



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA

Y REDES DE COMUNICACIÓN

**TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN**

TEMA

**DISEÑO DE SISTEMA DE SEGURIDAD A NIVEL DE CAPA DE ENLACE DE DATOS
EN REDES CABLEADAS MEDIANTE EL ESTÁNDAR IEEE 802.1X EN LA LAN DE
LA UNIVERSIDAD TÉCNICA DEL NORTE.**

AUTOR: Edison Mauricio Vallejos Garzón

DIRECTOR: Ing. Carlos Alberto Vásquez Ayala, MSc

Ibarra-Ecuador

2019



UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE.

1. IDENTIFICACIÓN DE LA OBRA.

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DEL CONTACTO			
CÉDULA DE IDENTIDAD:	171807624-1		
APELLIDOS Y NOMBRES:	Vallejos Garzón Edison Mauricio		
DIRECCIÓN:	Ibarra – El Sagrario		
EMAIL:	emvallejos@utn.edu.ec		
TELÉFONO FIJO:	06-2-606-109	TELÉFONO MÓVIL:	0969858868

DATOS DE LA OBRA	
TÍTULO:	DISEÑO DE SISTEMA DE SEGURIDAD A NIVEL DE CAPA DE ENLACE DE DATOS EN REDES CABLEADAS MEDIANTE EL ESTÁNDAR IEEE 802.1X EN LA LAN DE LA UNIVERSIDAD TÉCNICA DEL NORTE.
AUTOR (ES):	Edison Mauricio Vallejos Garzón
FECHA:	01 de abril 2019
PROGRAMA	<input checked="" type="checkbox"/> PREGRADO <input type="checkbox"/> POSGRADO
TÍTULO POR EL QUE OPTA:	Ingeniero en Electrónica y Redes de Comunicación
TUTOR / DIRECTOR:	Ing. Carlos Alberto Vásquez, MSc.

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD.

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD.

Yo, Edison Mauricio Vallejos Garzón, con cédula de identidad Nro.171807624-1, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.



Edison Mauricio Vallejos Garzón

CI: 171807624-1

Ibarra, 01 de abril 2019

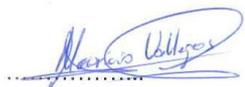
3. CONSTANCIAS.

3. CONSTANCIAS.

Yo, EDISON MAURICIO VALLEJOS GARZÓN declaro bajo juramento que el trabajo aquí escrito es de mi autoría; y que este no ha sido previamente presentado para ningún grado o calificación profesional y que he consultado las referencias bibliográficas que se presentan en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondiente a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las leyes de propiedad intelectual, reglamentos y normatividad vigente de la Universidad Técnica del Norte.

En la ciudad de Ibarra, 01 abril de 2019



Edison Mauricio Vallejos Garzón

CI: 1718076241



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN DE AUTORÍA

Yo, Edison Mauricio Vallejos Garzón, con la cedula de identidad Nro. 171807624-1 declaro bajo juramento que el trabajo aquí escrito es de mi autoría; y que este no ha sido previamente presentado para ningún grado o calificación profesional y que he consultado las referencias bibliográficas que se presentan en este documento. A través de la presente declaración cedo mis derechos de propiedad intelectual correspondiente a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las leyes de propiedad intelectual, reglamentos y normatividad vigente de la Universidad Técnica del Norte.

En la ciudad de Ibarra, 01 de abril 2019

A handwritten signature in blue ink, reading 'Edison Mauricio Vallejos Garzón', is written over a horizontal line.

Edison Mauricio Vallejos Garzón

CI: 171807624-1



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN.

MAGISTER CARLOS ALBERTO VÁSQUEZ AYALA, DIRECTOR DEL
PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que, el presente trabajo de Titulación “DISEÑO DE SISTEMA DE SEGURIDAD A
NIVEL DE CAPA DE ENLACE DE DATOS EN REDES CABLEADAS MEDIANTE EL
ESTÁNDAR IEEE 802.1X EN LA LAN DE LA UNIVERSIDAD TÉCNICA DEL NORTE.”
Ha sido desarrollado por el señor Edison Mauricio Vallejos Garzón bajo mi supervisión.

Es todo en cuanto puedo certificar en honor de la verdad.

A handwritten signature in blue ink, appearing to read "C. Vásquez", is written over a horizontal dotted line.

Ing. Carlos Alberto Vásquez Ayala

DIRECTOR



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA.

A mis padres Rosa Garzón y Augusto Vallejos, por ser un ejemplo de tenacidad y sacrificio en todos los aspectos de la vida en las latitudes que nos ha tocado vivir, por sus sabias palabras de aliento, la unión incondicional que tenemos en la familia y su confianza plena en mí.



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTO

Agradezco a mis padres Rosa Garzón y Augusto Vallejos, por su inmenso y absoluto apoyo para la culminación de mi tesis.

A mis queridos abuelitos Jaime Vallejos y Aida Arias, por siempre inculcarme a tener la máxima consideración a los valores familiares, la unión de la misma y por transmitirme sus conocimientos y experiencias de vida. Me gustaría citar una frase de mi abuelito que la ha acompañado a lo largo de su vida “*En la vida hay que ser desprendidos de las cosas materiales*”, muchas gracias por todo.

Al Ing. Vinicio Guerra, encargado de la Dirección de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte y al Ing. Edison Carrión por su ayuda, asistencia y respaldo en todo momento para poder realizar este proyecto.

A mi director de tesis ingeniero Carlos Vásquez, MSc por su disposición, consejos y orientación para el cumplimiento y desarrollo de este proyecto de titulación.

A mis compañeros de lucha que he conocido en la Universidad, por todas las experiencias vividas dentro y fuera de las aulas, por la unión y la gran amistad que hemos formado entre todos.

ÍNDICE DE CONTENIDO

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE	I
1. IDENTIFICACIÓN DE LA OBRA.	I
3. CONSTANCIAS.	III
DECLARACIÓN DE AUTORÍA	IV
CERTIFICACIÓN.....	V
DEDICATORIA.....	VI
AGRADECIMIENTO	VII
ÍNDICE DE CONTENIDO.....	VIII
ÍNDICE DE FIGURAS.....	X
ÍNDICE DE TABLAS	XV
RESUMEN.....	XVIII
ABSTRACT	XIX
CAPÍTULO I.....	1
INTRODUCCIÓN	1
1.1 TEMA	1
1.2 PROBLEMA	1
1.3. OBJETIVOS.....	2
1.3.1. Objetivo General.....	2
1.3.2. Objetivo Específicos	2
1.4. ALCANCE.....	3
1.5. JUSTIFICACIÓN.....	4
CAPÍTULO II.....	6
MARCO TEÓRICO	6
2.1 ESTÁNDAR IEEE 802.2	6
2.2 ESTÁNDAR IEEE 802.3	7
2.2.1 Introducción a Ethernet.	7
2.2.2 Formato de la trama Ethernet.	8
2.2.3 Tecnología y velocidades de Ethernet.....	9
2.3 CONMUTACIÓN EN IEEE 802.3.....	11
2.3.1 Switch no administrable.	12
2.3.2 Switch administrable.	12
2.4 PRINCIPIOS DE SEGURIDAD EN UNA RED.....	17
2.4.1 Confidencialidad.....	17
2.4.2 Integridad.....	17
2.4.3 Disponibilidad.....	17
2.4.4 Autenticación.....	18
2.4.5 Autorización.....	18
2.4.6 No repudio.....	18

2.4.7 Amenaza.....	18
2.4.8 Vulnerabilidad.....	18
2.4.9 Ataque.....	19
2.5 PROTOCOLOS DE AUTENTICACIÓN.....	19
2.5.1 IEEE 802.1X.....	19
2.5.2 Autenticación EAP.....	22
2.6 REMOTE AUTHENTICATION DIAL-IN USER SERVER (RADIUS).....	32
2.6.1 Protocolo Radius AAA.....	32
2.6.2 Estructura del formato del protocolo Radius.....	33
2.7 LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP).....	35
2.7.1 Modelo de información LDAP.....	36
2.7.2 Operaciones dentro de LDAP.....	37
2.7.3 Estructura de la LDAP.....	37
2.7.4 LDAP arquitectura Cliente/Servidor.....	40
CAPÍTULO III.....	42
SITUACIÓN ACTUAL.....	42
3.1 SITUACIÓN ACTUAL DE LA RED CABLEADA “UNIVERSIDAD TÉCNICA DEL NORTE”.....	42
3.2 DESCRIPCIÓN DE LA RED POR FACULTAD.....	48
3.2.1 FICA.....	48
3.2.2 FICAYA.....	64
3.2.3 FACAE.....	65
3.2.4 FECYT.....	66
3.2.5 FCCSS.....	67
3.3 DESCRIPCIÓN DE LA RED EN OTRAS DEPENDENCIAS.....	68
3.3.1 Edificio central.....	68
3.3.2 Edificio posgrados.....	70
3.3.3 U. EMPRENDE, CAI.....	71
3.3.4 Biblioteca.....	72
3.3.5 Bienestar universitario.....	73
3.3.6 Complejo acuático.....	74
3.3.7 Auditorio Agustín Cueva.....	74
3.3.8 Colegio universitario.....	74
3.4 SWITCH COMPATIBLES CON EL PROTOCOLO 802.1X.....	75
CAPÍTULO IV.....	77
DISEÑO DEL SISTEMA DE SEGURIDAD.....	77
4.1 DISEÑO EN CAPA DE ACCESO POR FACULTADES.....	77
4.1.1 FICA.....	78
4.1.2 FICAYA.....	88
4.1.3 FACAE.....	90
4.1.4 FECYT.....	92

4.1.5 FCCSS	94
4.2 DISEÑO EN OTRAS DEPENDENCIAS	96
4.2.1 Edificio central.....	96
4.2.2 Edificio de posgrado.	99
4.2.3 U. EMPRENDE, CAI.	100
4.2.4 Biblioteca.....	102
4.2.5 Bienestar Universitario.....	103
4.2.6 Complejo Acuático.	104
4.2.7 Auditorio Agustín Cueva.	105
4.3 DISEÑO EN CAPA DE DISTRIBUCIÓN Y NÚCLEO.	105
4.3.1 FICA.....	105
4.3.2 FICAYA.	108
4.3.3 FACAE.....	108
4.3.4 FECYT.	111
4.3.5 FCCSS.....	111
4.3.6 Edificio Central.....	113
4.4 INSTALACIÓN DEL SERVIDOR RADIUS-LDAP-MYSQL.....	115
4.4.1 Instalación paquetes Freeradius	116
4.4.2 Confirmación de método de autenticación EAP-TTLS	117
4.4.3 Integración Openldap a Freeradius.	120
4.4.4 Integración MySQL a Freeradius.	122
4.4.5 Configuración de los clientes	124
CAPÍTULO V	126
5.1 IMPLEMENTACIÓN EN AMBIENTE CONTROLADO Y PRUEBAS DE FUNCIONAMIENTO	126
5.1.1 Interconexión del servidor al switch 4506.	127
5.1.2 Configuración protocolo 802.1X Laboratorio 3.	130
5.1.3 Pruebas de funcionamiento.....	130
5.2 CONCLUSIONES.....	143
5.3 RECOMENDACIONES.....	145
BIBLIOGRAFÍA	148
ANEXO I.....	151
ANEXO II	156
ANEXO III.....	167
ANEXO IV.....	186

ÍNDICE DE FIGURAS

Figura 1: Formato de la trama 802.2.....	6
--	---

Figura 2: Formato de la trama IEEE 802.3	9
Figura 3: Elección root bridge	14
Figura 4: Transición de estado del puerto	16
Figura 5: 802.1X para la autenticación de usuario de LAN	20
Figura 6: Formato trama EAP	22
Figura 7: Mensajes del protocolo EAP	24
Figura 8: La negociación de los cuatro tipos básicos de mensajes EAPOL	25
Figura 9: Formato del mensaje EAP-TLS.....	25
Figura 10: EAP TLS Handshake	28
Figura 11: Estructura EAPOL-TTLS.....	29
Figura 12: Estructura PEAP	30
Figura 13: Datagrama Radius.....	33
Figura 14: Relación entre entrada, atributos y valores	38
Figura 15: Apertura de conexión Cliente/Servidor.....	41
Figura 16: Búsquedas Cliente/Servidor	41
Figura 17: Cerrar conexión Cliente/Servidor	42
Figura 18: Topología física UTN	45
Figura 19: Topología lógica UTN	46
Figura 20: Topología Física FICA-UTN	49
Figura 21: Topología Lógica FICA-UTN.....	50
Figura 22: Planta Baja FICA-UTN.....	51
Figura 23: Primera Planta FICA-UTN.....	52
Figura 24: Segunda planta FICA-UTN.....	58
Figura 25: Cuarta planta FICA-UTN.....	60
Figura 26: Topología física FICAYA-UTN.....	64
Figura 27: Topología física FACAE-UTN.....	65
Figura 28: Topología física FECYT -UTN.....	66
Figura 29: Topología física FCCSS -UTN.....	67
Figura 30: Topología física Edificio Central - UTN.....	69
Figura 31: Topología física Edificio Posgrados - UTN.....	70

Figura 32: Topología física U Emprende, CAI - UTN	71
Figura 33: Topología física Biblioteca - UTN	72
Figura 34: Topología física Biblioteca- UTN	73
Figura 35: Topología física Complejo Acuático - UTN	74
Figura 36: Ubicación del servidor RADIUS – LDAP	77
Figura 37: Diseño sistema de seguridad facultad FICA	78
Figura 38: Diagrama capa acceso FICA – Laboratorio 1	79
Figura 39: Diagrama capa acceso FICA – Laboratorio 2	81
Figura 40: Diagrama capa acceso FICA – Laboratorio 3	82
Figura 41: Diagrama capa acceso FICA – Laboratorio 4	82
Figura 42: Diagrama capa acceso FICA – Laboratorio 5	83
Figura 43: Diagrama capa acceso FICA – Laboratorio 6	86
Figura 44: Diagrama capa acceso FICA – Laboratorio 9	86
Figura 45: Diagrama capa acceso FICA – Cubículos 1	87
Figura 46: Diagrama capa acceso FICA – Cubículos 2.....	88
Figura 47: Diagrama capa acceso FICAYA – Planta Baja	88
Figura 48: Diagrama capa acceso FICAYA – Laboratorio 4.....	89
Figura 49: Diagrama capa acceso FICAYA – Laboratorio 8.....	90
Figura 50: Diagrama capa acceso FACAE – Laboratorio 3.....	91
Figura 51: Diagrama capa acceso FACAE – Laboratorio 4.....	91
Figura 52: Diagrama capa acceso FECYT – Laboratorio 1	92
Figura 53: Diagrama capa acceso FECYT – Laboratorio 2.....	93
Figura 54: Diagrama capa acceso FECYT – Laboratorio MAC	93
Figura 55: Diagrama capa acceso FECYT – Laboratorio Inglés	94
Figura 56: Diagrama capa acceso FCCSS – Laboratorio 1.....	95
Figura 57: Diagrama capa acceso FCCSS – Laboratorio 2.....	96
Figura 58: Diagrama capa acceso Edificio Central - Planta Baja.....	97
Figura 59: Diagrama capa acceso Edificio Central - Primera planta.....	97
Figura 60: Diagrama capa acceso Edificio Central - Segunda planta.....	97
Figura 61: Diagrama capa acceso Edificio Central - Tercera planta	98

