a utilizar para el diseño de la red LAN en la Escuela Superior de Policía.

Equipos	Cantidad
Router Mikrotik RB2100	1
Switch Catalyst 3850	1
Switch 2960	12
Access Point Cisco	17
Ruckus Zoneflex 7762-AC	2
Ubiquiti Unifi-AC-PRO	21
Cyber Power (UPS)	2

En la tabla se muestran los equipos necesarios para realizar el diseño de la red LAN, los equipos que se mencionan han sido comparados en el punto 3.5.1, el switch 3850 y un switch 2960 se colocarán en el centro de datos mientras que los demás switch 2960 serán colocados en cada uno de los departamentos existentes en la escuela de la policía, y los access point con los que cuenta y se desea adquirir en la Escuela de Policía que en total son 40 APs.

3.6. Diseño lógico de la red WLAN

Para el diseño de la WLAN en la Escuela Superior de Policía se realizó un estudio del sitio en donde se pudo comprobar la ausencia de cobertura de la red inalámbrica para el personal administrativo, instructores, cadetes e invitados. Es por lo que se desea implementar AP en lugares en específicos que permita tener mayor accesibilidad al internet y dar una buena experiencia al usuario por lo cual se deben considerar los siguientes parámetros:

3.6.1. Áreas de cobertura

De acuerdo con los requerimientos que la institución necesita se pretende dar cobertura únicamente a las zonas de mayor interés, teniendo en cuenta la infraestructura y la cantidad de paredes que deberá atravesar la señal de radiofrecuencia, para lo cual se utilizarán los 17 access point de la marca Cisco Aironet 16002i, 2 de la marca Ruckus que se muestra en la tabla 2.2 del capítulo 2, que ya posee la institución y además incrementar 21 APs de la marca Ubiquiti.

Teniendo en cuenta que los APs cisco que dispone la Escuela Superior de Policía ya no se encuentran vigentes, pero si se puede utilizar para este diseño de forma autónoma estarán localizados en las zonas de menor afluencia; mientras que los nuevos equipos serán colocados en lugares de mayor concurrencia debido a que estos van a ser controlados mediante el software UniFi controller, con licencia gratis hasta 100 APs instalados y configurados.

Las áreas que van a ser cubiertas son: Dirección, Jefatura Financiera, Jefatura de Instrucción, aulas nuevas, aulas antiguas, sala de instructores, comedor, tribuna y el auditorio.

3.6.2. Densidad de usuarios

El número de usuarios de la red inalámbrica depende de la concentración de los usuarios potenciales en cada piso de las aulas, es decir para cada piso del edificio existirán usuarios en su mayoría normales y posiblemente pocos usuarios invitados; sin embargo, el diseño debe tomar el caso más crítico, cuando todos los usuarios normales e invitados se encuentran conectados.

Los usuarios que requieren del servicio de internet se encontrarán en cada departamento con un mínimo de 3 dispositivos cada uno, por lo que en la tabla 3.5 se detallan la cantidad de dispositivos que serán conectados a través de la WLAN.

Tabla 0.5 Cantidad de dispositivos conectados en WLAN

	Usuarios	Dispositivos
Dirección	25	75
Jefatura financiera	15	45
Jefatura de instrucción	8	24
Aulas nuevas	90	270
Aulas antiguas	90	270
Sala de instructores	8	24
Tribuna	100	300
TOTAL	611	1008

Elaborado por: Alpusig Estefany, Granda Ricardo

3.6.3. Segmentación y direccionamiento Ipv4 de la WLAN

Para organizar la parte lógica de la red inalámbrica se crean VLANs de acuerdo con la distribución de los usuarios que existen en la escuela siendo estos: docentes, administrativos, instructores y cadetes.

En el direccionamiento ipv4 se crean 4 VLANs de acuerdo con la cantidad de usuarios que se especifica en la tabla 3.5 por lo que se opta en elegir una red de clase B con máscara 255.255.255.0 de longitud fija, mostrada en la tabla 3.6

Tabla 0.6 Direccionamiento IPv4

vlan	descripción	Dirección IP	máscara
Vlan2	ESPN_ADMIN	172.20.0.0	/24
Vlan3	ESPN_CADETES	172.20.1.0	/24
Vlan4	ESPN_INSTRUCTORES	172.20.2.0	/24
Vlan5	ESPN INVITADOS	172.20.3.0	/24

Elaborado por: Alpusig Estefany, Granda Ricardo

El SSID permite la autenticación de los usuarios en una red inalámbrica con un único nombre que identifica a un grupo en específico, para lo cual se ha diseñado 3 grupos que será utilizado para la creación de grupos en el software UniFi Controller de Ubiquiti que permite asignar por cada grupo un máximo de 4 SSID. A continuación, se detalla en la tabla 3.7.

Tabla 0.7 Grupos de usuarios con SSID

GRUPOS	SSID
	EPN_admin
Administrativo	EPN_instructores
	EPN_invitados
Cadatas	EPN_instructores
Cadetes	EPN_cadetes
	EPN_instructores
Invitados	EPN_cadetes
	EPN_invitados

Elaborado por: Alpusig Estefany, Granda Ricardo

En cada AP se le configura una dirección IP estática de 172.20.10.0/22 y se le asigna a un grupo con su correspondiente SSID, su respectivo canal, mostrado en el anexo 29.

Con el direccionamiento obtenido anteriormente se procede a realizar el diagrama lógico de la red inalámbrica, para lo cual se utilizó el switch que se encuentra en cada departamento y este estará conectado a cada AP que le corresponda, mostrándose en la figura 3.7 y en el anexo 30 se muestra el diagrama más detallado de acuerdo con el canal, dirección de cada AP y grupo SSID al que pertenecen.

INET VIAN 2:ESPN_admir Seguridad:WPAV2 IP: 172:20.0:0/24 Seguridad: WFAV IP: 172.20.10.12 SSID: EPN_cadete SSID: EPN_admin VIAN 4: VLAN 4: Seguridad:WPAV: IP: 172.20.2.0/24 DS VLAN 5 ESPN_imitados Seguridad:WPAV2 P: 172.20.3.0/24 P: 172.20.3.0/24 SEI: EPN_invitado Seguridad WPAV2 IP: 172.20.1.0/24 SSID: EPN cadetes VIAN 4: VIAN 4: ESFN_instructores Seguridad WFAV2 IP: 172.30.2.0/24 SSID: EPN_instructores

Figura 0.7 Diagrama lógico de la red inalámbrica

Elaborado por: Alpusig Estefany, Granda Ricardo

3.7. Diseño físico de la red WLAN

3.7.1. Ubicación de las Access Point

Uno de los problemas existentes en cualquier diseño de red inalámbrica es la infraestructura, debido a que existen diferentes tipos de obstáculos como paredes de concreto, ventanas, entre otros, que ocasionan que la señal sea atenuada, por lo tanto, el alcance del radio de cobertura puede encontrarse congestionada, por lo que se toma en consideración estas contrariedades para la correcta ubicación de los APs. En la tabla 3.8 se puede observar las pérdidas que son generadas por los materiales de la construcción que en este caso son de estructuras metálicas y bloques.

Tabla 0.8 Atenuaciones de acuerdo con los materiales de construcción

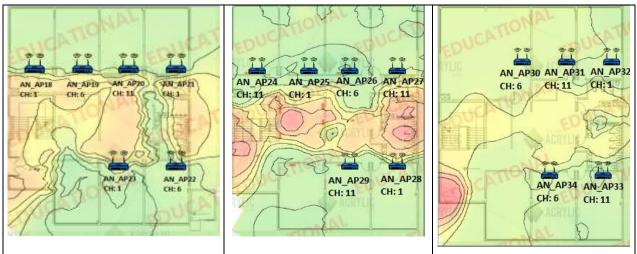
Tipo de material	Pérdida en dB
Bloques de concreto	13
Pared de concreto	15
Vidrio templado	4
Pared gruesa	20
Teja	23
Metal	26
Piso de concreto	10

Fuente: (Lara & Muñoz, 2012)

Mediante el software Acrylic Heatmaps demo con licencia de estudiante se puede obtener la cobertura en las áreas en donde se dese dar servicio de la red inalámbrica para lo cual en el edificio de aulas nuevas será implementado 17 APs de la marca Ubiquiti, que serán distribuidos en cada aula. En la figura 3.8 se muestra la cobertura de las aulas nuevas.

Figura 0.8 Área de cobertura en las aulas nuevas

Primer piso	Segundo Piso	Tercer Piso
-------------	--------------	-------------



Elaborado por: Alpusig Estefany, Granda Ricardo

En los anexos 31 al 36, se muestran los mapas de cobertura de los sitios que son requeridas la red inalámbrica en el campus.

En el anexo 37, muestra el diagrama físico de la red WLAN incluyendo los puertos y lugar donde van a hacer conectados.

3.7.2. Configuración del AP cisco 1602i

Se configura el switch 2960 por medio de la consola con los comandos que se muestra en la figura 3.9. Como referencia se configuró el AP que se encuentra ubicado en las aulas nuevas con los datos que se proporcionan en el anexo 10, por lo cual el grupo de VLAN que se necesita en esta área para el ingreso a internet son los cadetes, e instructores.

Figura 0.9 Configuración del sw conectado al AP

```
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 9,4
switchport mode trunk
```

Elaborado por: Alpusig Estefany, Granda Ricardo

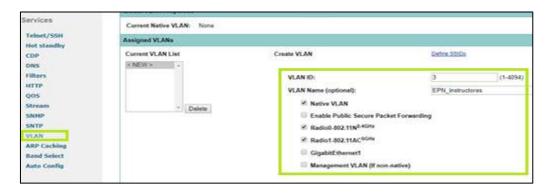
Se configura el punto de acceso por medio de consola, con los comandos que se muestra en la figura 3.10 en el cual permite asignar una IP al Access point para realizar las configuraciones en modo gráfico, utilizando la dirección del anexo 29.

Figura 0.10 Configuración del al AP

```
ap(config)#int bvi1
ap(config-if)#ip address 172.20.10.12 255.255.255.0
ap(config-if)#no shut
ap(config-if)#exit
```

Con la dirección IP que ha sido configurada se procede a ingresar a una página web para realizar la configuración de las VLAN en la pestaña services luego VLAN, como se muestra en la figura 3.11.

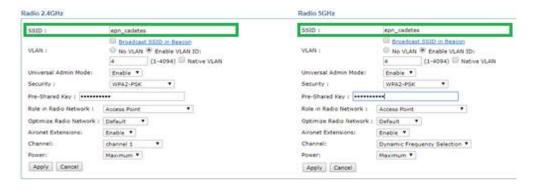
Figura 0.11 Configuración de vlan en el AP



Elaborado por: Alpusig Estefany, Granda Ricardo

La configuración del SSID se lo realiza como se muestra en la figura 3.12, mediante las dos bandas que son la de 2.4 y 5 GHz, en lo cual se le asigna la VLAN correspondiente, contraseña y número de canal.

Figura 0.12 Configuración del SSID en el AP



Elaborado por: Alpusig Estefany, Granda Ricardo

3.7.3. Configuración del access point ubiquiti ac pro

La configuración de los puntos de acceso se lo realiza mediante el software Unifi Controller de ubiquiti versión 3.9.27 para Windows, que se descarga a través de la página oficial y posteriormente se procede a la instalación.

Los parámetros que son requeridos por primera vez son: idioma, país, nombre y contraseña del administrador, es muy importante recordar estos dos últimos datos debido a que serán necesarios para el acceso al controlador.

Una vez accedido con las credenciales se puede ver una visión general del controlador, en donde se puede cargar los mapas y colocar los APs de forma visual, como se muestra en la figura 3.13



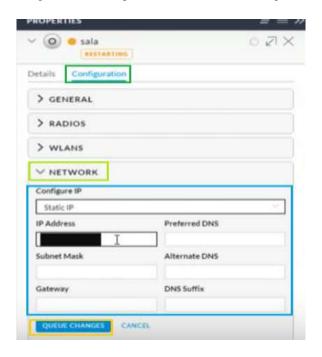
Figura 0.13 Ventana principal del sofware Unifi Controller de Ubiquiti

Fuente: (UniFi Enterprise, 2018)

La configuración IP de los Access point se describe en el anexo 17 y se muestra en la figura 3.14

- Seleccionar un AP en Name/Mac Address
- Configuration
- Network Settings
- Static IP: se coloca la dirección, máscara, gateway, dns

Figura 0.14 Configuración IP de los AP's Ubiquiti



Fuente: (UniFi Enterprise, 2018)

Para la creación de los SSID se debe colocar el nombre, seleccionar el tipo de seguridad la cual se recomienda WPA- personal y la clave tiene que contener alfanuméricos y algún símbolo, además se debe colocar el ID de la VLAN, esto se muestra en la figura 3.15.

Figura 0.15 Creación de SSID



Fuente: (UniFi Enterprise, 2018)

Para la creación de grupos de WLAN se lo realiza mediante la tabla 3.9 que nos permite separar las redes inalámbricas según las funciones que desempeñen con la finalidad de tener una mejor organización en la red. En la figura 3.16 se muestra la configuración del grupo de WLAN.

- Configuration
- Wireless network
- Wireless grupo add

Figura 0.16 Parámetros de configuración de un grupo de WLAN



Fuente: (UniFi Enterprise, 2018)

3.7.4. Análisis de los equipos para la red WLAN

3.7.4.1. Access Point

En el anexo 38 se muestran las especificaciones técnicas de tres tipos de marcas de los cuales Cisco y Aruba se encuentran en el cuadrante de Garner, mientras que el otro es Ubiquiti, aunque no se encuentra en el cuadrante de Garner, pero si a nivel nacional por sus costos y beneficios.

Las características más importantes se detallan a continuación.

- Todos los dispositivos tienen la interfaz 10/100/1000BASE-T y antena omnidireccional, con una velocidad de datos a 2.5 GHz y 5 GHz.
- Los algoritmos de seguridad para las redes inalámbricas que tienen los equipos son WEP, WPA-PSK, WPA2 que nos permite cifrar los datos.
- Los SSID o identificador de servicio de paquetes nos permite diferenciar de múltiples redes wifi en el área en el que está implementando para lo cual esto debe tener al menos de 4 conexiones por radio.

A continuación, en la tabla 3.9 se realiza una comparación de los equipos dando una ponderación numérica de: $1 \rightarrow \text{malo}$, $2 \rightarrow \text{regular}$, $3 \rightarrow \text{bueno}$.

Tabla 0.9 Tabla comparativa de los equipos de Access Point

Parámetros	Cisco Aironet AIR- SAP16021-A- K9	Ubiquiti Unifi AC-PRO	Aruba 220
Estándar AC	3	3	3
Banda Dual	3	3	3
Potencia de transmisión	2	3	2
Cantidad de usuarios	1	3	2
Memoria del sistema	3	1	2
Consumo de energía	3	2	2
SSID	2	3	3
Precio	1	3	2
Total	18	21	19

El consumo de energía y el precio es un gran diferenciador en la Institución por lo que el equipo Ubiquiti unifi-AC-PRO es el escogido para el incremento de los AP que se necesitan para este diseño debido a que estos se encontrarán conectados todo el tiempo.

3.8. Centro de datos y granja de servidores

El centro de datos que se va a diseñar para el campus de la escuela de la policía va a proporcionar recursos de servicios internos para los usuarios, los servidores que se va a implementar son los siguientes:

Servidor Antivirus para así controlar el acceso de virus y software malicioso en los dispositivos del campus de la policía.

Servidor Active Directory y DNS para controlar el acceso de los usuarios y tener la disponibilidad de tener un dominio establecido para el campus de la policía. También para tener un registro de los usuarios que pertenecen a la escuela de la policía.

Servidor de correo el cual los usuarios lo utilicen dentro del campus utilizando un dns establecido para la escuela de la policía y así poder gestionar correo.

Estos servidores nos van a permitir tener un control y registro de lo que sucede en el campus para así poder resolver cualquier problema que pueda existir y tener una buena administración de la red. El servidor AD, DNS y de correo se lo realizo utilizando Windows server 2012. La configuración de los servidores se entregará en un documento aparte.

CAPÍTULO 4

SIMULACIÓN DE LA RED

4.1. Simulación en Packet Tracer

A continuación, se puede observar en la figura 4.1 la topología realizado en el simulador Packet Tracer, en cual se realizó la configuración de los equipos tanto del switch de núcleo colapsado como del switch de acceso.

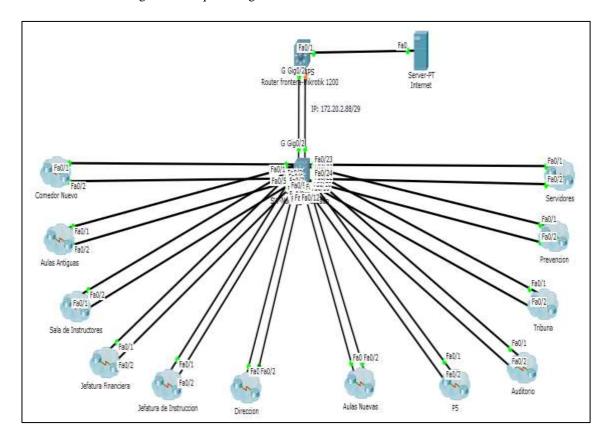


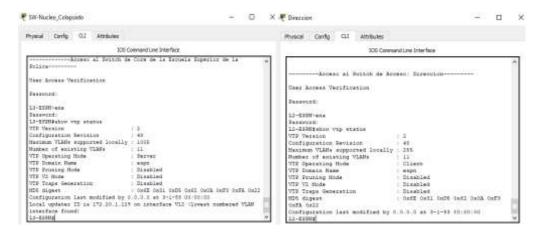
Figura 0.1 Esquema lógico realizado en el software de simulación

Elaborado por: Alpusig Estefany, Granda Ricardo

4.2. Prueba de la configuración básica y VTP en el switch de núcleo colapsado y switch de acceso

En la figura 4.2, se muestra la configuración básica y la configuración VTP, para la administración de la vlan's el switch de núcleo colapsado será configurado como servidor y cada switch de acceso como cliente, para que los cambios solo se los realice en el servidor.

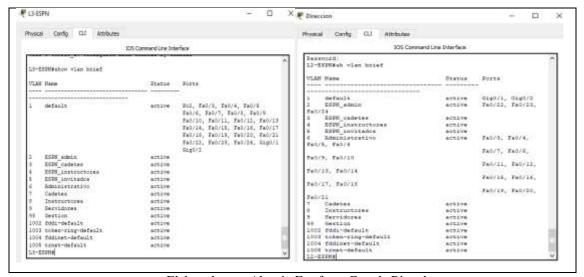
Figura 0.2 Configuración básica y vtp



4.3. Prueba de la configuración VLAN en el switch de núcleo colapsado y switch de acceso

El código de configuración se muestra en el anexo 8.

Figura 0.3 Configuración de las VLAN's



Elaborado por: Alpusig Estefany, Granda Ricardo

En la figura 4.3, se muestra los nombres de cada una de las VLAN's creadas para los departamentos que se encuentran en la institución.

4.4. Prueba de la configuración de las interfaces en el switch de núcleo colapsado

En la figura 4.4, se muestra el estado de las interfaces en el switch de núcleo colapsado como son los port channel, interfaces fastEthernet, interfaces gigaEthernet y las VLAN's.