Figura 62: Diagrama capa acceso Edificio Central - Cuarta planta.....	98
Figura 63: Diagrama capa acceso Edificio de Posgrados	100
Figura 64: Diagrama capa acceso– Planta baja	100
Figura 65: Diagrama capa acceso– Primer Piso	101
Figura 66: Diagrama capa acceso Escuela de Conducción – Segundo Piso	101
Figura 67: Diagrama capa acceso U. EMPRENDE – Tercer Piso	101
Figura 68: Diagrama capa acceso CAI – Cuarto Piso.....	101
Figura 69: Diagrama capa acceso Biblioteca – Planta Baja.....	102
Figura 70: Diagrama capa acceso Biblioteca – Primer Piso	102
Figura 71: Diagrama capa acceso Biblioteca – Segundo Piso	103
Figura 72: Diagrama capa acceso Bienestar Universitario – Planta Baja.....	103
Figura 73: Diagrama capa acceso Bienestar Universitario – Cuarto Piso	104
Figura 74: Diagrama capa acceso Complejo Acuático	104
Figura 75: Diagrama capa acceso Auditorio Agustín Cueva	105
Figura 76: Diagrama capa distribución - FICA.....	106
Figura 77: Diagrama capa distribución - FACAE.....	109
Figura 78: Diagrama capa distribución - FACAE.....	111
Figura 79: Diagrama capa distribución - FCCSS	112
Figura 80: Diagrama capa distribución – Edificio Central	113
Figura 81: Árbol de distribución LDAP - UTN	116
Figura 82: Instalación paquetes freeradius, módulos LDAP y Mysql	116
Figura 83: Elección método de autenticación EAP-TTLS.....	117
Figura 84: Autoridad Certificadora.....	118
Figura 85: Certificado del servidor	118
Figura 86: Servidor del usuario	118
Figura 87: Creación CA y certificados	119
Figura 88: Comprobación de archivos creados	119
Figura 89: Parámetros LDAP.....	120
Figura 90: Habilitar autorización y autenticación con LDAP	120
Figura 91: Creación tabla ldif Radius	121

Figura 92: Asignar valores corrector Radius.ldif	121
Figura 93: Agregar y comprobar Radius.ldif	121
Figura 94: Crear base de datos y configurar parámetros	122
Figura 95: Exportar plantillas y comprobación	122
Figura 96: Incluir librería “sql” en Freeradius	123
Figura 97: Enlazar base de datos y sus parámetros con Freradius	123
Figura 98: Elegir método SQL para autorización, contabilidad, sesión post-auth.....	124
Figura 99: Definir segmento de red de switch	124
Figura 100: Comprobar acceso Radius-LDAP y NAS	125
Figura 101: Topología FICA ambiente controlado	126
Figura 102: Asignación de puerto RADIUS - LDAP	127
Figura 103: Configurar interfaz de red servidor.....	127
Figura 104: Enlazar IP LDAP con Radius	128
Figura 105: Conectividad servidor y VLAN-ADMINISTRATIVOS	128
Figura 106: Conectividad servidor y VLAN-LABORATORIOS	128
Figura 107: Conectividad servidor y VLAN-ADMINISTRATIVA	128
Figura 108: Administración LDAP	129
Figura 109: Administración MySQL	129
Figura 110: Ingreso de credenciales	131
Figura 111: Estado del puerto dot1x FastEthernet 1/7.....	131
Figura 112: Mensaje EAP del tipo Request, Identity	132
Figura 113: Mensaje EAPOL del tipo Start	132
Figura 114: Mensaje EAP Response, Identity.....	133
Figura 115: Paquete RADIUS Access request Id=9.....	133
Figura 116: Paquete RADIUS Access-Challenge Id=9	134
Figura 117: Mensaje EAP Request, Tunneled TLS EAP (EAP-TTLS).....	134
Figura 118: Negociación del canal TLS	135
Figura 119: Paquete RADIUS Access request Id=10.....	135
Figura 120: Paquete RADIUS Access Challenged Id=10	136
Figura 121: Paquete EAP respuesta TLS	136

Figura 122: Paquete EAP TLSv1 cifrar canal	137
Figura 123: Paquete RADIUS Access request Id=11	137
Figura 124: Paquete RADIUS Access Challenged Id=11	138
Figura 125: Confirmación EAP-TTLS	138
Figura 126: Validación fallida RADIUS	139
Figura 127: Validación fallida cliente.....	139
Figura 128: Validación correcta Radius.....	140
Figura 129: Validación correcta cliente	140
Figura 130: Validación puerto switch.....	141
Figura 131: Paquete Radius Accounting-Request	142
Figura 132: Paquete Radius Accounting-Response.....	142

ÍNDICE DE TABLAS

Tabla 1: IEEE 802.3 10BASE 10-Mbps	10
Tabla 2: IEEE 802.3 100BASE-T	10
Tabla 3: IEEE 802.3 1000BASE-T.....	11
Tabla 4: STP estado de puertos	15
Tabla 5: Comparación de métodos EAP.....	30
Tabla 6: Tipo de paquete Radius	33
Tabla 7: Tipo de atributos Radius.....	34
Tabla 8: Modelos de información LDAP	36
Tabla 9: Algunas de las sintaxis de los atributos LDAP.....	38
Tabla 10: <i>Atributos comunes LDAP</i>	38
Tabla 11: <i>Clases de objetos y atributos requeridos</i>	39
Tabla 12: Representación del String según tipo de atributo	40
Tabla 13: Distribución De Subredes (VLANS).....	47
Tabla 14: Equipos Data Center – FICA	51
Tabla 15: Servidores – FICA.....	52

Tabla 16: Equipos Lab.1 - FICA	53
Tabla 17: Mapeo de red Lab.1 – FICA	53
Tabla 18: Equipos Lab.2 – FICA.....	54
Tabla 19: Mapeo de red Lab.2 – FICA.....	54
Tabla 20: Equipos Lab.3 – FICA.....	55
Tabla 21: Mapeo de red Lab.3 – FICA.....	55
Tabla 22: Equipos Lab.4 – FICA.....	56
Tabla 23: Mapeo de red Lab.4 – FICA	57
Tabla 24: Mapeo de red Lab.5 – FICA	58
Tabla 25: Mapeo de red Lab.6 – FICA.....	59
Tabla 26: Equipos Lab.9 – FICA.....	60
Tabla 27: Mapeo de red Lab.9 – FICA.....	61
Tabla 28: Equipos Cubículos docentes 1 – FICA.....	62
Tabla 29: Mapeo de red cubículos docentes 1	62
Tabla 30: Equipos cubículos docentes 2 – FICA	63
Tabla 31: Mapeo de red cubículos docentes 2	63
Tabla 32: <i>Equipos de Telecomunicaciones – FICAYA</i>	64
Tabla 33: Equipos de Telecomunicaciones – FACAE	65
Tabla 34: <i>Equipos de Telecomunicaciones – FECYT</i>	66
Tabla 35: Equipos de Telecomunicaciones – FCCSS	67
Tabla 36: Equipos de Telecomunicaciones – Edificio Central	69
Tabla 37: Equipos de Telecomunicaciones – Edificio de Posgrado.....	70
Tabla 38: Equipos de Telecomunicaciones – U. EMPRENDE, CAI	71
Tabla 39: Equipos de Telecomunicaciones – Biblioteca	72
Tabla 40: Equipos de Telecomunicaciones – Bienestar Universitario	73
Tabla 41: Equipos de Telecomunicaciones – Complejo Acuático	74
Tabla 42: Equipos de Telecomunicaciones – Auditorio Agustín Cueva	74
Tabla 43: Equipos de Telecomunicaciones – Colegio Universitario.....	75
Tabla 44: Listado de switch UTN.....	75
Tabla 45: Habilitar y configurar protocolo 802.1X switch cisco 2960.....	79

Tabla 46: Habilitar y configurar protocolo 802.1X switch 3COM 4200,4400	83
Tabla 47: Habilitar y configurar protocolo 802.1X switch cisco 3850.....	98
Tabla 48: Puertos vlan FICA-ADMINISTRATIVOS activos SW-4506	106
Tabla 49: Habilitar y configurar protocolo 802.1X switch cisco 4506.....	107
Tabla 50: Puertos vlan ADMINSTRATIVOS, LABORATORISO activos FACAE SW-4506.....	110
Tabla 51: Puertos vlan FECYT-ADMINISTRATIVOS activos SW-3850.....	111
Tabla 52: Puertos vlan FCCSS - ADMINISTRATIVOS activos SW-3850.....	112
Tabla 53: Puertos vlans activos Edificio - Central SW-4510.....	113
Tabla 54: Habilitar y configurar protocolo 802.1X switch cisco 4510.....	114

RESUMEN

El presente proyecto consiste en el diseño de un sistema de seguridad a nivel de capa de enlace de datos en redes cableadas mediante el estándar IEEE 802.1X en la LAN de la Universidad Técnica del Norte, el cual se lo desarrolla con el objetivo de aumentar el nivel de seguridad presente en la institución. El empleo de este protocolo permite asegurar que solo usuarios previamente validados puedan acceder a los servicios presentes en la red, dando seguridad en puertos.

En primer lugar, se realiza un estudio del funcionamiento del estándar IEEE 802.1X y sus distintos métodos EAP de autenticación, con el fin de determinar cuál es el más idóneo para el diseño del sistema. A su vez, se detalla todos los elementos propios de un servidor AAA (Autenticación, Autorización, Contabilidad).

Se efectúa un análisis de la situación actual de la red en la casona universitaria para identificar los switch con los que cuenta y a su vez establecer cuales soportan el estándar IEEE 802.1X. A continuación, se realiza el diseño del sistema teniendo en cuenta los switch en la capa de acceso y distribución presente en todas las dependencias.

Finalmente, se levanta un servidor AAA y se realiza pruebas de funcionamiento en un ambiente controlado dentro de la infraestructura de red de la Facultad de Ingeniería en Ciencias Aplicadas. Este apartado demuestra que el diseño es ejecutable y se puede replicar dentro de cualquier ubicación de la Universidad.

ABSTRACT

The present project consists of the design of a security system at the level of data link layer in wired networks through the IEEE 802.1X standard in the LAN of the Technical University of the North, which is developed with the objective of increasing the level of security present in the institution. The use of this protocol ensures that only previously validated users can access the services present in the network.

First of all, a study is made of the operation of the IEEE 802.1X standard and its different EAP authentication methods, in order to determine which is the most suitable for the design of the system. In turn, it details all the elements of an AAA server (Authentication, Authorization, Accounting).

An analysis of the current situation of the network in the university house is made to identify the switches it has and in turn establish which support the IEEE 802.1X standard. Next, the system design is determined taking into account the access and distribution layer present in all the dependencies.

Finally, an AAA server is raised and tests are performed in a controlled environment within the network infrastructure of the Faculty of Engineering in Applied Sciences. This section shows that the design is executable and can be replicated within any location of the University.

Capítulo I

Introducción

1.1 Tema

Diseño de sistema de seguridad a nivel de capa de enlace de datos en redes cableadas mediante el estándar IEEE 802.1X en la LAN de la Universidad Técnica del Norte.

1.2 Problema

En todas las compañías o campus universitarios se manejan datos y configuraciones sensibles que requieren tener un nivel alto de seguridad. Para un administrador de red, la seguridad es un tema muy significativo dentro de una infraestructura de red. No solo debe limitarse al cuidado y buen funcionamiento de la red procedente del tráfico exterior, vigilancia y toma de acciones en la red externa; sino que también tiene que preservar la seguridad en la red interna que habitualmente no se le presta las medidas pertinentes. Al no poseer los controles suficientes y también por confiar en los usuarios que usan la red, se tiene puntos de vulnerabilidad los cuales pueden ser explotados por personas mal intencionadas. Por ello es importante tener criterios de seguridad para avalar que el equipo terminal este controlado en su acceso y sea un usuario válido; “ser quien dice ser”. Los daños que puede generar la falta de control en las redes cableadas por no autenticar a los usuarios son muy diversos según la naturaleza del ataque al que es objeto, ya sea negación de servicio, modificación, autenticación, etc. También existe daños involuntarios por parte de los estudiantes al realizar sus prácticas de laboratorio que puede afectar a la topología de la red de la universidad.

En la actualidad la Universidad Técnica del Norte cuenta con una infraestructura de red que es administrada por la Dirección de Desarrollo Tecnológico e Informático (DDTI) ubicado en el edificio central, el cual cuenta con un despliegue de seguridad perimetral que posee

distintos equipos y configuraciones que gestionan el tráfico entre la red externa y la red interna. La importancia de preservar la red de los ataques internos da lugar a expandir los niveles de seguridad y enfocarse en una seguridad integral que abarque tanto los posibles ataques desde fuera de la red como los procedentes de su interior.

Para consolidar la seguridad que se encuentra implementada en la UTN, se efectuará el estudio para los posibles cambios de configuraciones en la red interna a nivel de switch. El diseño ayudará a controlar la seguridad interna de la red enfocándose en la capa de acceso y no en recursos ni servicios de esta. Al valerse de este mecanismo se establece el acceso a la red a través de puertos de switch mediante la autenticación; solo permitiendo el acceso a la red a los usuarios previamente validados.

1.3. Objetivos

1.3.1. Objetivo General

Diseñar el sistema de seguridad a nivel de capa de enlace de datos en redes cableadas mediante el estándar IEEE 802.1X en la LAN de la Universidad Técnica del Norte.

1.3.2. Objetivo Específicos

- Definir el funcionamiento del estándar IEEE 802.1X y sus distintos métodos de autenticación.
- Identificar los dispositivos que trabajan en la capa de enlace de datos que soporten el estándar IEEE 802.1X en redes cableadas.
- Diseñar el sistema de seguridad dentro de la Universidad Técnica del Norte.
- Realizar pruebas de funcionamiento en un ambiente controlado dentro de la infraestructura de red de la Facultad de Ingeniería en Ciencias Aplicadas (FICA).

1.4. Alcance

Para elaborar el proyecto inicialmente se comprenderá el funcionamiento del estándar IEEE 802.1X abarcando términos propios del estándar tales como suplicante, NAS, servidor Radius, entre otros e identificando cual es el método de autenticación más adecuado para la realización del proyecto. A continuación, el proceso de desarrollo técnico se establece en cuatro fases.

La primera fase es el levantamiento de información de equipos, situación actual de la red y análisis de compatibilidad con el estándar 802.1X. Para realizar esta fase se contará con la ayuda de la Dirección de Desarrollo Tecnológico e Informático (DDTI) ubicado en el edificio central y el ingeniero encargado de la administración de la red de la Facultad de Ingeniería en Ciencias Aplicadas (FICA).

Como segunda fase se desarrolla el diseño de seguridad en capa de enlace sobre los equipos que conforman la topología de red de la Universidad Técnica Del Norte. Enfocándose en conceptos como red acceso, seguridad de puertos, control MAC como prebendas para garantizar la seguridad.

La siguiente fase consiste en el levantamiento de un servidor Radius que permita comprobar que la información de usuarios que accedan a la red es correcta utilizando esquemas de autenticación enlazado con una LDAP y las configuraciones pertinentes dentro del switch.

La última fase consiste en realizar pruebas de funcionamiento en un ambiente controlado dentro de la infraestructura de red de la Facultad de Ingeniería en Ciencias Aplicadas (FICA). Esta última fase permitirá demostrar que el sistema previamente diseñado en este comportamiento es ejecutable, por lo que mediante la entrega de manuales tanto de

administrador como de usuario se garantizará que a partir del estudio se puede usar para una futura implementación.

El sistema será una primera etapa enmarcada en la seguridad interna de la red, por ello se tendrá en cuenta recomendaciones a manera de políticas que pueden ser desarrolladas posteriormente.

1.5. Justificación

En la actualidad la Universidad Técnica del Norte cuenta con un despliegue de seguridad perimetral que posee distintos equipos y configuraciones que gestionan el tráfico entre la red externa y la red interna en su infraestructura de red, que la asegura de los ataques informáticos. La red de la institución es objeto de continuos ataques por personas que quieren acceder a la información dentro de la red o causar algún daño.

Los atacantes van mejorando sus técnicas e investigando nuevas formas para vulnerar las seguridades implementadas en la topología de red. Dada la importancia de los datos e información que viajan a través de la infraestructura de red de la Universidad Técnica del Norte se ha visto la necesidad de ampliar la seguridad de la red para posibles ataques internos, para lo cual se trabajará en seguridad a nivel de los puertos de acceso del switch.

A pesar de que el Código Orgánico Integral Penal (COIP) establece sanciones de acuerdo con los delitos informáticos expuestos en los artículos Art. 178 violación a la intimidad y Art. 229 revelación ilegal de bases de datos, esto no ahuyenta a los posibles atacantes y buscan formas para vulnerar la red. Por ello siguiendo la línea de investigación “Desarrollo, aplicación de software y cyber security” que persigue la Universidad Técnica del Norte y específicamente la propuesta por la Facultad De Ciencias Aplicadas (FICA) “Innovación y Transferencia Tecnológica”. Este proyecto arrojará información e identificará los

emplazamientos donde se puede dar seguridad a nivel de enlace de datos y así elevar los niveles de seguridad integral.