SW-Nuclea_Colepsedo X SW-Nucleo_Colegnado Physical Config CLI Physical Config CLI Attributes 305 Command Line Interface OCT Maxical Paston TestSthurtet0/15 imakelyned YES unset ig qu. zesmu kilir unwesigned unexwitmed YES unset up massigned Kits unser up YES unset up unassigned PautSchennet0/19 onessigned TER United 10 YES unset up merel good res unsei up FastEthernet0/11 unexplored. TRS unset in Faur Scharmand / 22 VES Union unessimped YES meet up unassigned VES unset up YES unset to unesslymed. YES meet up With more tip unessigned res unset dministratively over down
Ten2 170.20.0.1 ort-channel 13 unsesigned VES maset up TIN tempes) up 112.20.2.09 172 20 1 2 YES manual by unxestgreet YES unset up 172,20,212 YEN BRIGHT 10 FastEthernet0/1 unassigned YES unset up 170.30.9.1 unessigned 112.20.8.1 TES named up FactSthernet0/4 unnestyped YES meet up 150.00.6.1 restitionments/h unassigned TES inset VIS mettial up 172.20.7.1 VER mercial up up FastEthernet0/4 unsestaned YES where up 172.20.7.17 TER second or ap. FactSthernet//7 unnesigned YES meet up

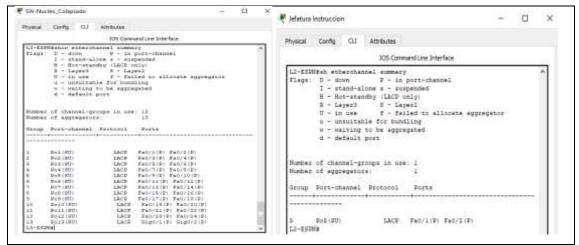
Figura 0.4 Configuración de las interfaces

Elaborado por: Alpusig Estefany, Granda Ricardo

4.5. Prueba de la configuración de la redundancia en el switch de núcleo colapsado y del switch de acceso

En la figura 4.5, se muestra la configuración del protocolo de control de agregación de enlaces (LACP), el cual se utilizó para establecer la redundancia entre el switch de núcleo colapsado y cada uno de los switch de acceso.

Figura 0.5 Configuración de redundancia



4.6. Prueba de la configuración de los puntos de acceso con su dirección IP y su respectivo SSID.

En la figura 4.6, se muestra la configuración que se va a realizar en los routers inalámbricos en cada departamento.

Figura 0.6 Configuración de los puntos de acceso



Elaborado por: Alpusig Estefany, Granda Ricardo

4.7. Prueba de la configuración de las listas de acceso y control de ancho de banda en el switch de núcleo colapsado.

En la figura 4.7, se muestra las listas de acceso, clases y políticas creadas para la red del campus, en las cuales se garantiza un ancho de banda específico para cada vlan y proporciona seguridad mediante las listas de acceso ya que se permiten o se niegan varios protocolos y servicios de la red administrativa. El código de configuración se muestra en el anexo 20 y 21.

Figura 0.7 Configuración de las listas de acceso y QoS.

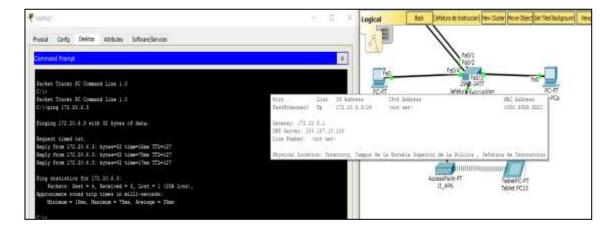


Elaborado por: Alpusig Estefany, Granda Ricardo

4.8. Prueba de comunicación de datos.

En la figura 4.8, se muestra que existe comunicación entre la sala de instructores con la jefatura de instrucción.

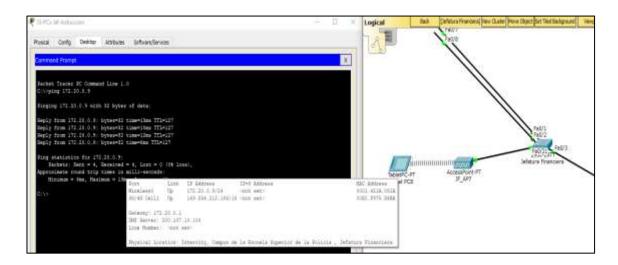
Figura 0.8 Comunicación de datos entre la sala de instructores y jefatura de instrucción



Elaborado por: Alpusig Estefany, Granda Ricardo

En la figura 4.9, se muestra que existe comunicación entre la jefatura de instrucción a un dispositivo inalámbrico de la jefatura financiera

Figura 0.9 Comunicación de datos entre Jefatura de instrucción a un dispositivo inalámbrico de la jefatura financiera



4.9. Prueba de la configuración SSH

En la figura 4.10, se muestra el acceso de manera remota al switch de núcleo colapsado mediante el protocolo SSH.

Advanced Code Delice Winkings Subsequence

| Comment Of Code Delice Winkings Subsequence | Comment Of Code Delice | Code Delic

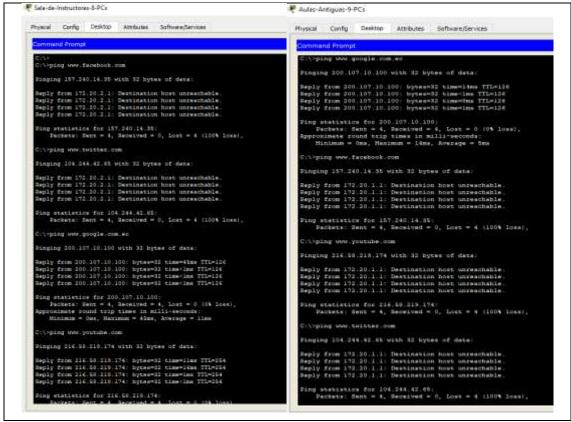
Figura 0.10 Funcionamiento de acceso al switch mediante SSH.

Elaborado por: Alpusig Estefany, Granda Ricardo

4.10. Prueba de la configuración de las listas de acceso

En la figura 4.11, según las listas de acceso el departamento de sala de instructores tiene acceso a Google y youtube, pero no tiene acceso a Facebook o twitter y según las listas de acceso cadetes tiene acceso a Google y youtube, pero no tiene acceso a facebook, twitter y youtube.

Figura 0.11 Prueba de funcionamiento de las listas de acceso



Elaborado por: Alpusig Estefany, Granda Ricardo

4.11. Prueba de la configuración del servidor de la escuela de la policía

En la figura 4.12, se muestra el funcionamiento del servidor dns (espn.edu.ec) y http en el departamento P5.

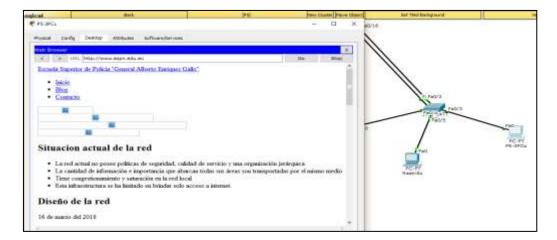


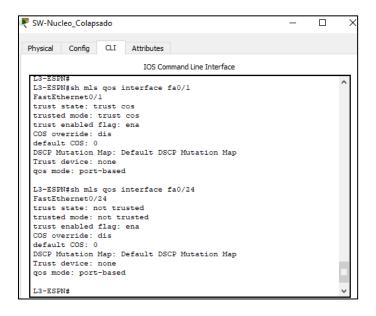
Figura 0.12 Funcionamiento del servidor dns y http

Elaborado por: Alpusig Estefany, Granda Ricardo

4.12. Prueba de la configuración de QoS

En la figura 4.13, se muestra la configuración de auto QoS en la interfaz fastethernet 0/1 y fastethernet 0/24, se demuestra que cada interfaz del switch de core se encuentra habilitado auto QoS con las mismas características.

Figura 0.13 Funcionamiento de Qos en la interfaz fa0/1



Elaborado por: Alpusig Estefany, Granda Ricardo

4.13. Prueba de asociación de la WLAN por interfaz de radio

Para observar la configuración de los BSSID se realiza mediante consola y con el comando que se muestra en la figura 4.14, en lo cual se observa que se encuentran ya levantadas.

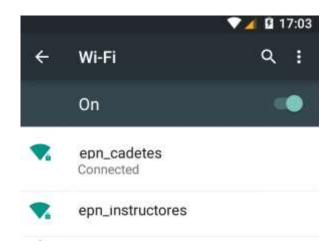
Figura 0.14 Comprobación del BSSID por interfaz de radio

```
AN AP18#show dot11 bssid
                 BSSID
                                           SSID
Interface
                                   Guest
                e00e.da32.da60
Dot11Radio0
                                    Yes
                                         epn_cadetes
                e00e.da32.da61
e00e.da19.79a0
e00e.da19.79a1
Dot11Radio0
                                    Yes
                                          epn_instructores
Dot11Radio1
                                    Yes
                                          epn_cadetes
Dot11Radio1
                                    Yes
                                          epn_instructores
AN_AP18#_
```

Elaborado por: Alpusig Estefany, Granda Ricardo

Mediante un dispositivo inalámbrico ya se puede conectar a la red con su respectivo SSID y contraseña, como se observa en la figura 4.15

Figura 0.15 Conexión de la red wlan con su respectivo SSID



Elaborado por: Alpusig Estefany, Granda Ricardo

CAPÍTULO 5

ANÁLISIS DE COSTOS

5.1. Introducción

En este capítulo se analiza el costo de inversión que tendrá el proyecto, tanto en equipos, implementación y configuración de los equipos para lo cual se va a conocer la viabilidad del proyecto mediante la tasa interna de rentabilidad (TIR), el uso del valor neto (VAN) y el período de la recuperación del capital.

5.2. Costos de equipos

De acuerdo con el análisis desarrollado en el capítulo 3 sobre las diferentes marcas de los equipos que existen en el mercado, se realizó unas tablas de decisión que permitieron el análisis de las características técnicas y económicas de los equipos. En la tabla 5.1 se detallan los equipos necesarios para este proyecto.

Tabla 0.1 Costo de equipos para la ESP

ITEM	DESCRIPCION	CANT	V/UNIDAD (USD)	V/TOTAL (USD)
2	Switch Cisco Catalyst 3850-24p	1	\$1.750,00	\$1.750,00
3	Switch Cisco 2960 Catalyst 24p	12	\$749,00	\$8.988,00
4	Ubiquiti Unifi-AC-PRO	21	\$240,00	\$5.040,00
5	APCBack-UPSBX	2	\$181,00	\$362,00
	TOTAL (no incluye IVA)			

Elaborado por: Alpusig Estefany, Granda Ricardo

5.3. Costo de implementación

El costo referencial del soporte técnico de un ingeniero electrónico con conocimiento en redes se lo estipula mediante la tabla vigente del mercado nacional, que se muestra en la tabla 5.3

Tabla 0.2 Costo de ingeniería de proyecto

ITEM	DESCRIPCION	Personas	CANT (horas)	V/UNIDAD (USD)	V/TOTAL (USD)
1	Diseño y configuración de los equipos LAN y WLAN	1	30	\$30,00	\$900,00
3	Pruebas de conectividad		15	\$30,00	\$450,00
2	Técnicos	2	30	\$10,00	\$600,00
4	Capacitación al personal encargado de monitorear la red		4	\$10,00	\$40,00
	TOTAL				\$1.990,00

5.4. Costo total del proyecto

En la tabla 5.3 se muestra el costo total que tendrá este proyecto sumando tanto el costo de equipos, materiales e implementación, teniendo en cuenta que estos valores son referenciales y pueden variar.

Tabla 0.3 Costo total del proyecto para la ESP

ITEM	DESCRIPCION	V/TOTAL (USD)	
1	Costo total de adquisición de equipos	\$16.140,00	
2	2 Costo total de implementación		
	TOTAL (USD)		

Elaborado por: Alpusig Estefany, Granda Ricardo

5.5. Valor actual neto (VAN)

El valor actual neto (VAN) es un indicador financiero que permite determinar la viabilidad de un proyecto. (Santa Cruz, 2017) Cuando el VAN es mayor a cero la inversión es viable, mientras que si es menor el proyecto generará pérdidas por lo que es recomendable descartarlo.

La ecuación para calcular el VAN se muestra a continuación:

$$VAN = -I_o + \sum_{t=1}^{n} \frac{F_t}{(1+k)^t}$$
 Ec. 0.1

En donde:

 I_o : inversión inicial

 F_t : Flujos de caja en cada periodo de tiempo

n: Número de periodos de tiempo

k: Tasa de descuento

5.5.1. Tasa de descuento

La tasa de interés de descuento se obtuvo mediante las tablas que se encuentra publicados mensualmente en el banco central del Ecuador con el 8.23 % anual en la inversión pública. (Banco Central del Ecuador, 2018)

El flujo de caja es un estado de cuenta sobre los ingresos y egresos de la institución en donde se generan los valores de la inversión por pagos de los servicios, como se muestra en la tabla 5.4

Tabla 0.4 flujo de caja aproximado

ITEM	DESCRIPCION	V/TOTAL (USD)	
1	Ingresos aproximados	\$2.852,00	
2	Egresos aproximados	\$1.200,00	
3	Flujo de caja mensual aproximado	\$1.652,00	
4	Flujo de caja anual aproximado	\$19.824,00	

Elaborado por: Alpusig Estefany, Granda Ricardo

5.5.2. Cálculo del VAN

$$VAN = -18,130 + \frac{19824}{1 + 0.0823}$$

$$VAN = $186.55$$

El cálculo del valor del VAN es mayor que cero, por lo tanto, es factible para realizar este proyecto.

5.6. Tasa interna de retorno (TIR)

La tasa interna de retorno (TIR) permite saber si es factible invertir en el proyecto mediante un porcentaje del beneficio o pérdidas que tendrá al realizar esta inversión. (Sevilla Arias, 2017). La ecuación se muestra a continuación:

$$VAN = -I_o + \sum_{t=0}^{n} \frac{F_n}{(1+r)^t} = 0$$
 Ec. 5.2

En donde:

 I_o : Inversión inicial

 F_n : Flujo neto

n: Periodos considerados

r: Tasa interna de rentabilidad (por ser VAN=0)

A lo que la ecuación al despejarse se obtiene la siguiente fórmula.

$$TIR = \frac{F_n - I_o}{I_o}$$

Reemplazando sus valores de: inversión inicial $I_o = 18,130.00$ en periodo de año cero y un flujo de caja de $F_n = \$19,824,00$, se obtiene el siguiente resultado:

$$TIR = 0.0934$$

$$TIR = 9.34\%$$

Como el cálculo dio positivo del TIR se puede garantizar unas ganancias en la Escuela Superior De Policía.

5.7. Periodo de recuperación del capital (PRC)

Determina el periodo de recuperación de la inversión del proyecto, por lo que mientras más corto sea el plazo puede ser más rentable. (Velayos Morales, 2017). La fórmula se encuentra dado a continuación

$$PRC = \frac{I_0}{F_m}$$
 Ec. 0.2

Donde:

*I*_o: Inversión inicial

 F_m : Flujo de caja mesual

$$PRC = \frac{18,130.00}{1652}$$

$$PRC = 11 meses$$

CONCLUSIONES

El levantamiento de la línea base permitió demostrar de manera técnica los problemas que existen actualmente en la red LAN y WLAN de la Escuela Superior de Policía, justificando así la necesidad de diseñar un modelo de red corporativo que resuelva los problemas de conectividad, movilidad y comunicación dentro de la institución.

El diseño de Red LAN y WLAN propuesto para la Escuela Superior de Policía garantiza una mayor eficiencia en la productividad de los usuarios al contar con una red confiable, capaz de brindar una comunicación eficaz entre cada departamento gracias a un esquema de direccionamiento adecuado con el número de usuarios existente en el campus.

Los resultados de la evaluación de equipos activos de capa 2 y capa 3, demostraron que el fabricante Cisco es la mejor opción, gracias entre otros aspectos a la versatilidad en su configuración, el soporte de una variedad de protocolos de networking tanto propietarios como estandarizados, así como su adecuada integración en el modelo de red corporativo que se utilizó como referencia.

El análisis económico realizado a partir del cálculo del TIR, VAN y PCR, demuestran la factibilidad de ejecutar este proyecto evidenciando que en el corto plazo representarán rentabilidad, ganancia y la respectiva recuperación de la inversión que implica su implementación.

RECOMENDACIONES

Debido a que la Escuela Superior de Policía no cuenta con una conexión de red hacia el edificio nuevo en donde se encuentran los centros de cómputo de los cadetes, se propone utilizar una conexión de fibra que interconecte este sitio con el centro de datos.

Se sugiere realizar un estudio técnico para diseñar el centro de datos de la institución debido a que en esta área se gestiona y almacena toda la información, por lo tanto, se tiene que cumplir con los estándares tanto en las condiciones físicas como ambientales.

Se recomienda utilizar el sistema de energía para mantener la operatividad y el funcionamiento de los equipos sin ningún tipo de problema para así evitar que exista pérdida de información.

Para que exista mayor seguridad en la red inalámbrica es aconsejable que la Institución disponga de un portal cautivo con la finalidad de controlar y regular el acceso a la red por parte de los usuarios permanentes y temporales.

BIBLIOGRAFÍA

- 3850, C. (2016). Cisco Catalyst 3850-48T-S Switch.
- Banco Central del Ecuador. (2018, Mayo 1). *Banco Central del Ecuador*. Retrieved from https://contenido.bce.fin.ec/docs.php?path=/documentos/Estadisticas/SectorMon Fin/TasasInteres/Indice.htm
- Cisco. (2016). Direccionamiento de IP . https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocolrip/13788-3.html.
- Lara, D., & Muñoz, D. (2012). Factores de atenuación. In D. Lara, *Sistemas inalámbricos de comunicación personal* (pp. 129-131). Monterrey: Alfaomega.
- Mikrotik. (2016). RB1200.
- Oppenheimer, P. (2011, Agosto). Top-Down Network Design. (3). Indianapolis: Cisco Systems, Inc. Retrieved from http://www.teraits.com/pitagoras/marcio/gpi/b_POppenheimer_TopDownNetwo rkDesign_3rd_ed.pdf
- Prashanth, S. (2017, Octubre 23). *CIsco blogs*. Retrieved from https://blogs.cisco.com/wireless/cisco-a-leader-gartner-wired-and-wireless-lan
- Santa Cruz, E. (2017, Enero 24). *conexionesan*. Retrieved from https://www.esan.edu.pe/apuntes-empresariales/2017/01/fundamentos-financieros-el-valor-actual-neto-van/
- Sevilla Arias, A. (2017, Mayo 23). *Economipedia*. Retrieved from http://economipedia.com/definiciones/tasa-interna-de-retorno-tir.html
- Tajamar, T. (2018). Diseño LAN. *Cisco CCNA R&S*, https://techclub.formaciontajamar.com/diseno-lan/.
- TecnoSmart. (2016). Cloud Router Switch MikroTik CRS125-24G-1S-RM 24x 10/100/1000Mbps + 1x SFP. http://www.tecnosmart.com.ec/v2/cloud-router-switch-mikrotik-crs125-24g-1s-rm-24x-10-100-1000mbps-1x-sfp.html.
- Ubiquiti. (2016, Octubre 11). *Ubiquiti*. Retrieved from https://unifi-hd.ubnt.com/
- UniFi Enterprise. (2018, Mayo 22). *Ubiquiti Networks*. Retrieved from https://help.ubnt.com/hc/en-us/articles/360003205114-UniFi-Configuring-Access-Policies-802-1X-for-Wired-Clients
- Velayos Morales, V. (2017, Abril 15). *economipedia*. Retrieved from http://economipedia.com/definiciones/payback.html#comments
- Vialfa, C. (2017, Septiembre 13). *CCM Benchmark*. Retrieved from http://es.ccm.net/contents/286-vlan-redes-virtuales
- Walton, A. (2018, enero 30). *Arquitectura de Red Empresarial Cisco*. Retrieved from https://ccnadesdecero.es/arquitectura-red-empresarial-cisco/