Capítulo II

Marco Teórico

2.1 Estándar IEEE 802.2

La capa de enlace de datos asegura la entrega de datos entre nodos; usando las direcciones físicas de los nodos; control de flujo de datos y proporciona una notificación de error a las capas superiores cuando un dato tiene un error de transmisión. (Sandberg, 2015)

El IEEE divide la capa de enlace de datos en dos subcapas: el enlace lógico Subcapa de control (LLC¹) y subcapa de control de acceso a medios (MAC²).

El encabezado de la subcapa LLC contiene información sobre el comando, la respuesta y el número de secuencia para admitir el servicio orientado a la conexión y sin conexión a la capa de enlace. A su vez contiene un campo de control para reconocimiento de datos, recuperación de errores y control de flujo que son necesarios para la entrega confiable y orientada a la conexión en la capa de enlace. (Wu & Irwin, 2013)

La subcapa MAC define el formato de trama, incluidos el encabezado MAC y el trailer. El encabezado de MAC contiene direcciones MAC de origen y de destino, y el trailer información de detección de errores. (Wu & Irwin, 2013)

El formato de la trama 802.2 consta de DSAP, SSAP, control y datagrama IP como muestra la Figura 1.

DSAP	SSAP	Control	IP
8 bits	8 bits	8 o 16 bits	Datagram

Figura 1: Formato de la trama 802.2

Fuente: (Wu & Irwin, 2013)

SSAP (Punto de acceso de servicio de origen)
DSAP (Punto de acceso de servicio de destino)

¹ Control de enlace lógico.

² El control de acceso a medios.

2.2 Estándar IEEE 802.3

En este apartado se explica las principales características que posee el estándar IEEE³ 802.3 tales como; control de acceso al medio, formato de la trama, comparación de tecnologías y velocidades.

2.2.1 Introducción a Ethernet.

El estándar IEEE 802.3 describe el nivel físico y el subnivel MAC de una familia de redes de área local que usan un medio de transmisión de difusión (con topología de bus en su origen) al que acceden las estaciones según un protocolo de acceso aleatorio de tipo CSMA/CD (Carrier Sense Multiple Access / Collision Detection). (Sandberg, 2015)

Para acceder al medio emplea CSMA⁴ 1-persistente, las estaciones que pretendan transmitir lo hacen tan rápido como detecten que el medio está libre. Con ello se intenta reducir los tiempos muertos en el medio, llegando a reducir el retardo de acceso. La descripción del funcionamiento del algoritmo, de acuerdo con el libro *Data And Computer Communications* (Stallings, 2013) son las siguientes:

1. Si el medio está inactivo, transmita; de lo contrario, vaya al paso 2.
2. Si el medio está ocupado, continúe escuchando hasta que el canal esté inactivo, luego transmita de inmediato.
3. Si se detecta una colisión durante la transmisión, transmita una breve señal de interferencia para asegurarse de que todas las estaciones saben que ha habido una colisión y luego cese la transmisión.

³ Instituto de Ingenieros Eléctricos y Electrónicos.

⁴ Acceso múltiple con escucha de portadora.

4. Después de transmitir la señal de interferencia, espere un tiempo aleatorio, referido como el retardo, luego intente transmitir nuevamente (repita desde el paso 1).

2.2.2 Formato de la trama Ethernet.

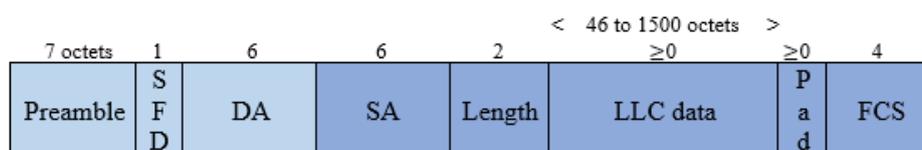
La subcapa MAC tiene dos responsabilidades principales, de acuerdo con el libro Introduction to Networks (CISCO, 2014) que son:

- Encapsulación de datos, incluido el ensamblaje de trama antes transmisión, y análisis de trama / detección de errores durante y después de la recepción.
- Control de acceso a los medios, incluida la iniciación de la transmisión de tramas y recuperación de la falla de la transmisión.

El formato de la trama ethernet consta de los siguientes elementos (Stallings, 2013) y (CISCO, 2014) como se muestra en la Figura 2:

- Preámbulo (Pre) - 7 bytes. El PRE es una alternancia patrón de unos y ceros que le dice a las estaciones receptoras que viene una trama, y que proporciona un medio para sincronizar las porciones de recepción de fotograma de recepción capas físicas con el flujo de bits entrante.
- Inicio de trama (SFD) -1 byte. La SFD es un patrón alterno de unos y ceros, que termina con dos bits consecutivos de 1 que indican que el siguiente bit es el bit más a la izquierda en el byte más a la izquierda del destino dirección.
- Dirección de destino (DA) - 6 bytes. El campo DA identifica qué estación o estaciones debe recibir la trama.
- Direcciones de origen (SA) - 6 bytes. El campo SA identifica la estación de envío.

- Longitud / Tipo- 2 bytes. Este campo indica el número de bytes de datos MAC-cliente que están contenidos en el campo de datos de trama, o el tipo de trama ID⁵ si la trama se ensambla utilizando un formato opcional.
- Datos: es una secuencia de n bytes ($46 = <n = <1500$) de algún valor. El mínimo total de trama es de 64bytes.
- Secuencia de verificación de trama (FCS⁶) - 4 bytes. Esta secuencia contiene una verificación de redundancia cíclica de 32 bits (CRC⁷) valor, que es creado por el MAC que envía y es recalculado por el MAC receptor para verificar las tramas dañadas



SFD = Start of frame delimiter

DA = Destination address

SA = Source address

FCS = Frame check sequence

Figura 2: Formato de la trama IEEE 802.3

Fuente: (*Stallings, 2013*)

2.2.3 Tecnología y velocidades de Ethernet.

El estándar IEEE 802.3 define una cantidad de configuraciones físicas variables y ha desarrollado una notación concisa que se explicará por medio de tablas. Teniendo en cuenta la tecnología empleada, la técnica de señalización, la topología que soporta, longitud máxima del segmento, data rate entre otras características. Como se muestra a continuación en la Tabla 1, Tabla 2 y Tabla 3.

⁵ Identificador.

⁶ Secuencia de verificación de trama.

⁷ Verificación de redundancia cíclica.

Tabla 1: *IEEE 802.3 10BASE 10-Mbps*

	10BASE5	10BASE2	10BASE-T	10BASE-FP
Medio de Tx	Cable coaxial (50 ohm)	Cable coaxial (50 ohm)	Unshielded par trenzado	850-nm óptica par de fibra
Codificación	Manchester	Manchester	Manchester	Manchester on-off
Topología	Bus	Bus	Estrella	Estrella
Longitud máx. segmento (m)	500	185	100	500
Nodos por segmento	100	30	-	33
Diámetro cable (mm)	10	5	0,4 a 0,6	62.5/125 μ m

Fuente: Adaptado de (Stallings, 2013)

Tabla 2: *IEEE 802.3 100BASE-T*

	100BASE-TX	100BASE-FX	100BASE-T4
Medio de Tx	2 pares, STP ⁸	2 pares, Cat 5 UTP ⁹	2 fibras ópticas 4 pares, Cat 3, 4, o 5 UTP
Codificación	MLT-3 ¹⁰	MLT-3	4B5B, NRZI ¹¹ 8B6T, NRZ
Data rate	100 Mbps	100 Mbps	100 Mbps
Longitud máx. segmento (m)	100 m	100 m	100 m
Alcance de la red	200 m	200 m	400 m 200 m

Fuente: Adaptado de (Stallings, 2013)

⁸ Cable par trenzado blindado.⁹ Cable par trenzado sin blindaje.¹⁰ Transmisión multinivel.¹¹ No Retorno al Cero Invertido.

Tabla 3: *IEEE 802.3 1000BASE-T*

	100BASE-SX	100BASE-LX	100BASE-CX	100BASE-T
Medio de Tx	Fibra óptica (multimodo)	Fibra óptica (multi o monomodo)	STP	UDP
Codificación	8B/10B	8B/10B	8B/10B	PAM ¹² 5x5
Señal	Láser de onda corta	Láser de onda larga	Eléctrica	Eléctrica
Distancia máx.	550 m	550 m multimodo 50000 m monomodo	25 m	100 m

Fuente: Adaptado de (Stallings, 2013)

2.3 Conmutación en IEEE 802.3

Para la transmisión de datos más allá de un área local, la comunicación se logra mediante la transmisión de datos desde el origen hasta el destino a través de una red de nodos de conmutación intermedios. Los nodos de conmutación no se preocupan por el contenido de los datos; más bien, su propósito es proporcionar una instalación de conmutación que moverá los datos de nodo a nodo hasta que lleguen a su destino. (Stallings, 2013)

Los switch tienen una tabla de conmutación y las entradas en esta tabla son la dirección MAC de un host, la interfaz para llegar al host y una marca de tiempo o TTL¹³ (Time to Live). Estas entradas en la tabla MAC se crean y mantienen mediante un proceso de aprendizaje. (Wu & Irwin, 2013)

¹² Modulación de Amplitud de Pulso.

¹³ Tiempo de vida.

Cuando se recibe una trama, el switch aprende el número de puerto del emisor o del segmento LAN entrante, y registra la dirección MAC del remitente y el par de número de puerto en una tabla del switch. De esta manera, el switch aprende cómo llegar a cada host.

2.3.1 Switch no administrable.

Los switch de capa 2 son dispositivos de capa de enlace; desarrollan y mantienen tablas de switch e implementan algoritmos de filtrado y aprendizaje. (Wu & Irwin, 2013)

Hay dos tipos de switches de capa 2 según el libro *Data And Computer Communications* (Stallings, 2013) que son:

- Store-and-forward switch: el conmutador de capa 2 acepta una trama en una línea de entrada, lo almacena brevemente y luego lo encamina a la línea de salida adecuada.
- Cut-through switch: el interruptor de capa 2 aprovecha el hecho de que la dirección de destino aparece al comienzo de la trama MAC. El switch de capa 2 comienza a repetir la trama entrante en la línea de salida apropiada tan pronto como el switch reconoce la dirección de destino.

2.3.2 Switch administrable.

Los switches de Capa 3 han reemplazado la necesidad de decisiones lógicas de software y algunos de los que dependen de los enrutadores con circuitos integrados para realizar estas tareas. Toman decisiones de enrutamiento basadas en la misma información de tabla de enrutamiento que un enrutador tradicional. (Wu & Irwin, 2013)

Existen varios esquemas de capa 3 diferentes y se dividen en dos categorías. El switch de paquete por paquete funciona de la misma manera que un enrutador tradicional. Debido a que la lógica de reenvío está en el hardware. También el switch basado en flujo intenta mejorar

el rendimiento identificando flujos de paquetes IP que tienen el mismo origen y destino. (Kim & Solomon, 2018).

2.3.2.1 Bridge Protocol Data Units (BPDU).

Una unidad de datos de protocolo de puente (BPDU¹⁴) es un mensaje de datos transmitido a través de una red de área local para detectar bucles en topologías de red. Una BPDU contiene información sobre puertos, conmutadores, prioridad de puerto y direcciones.

Las BPDU contienen la información necesaria para configurar y mantener la topología de árbol de expansión. No son reenviados por switches, pero los switches utilizan la información para calcular sus propias BPDU para el paso de información.

Cuando los dispositivos se conectan inicialmente a los puertos del conmutador, no inician la transmisión de datos de inmediato. En cambio, se mueven a través de diferentes estados mientras que el procesamiento de BPDU determina la topología de la red.

2.3.2.2 Spanning Tree Protocol (STP).

Spanning Tree Protocol (STP¹⁵) es un protocolo de Capa 2 el cual asegura una topología libre de bucles para cualquier LAN¹⁶ en puente. Crea un árbol de expansión dentro de una red interconectados típicamente switches Ethernet, al deshabilitar los enlaces que no son parte de un árbol particular dejando una sola ruta activa entre dos estaciones de red. (Wu & Irwin, 2013)bb

¹⁴ Unidad de Datos de Protocolo de Puente.

¹⁵ Protocolo de Árbol de Expansión.

¹⁶ Red de Área Local.

STP proporciona enlaces redundantes que generan rutas de respaldo automáticas si falla un enlace activo, sin el peligro de bucles de puente, o la necesidad de habilitar / deshabilitar manualmente estos enlaces de respaldo. (Wu & Irwin, 2013)

2.3.2.3 Root Bridge (Puente Raíz).

El puente raíz del árbol de expansión es el puente con el ID de puente más pequeño (más bajo) y un número de prioridad configurable. Un número de prioridad configurable es controlado por el administrador que selecciona el puente raíz. (Wu & Irwin, 2013)

Según el libro *Introduction to Computer Networks and Cybersecurity* (Wu & Irwin, 2013) la prioridad se compara primero y el puente con el número de prioridad más pequeño se designa como el puente raíz. Si la prioridad es la misma, entonces el puente con la ID más pequeña se designa como el puente raíz. Los puentes colectivamente determinan qué puente tiene la ruta de menor costo desde el segmento de red a la raíz. Como muestra la Figura 3.

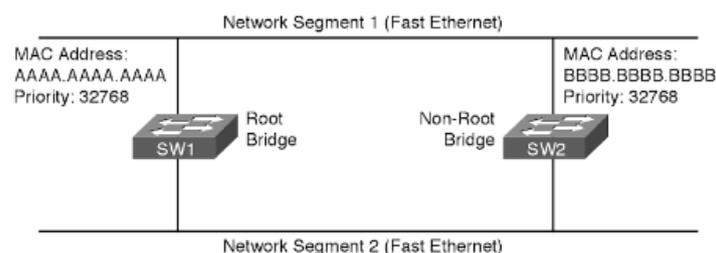


Figura 3: Elección root bridge
Fuente: (Barker & Wallace, 2015)

2.3.2.5 Puertos designados.

Cada segmento de red tiene un solo puerto designado, que es el puerto en ese segmento que está más cerca del puente raíz, en términos de costo. Por lo tanto, todos los puertos en un puente raíz son puertos designados. (Barker & Wallace, 2015)

2.3.2.6 Puertos no designados.

Los puertos bloquean el tráfico para crear una topología sin bucles, puertos en estado de bloqueo.

2.3.2.7 Estados de los puertos.

La siguiente tabla identifica cada uno de los estados en los cuales puede funcionar un puerto y a su vez un esquema donde se ve la transición de cada estado. Como muestra a continuación en la Tabla 4 y Figura 4.

Tabla 4: *STP estado de puertos*

Estado del puerto	Descripción
Disabled	El puerto está administrativamente inactivo y no puede enviar ni recibir ninguna trama.
Blocking	El puerto solo puede recibir tramas STP; no puede enviar tramas STP ni reenviar tramas de datos de usuario.
Listening	El puerto puede enviar y recibir tramas STP, pero no puede aprender la dirección MAC o no puede reenviar tramas de datos de usuario
Learning	El puerto puede enviar y recibir tramas STP y puede aprender la dirección MAC, pero no puede reenviar tramas de datos de usuario
Forwarding	El puerto puede enviar y recibir tramas STP, aprender la dirección MAC y reenviar tramas de datos de usuario

Fuente: Adaptado de (Huawei Technologies Co., 2016)

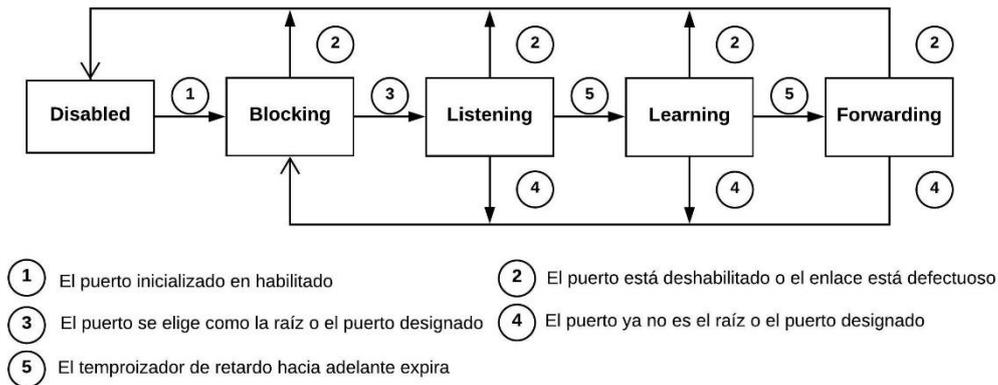


Figura 4: Transición de estado del puerto
Fuente: Adaptado de (Huawei Technologies Co., 2016)

2.3.2.8 Temporizadores.

Los temporizadores que operan en STP son el de hello, forward-delay y max-age; son los encargados de determinar las características de operación.

Según el libro *NX-OS and Cisco Nexus Switching: Next-Generation Data Center* (Fuller, Jansen, & McPherson, 2013) los temporizadores funcionan de la siguiente manera:

- Hello define la frecuencia con la que bridge envía BPDU a los dispositivos conectados. El valor predeterminado es de 2 segundos, pero se puede configurar de 1 a 10 segundos.
- Forward-delay especifica cuánto tiempo permanece el bridge en los estados de escucha y aprendizaje antes de pasar a una estancia de reenvío. Espera 15 segundos antes de pasar el puerto de escuchar para aprender, y de aprender a reenviar. El temporizador de retardo directo se puede configurar de 15 a 30 segundos.
- Max-age sirve para garantizar la compatibilidad con los entornos stp 802.1D tradicionales especificando el tiempo que se almacena una BPDU en un puerto determinado. El tiempo es de 20 segundos y se puede configurar de 6 a 40 segundos.

2.4 Principios de seguridad en una red

Hay tres conceptos claves que cualquier persona que proteja un sistema de información debe comprender (CIA): confidencialidad, integridad y disponibilidad. Los profesionales de la seguridad de la información se dedican a garantizar la protección de estos. Además, hay tres conceptos que se deben comprender para hacer cumplir los principios de la CIA correctamente: autenticación, autorización y no repudio. (Kim & Solomon, 2018)

2.4.1 Confidencialidad.

La confidencialidad es la garantía de que la información no se divulga a personas, procesos o dispositivos no autorizados. Asegurar que las partes no autorizadas no tengan acceso es a una tarea compleja. (Kim & Solomon, 2018)

2.4.2 Integridad.

Implica controles para preservar la confiabilidad y precisión de los datos y procesos contra la modificación no autorizada. Los controles de integridad incluyen defensas de malware, protección contra la corrupción o eliminación de datos, código de validación etc. (Barrett, Weiss, & Hausman, 2015)

2.4.3 Disponibilidad.

Implica controles para preservar las operaciones y los datos frente a fallas de servicio, desastre o variación de capacidad. Los controles de disponibilidad incluyen equilibrio de carga, servicios redundantes y hardware, soluciones de respaldo y controles destinados a superar interrupciones que afecten a las redes. (Barrett, Weiss, & Hausman, 2015)

2.4.4 Autenticación.

Este es un proceso en el que las credenciales se comparan con lo que se almacena en el archivo durante una interacción. La autenticación es un método para identificar quién está solicitando o intentando el acceso. (Deng, Weng, Ren, & Yegneswaran, 2016)

2.4.5 Autorización.

Método que otorgar acceso a recursos especificados. Este es otra forma de control de acceso. Al intentar obtener acceso a un recurso dentro de un entorno, la autorización únicamente permitirá que el individuo autenticado con la autorización correcta pueda acceder al recurso. (Deng, Weng, Ren, & Yegneswaran, 2016)

2.4.6 No repudio.

No repudio es la garantía de que el remitente de los datos está provisto con la prueba de la entrega y se proporciona una prueba de la identidad del remitente, por lo que ninguno de los dos puede negarlo habiendo procesado los datos. (Kim & Solomon, 2018)

2.4.7 Amenaza.

La amenaza de seguridad para los sistemas informáticos surge de una serie de factores que incluyen debilidades en la infraestructura de red y protocolos de comunicación que crean una puerta para posibles ataques de hackers. (Kizza, 2015)

2.4.8 Vulnerabilidad.

La vulnerabilidad del sistema se define como una condición, una debilidad o ausencia de un procedimiento de seguridad, o controles técnicos, físicos u otros que podrían ser explotados por una amenaza. (Kizza, 2015)

2.4.9 Ataque.

Un ataque es una amenaza a la seguridad de la información que involucra un intento de obtener, alterar, destruir, eliminar, implantar o revelar información sin acceso o permiso autorizado. Le sucede a individuos y organizaciones. (Wu & Irwin, 2013)

2.5 Protocolos de autenticación

En este apartado se explica el funcionamiento del estándar IEEE 802.1X, los términos propios del mismo y los distintos métodos de autenticación EAP¹⁷ (Protocolo de Autenticación Extensible).

2.5.1 IEEE 802.1X.

Estándar para el control de acceso a la red basado en el puerto en una LAN. 802.1X proporciona autenticación basada en puertos para comunicaciones de tres partes que involucran un Suplicante, Autenticador y Servidor de Autenticación. (Wu & Irwin, 2013)

El estándar IEEE 802.1X usa el Protocolo de Autenticación Extensible (EAP) sobre una LAN alámbrica o inalámbrica. Se usa para el control de acceso, proporcionando capacidad de permitir o denegar la conectividad de red, controlar el acceso de VLAN¹⁸ y aplicar la política de tráfico, basada en la identidad del usuario o de la máquina. (Barrett, Weiss, & Hausman, 2015)

El proceso de 802.1X para la autenticación con EAP y Radius consta de cuatro pasos, como muestra la Figura 5.

¹⁷ Protocolo de Autenticación Extensible.

¹⁸ Red de Área Local Virtual.

1. Inicialización, después de que el autenticador detecta que un dispositivo está conectado a su puerto, este puerto se establece en estado "no autorizado" y solo permitirá el tráfico 802.1X. Otro tráfico, como UDP o TCP no está permitido.
2. Iniciación, el autenticador solicitará la identidad del suplicante. Cuando el autenticador recibe esta información lo reenviará al servidor de autenticación por medio del protocolo RADIUS.
3. Negociación, el servidor de autenticación verifica la identidad del suplicante y envía un desafío al suplicante a través del autenticador. Este desafío también contiene el método de autenticación, que podría basarse en un nombre de usuario y contraseña.
4. Autenticación, el servidor de autenticación y el suplicante acuerdan un método de autenticación y el suplicante responderá con el método apropiado al proporcionar sus credenciales configuradas. Si la autenticación es exitosa, el autenticador permite al suplicante acceso a los recursos de red definidos. Como muestra la Figura 5.

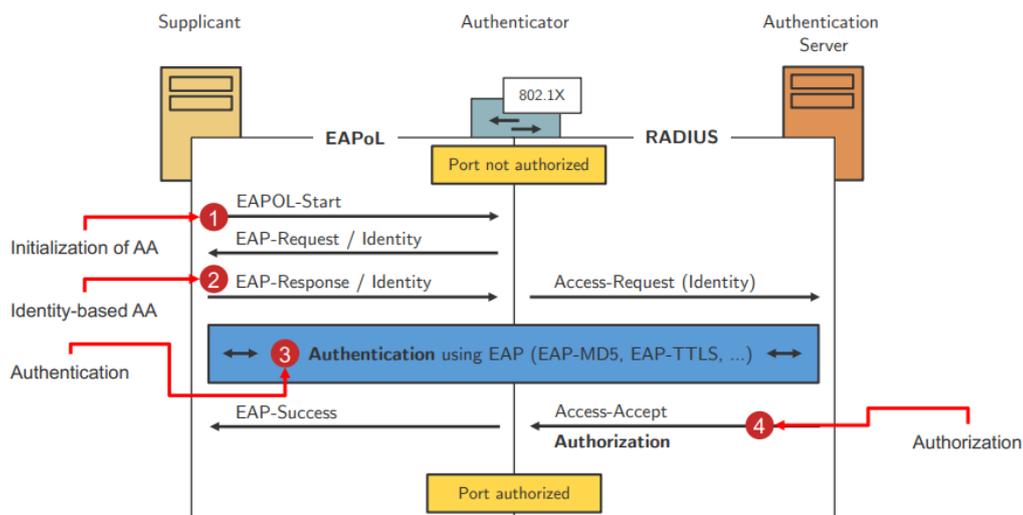


Figura 5: 802.1X para la autenticación de usuario de LAN
Recuperado: Adaptado de (Junipers, 2016)

2.5.1.1 Suplicante.

Un adaptador de red de una estación de trabajo, o referirse como cliente, puede desempeñar el papel del suplicante. Un puerto de elemento de red también puede ser un suplicante. Los ejemplos son, el puerto del switch que se conecta al puerto de otro switch, y un puente no raíz inalámbrico que se conecta a un puente inalámbrico raíz. (Wu & Irwin, 2013)

2.5.1.2 Autenticador NAS (Network Access Server).

“El Autenticador es típicamente un conmutador Ethernet o un punto de acceso inalámbrico (punto de aplicación)”. (Wu & Irwin, 2013, p1130)

El autenticador es un punto de acceso inalámbrico o conmutador (acceso a la red NAS¹⁹). El autenticador mantiene la red (WLAN ²⁰o LAN) en estado cerrado a todo el tráfico no autenticado. No hace autenticación directamente, sino que requiere un protocolo de autenticación extensible a un servidor de autenticación.

2.5.1.3 Servidor de autenticación.

“Servidor de Autenticación emplea elementos como un servidor de Servicio de Usuario de Acceso Remoto (RADIUS), Kerberos y el Directorio Liger Protocolo de acceso (LDAP) o Active Director”. (Wu & Irwin, 2013, p1130).

El servidor de autenticación almacena los nombres de usuario, las contraseñas y verifica que el valor correcto se envió antes de autenticar al usuario.

¹⁹ Servidor de acceso a red

²⁰ Red de Área Local Inalámbrica

2.5.2 Autenticación EAP.

EAP aborda el requisito de desacoplar un protocolo de autenticación del protocolo de transporte que lo transporta. Esto permite que el protocolo EAP sea transportado por protocolos de transporte, tales como 802.1X, UDP o RADIUS sin cambios en el protocolo de autenticación. (Cisco, 2013)

Una trama EAP consta de los siguientes campos como muestra la Figura 6.

- Código: identifica el tipo de paquete EAP
 - 1 = Request
 - 2 = Response
 - 3 = Success
 - 4 = Failure
- Identificador: utilizado para unir respuestas y solicitudes.
- Longitud: indica la longitud del paquete EAP, incluidos el encabezado y los datos.
- Datos: contiene los datos de la trama EAP, como la negociación TLS²¹.

Code (1 byte)	Identifier (1 byte)	Packet Length (2 bytes)
Data (0+ bytes)		

Figura 6: Formato trama EAP
Recuperado: (Adler, 2014)

El tipo de EAP determina la naturaleza de la trama EAP. Hay una variedad de tipos de EAP disponibles. Algunos ejemplos de los tipos de EAP son:

- EAP-TLS (Type 13)
- EAP-TTLS²² (Type 21)

²¹ Seguridad de la capa de transporte.

²² Seguridad de la capa de transporte en túnel

- EAP-PEAP²³ (Type 25)
- EAP-FAST (Type 43)

Según el documento *CI Network Security de Cisco* (Cisco, 2013), EAP está compuesto por cuatro tipos de paquetes. Como se muestra a continuación en la Figura 7.

- EAP request: el autenticador envía el paquete de solicitud al suplicante. Cada solicitud tiene un tipo campo que indica qué se está solicitando, como la identidad del solicitante y el tipo de EAP que se utilizará. Un número de secuencia permite que el autenticador y el par coincidan con una respuesta EAP para cada EAP solicitud.
- EAP request: el solicitante envía el paquete de respuesta al autenticador y utiliza una secuencia número para que coincida con la solicitud EAP de inicio. El tipo de respuesta EAP generalmente coincide con el Solicitud de EAP, a menos que la respuesta sea NAK²⁴.
- EAP success: el autenticador envía el paquete de éxito luego de la autenticación exitosa al suplicante.
- EAP failure: el autenticador envía el paquete de falla luego de una autenticación fallida al suplicante.

²³ Protocolo de autenticación extensible protegido

²⁴ Reconocimiento Negativo.

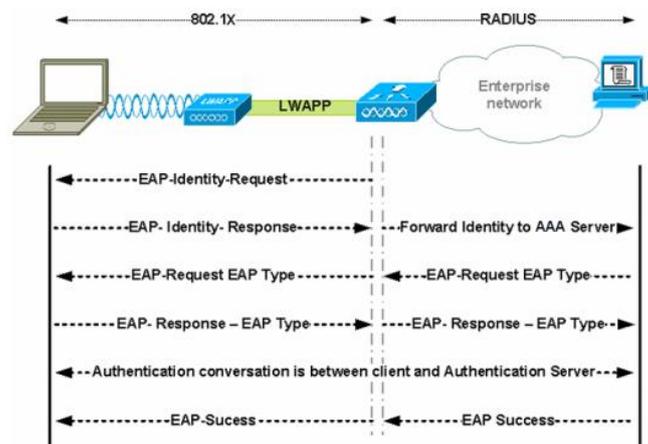


Figura 7: Mensajes del protocolo EAP
Recuperado: (Cisco, 2013)

Cuando se usa el protocolo EAP sobre LAN se llama EAPOL²⁵, este es simplemente una manera de transportar paquetes EAP de un suplicante al autenticador. En este caso, el solicitante es un usuario con un ordenador conectado a un puerto Ethernet, y el autenticador es el conmutador con capacidad para 802.1X que el usuario está conectado. (Wright & Cache, 2015)

La negociación del protocolo EAPOL se describe en la figura 8 y además se explica cada uno de los mensajes que se realizan en la negociación.

- EAPOL-packet: estos paquetes son simples contenedores para el transporte de paquetes EAP a través de una LAN, por ejemplo, la computadora de un usuario para el switch o punto de acceso habilitado para 802.1X.
- EAPOL-start: el solicitante puede usar este paquete para informar al autenticador que desea autenticarse. En muchos casos, esto es innecesario, ya que el autenticador puede percibir el solicitante está conectado antes de transmitir un mensaje de inicio EAPOL.

²⁵ Protocolo de Autenticación Extensible sobre LAN

- EAPOL-logout: este mensaje informa al autenticador de que el solicitante está desconectando de la red también innecesaria en muchos casos.
- EAPOL-key: el estándar 802.1X proporciona soporte para la distribución de claves, lo cual es muy importante cuando se trata de proteger las redes.

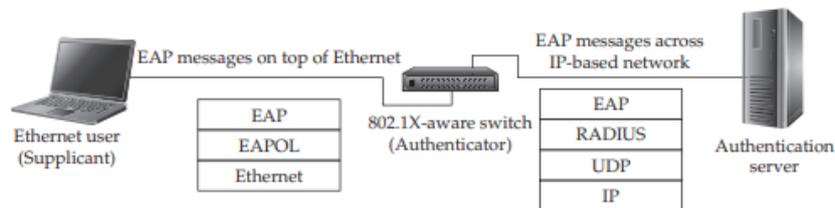


Figura 8: La negociación de los cuatro tipos básicos de mensajes EAPOL
Fuente: (Wright & Cache, 2015)

2.5.2.1 Transport Layer Security (EAP-TLS).

El método EAP-Transport Layer Security (EAP-TLS) para autenticación mutua. EAP-TLS utiliza tanto el certificado del servidor para autenticar el servidor para suplicantes, como un certificado de cliente que el servidor de autenticación verifica para establecer la identidad del solicitante. (Elenkov, 2015)

Conceder acceso a la red requiere emitir y distribuir certificados de cliente, y así mantener una infraestructura de clave pública. Se puede bloquear el acceso de los clientes existentes a la red revocando sus certificados de solicitante. (Elenkov, 2015)

El formato del mensaje EAP-TLS, como muestra la figura 9

Code	Identifier	Length	'13'	Flags	Length	EAP-TLS Data
------	------------	--------	------	-------	--------	--------------

Figura 9: Formato del mensaje EAP-TLS.
Fuente: (Baheti, 2015)

Durante el Handshake, el servidor y el cliente intercambiarán información importante sobre las propiedades bajo las cuales se establecerá la conexión. Se usa un híbrido de encriptación asimétrica y simétrica para garantizar la seguridad. El Handshake que ocurre

mediante la interacción entre cliente y servidor con el método de autenticación EAP-TLS se muestra en la Figura 10 y Figura 11.