ANEXOS

Anexo 1 Tendido de Fibra Óptica en la ESP

	LONGITUD DE FIBRAS INSPECCIONADAS								
#	NOMBRE	TIPO DE FIBRA	ORIGEN	DESTINO	LONGITUD EN METROS				
#	NOWBRE	TIPO DE FIBRA		DESTINO	FIBRA 2H	FIBRA 24H	FIBRA 48H	FIBRA 96H	
1	Nodo- Aulas 3er Año	FIBRA CORE	Nodo Data Center	Aulas 3er Año		216,29			
2	Nodo- Manga ESP	FIBRA CORE	Nodo Data Center	Manga ESP		20			
3	Nodo Telconet- Manga ESP	FIBRA CORE	Nodo Telconet	Manga ESP			281,71		
4	Ruckus Villas	FIBRA CLIENTE	CAJA 2	Ruckus Villas	310,28				
5	Nodo- Area escuela lado oriental	FIBRA CORE	Nodo Telconet	Manga ESP				1208,23	
6	Ruckus Dormitorio Mujeres	FIBRA CLIENTE	CAJA 2	Ruckus Dormitorio Mujeres	148,9				
7	Dormitorio Mujeres	FIBRA CLIENTE	CAJA 4	Dormitorio Mujeres	110,83				
8	Bodega 1	FIBRA CLIENTE	CAJA 7	Bodega 1	116,76				
9	Dispensario Médico	FIBRA CLIENTE	CAJA 4	Dispensario Médico	84,29				
10	Dormitorio Hombres	FIBRA CLIENTE	CAJA 3	Dormitorio Hombres	65,2				
11	Cultura física	FIBRA CLIENTE	CAJA 8	Cultura física	80,91				
12	Tribuna	FIBRA CLIENTE	CAJA 7	Tribuna	45,22				
13	Aulas 2	FIBRA CLIENTE	CAJA 1	Aulas 2	70				
14	Villas	FIBRA CLIENTE	CAJA 4	Villas	106,63				
15	Aula Posterior	FIBRA CLIENTE	CAJA 1	Aula Posterior	70				
16	Auditorio	FIBRA CLIENTE	CAJA 8	Auditorio	38,99				
17	Castillo de Greisol	FIBRA CLIENTE	CAJA 6	Castillo de Greisol	35,5				
18	Ruckus Aulas Nuevas	FIBRA CLIENTE	CAJA 2	Ruckus Aulas Nuevas	89,18				
19	Aulas 1	FIBRA CLIENTE	CAJA 1	Aulas 1	70				
20	Ruckus Casa Blanca	FIBRA CLIENTE	CAJA 2	Ruckus Casa Blanca	112,88				
21	Ruckus Dormitorios Occidente	FIBRA CLIENTE	CAJA 2	Ruckus Dormitorios Occidente	47,15				
22	Jefatura Financiera	FIBRA CLIENTE	CAJA 7	Jefatura Financiera	76,04				
23	Jefatura Instrucción	FIBRA CLIENTE	CAJA 6	Jefatura Instrucción	20,2				
24	Aulas Nuevas	FIBRA CNT	CAJA CNT	Aulas Nuevas	125,4				
25	Aulas Antiguas	FIBRA CNT	CAJA CNT	Aulas Antiguas	180				
	CANTIDAD ESTIMADA EN METROS: 2004,36 236,29 281,71 1208,23								

Anexo 2 Datos obtenidos de los usuarios y número de puntos en la ESP

	· ·		Terminales de datos		
Edificios	Areas	Host	Pared	Techo	
	Ayudantía	2	4	0	
	Dirección	1	1	1	
	Compras públicas	3	3	0	
	Sala de Reuniones	22	1	1	
	Jurídico	4	4	0	
	Recepción de documentos	1	1	0	
Dirección	Subdirección	2	1	0	
Direction	Jefe de estudios-Asesoría pedagógica-Consejo directivo	4	1	0	
	Archivo	1	1	0	
	Sala de espera de dirección AP	10	0	1	
	TIC	4	2	0	
	Casino	20	2	1	
	Universidad Central del Ecuador	7	8	0	
	Cultura física	14	5	0	
Auditorio	Procesamiento de datos	3	2	0	
Jefatura de Instrucción		10	7	0	
	Logística	5	6	0	
Jefatura financiera	Finanzas	8	15	0	
	Dormitorio Oficiales	4	1	0	
	P5	4	1	0	
P5	Archivo	8	2	0	
	Rastrillo	3	1	0	
Tribuna	Bodega Yusco	3	1	0	
	Planta baja	-	1	0	
Aulas Antiguas	1era Planta	5	1	0	
	2da Planta	-	1	0	
	1era Planta	40	6	2	
	2da Planta	40	40	0	
Aulas Nuevas	3era Planta	50	40	2	
	4ta Planta	-	-	1	
Garita	Prevención	2	1	0	
Comedor		20	2	0	
	Dormitorio Hombres 3ero	-	1	0	
_	Dormitorio Mujeres		1	0	
Dormitorios	Dormitorio 1er año	-	0	1	
	Dormitorio 2do año	-	0	1	
TOTAL 300				11	

Anexo 3 Disponibilidad de equipos en ESP

Equipamiento del centro de datos				
Nο	Descripción	Cantidad		
1	Router Cisco 881	1		
2	Switch D-Link D65-2100-24	1		
3	Router Board 1200 Mikrotik	1		
4	Switch Catalyst 2960-x Serie	1		
5	Switch Catalyst 37500-x Serie	1		
6	Ups APC 2 KVA	1		
7	Estantería de baterías	1		
8	Baterías de respaldo	1		
9	Rack de Piso 2.10 m Beaucoup	1		
10	Rack de Piso 1.3 m Beaucoup	1		
11	ODF	1		

Anexo 4 Vlan's de gestión y de acceso para cada departamento

Departamento	IP (/28)	Acceso para el Switch			
	Vlan 99	Vlan 6	Vlan 7	Vlan 8	Vlan 9
Comedor Nuevo	172.20.7.18			X	
Aulas Antiguas	172.20.7.19		Х		
Sala de Instructores	172.20.7.20			Х	
Jefatura Financiera	172.20.7.21	х			
Jefatura de Instrucción	172.20.7.22			Х	
Dirección	172.20.7.23	Х			
Aulas Nuevas	172.20.7.24		х		
P5	172.20.7.25	х			
Auditorio	172.20.7.26	х			
Tribuna	172.20.7.27			х	
Prevención	172.20.7.28	Х			
Servidores	172.20.7.29				Х

Anexo 5 Configuración Básica

Anexo 6 Configuración SSH

```
ip ssh version 2
ip ssh time-out 30
ip domain-name espn
username administrador privilege 15 password 0 espn2018
line vty 0 4
password espn2018
login local
transport input ssh
```

```
vtp mode server
vtp domain espn
vtp password espn2018
```

Anexo 8 Configuración del nombre de las VLAN en el switch de núcleo colapsado

```
vlan 2
name ESPN_admin
name ESPN cadetes
vlan 4
name ESPN_instructores
vlan
name ESPN_invitados
vlan 6
name Administrativo
vlan 7
name Cadetes
vlan 8
name Instructores
vlan 9
name Servidores
vlan 99
name Gestion
```

Anexo 9 Configuración de las interfaces de las vlan's en el switch de núcleo colapsado

```
interface Vlan 2
description "Vlan inalambrica para los administrativos"
ip address 172.20.0.1 255.255.255.0
interface Vlan 3
description "Vlan inalambrica para los cadetes"
ip address 172.20.1.1 255.255.255.0
interface Vlan 4
description "Vlan inalambrica para los instructores"
ip address 172.20.2.1 255.255.255.0
interface Vlan 5
description "Vlan inalambrica para los invitados"
ip address 172.20.2.1 255.255.255.0
interface Vlan 6
description "Vlan administrativos "
ip address 172.20.3.1 255.255.255.0
interface Vlan 7
description "Vlan cadetes"
ip address 172.20.5.1 255.255.255.0
interface Vlan 8
description "Vlan instructores"
ip address 172.20.6.1 255.255.255.0
interface Vlan 9
description "Vlan servidores"
ip address 172.20.7.1 255.255.255.224
interface Vlan 9
description "Vlan gestion"
ip address 172.20.7.33 255.255.255.192
```

Anexo 10 Configuración DHCP en el switch de núcleo colapsado

```
ip dhcp pool ESPN admin
                                    ip dhcp pool Administrativo
network 172.20.0.0 255.255.255.0
                                   network 172.20.4.0 255.255.255.0
default-router 172.20.0.1
                                   default-router 172.20.4.1
dns-server 200.107.10.100
                                   dns-server 200.107.10.100
lease 1 0 0
                                   lease 1 0 0
ip dhcp pool ESPN_cadetes
                                   ip dhcp pool Cadetes
network 172.20.1.0 255.255.255.0 network 172.20.5.0 255.255.255.0
default-router 172.20.1.1
                                   default-router 172.20.5.1
dns-server 200.107.10.100
                                   dns-server 200.107.10.100
lease 1 0 0
                                   lease 1 0 0
ip dhcp pool ESPN_instructores
                                   ip dhcp pool Instructores
network 172.20.2.0 255.255.255.0
                                   network 172.20.6.0 255.255.255.0
default-router 172.20.2.1
                                   default-router 172.20.6.1
dns-server 200.107.10.100
                                   dns-server 200.107.10.100
lease 1 0 0
                                   lease 1 0 0
ip dhcp pool ESPN_invitados
                                   ip dhcp pool Servidores
network 172.20.3.0 255.255.255.0
                                   network 172.20.7.0 255.255.255.240
default-router 172.20.3.1
                                   default-router 172.20.7.1
dns-server 200.107.10.100
                                   dns-server 200.107.10.100
lease 1 0 0
                                   lease 1 0 0
```

```
ip dhcp excluded-address 172.20.0.1
ip dhcp excluded-address 172.20.1.1
ip dhcp excluded-address 172.20.2.1
ip dhcp excluded-address 172.20.3.1
ip dhcp excluded-address 172.20.4.1 172.20.4.100
ip dhcp excluded-address 172.20.5.1 172.20.5.100
ip dhcp excluded-address 172.20.6.1 172.20.6.100
ip dhcp excluded-address 172.20.7.1 172.20.7.100
```

Anexo 11 Configuración del protocolo de enrutamiento en el switch de núcleo colapsado

```
ip route 0.0.0.0 0.0.0.0 172.20.7.34
```