1. Client Hello, el cliente envía un saludo “Hello” con los siguientes componentes:
 - Client_version: lista de todas las versiones del protocolo TLS.
 - Random: datos aleatorios de 32 bytes, 4 bytes representan la fecha y hora actual del cliente (en formato epoch²⁶) y los 28 bytes restantes, un número generado aleatoriamente. Los datos aleatorios del cliente y del servidor se usarán posteriormente para generar la clave con la que se cifrarán los datos.
 - session_id: identificación de la sesión que se usará para la conexión.
 - compression_methods: el método que se usará para comprimir los paquetes SSL.
 - cipher_suites: los conjuntos de cifrado son una combinación de algoritmos criptográficos que se utilizan para definir la seguridad general de la conexión que se establecerá.
2. Server Hello, si encuentra un conjunto aceptable de algoritmos en la solicitud del cliente, responderá al aceptar esas opciones y proporcionar su certificado. Si el servidor no cumple con los requisitos del cliente, responderá con un mensaje de falla de saludo.
 - server_version: el servidor seleccionará la versión preferida del cliente del protocolo TLS.
 - Random: igual que en el apartado del cliente.

²⁶ El tiempo epoch es un sistema de referencia medido en número de segundos desde la época Unix.

- `session_id`: es la identificación de la sesión que se usará para la conexión.
 - `compression_methods`: si es compatible, el servidor acordará el método de compresión preferido del Cliente.
 - `cipher_suites`: si es compatible, el servidor acordará el conjunto de cifrado preferido del Cliente.
3. `Server certificate`, da el certificado firmado del servidor que demuestra la identificación del cliente. También contiene la clave pública del servidor.
 4. `Server Key Exchange`, el mensaje de intercambio de clave del servidor se envía solo si el certificado proporcionado por el servidor no es suficiente para permitir que el cliente intercambie una clave pre-maestra.
 5. `Server Hello Done`, se envía al cliente como una confirmación de que el mensaje Hola del servidor se ha completado.
 6. `Client Key Exchange`, el mensaje de intercambio de clave de cliente se envía inmediatamente después de que se recibe el servidor Hello Done del servidor. Si el servidor solicita un certificado de cliente, se enviará el intercambio de clave de cliente después de eso. Durante esta etapa, el cliente creará una clave pre-maestra.
 7. `Clave pre-maestra`, es creada por el cliente (el método de creación depende del conjunto de cifrado que se utilizará) y luego se comparte con el servidor. Antes de enviar la clave pre-máster al servidor, el cliente lo cifra mediante la clave pública del servidor que se extrajo del certificado proporcionado por el servidor. Esto significa que solo el servidor puede descifrar el mensaje ya que el cifrado asimétrico se está utilizando para el intercambio de clave pre-maestra.

8. Clave Maestra (48 bytes), una vez que el servidor recibe la clave secreta pre-maestra, usa su clave privada para descifrarla. Ahora tanto el cliente como el servidor calcularán la clave maestra secreta basada en los valores aleatorios intercambiados anteriormente usando una función pseudoaleatoria. Tanto el cliente como el servidor usarán la clave maestra para generar las claves de las sesiones que consistirán en cifrar / descifrar los datos.
9. Change Cipher-Spec, el cliente como el servidor están listos para cambiar a un ambiente seguro y encriptado. Este protocolo se usa para cambiar el cifrado utilizado por el cliente y el servidor Todos los datos intercambiados entre las dos partes ahora se cifrarán con la clave compartida simétrica que tienen.
10. Finished, este mensaje es el último del proceso de Handshake y el primero encriptado en la conexión segura, que ambas partes intercambian.



Figura 10: EAP TLS Handshake
Recuperado: (Baheti, 2015)

2.5.2.2 Tunneled Transport Layer Security (EAP-TTLS).

EAP-TTLS (seguridad de la capa de transporte con túnel de EAP) realiza la autenticación sobre el túnel TLS mediante un "método de autenticación interna". Estos

métodos incluyen MSCHAPv2²⁷, MSCHAP, CHAP²⁸ y PAP²⁹. Los métodos de autenticación interna están protegidos por el túnel TLS. El túnel TLS no requiere un certificado de cliente. (Adler, 2014)

EAP-TTLS es un protocolo EAP donde se usa un Handshake de TLS para autenticarse mutuamente un cliente y servidor. Extiende esta negociación de autenticación mediante el uso de la conexión segura establecida por el Handshake de TLS para intercambiar información adicional entre cliente y servidor. Como se muestra en la Figura 11:

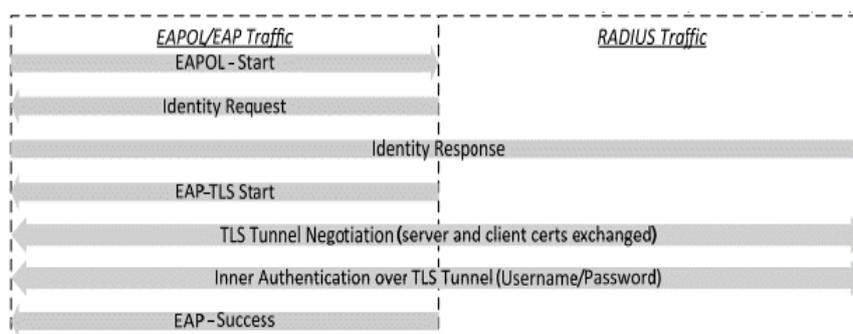


Figura 11: Estructura EAPOL-TTLS
Recuperado: (Funk, Software, Blake, & Industries, Inc, 2005)

2.5.2.3 PEAP (Protected EAP).

PEAP-EAP (Protocolo de autenticación extensible protegido) es una variación para el método EAP. Es similar a EAP-TLS, pero no tiene el requisito de certificados de cliente. La autenticación se realiza en un túnel TLS usando un nombre de usuario y contraseña con MSCHAPv2. Proporciona buena seguridad sin la infraestructura PKI³⁰ necesaria. (Adler, 2014)

La diferencia que existe con los métodos anteriores radica en que PEAP requiere encriptación con MSCHAPv2, como se muestra en la Figura 12:

²⁷ Protocolo de Autenticación de Microsoft Challenge Handshake versión 2.

²⁸ Protocolo de Autenticación Challenge Handshake

²⁹ Protocolo de Autenticación de Contraseña

³⁰ Infraestructura de Clave Pública

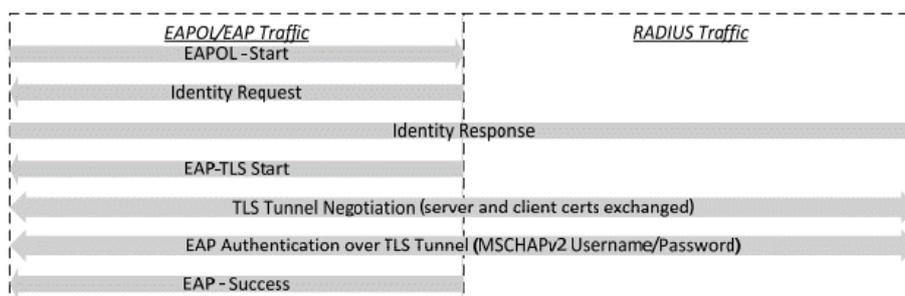


Figura 12: Estructura PEAP
Recuperado: (Palekar, y otros, 2004)

2.5.2.5 Comparación entre protocolos de autenticación.

En este apartado se identifica los principales tipos de 802.1x EAP y se hace una comparación entre cada uno de ellos. Como se muestra en la Tabla 5.

Tabla 5: Comparación de métodos EAP.

EAP/TIPOS	EAP-MD5	EAP-TLS	EAP-TTLS	EAP-PEAP	EAP-FAST	EAP-LEAP
Certificado de cliente	No	Si	Opcional	No	No (PAC ³¹)	No
Certificado de servidor	No	Si	No	Si	No (PAC)	No
Atributos de autenticación	Una manera	Mutua	Mutua	Mutua	Mutua	Mutua
Credenciales	MD5 ³²	Certificados	CHAP, PAP, MS-CHAP	EAP-MSCHAP, EAP-GTC	PAC	MS - CHAP
Túnel	No	Si	Si	Si	Si	No
Ocultación de identidad de usuario	No	No	Si	Si	Si	Si
Ataques:	Si	No	No	No	No	Si

³¹ Credencial de acceso protegido

³² Algoritmo de Resumen del Mensaje 5

Secuestro de sesión, MitM						
ataque de diccionario.						
Despliegue	Fácil	Difícil	Moderado	Moderado	Moderado	Moderado
Proveedor	MS	MS	Funk	MS	Cisco	Cisco

Fuente: Adaptado (Kothaluru & Shameel, 2012)

El EAP-MD5 es relativamente fácil de implementar, pero al no tener unos estándares de seguridad altos; no lo hace apto para un despliegue en una infraestructura de red. Las contraseñas de los usuarios se almacenan en texto plano así que esta información puede ser captada por posibles atacantes.

En cuanto a la variante de autenticación EAP-TLS proporciona modificación dinámica y autenticación mutua. A su vez proporciona un túnel seguro para el intercambio de certificados. El problema que surge al optar por este tipo de autenticación es el alto costo de su mantenimiento, ya que el certificado mutuo debe ser intercambiado entre el suplicante y el servidor de autenticación.

El método EAP-TTLS tiene mejores prestaciones como se muestra en la Tabla 5. Al poseer un túnel SSL seguro aumenta los niveles de seguridad, ya que el túnel estará cifrado en los dos extremos. Otra ventaja es la posibilidad de usar métodos de autenticación heredados y la modificación dinámica; la identidad del usuario está protegida. Este método es el que se recomienda para el uso en una infraestructura de red ya que no se tiene que crear certificados por cada cliente, sino solo en la parte del servidor.

2.6 Remote Authentication Dial-In User Server (RADIUS)

El servicio de usuario de marcado de autenticación remota (RADIUS) se define en RFC 2865 y la contabilidad RADIUS se define en RFC³³ 2866. RADIUS se preocupa por la administración de acceso a la red de AAA y es el transporte para EAP entre el autenticador y el servidor de autenticación. Además, RADIUS también se usa para llevar las instrucciones de política al autenticador en forma de pares de AV³⁴. (Rigney, Rubens, Simpson, & Willens, 2000)

2.6.1 Protocolo Radius AAA.

Autenticación: un cliente envía una solicitud de acceso a la red en la capa de enlace. Esta solicitud contiene credenciales de usuario o un certificado de usuario. El autenticador empaqueta esto en formato RADIUS como un mensaje de Solicitud de Acceso y lo reenvía a un servidor RADIUS. El servidor RADIUS verifica la coincidencia de una base de datos de usuario y luego decide si autentica o no al usuario. Los mensajes utilizados son:

- Rechazo de acceso
- Desafío de acceso (solicitar más información)
- Aceptar acceso.

Autorización: el servidor RADIUS estipula los términos de acceso para el usuario, es decir, lo que el usuario puede hacer en la red.

Contabilidad: si se requieren estadísticas e información de acceso de usuario, la autenticación RADIUS se habilita mediante el autenticador que emite una solicitud de inicio de contabilidad al servidor RADIUS.

³³ Solicitud de comentarios

³⁴ Valor-Atributo

El protocolo RADIUS usa los puertos UDP 1812 para autorización y 1813 para contabilidad como estándar.

2.6.2 Estructura del formato del protocolo Radius.

El datagrama de RADIUS tiene la siguiente estructura según el *rfc2865 Remote Authentication Dial In User Service (RADIUS)* y sus tipos de paquetes radius como se muestran respectivamente en la Figura 13 y Tabla 6.

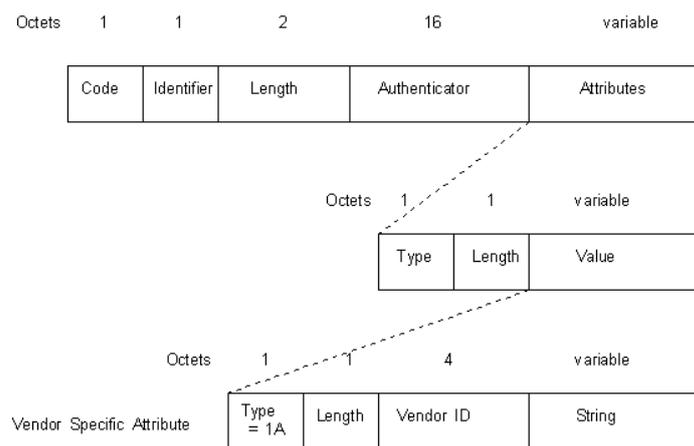


Figura 13: Datagrama Radius

Fuente: Adaptado de (Rigney, Rubens, Simpson, & Willens, 2000)

Código: indica el tipo de paquete RADIUS.

Tabla 6: *Tipo de paquete Radius*

CÓDIGO	TIPO DE PAQUETE RADIUS
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)

13	Status-Client (experimental)
255	Reserved

Fuente: Adaptado de (Rigney, Rubens, Simpson, & Willens, 2000)

Delimitador - coincide con la solicitud con respuesta.

Longitud: indica la longitud del paquete completo, que puede variar entre 20 y 4096 bytes.

Autenticador: contiene la información que el cliente y el servidor utilizan para autenticarse entre sí.

Atributos: este campo contiene autenticación específica, autorización, información, más detalles de configuración para paquetes RADIUS.

Tipo: este es el tipo de atributo y toma uno de los siguientes números (de 192 a 255 están reservados), en la Tabla 7 se muestra su valor y lo que representa.

Tabla 7: *Tipo de atributos Radius*

CÓDIGO	TIPO DE ATRIBUTO	CÓDIGO	TIPO DE ATRIBUTO
1	User-Name	13	Framed-Compression
2	User-Password	19	Reply-Message
3	CHAP-Password	24	State
4	NAS-IP-Address	25	Class
5	NAS-Port	26	Vendor-Specific
6	Service-Type	27	Session-Timeout
7	Framed-Protocol	28	Idle-Timeout
8	Framed-IP-Address	29	Termination-Action
9	Framed-IP-Netmask	32	NAS-Identifier
10	Framed-Routing	61	NAS-Port-Type

11	Filter-ID	62	Port-Limit
12	Framed-MTU		

Recuperado: Adaptado de (Rigney, Rubens, Simpson, & Willens, 2000)

Longitud: la longitud del atributo.

Valor: el tamaño de este campo varía y contiene información específica sobre el atributo. La estructura de un atributo Vendor Specific Attribute (VSA) es la siguiente:

Tipo: está configurado como 0x1A.

Longitud: longitud del VSA en bytes.

Vendor-ID: construido como 0x00SSSSSS donde los números 'S' representan la estructura y la identificación de la información de administración (SMI³⁵). Network Management Private Enterprise Code of the vendor.

Cadena: contiene un campo vendor type de 1 byte, un campo de vendor length de 1 byte y un campo variable de atributo específico que contiene los datos para el atributo de proveedor específico.