Anexo 12 Configuración de las ACL's para restringir acceso entre vlan's en el switch de núcleo colapsado.

```
access-list 101 deny ip 172.20.0.0 0.0.0.255 172.20.1.0 0.0.0.255
access-list 101 deny ip 172.20.0.0 0.0.0.255 172.20.2.0 0.0.0.255
access-list 101 deny ip 172.20.0.0 0.0.0.255 172.20.3.0 0.0.0.255
access-list 101 deny ip 172.20.1.0 0.0.0.255 172.20.0.0 0.0.0.255
access-list 101 deny ip 172.20.1.0 0.0.0.255 172.20.2.0 0.0.0.255
access-list 101 deny ip 172.20.1.0 0.0.0.255 172.20.3.0 0.0.0.255
access-list 101 deny ip 172.20.2.0 0.0.0.255 172.20.0.0 0.0.0.255
access-list 101 deny ip 172.20.2.0 0.0.0.255 172.20.1.0 0.0.0.255
access-list 101 deny ip 172.20.2.0 0.0.0.255 172.20.3.0 0.0.0.255
access-list 101 deny ip 172.20.3.0 0.0.0.255 172.20.0.0 0.0.0.255
access-list 101 deny ip 172.20.3.0 0.0.0.255 172.20.1.0 0.0.0.255
access-list 101 deny ip 172.20.3.0 0.0.0.255 172.20.2.0 0.0.0.255
access-list 101 deny ip 172.20.4.0 0.0.0.255 172.20.5.0 0.0.0.255
access-list 101 deny ip 172.20.4.0 0.0.0.255 172.20.6.0 0.0.0.255
access-list 101 deny ip 172.20.5.0 0.0.0.255 172.20.4.0 0.0.0.255
access-list 101 deny ip 172.20.5.0 0.0.0.255 172.20.6.0 0.0.0.255
access-list 101 deny ip 172.20.6.0 0.0.0.255 172.20.4.0 0.0.0.255
access-list 101 deny ip 172.20.6.0 0.0.0.255 172.20.5.0 0.0.0.255
access-list 101 permit tcp any any eq 20
access-list 101 permit tcp any any eq 21
access-list 101 permit tcp any any eq 22
access-list 101 permit tcp any any eq 23
access-list 101 permit tcp any any eq 53
access-list 101 permit tcp any any eq 25
access-list 101 permit tcp any any eq 80
access-list 101 permit tcp any any eq 443
access-list 101 permit tcp any any eq pop3
```

Anexo 13 Configuración de las ACL's para restringir servicios en el switch de núcleo colapsado

```
access-list 101 permit ip 172.20.0.0 0.0.3.255 host 200.107.10.100 access-list 101 permit ip 172.20.0.0 0.0.3.255 host 216.58.219.174 access-list 101 permit ip 172.20.0.0 0.0.3.255 host 157.240.14.35 access-list 101 permit ip 172.20.0.0 0.0.3.255 host 104.244.42.65 access-list 101 permit ip 172.20.4.0 0.0.0.255 host 200.107.10.100 access-list 101 permit ip 172.20.4.0 0.0.0.255 host 216.58.219.174 access-list 101 permit ip 172.20.4.0 0.0.0.255 host 157.240.14.35 access-list 101 permit ip 172.20.4.0 0.0.0.255 host 157.240.14.35 access-list 101 permit ip 172.20.4.0 0.0.0.255 host 200.107.10.100 access-list 101 permit ip 172.20.5.0 0.0.0.255 host 200.107.10.100 access-list 101 permit ip 172.20.6.0 0.0.0.255 host 200.107.10.100 access-list 101 permit ip 172.20.6.0 0.0.0.255 host 216.58.219.174 access-list 101 permit ip 172.20.6.0 0.0.3.255 host 200.107.10.100
```

Anexo 14 Grupo de listas de acceso

Departamento	Grupo de Listas de Acceso							
	102	103	104	105	106	107	108	109
Comedor Nuevo	Х	Х	Х				Х	
Aulas Antiguas		Х	Х			Х		
Sala de Instructores			Х				Х	
Jefatura Financiera	Х				Х			
Jefatura de Instrucción	Х		Х				Х	
Dirección	Х	Х		Х	Х			
Aulas Nuevas		Х	Х			Х		
P5	Х				Х			
Auditorio			Х	Х	Х			
Tribuna	Х		Х	Х			Х	
Prevención	Х				Х			
Servidores								Х

Anexo 15 Configuración de LACP en el switch de núcleo colapsado

```
interface port-channel 1
switchport trunk encapsulation dot1q
switchport mode trunk
no shut
exit
interface range FastEthernet0/1-2
channel-protocol lacp
channel-group 1 mode active
no shut
```

Anexo 16 Configuración VTP en el switch de acceso

```
vtp mode client
vtp domain espn
vtp password espn2018
```

Anexo 17 Configuración de LACP en el switch de acceso

```
interface range fastEthernet 0/1-2 channel-protocol lacp channel-group 1 mode passive no shutdown exit interface port-channel 1 switchport mode trunk ip dhcp snooping trust
```

Anexo 18 Configuración de las interfaces en el switch de núcleo colapsado

```
interface range FastEthernet0/1-2
description "Comedor nuevo-Permitir el acceso a la
vlan 2-5 de inalámbricas"
switchport trunk allowed vlan 2,3,4,5
channel-protocol lacp
channel-group 1 mode active
no shut
```

```
ip dhcp snooping
ip dhcp snooping vlan 3,7
interface range fastEthernet 0/1-2
channel-protocol lacp
channel-group 2 mode passive
ip dhcp snooping trust
no shutdown
interface Vlan99
ip address 172.20.7.35 255.255.255.192
exit
interface range FastEthernet0/3-20
description "Aulas antiguas-Permitir el acceso a la
vlan 7 de cadetes"
switchport mode access
switchport access vlan 7
switchport port-security
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security mac-address sticky
exit
interface range FastEthernet0/21-24
description "Aulas antiguas-Permitir el acceso a la
vlan 2-5 de inalámbricas
witchport mode access
switchport access vlan 3
```

Anexo 20 Configuración de QoS con CoS de 0.

```
cdp run
mls qos
int range fa0/1-24
mls qos trust cos
```

Anexo 21 Configuración de QoS estándar.

```
mls qos
int range fa0/1-24
switchport access vlan 6
switchport voice vlan 20
mls qos trust cos
mls qos cos 5
switchport priority extend cos 2
```

Anexo 22 Listas de acceso que van a hacer aplicadas en CoS y políticas

```
access-list 102 remark RestriccionVlan2
access-list 102 permit ip 172.20.0.0 255.255.255.0 any
access-list 102 permit ip any 172.20.0.0 255.255.255.0
access-list 103 remark RestriccionVlan3
access-list 103 permit ip 172.20.1.0 255.255.255.0 any
access-list 103 permit ip any 172.20.1.0 255.255.255.0
access-list 104 remark RestriccionVlan4
access-list 104 permit ip 172.20.2.0 255.255.255.0 any
access-list 104 permit ip any 172.20.2.0 255.255.255.0
access-list 105 remark RestriccionVlan5
access-list 105 permit ip 172.20.3.0 255.255.255.0 any
access-list 105 permit ip any 172.20.3.0 255.255.255.0
access-list 106 remark RestriccionVlan6
access-list 106 permit ip 172.20.4.0 255.255.255.0 any
access-list 106 permit ip any 172.20.4.0 255.255.255.0
access-list 107 remark RestriccionVlan7
access-list 107 permit ip 172.20.5.0 255.255.255.0 any
access-list 107 permit ip any 172.20.5.0 255.255.255.0
access-list 108 remark RestriccionVlan8
access-list 108 permit ip 172.20.6.0 255.255.255.0 any
access-list 108 permit ip any 172.20.6.0 255.255.255.0
access-list 109 remark RestriccionVlan9
access-list 109 permit ip 172.20.7.0 255.255.255.0 any
access-list 109 permit ip any 172.20.7.0 255.255.255.0
```

Anexo 23 Clases de servicio y políticas utilizando las listas de acceso

```
class-map match-all SegmentoV2 policy-map Segmentacion class SegmentoV2
match access-group 102
match access-group 102

class-map match-all SegmentoV3

exceed-action drop
                               class SegmentoV3
match access-group 103
class-map match-all SegmentoV4 exceed-action drop
                               class SegmentoV4
match access-group 104
                               police cir 4096000
class-map match-all SegmentoV5 exceed-action drop
                               class SegmentoV5
match access-group 105
match access-group 105

class-map match-all SegmentoV6

exceed-action drop
                              class SegmentoV6
match access-group 106
class-map match-all SegmentoV7 exceed-action drop
                               class SegmentoV7
match access-group 107
class-map match-all SegmentoV8 exceed-action drop
                              class SegmentoV8
match access-group 108
match access-group 108

class-map match-all SegmentoV9

police cir 5120000
exceed-action drop
                               class SegmentoV9
match access-group 109
                               police cir 2048000
exit
                               exceed-action drop
```

Anexo 24 Configuración de LACP en el switch de núcleo colapsado

```
interface range GigabitEthernet0/1-2
description "Redundancia al Router frontera-LACP"
channel-protocol lacp
channel-group 13 mode active
no shutdown
interface port-channel 13
no switchport
ip address 172.20.7.97 255.255.258
```

Anexo 25 Configuración de LACP en el router frontera

```
interface range GigabitEthernet0/1-2
description "Redundancia al Switch de Core-LACP"
channel-protocol lacp
channel-group 1 mode passive
no shutdown
exit
interface port-channel 1
no switchport
ip address 172.20.7.98 255.255.255.248
no shutdown
```

Anexo 26 Especificaciones técnicas de las fuentes de alimentación

Serie	APC Back-UPS	CP900EPFCLCD	VTN		
	BX				
Marca	APC	Cyber power	Computer Power		
Potencia	1400 VA/700 W	900 VA/540W	6000 VA/5400W		
Voltaje	110/230 V	110 /230 V	110/230 V		
Dimensiones	33,6 x 21,5 x 13 cm	23 x 10 x 27,5 cm	59,2 x 25 x 57,6 cm		
Características	Back-UPS BX Proporciona alimentación garantizada y protección contra sobretensiones, a ordenadores, HDD multimedia, WIFI, consolas de juegos, y otros dispositivos electrónicos	Protección de energía: sobrevoltaje, sobrecarga, cortocircuito, Sistemas operativos compatibles: Windows 7/ Vista/ XP/ 2000/ Linux, Pantalla LCD, indicadores LED	Estos equipos incluyen: pantalla LCD amigable, controlador DSP, modo de conversión de frecuencia 50/60 Hz y función de apagado de emergencia (EPO). Diseño de baterías hot-swappable, bypass automático, bypass switch para mantenimiento		
Tiempo de carga	8 horas	7 horas	5 horas		
Energía de respaldo	10 minutos	15 minutos	25 minutos		
Cantidad de salidas	4 salidas tipo Schuko	6 salidas AC	6 salidas		
Puertos ethernet	No	Si	Si		
Puertos USB	No	Si	Si		
Imagen del dispositivo	APC Back-UPS BX 1400VA Fuente: (Amazon, 2016)	Cyber Power CP900EPFCLCD Fuente: (Amazon, amazon.es, 2017)	UPS COMPUTER POWER SERIES VTN Fuente: (Firmeza, 2016)		
Costos	\$ 181	\$ 230	\$400		