2.7 Lightweight Directory Access Protocol (LDAP)

En el RFC 4511 Lightweight Directory Access Protocol (LDAP) se identifica los elementos del protocolo, junto con su semántica y codificaciones. LDAP proporciona acceso a servicios de directorio distribuidos que actúa de acuerdo con los datos X.500³⁶ y los modelos

³⁵ Identificación de la información de administración

³⁶ Unión de estándares sobre servicios de directorio.

de servicio. Dentro del protocolo los elementos se basan en los que se describen en el acceso al directorio X.500 Protocolo (DAP³⁷). (Sermersheim, 2006)

En el Lightweight Directory Access Protocol las credenciales del usuario se almacenan y administran en una sola ubicación. Si un usuario inicia sesión en el sistema, las credenciales se envían al servidor LDAP para autenticación. Tras la conformación positiva, el usuario tiene permitido el acceso a la aplicación específica en la que iniciaron sesión. (Magan , 2013)

LDAP es el modelo de información, que trata del tipo de información almacenada en los directorios y la estructuración de la información. El modelo de información gira en torno a una entrada, que es una colección de atributos con tipo y valor. Las entradas se organizan en una estructura llamada árbol de información de directorio.

2.7.1 Modelo de información LDAP.

LDAP se puede entender mejor si se consideran los cuatro modelos sobre los que está basado, en la Tabla 8 se explica cada uno de los existentes y su función.

Tabla 8: *Modelos de información LDAP*

Modelo	Función
Información	Se refiere a la estructura de la información guardada en un LDAP.
Nombrado	Se refiere a la organización de la información en un directorio LDAP e identificado.
Funcional	Se refiere a cada una de las operaciones, se pueden realizar sobre la información almacenada en un directorio LDAP.
Seguridad	Hace relación a cómo puede ser la información en un directorio LDAP protegido del acceso no autorizado.

Recuperado: Adaptado de (Virtanen & Curtis, 2018)

³⁷ Protocolo de acceso a directorios

2.7.2 Operaciones dentro de LDAP.

LDAP define operaciones para acceder y modificar entradas de directorio que son las siguientes:

- Búsqueda de entradas que cumplen los criterios especificados por el usuario.
- Agregar una entrada.
- Eliminar una entrada.
- Modificar una entrada.
- Modificar el nombre distinguido o el nombre completo relativo de una entrada (mover).
- Comparación de una entrada.

2.7.3 Estructura de la LDAP.

La unidad básica de información almacenada en el directorio se llama entrada. Las entradas representan objetos pueden ser personas, organizaciones etc. Las entradas se componen de una colección de atributos que contienen información sobre el objeto. Cada atributo tiene un tipo y uno o más valores.

El tipo del atributo está asociado con una sintaxis. La sintaxis especifica qué tipo de valores se pueden almacenar. La sintaxis está asociada a un tipo de atributo y se especifica con valores. Es posible que la entrada del directorio contenga múltiples valores en un atributo. Como se muestra en la Figura 14.

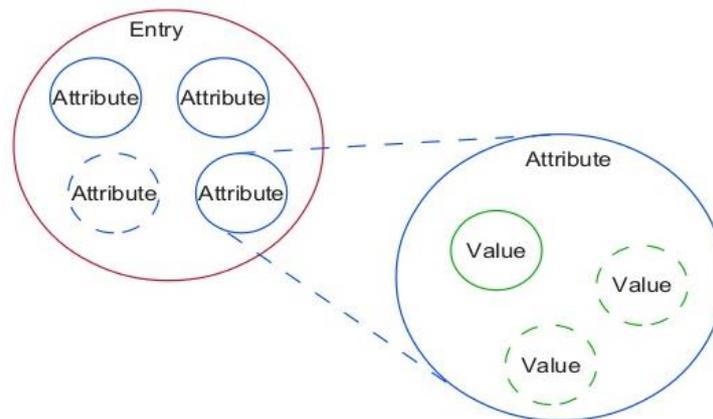


Figura 14: Relación entre entrada, atributos y valores
Recuperado: Adaptado de (LinID,2013)

En la estructura de la LDAP los atributos y su sintaxis ya están establecidos para limitar el tipo y tamaño del dato que se puede almacenar. Los atributos poseen un alias y una determinada sintaxis. A su vez se identifica las clases de objetos, atributos requeridos y la representación del String según tipo de atributo. Como muestra la Tabla 9, Tabla 10, Tabla 11 y Tabla 12.

Tabla 9: *Algunas de las sintaxis de los atributos LDAP*

Sintaxis	Descripción
bin	Información binaria
ces	El string debe ser exacto (búsqueda)
cis	El string es diferente (búsqueda)
tel	Número de teléfono (tratado como texto)
dn	Nombre distinguido

Fuente: Adaptado de (Howes, Smith, & Good, 2003)

Tabla 10: *Atributos comunes LDAP*

Atributo, alias	Sintaxis	Descripción	Ejemplo
commonName, cn	cis	Nombre común de una entrada.	Ashley Vallejos
surname, sn	cis	Apellido de la persona	Vallejos
telephoneNumber	tel	# de teléfono	2-606-109
organizationalUnitname, ou	cis	Nombre de una unidad organizativa	
owner	dn	Nombre distinguido de la persona que posee la entrada.	cn= Ashley Vallejos o=UTN, c=ECU
organization, o	cis	Nombre de la organización	UTN
jpegPhoto	bin	Fotografía en formato jpeg	Fotografía de Ashley Vallejos

Fuente: Adaptado de (Howes, Smith, & Good, 2003)

Tabla 11: *Clases de objetos y atributos requeridos*

Clase de objeto	Descripción	Atributos requerido
IngOrgPerson	Define entradas para personas	commonName, (cn) surname, (sn) objectClass
organizationalUnit	Define entradas para organizationalUnit	ou objectClass
organization	Define entradas para organizations	ou objectClass

Fuente: Adaptado de (Howes, Smith, & Good, 2003)

Tabla 12: Representación del String según tipo de atributo

Tipo de atributo	String
CommonName	CN
LocalityName	L
StateOrProvinceName	ST
OrganizationName	O
OrganizationalUnitName	OU
CountryName	C
StreetAddress	STREET
domainComponet	DC
Userid	UID

Fuente: Adaptado de (Howes, Smith, & Good, 2003)

2.7.4 LDAP arquitectura Cliente/Servidor.

Según el libro *Ldaptor* (Virtanen & Curtis, 2018) la comunicación de protocolo LDAP promedio consta de tres etapas:

1. Apertura de la conexión

En la primera etapa, al abrir una conexión, un cliente LDAP abre una conexión TCP al servidor LDAP, ya sea como simple texto, encriptado por TLS o comenzando con texto plano y cambiando para usar TLS con STARTTLS. El cliente hace una petición de establecimiento de conexión dependiendo del método de autenticación procede el servidor a establecer la conexión. Si los parámetros establecidos en la negociación entre ambas partes son los correctos ambos empiezan a transmitir, en caso contrario la conexión falla. Como se muestra en la Figura 15.

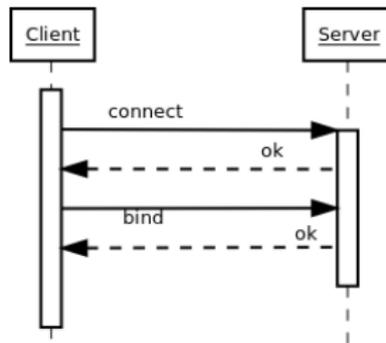


Figura 15: Apertura de conexión Cliente/Servidor
Recuperado: (Virtanen & Curtis, 2018)

2. Hacer una o más búsquedas

El cliente se autentica a sí mismo y / o al usuario, proporcionando cualquier información de autenticación necesaria. Se llama Unión. Normalmente, la conexión no está realmente autenticada, sino que se deja como anónima; el mensaje de enlace se envía sin información de usuario o contraseña. Como se muestra en la Figura 16.

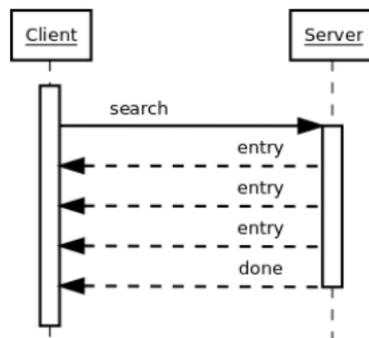


Figura 16: Búsquedas Cliente/Servidor
Recuperado: (Virtanen & Curtis, 2018)

3. Cerrar la conexión

Al momento que el cliente ya quiera interrumpir la conexión envía un mensaje de cierre de sesión para desenlazarse. El servidor le envía un mensaje de confirmación para que se pueda cerrar la sesión y acto seguido el cliente ya se desconecta. Como se muestra en la Figura 17.

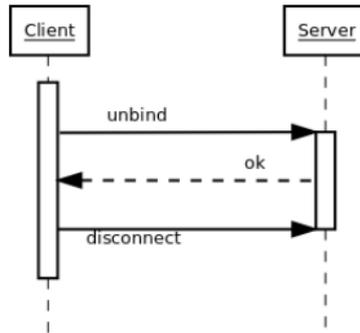


Figura 17: Cerrar conexión Cliente/Servidor
 Recuperado: (Virtanen & Curtis, 2018)

Capítulo III

Situación Actual

3.1 Situación actual de la red cableada “Universidad Técnica Del Norte”

La topología de red de la Universidad Técnica del Norte consta de tres capas claramente identificadas, Core, distribución y acceso. Dentro de cada una de ellas existen determinados equipos que cumple una función específica que a continuación se va a identificar.

La capa de Core posee un router de borde que está ubicado en el Edificio Central el cual es suministrado por el proveedor de internet Telconet. Este equipo está conectado con un switch Cisco 3750 que aporta IPs públicas, el cual permite la interconexión del router de borde con un Firewall ASA 5520. A demás otro equipo que integra esta capa es un switch NEXUS que está

conectado al Firewall ASA 5520 y da conectividad a los servidores de la DMZ³⁸. Por último, el equipo EXINDIA que se encarga de la administración de anchos de banda que se emplea en la red de la UTN y conecta con la capa de distribución.

En la capa de distribución la universidad tiene dos equipos de conmutación un switch Cisco 4510-E y un switch Cisco 4503-E ubicados en el Edificio Central, utilizados para la propagación de VLAN a lo largo de la capa de acceso. Ambos equipos están interconectados, pero el Cisco 4503-E switch solo posee conexiones para dar conectividad a acces point y cámaras presentes en el edificio central.

La capa de acceso está dividida entre distintas dependencias las cuales están distribuidas por facultades, edificio central, edificio de posgrado, instituto de educación física, biblioteca, bienestar universitario, auditorio Agustín Cueva y las extensiones que se encuentran fuera de la Universidad. Esta organización se emplea para facilitar la administración, por medio de VLAN.

La Universidad posee la siguiente topología física como se muestra en la Figura 18, la topología lógica como se muestra en la Figura 19 y el direccionamiento de VLAN como se muestra en la Tabla 13.