Anexo 27 Especificaciones técnicas de los switch de distribución

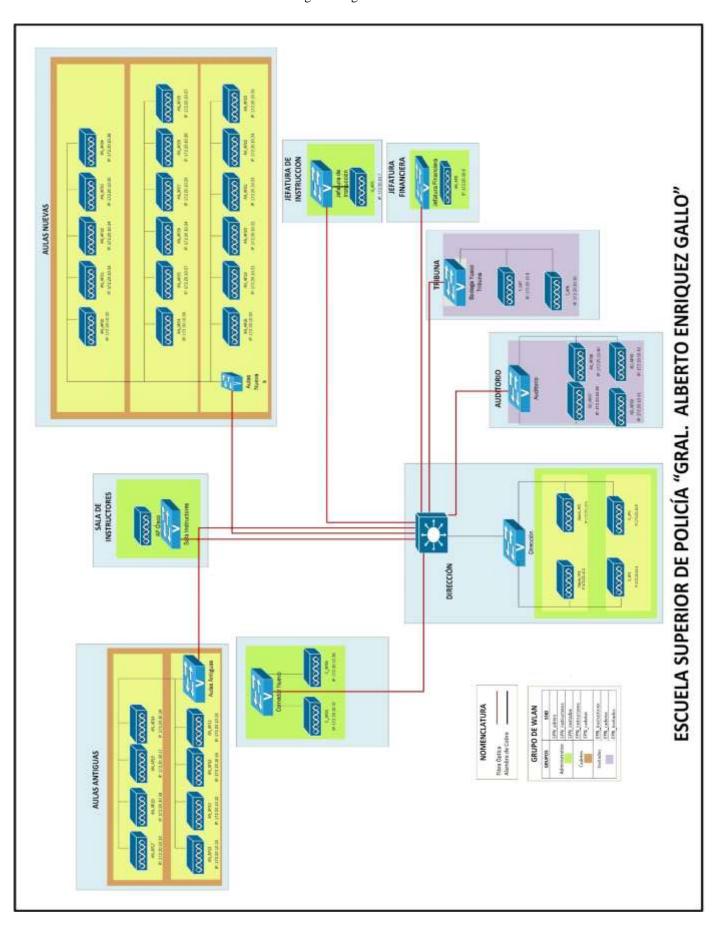
Memoria RAM	Mikrotik Crs 125-24g-1s-rm 128 MB	Cisco Catalyst 3850 4 GB	Aruba-2930f 1 GB		
Memoria Flash	128 MB Flash	2 GB (4 GB on 12-port and 24-port SFP+ models, 8 GB on 48-port SFP+	4 GB		
SWINGSTON SAND SHOWS SELECTION	58.000000 58.000000000000000000000000000	model)	2000 F236		
Protocolo de gestión remota	10 Gbps SNMP 1, SNMP 2, TFTP, SSH, CLI	480 Gbps RMON I and II standards SNMPv1, SNMPv2c, and SNMPv3, HTTP, HTTPS, TFTP, SSH	128 Gbps IMC – Intelligent Management Center; Command-line Interface; Web browser; Configuration menu; SNMP manager; Telnet; RMON1; FTP; Out-of- band management (serial RS- 232C or micro USB)		
Alimentación	CA 110/220 V (50/60 Hz) + PoE	CA 120/230 V (50/60 Hz) - PoE	100 - 127 / 200 - 240 VAC (50/60 Hz)		
Características	Soporte VLAN, Spanning Tree Protocol (STP), snooping DHCP, soporte de Dynamic Trunking Protocol, RouterOS gateway/firewall/VPN router, Access Control List (ACL), Quality of Service (QoS),	Sustitución módulo hot swap, conmutación Layer 2, soporte de DHCP, negociación automática, soporte ARP, concentración de enlaces, soporte VLAN, MDI/MDI-X automático, Storm Control, RSTP, snooping DHCP, DTP, PAgP, soporte de Trivial File Transfer Protocol TFTP, ACL, QoS, compatibilidad con Jumbo Frames, rastreador MLD, Dynamic ARP Inspection (DAI), PoE+, PVST, EIGRP, UDLD, SRR, LACP, RSPAN.	Serie de conmutadores Aruba Layer 3 con apilamiento VSF, estático, Rip and Access OSPF Routing, Tunnel Node, ACLs y QoS robusto. Experiencia coherente inalámbrica constante, AirWave y Aruba ClearPass Policy Manager. Enlaces ascendentes incorporados de 1GbE o 10GbE y superiores a 740 W PoE +. API y soporte OpenFlow. Despliegue simple con Zero Touch Provisioning.		
802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE		IEEE 802.1s IEEE 802.1w IEEE 802.11 IEEE 802.1x IEEE 802.1x- Rev IEEE 802.3ad IEEE 802.3af IEEE 802.3at IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports IEEE 802.1D Spanning Tree Protocol IEEE 802.1p CoS prioritization IEEE 802.1Q VLAN IEEE 802.3 10BASE-T specification	IEEE 802.3 Type 10BASE-T, IEEE 802.3 Type 100BASE- TX, IEEE 802.3 ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 4 SFP+ 1/10GbE ports; PHY- less		
Peso	7.1 kg	7.02 Kg	2.41 Kg		
Dimensiones (Ancho x Profundidad x Altura)	443x142x44mm	44.5 cm x 45.0 cm x 4.45 cm	2.41 Ng 44.25 cm x 20.02 cm x 4.39 cm		
Numero de Puertos / Velocidad de los puertos	24x 10/100/1000	24 puertos 10/100/1000, 2 puertos Ethernet Gigabit	24 x 10/100/1000, 2 puertos Ethernet Gigabit		
Soporte PoE	8-28 V	8-28 V	8-28 V		
Rendimiento	160 Gbps	2 Tbps	1.2 Tbps		
Ethernet	No	Si	Si		
Channel					
Soporta VLAN Soporte STP /	Si	Si	Si		
TFTP	Si	Si	SI		
Soporte Telnet / SSH	Si	Si	Si		
SNMP	No	Si	Si		
IGMP	Si	Si	Si		
Soporte Stacking	No	Si	SI		
Calidad de servicio	No	Si	Si		
Soporte ACL	No	Si	Si		
Enrutamiento	No	Si	Si		
lmagen del dispositivo	Mikrotik Crs 125-24g-1s-rm Fuente: (TecnoSmart, 2016)	Cisco Catalyst 3850 Fuente: (3850, 2016)	Aruba 2930f Fuente: (SERVER, 2016)		
Costo	\$400	\$ 1,750	\$ 2.270		

Anexo 28 Especificaciones técnicas del switch de acceso

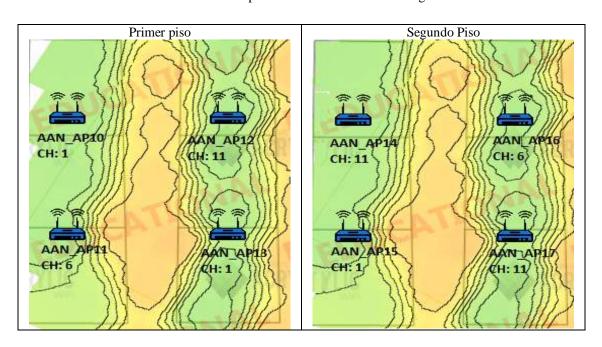
	SWITCH CISCO 2960 CATALYST
Tipo de dispositivo:	Cisco 2960 Integrated Services Router - encaminador
Número de puertos / Velocidad	24 x 10/100 2 x 10/100/1000-TX
de los puertos	Total 24 puertos
Peso	3600 g
Dimensión	445 x 236 x 44 mm
DRAM Memoria	64 MB
Tamaño de tabla de dirección	8000 entradas
MAC	
Capacidad de Conmutación	16 Gbit/s
Memoria Flash	32 MB
Certificaciones	CE, TUV GS, cUL, EN 60950, EN55022, NOM, VCCI Class A ITE, IEC
	60950, EN55024, FCC Part 15, UL 1950 (3), CSA 22.2 No. 950 (3)
Protocolo de direccionamiento	ACL, ARP, DiffServ, IGMP, IP, RADIUS, SSH, TCP, UDP, DHCP, TFTP
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Características	Full duplex capability, BOOTP support, ARP support, VLAN support,
	Syslog support, DiffServ support, IPv6 support, Spanning Tree
	Protocol (STP) support, Rapid Spanning Tree Protocol (RSTP)
	support, Multiple Spanning Tree Protocol (MSTP) support, DHCP
	snooping, Port Aggregation Protocol (PAgP) support, Trivial File
	Transfer Protocol (TFTP) support, Quality of Service (QoS), Dynamic ARP Inspection (DAI), Cisco EnergyWise technology, Shaped Round
	Robin (SRR), LLDP support, DHCP relay, Link Aggregation Control
	Protocol (LACP), MAC Address Notification, Management
	Information Base (MIB), Class of Service (CoS), DiffServ Code Point
	(DSCP) support
Protocolo de gestión remota	Telnet, RMON 2, RMON 1, SNMP 1, SNMP 3, SNMP 2c, TFTP, SSH
Seguridad	UL, C-UL, TUV/GS, CB, NOM, CE
Cumplimiento de normas	IEEE 802.1d, IEEE 802.1p, IEEE 802.1Q, IEEE 802.3 CSMA/CD, IEEE
	802.3u, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3z, IEEE 802.1w, IEEE
	802.3x, IEEE 802.1x, IEEE 802.1s
Temperatura	-25 - 70 °C
Soporte PoE	Si
Rendimiento	216 Gbps
Ethernet Channel	Şi
Soporta VLAN	SI
Soporte STP / TFTP	Şi
Soporte Telnet / SSH	Si Si
SNMP	Şi
IGMP	Şi
Soporte Stacking	Si Si
Calidad de servicio	Si Si
Soporte ACL	No.
soporte nue	T
Imagen del dispositivo	Circa Catalant 2000
	Cisco Catalyst 2960
Costo	Fuente: (Cisco, 2014) \$ 749.00
COSTO	\$ 745.00

Anexo 29 Access Point distribuidos en toda la institución

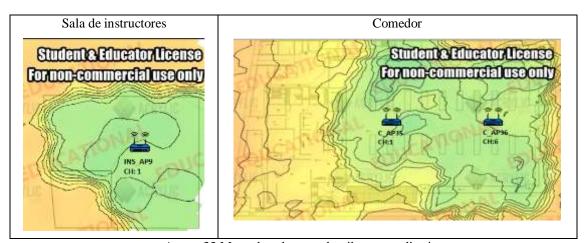
Edifi	icios	Access Point	Dirección IP	EPN_admin	EPN_instructores	EPN_invitados	EPN_cadetes	Canales	Marcas
Dirección _	Primer	Casino_AP1	172.20.10.2	X	X	X		1	Cisco 1602i
	Piso	Casino_AP2	172.20.10.3	X	X	X		6	
	Segundo	D_AP3	172.20.10.4	X	X	X		11	
	Piso	D_AP4	172.20.10.5	X	X	X		1	
Jefatura de Instrucción		JI_AP5	172.20.10.7	X	X			1	
Jefatura fii	nanciera	JF_AP6	172.20.10.8	X				6	
Tribuna		T_AP7	172.20.10.9	X	X	X		1	Ruckus
THOUILA		T_AP8	172.20.10.10	X	X	X		6	7762
Sala de Ins	structores	INS_AP9	172.20.10.11		X			1	
		AAN_AP10	172.20.10.12		X		X	1	
	Primer	AAN_AP11	172.20.10.13		X		X	6	
	Piso	AAN_AP12	172.20.10.14		X		X	11	G:
Aulas		AAN_AP13	172.20.10.15		X		X	1	Cisco 1602i
Antiguas		AAN_AP14	172.20.10.16		X		X	11	10021
	Segundo	AAN_AP15	172.20.10.17		X		X	1	
	Piso	AAN_AP16	172.20.10.18		X		X	6	
		AAN_AP17	172.20.10.19		X		X	11	
		AN_AP18	172.20.10.20		X		X	1	
	Primer	AN_AP19	172.20.10.21		X		X	6	
		AN_AP20	172.20.10.22		X		X	11	
	Piso	AN_AP21	172.20.10.23		X		X	1	
		AN_AP22	172.20.10.24		X		X	6	
		AN_AP23	172.20.10.25		X		X	1	
		AN_AP24	172.20.10.26		X		X	11	
		AN_AP25	172.20.10.20		X		X	1	
Aulas	G 1								
Nuevas	Segundo Piso	AN_AP26	172.20.10.28		X		X	6	
	1150	AN_AP27	172.20.10.29		X		X	11	ubiquiti
		AN_AP28	172.20.10.30		X		X	1	Networks UAP- AC-HD
		AN_AP29	172.20.10.31		X		X	11	
		AN_AP30	172.20.10.32		X		X	6	
	Tercer	AN_AP31	172.20.10.33		X		X	11	
	Piso	AN_AP32	172.20.10.34		X		X	1	
		AN_AP33	172.20.10.35		X		X	11	
		AN_AP34	172.20.10.36		X		X	6	
Com	Comedor	C_AP35	172.20.10.37	X	X	X		1	
		C_AP36	172.20.10.38	X	X	X		6	
		AD_AP37	172.20.10.39	X	X	X		1	
Andi	torio	AD_AP38	172.20.10.40	X	X	X		6	
Auditorio		AD_AP39	172.20.10.41	X	X	X		11	
		AD_AP40	172.20.10.42	X	X	X		1	



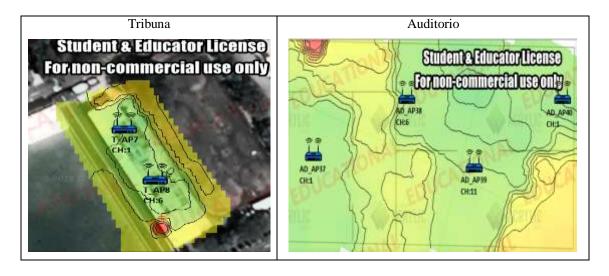
Anexo 31 Mapa de cobertura de las aulas antiguas



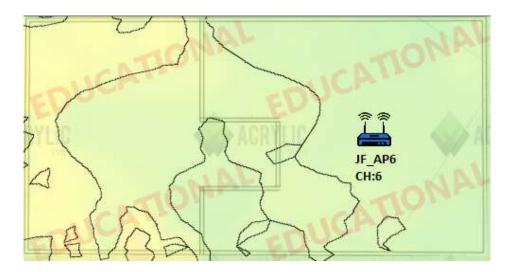
Anexo 32 Mapa de cobertura de sala de instructores y comedor



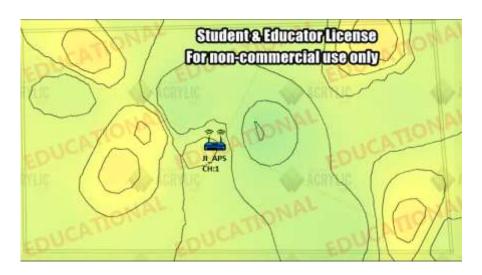
Anexo 33 Mapa de cobertura de tribuna y auditorio



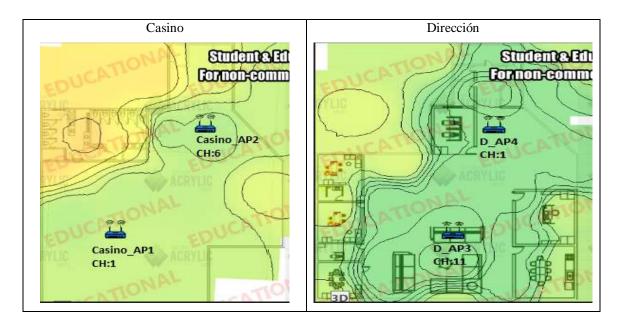
Anexo 34 Mapa de cobertura de la jefatura financiera



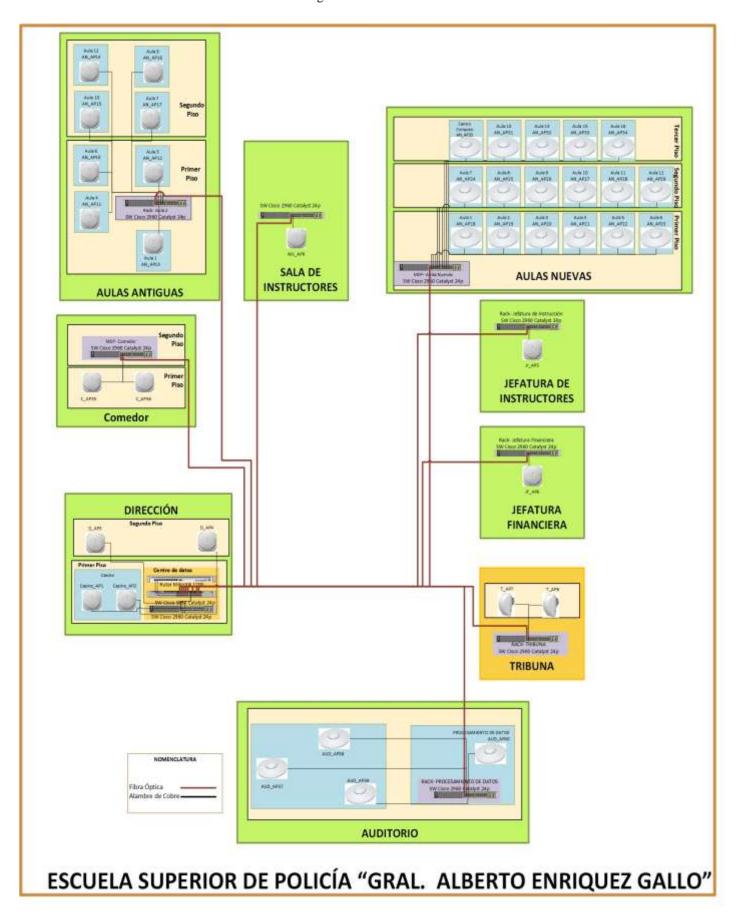
Anexo 35 Mapa de cobertura de la jefatura de instrucción



Anexo 36 Mapa de cobertura de dirección



Anexo 37 Diagrama físico de la red WLAN en la ESPN



Anexo 38 Especificaciones técnicas de los AP

Características	Cisco Aironet AIR- SAP16021-A-K9	Ubiquiti Networks UAP-AC-HD	Aruba 220 802.11a / n / ac/b/g		
Banda de radio	802.11a/g/n	802.11a / n / ac/b/g			
Tipo de antena	Omnidireccional	Omnidireccional	Omnidireccional		
Velocidad de datos	2.4 GHz and 5 GHz	2.4 GHz and 5 GHz	2.4 GHz and 5 GHz		
Velocidad de datos	2.4 GHz and 5 GHz	2.4 GHz and 5 GHz	2.4 GHz and 5 GHz		
Estándar IEEE	IEEE 802.11a/b/g, IEEE 802.11n, IEEE IEEE 802.3af		IEEE 802.3az, - 802.11n, 802.11d		
RJ-45 10/100/1000BASE-T		2 interfaces (RJ-45) de 10/100/1000 Eth	dos interfaces (RJ- 45)10/100/1000BASE T Ethernet network		
Memoria del sistema	DRAM de 256 MB Flash de 32 MB	DRAM de 100 MB Flash de 10 MB	DRAM de 100 MB Flash de 10 MB		
802.11i,802.110 802,1X MS-CHAP N Seguridad EAP, WPA2, WPA, 802.1X, AE TKIP, TTLS, EAP, T		WEP, WPA-PSK, WPA- Enterprise (WPA/WPA2, TKIP/AES) 802.11w/PMF	WEP, WPA-PSK, WP WPA2		
Potencia de 22 dBm		25dBm	23 dBm		
SSID	SSID 4 por radio 8 por Radi		16 por radio		
Cantidad de 100		350	150		
Consumo de energía 12,95 W		17 W	17 W		
lmagen del dispositivo		U	ATRICA		
,	(Cisco, 2017)	(Ubiquiti, 2016)	(Aruba, 2017)		
Precio	695	240	568,35		