³⁸ Zona desmilitarizada

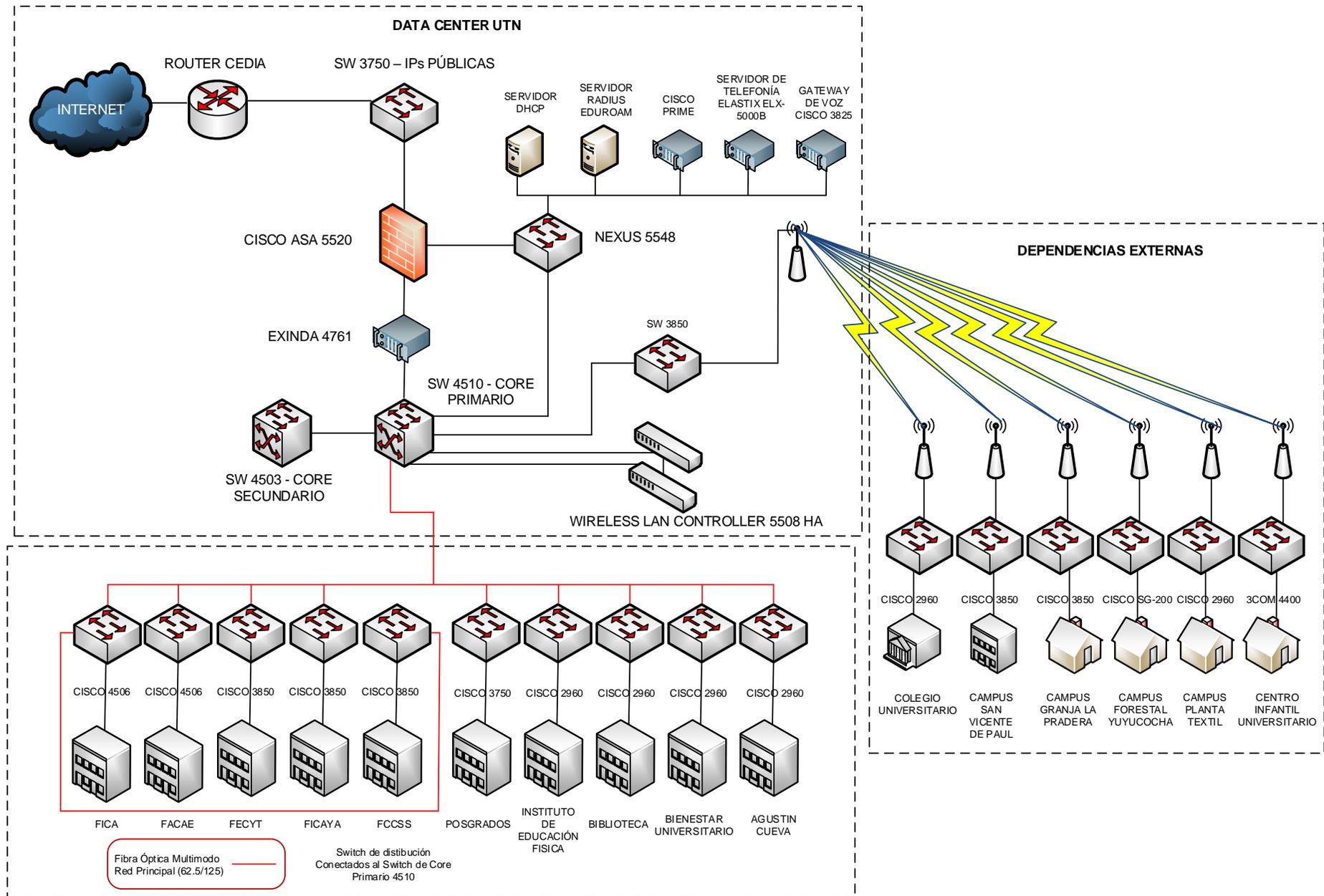


Figura 18: Topología física UTN
Fuente: Adaptado DDTI

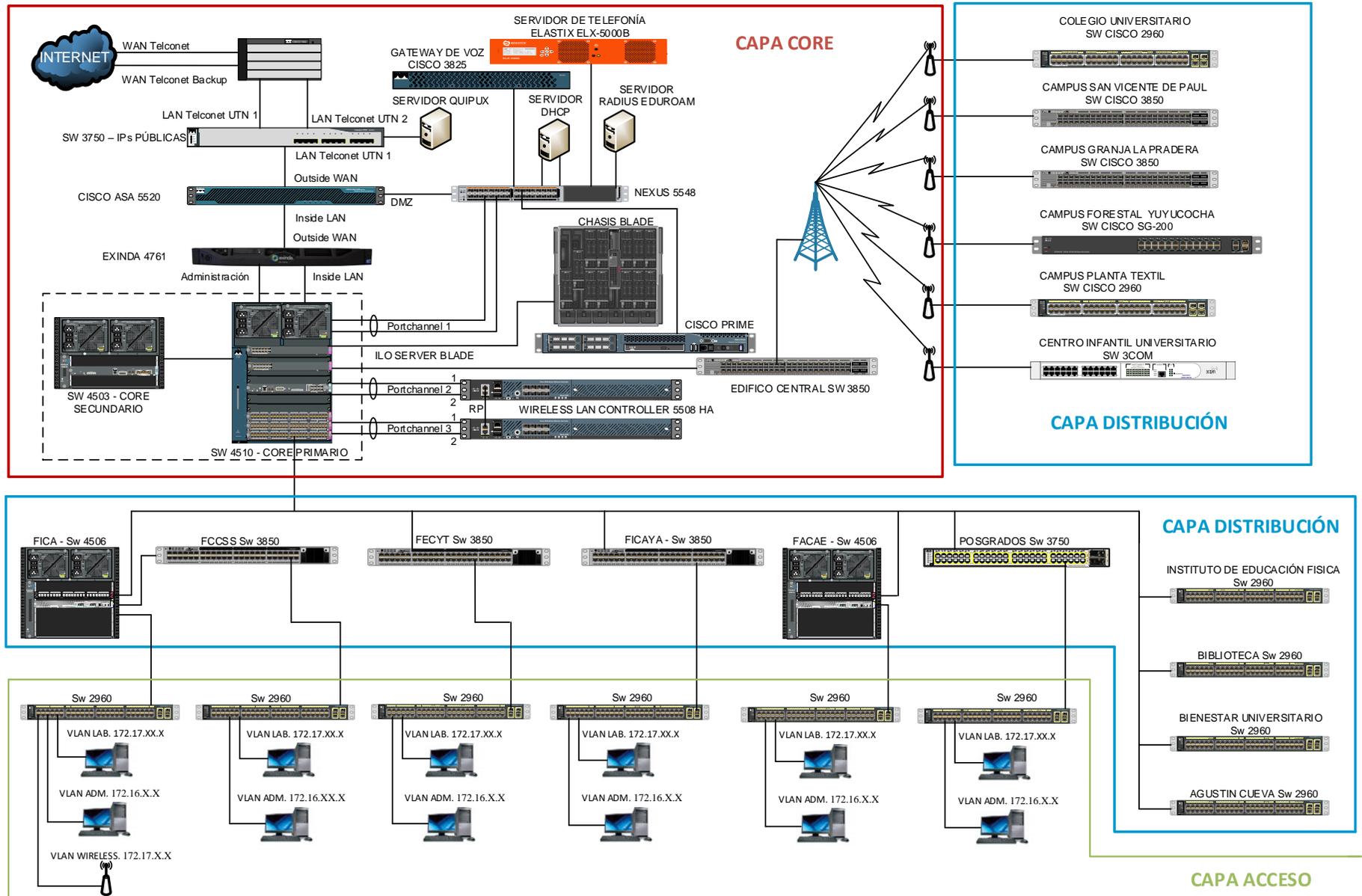


Figura 19: Topología lógica UTN
Fuente: Adaptado DDTI

Tabla 13: *Distribución De Subredes (VLANs)*

Nº	DESCRIPCIÓN	VLAN	DIRECCIÓN IP	MASCARA DE SUBRED	GATEWAY
1	ADMINISTRATIVA	X	172.1.X.X	255.255.255.0	172.16.X.X
2	DMZ	X	10.24.8.X.X	255.255.255.0	10.24.X.X
3	NAT-INTERNO-DMZ	X	172.16.X.X	255.255.255.0	172.16.X.X
4	EQUIPOS-ACTIVOS- WIRELESS	X	172.16.X.X	255.255.255.0	172.16.X.X
5	CCTV	X	172.16.X.X	255.255.255.0	172.16.X.X
6	RELOJES-BIOMETRICOS	X	172.16.X.X	255.255.255.0	172.16.X.X
7	TELEFONIA-IP-ELASTIX	X	172.16.X.X	255.255.252.0	172.16.X.X
8	AUTORIDADES	X	172.16.X.X	255.255.255.0	172.16.X.X
9	DDTI	X	172.16.X.X	255.255.255.0	172.16.X.X
10	FINANCIERO	X	172.16.X.X	255.255.255.0	172.16.X.X
11	COMUNICACION- ORGANIZACIONAL	X	172.16.X.X	255.255.255.0	172.16.X.X
12	ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
13	ADQUISICIONES	X	172.16.X.X	255.255.255.0	172.16.X.X
14	U-EMPRENDE	X	172.16.X.X	255.255.255.0	172.16.X.X
15	AGUSTIN-CUEVA	X	172.16.X.X	255.255.255.0	172.16.X.X
16	BIENESTAR-DOCENTES	X	172.16.X.X	255.255.255.0	172.16.X.X
17	BIENESTAR- ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
18	CLUBES-UTN	X	172.16.X.X	255.255.255.0	172.16.X.X
19	NATIVA	X	-----	-----	-----
20	FICA-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
21	FICA-WIRELESS	X	172.17.X.X	255.255.255.0	172.17.X.X
22	FICA-ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
23	FICAYA-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
24	FICAYA- ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
25	FECYT-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
26	FECYT-ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
27	FACAE-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
28	FACAE-ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
29	FCCSS-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
30	FCCSS-ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
31	POSTGRADO- LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
32	POSTGRADO- ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
33	CAI-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
34	CAI-ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
35	BIBLIOTECA- LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
36	BIBLIOTECA-DOCENTES	X	172.16.X.X	255.255.255.0	172.16.X.X

37	BIBLIOTECA- ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
38	COLEGIO-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
39	COLEGIO- ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
40	AHSVP	X	172.16.X.X	255.255.255.0	172.16.X.X
41	WIRELESS-DOCENTES	X	172.18.X.X	255.255.248.0	172.18.X.X
42	WIRELESS- ADMINISTRATIVOS	X	172.19.X.X	255.255.254.0	172.19.X.X
43	EDUROAM	X	172.20.X.X	255.255.224.0	172.20.X.X
44	WIRELESS-EVENTOS1	X	172.21.X.X	255.255.248.0	172.21.X.X
45	WIRELESS-EVENTOS2	X	172.22.X.X	255.255.248.0	172.22.X.X
46	WIRELESS-ESTUDIANTES	X	172.23.X.X	255.255.224.0	172.23.X.X
47	COPIADORA	X	172.24.X.X	255.255.255.0	172.24.X.X

Recuperado: Adaptado de DDTI

3.2 Descripción De La Red Por Facultad

3.2.1 FICA.

La facultad contiene un gran número de dependencias, por ello se procede a detallar de una manera independiente cada una de ellas. Identificando los equipos de telecomunicaciones que contiene y su mapeo de puertos. La topología física y lógica de esta facultad como se muestra respetivamente en las Figuras 20 y 21.

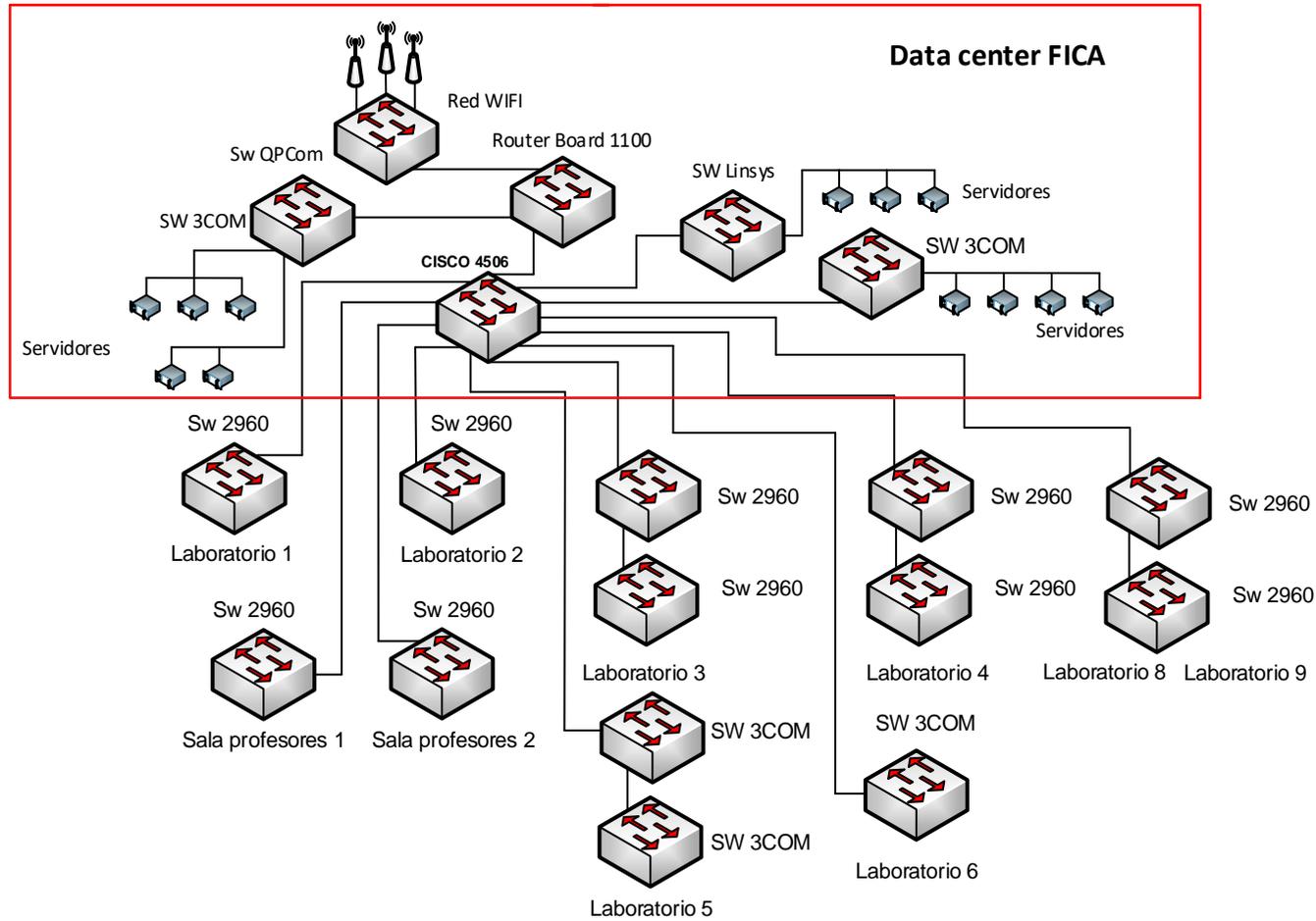


Figura 20: Topología Física FICA-UTN
 Fuente: Adaptado Data Center FICA

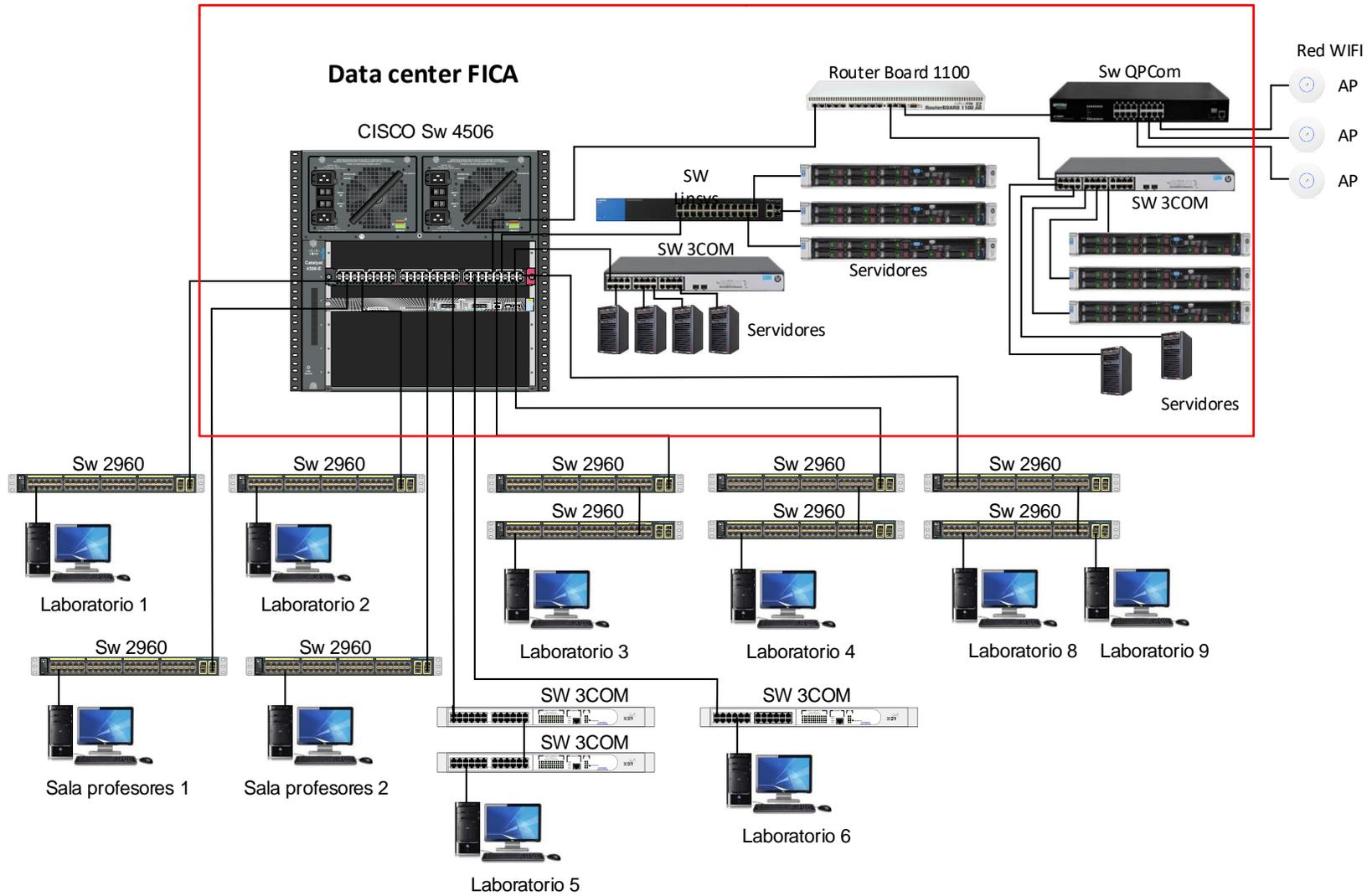


Figura 21: Topología Lógica FICA-UTN

Fuente: Adaptado Data Center FICA

3.2.1.1 Data Center.

Está ubicado en la planta baja de la FICA como se muestra en la Figura 22, los equipos de telecomunicaciones como se muestra en la Tabla 14 y los servidores como se muestra en la Tabla 15.

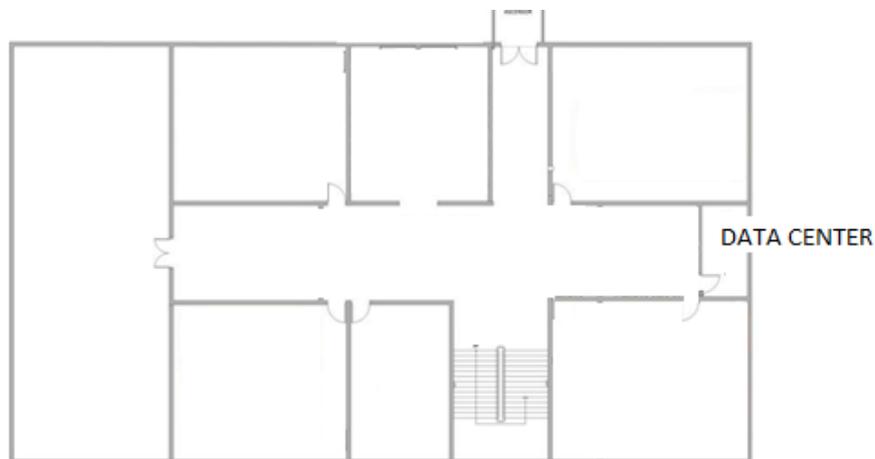


Figura 22: Planta Baja FICA-UTN
Fuente: DDTI - UTN

Tabla 14: *Equipos Data Center – FICA*

Dispositivo	Cantidad	Rack
Switch de Core	1	1
Switch Linksys	1	2
Switch QP-COM	1	3
Switch 3Com	1	2
Switch 3Com	1	3
Router Board 1100	1	2
Servidor Tipo Torre	2	2
Servidor Tipo Torre	4	3
Servidor Tipo Rack	6	2

Fuente: Adaptado de Data Center – FICA

Tabla 15: Servidores – FICA

Servicio	Tipo	Estado	Marca
Reactivos Moodle	Torre	Activo	IBM x3500 M4
Gestor de encuestas Opina	Torre	Activo	HP ProLiant ML150
Repositorio Digital Dspace	Torre	Activo	IBM x3500 M4
LDAP	Torre	Activo	IBM System x3200 M2
Control de Accesos	Torre	Activo	HP Proliant ML370
Sin Servicio	Torre	Activo	HP Proliant ML150 G5
Nube de la FICA	Rack	Activo	HP Proliant G9
Nube de la FICA	Rack	Activo	HP Proliant G9
Nube de la FICA	Rack	Activo	HP Proliant G9
Proyectos de CISIC	Rack	Activo	IBM System x3250
Proyectos de CISIC	Rack	Activo	IBM System x3250
Proyectos de CISIC	Rack	Activo	HP System x3650 M3

Fuente: Adaptado de Data Center – FICA

3.2.1.2 Laboratorio 1.

El laboratorio 1 ubica en la primera planta de la FICA como se muestra en la Figura 23, los equipos de telecomunicaciones presentes como se muestra en la Tabla 16 y su mapeo de puerto como se muestra en la Tabla 17.

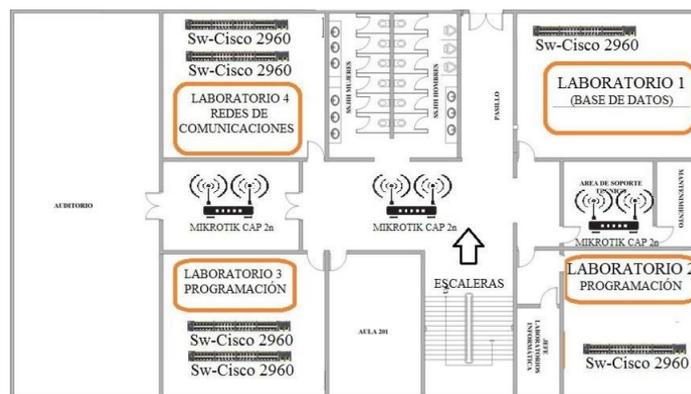


Figura 23: Primera Planta FICA-UTN

Fuente: DDTI - UTN

Tabla 16: Equipos Lab.1 - FICA

Equipos de Telecomunicaciones	Marca	Nombre	Dirección IP	Cantidad
Rack De Pared De 19"	Panduit	-----	-----	1
Patch Panel De 48 Puertos Cat. 6.	Newlink	-----	-----	1
Switch De 48 Puertos	WS-C2960-48TC-L	SW-Arquímedes	172.17.X.X	1

Fuente: Adaptado DDTI

Tabla 17: Mapeo de red Lab.1 – FICA

Modo VLAN	VAN	Switch Catalyst 2960 Laboratorio 1					Equipo conectado	
		Descripción	Puerto	Estado	PatchPanel	Punto Red/Nº	Nombre	IP
access	x	Laboratorios	Fa0/1	Disponible	1	Si/1	-	-
access	x	Laboratorios	Fa0/2	Activado	2	Si/2	PCFICA-312	172.17.X.X
access	x	Laboratorios	Fa0/3	Activado	3	Si/3	PCFICA-311	172.17.X.X
access	x	Laboratorios	Fa0/4	Disponible	4	Si/4	-	-
access	x	Laboratorios	Fa0/5	Activado	5	Si/5	PCFICA-313	172.17.X.X
access	x	Laboratorios	Fa0/6	Activado	6	Si/6	PCFICA-319	172.17.X.X
access	x	Laboratorios	Fa0/7	Activado	7	Si/7	PCFICA-318	172.17.X.X
access	x	Laboratorios	Fa0/8	Activado	8	Si/8	PCFICA-317	172.17.X.X
access	x	Laboratorios	Fa0/9	Disponible	9	Si/9	-	-
access	x	Laboratorios	Fa0/10	Disponible	10	Si/10	-	-
access	x	Laboratorios	Fa0/11	Activado	11	Si/11	PCFICA-325	172.17.X.X
access	x	Laboratorios	Fa0/12	Activado	12	Si/12	PCFICA-324	172.17.X.X
access	x	Laboratorios	Fa0/13	Disponible	13	Si/13	-	-
access	x	Laboratorios	Fa0/14	Activado	14	Si/14	PCFICA-331	172.17.X.X
access	x	Laboratorios	Fa0/15	Activado	15	Si/15	PCFICA-330	172.17.X.X
access	x	Laboratorios	Fa0/16	Disponible	16	Si/16	-	-
access	x	Laboratorios	Fa0/17	Activado	17	Si/17	PCFICA-329	172.17.X.X
access	x	Laboratorios	Fa0/18	Activado	18	Si/18	PCFICA-337	172.17.X.X
access	x	Laboratorios	Fa0/19	Disponible	19	Si/19	-	-
access	x	Laboratorios	Fa0/20	Disponible	20	Si/20	-	-
access	x	Laboratorios	Fa0/21	Activado	21	Si/21	PCFICA-336	172.17.X.X
access	x	Laboratorios	Fa0/22	Activado	22	Si/22	PC-5PPOIQ9	172.17.X.X
access	x	Laboratorios	Fa0/23	Disponible	23	Si/23	-	-
access	x	Laboratorios	Fa0/24	Disponible	24	Si/24	-	-
access	x	Laboratorios	Fa0/25	Disponible	25	Si/25	-	-
access	x	Laboratorios	Fa0/26	Activado	26	Si/26	PCFICA-314	172.17.X.X
access	x	Laboratorios	Fa0/27	Activado	27	Si/27	PCFICA-315	172.17.X.X
access	x	Laboratorios	Fa0/28	Disponible	28	Si/28	-	-
access	x	Laboratorios	Fa0/29	Disponible	29	Si/29	-	-
access	x	Laboratorios	Fa0/30	Activado	30	Si/30	PCFICA-322	172.17.X.X
access	x	Laboratorios	Fa0/31	Activado	31	Si/31	PCFICA-320	172.17.X.X
access	x	Laboratorios	Fa0/32	Activado	32	Si/32	PCFICA-321	172.17.X.X
access	x	Laboratorios	Fa0/33	Disponible	33	Si/33	-	-
access	x	Laboratorios	Fa0/34	Disponible	34	Si/34	-	-
access	x	Laboratorios	Fa0/35	Disponible	35	Si/35	-	-
access	x	Laboratorios	Fa0/36	Activado	36	Si/36	PCFICA-326	172.17.X.X
access	x	Laboratorios	Fa0/37	Activado	37	Si/37	PCFICA-328	172.17.X.X
access	x	Laboratorios	Fa0/38	Activado	38	Si/38	PCFICA-334	172.17.X.X
access	x	Laboratorios	Fa0/39	Activado	39	Si/39	PCFICA-332	172.17.X.X
access	x	Laboratorios	Fa0/40	Disponible	40	Si/40	-	-
access	x	Laboratorios	Fa0/41	Activado	41	Si/41	PCFICA-333	172.17.X.X
access	x	Laboratorios	Fa0/42	Activado	42	Si/42	PCFICA-340	172.17.X.X
access	x	Laboratorios	Fa0/43	Activado	43	Si/43	PCFICA-338	172.17.X.X
access	x	Laboratorios	Fa0/44	Activado	44	Si/44	PCFICA-339	172.17.X.X
access	x	Laboratorios	Fa0/45	Disponible	45	Si/45	-	-
access	x	Laboratorios	Fa0/46	Disponible	46	Si/46	-	-
access	x	Laboratorios	Fa0/47	Disponible	47	No	-	-
access	x	Administrativos	Fa0/48	Disponible	48	No	-	-
trunk			G1/0					
			G2/0					

Fuente: (Espinosa,2017)

1.2.1.1 Laboratorio 2.

Este laboratorio se encuentra la primera planta del edificio como se muestra en la Figura 23, los equipos de telecomunicaciones presentes como se muestra en la Tabla 18 y su mapeo de puerto como se muestra en la Tabla 19.

Tabla 18: *Equipos Lab.2 – FICA*

Equipos de Telecomunicaciones	Marca	Nombre	Dirección IP	Cantidad
Rack De Pared De 19"	Panduit	-----	-----	1
Patch Panel De 48 Puertos Cat. 6.	Newlink	-----	-----	1
Switch De 48 Puertos	WS-C2960-48TC-L	SW-Bernoulli	172.17.X.X	1

Fuente: Adaptado de Laboratorio 2 – FICA

Tabla 19: *Mapeo de red Lab.2 – FICA*

Modo VLAN	VAN	Switch Catalyst 2960 Laboratorio 2				Equipo conectado	
		Descripción	Puerto	Estado	PatchPanel	Nombre	IP
access	x	Laboratorios	Fa0/1	Disponible	1	-	-
access	x	Laboratorios	Fa0/2	Disponible	2	-	-
access	x	Laboratorios	Fa0/3	Activado	3	PCFICA-184	172.17.X.X
access	x	Laboratorios	Fa0/4	Activado	4	PCFICA-183	-
access	x	Laboratorios	Fa0/5	Disponible	5	-	172.17.X.X
access	x	Laboratorios	Fa0/6	Disponible	6	-	172.17.X.X
access	x	Laboratorios	Fa0/7	Activado	7	PCFICA-190	172.17.X.X
access	x	Laboratorios	Fa0/8	Activado	8	PCFICA-188	172.17.X.X
access	x	Laboratorios	Fa0/9	Activado	9	PCFICA-189	172.17.X.X
access	x	Laboratorios	Fa0/10	Activado	10	PCFICA-190	172.17.X.X
access	x	Laboratorios	Fa0/11	Activado	11	PCFICA-196	172.17.X.X
access	x	Laboratorios	Fa0/12	Activado	12	PCFICA-195	172.17.X.X
access	x	Laboratorios	Fa0/13	Disponible	13	-	-
access	x	Laboratorios	Fa0/14	Activado	14	PCFICA-199	172.17.X.X
access	x	Laboratorios	Fa0/15	Activado	15	PCFICA-243	172.17.X.X
access	x	Laboratorios	Fa0/16	Disponible	16	-	-
access	x	Laboratorios	Fa0/17	Activado	17	PCFICA-262	172.17.X.X
access	x	Laboratorios	Fa0/18	Disponible	18	-	-
access	x	Laboratorios	Fa0/19	Disponible	19	-	-
access	x	Laboratorios	Fa0/20	Disponible	20	-	-
access	x	Laboratorios	Fa0/21	Disponible	21	-	-
access	x	Laboratorios	Fa0/22	Activado	22	PCFICA-181	172.17.X.X
access	x	Laboratorios	Fa0/23	Disponible	23	-	-
access	x	Laboratorios	Fa0/24	Disponible	24	-	-
access	x	Laboratorios	Fa0/25	Disponible	25	-	-
access	x	Laboratorios	Fa0/26	Disponible	26	-	-
access	x	Laboratorios	Fa0/27	Activado	27	PCFICA-182	172.17.X.X
access	x	Laboratorios	Fa0/28	Disponible	28	-	-
access	x	Laboratorios	Fa0/29	Disponible	29	-	-
access	x	Laboratorios	Fa0/30	Activado	30	-	-
access	x	Laboratorios	Fa0/31	Disponible	31	-	-
access	x	Laboratorios	Fa0/32	Disponible	32	-	-
access	x	Laboratorios	Fa0/33	Activado	33	PCFICA-187	172.17.X.X
access	x	Laboratorios	Fa0/34	Activado	34	PCFICA-193	172.17.X.X
access	x	Laboratorios	Fa0/35	Activado	35	PCFICA-192	172.17.X.X
access	x	Laboratorios	Fa0/36	Disponible	36	-	-
access	x	Laboratorios	Fa0/37	Activado	37	PCFICA-191	172.17.X.X

access	x	Laboratorios	Fa0/38	Disponible	38	-	-
access	x	Laboratorios	Fa0/39	Activado	39	PCFICA-198	172.17.X.X
access	x	Laboratorios	Fa0/40	Activado	40	PCFICA-200	172.17.X.X
access	x	Laboratorios	Fa0/41	Disponible	41	-	-
access	x	Laboratorios	Fa0/42	Disponible	42	-	-
access	x	Laboratorios	Fa0/43	Disponible	43	-	-
access	x	Laboratorios	Fa0/44	Disponible	44	-	-
access	x	Laboratorios	Fa0/45	Disponible	45	-	-
access	x	Laboratorios	Fa0/46	Disponible	46	-	-
access	x	Laboratorios	Fa0/47	Disponible	47	-	-
access	x	Administrativos	Fa0/48	Activado	48	-	-
trunk			G1/0			-	-
			G2/0			-	-

Fuente: (Espinosa,2017)

1.2.1.2 Laboratorio 3.

Este laboratorio se encuentra en la primera plata del edificio como se muestra en la Figura 23, los equipos de telecomunicaciones presentes como se muestra en la Tabla 20 y su mapeo de puerto como se muestra en la Tabla 21.

Tabla 20: *Equipos Lab.3 – FICA*

Equipos de Telecomunicaciones	Marca	Nombre	Dirección IP	Cantidad
Rack De Pared De 19"	Panduit	-----	-----	1
Patch Panel De 24 Puertos Cat. 6.	Newlink	-----	-----	1
Switch De 48 Puertos	WS-C2960-48TC-L	SW-Copérnico	172.17.X.X	1
Switch De 24 Puertos	WS-C2960-24TC-L	SW-Coulomb	172.17.X.X	1

Fuente: Adaptado de Laboratorio 3 – FICA

Tabla 21: *Mapeo de red Lab.3 – FICA*

Switch Catalyst 2960 Laboratorio 3							Equipo conectado	
Modo VLAN	VAN	Descripción	Puerto	Punto Red/N°	Estado	PatchPanel	Nombre	IP
access	x	Laboratorios	Fa0/1	Si/A01	Activado	A01	PCFICA-390	172.17.X.X
access	x	Laboratorios	Fa0/2	Si/A02	Disponible	A02	-	-
access	x	Laboratorios	Fa0/3	Si/A03	Activado	A03	PCFICA-388	172.17.X.X
access	x	Laboratorios	Fa0/4	Si/A04	Activado	A04	PCFICA-389	172.17.X.X
access	x	Laboratorios	Fa0/5	Si/A05	Disponible	A05	-	-
access	x	Laboratorios	Fa0/6	Si/A06	Activado	A06	PCFICA-382	172.17.X.X
access	x	Laboratorios	Fa0/7	Si/A07	Activado	A07	PCFICA-383	172.17.X.X
access	x	Laboratorios	Fa0/8	Si/A08	Activado	A08	PCFICA-384	172.17.X.X
access	x	Laboratorios	Fa0/9	Si/A09	Activado	A09	PCFICA-378	172.17.X.X
access	x	Laboratorios	Fa0/10	Si/A10	Activado	A10	PCFICA-376	172.17.X.X
access	x	Laboratorios	Fa0/11	Si/A11	Activado	A11	PCFICA-377	172.17.X.X
access	x	Laboratorios	Fa0/12	Si/A12	Activado	A12	PCFICA-372	172.17.X.X
access	x	Laboratorios	Fa0/13	Si/A13	Activado	A13	PCFICA-371	172.17.X.X
access	x	Laboratorios	Fa0/14	Si/A14	Disponible	A14	-	-
access	x	Laboratorios	Fa0/15	Si/A15	Disponible	A15	-	-

access	x	Laboratorios	Fa0/16	Si/A16	Activado	A16	PCFICA-370	172.17.X.X
access	x	Laboratorios	Fa0/17	Si/A17	Disponible	A17	-	-
access	x	Laboratorios	Fa0/18	Si/A18	Activado	A18	PCFICA-366	172.17.X.X
access	x	Laboratorios	Fa0/19	Si/A19	Activado	A19	PCFICA-364	172.17.X.X
access	x	Laboratorios	Fa0/20	Si/A20	Activado	A20	PCFICA-365	172.17.X.X
access	x	Laboratorios	Fa0/21	Si/A21	Disponible	A21	-	-
access	x	Laboratorios	Fa0/22	Si/A22	Activado	A22	PCFICA-362	172.17.X.X
access	x	Laboratorios	Fa0/23	Si/A23	Activado	A23	PCFICA-361	172.17.X.X
access	x	Laboratorios	Fa0/24	Si/A24	Activado	A24	PCFICA-364	172.17.X.X
access	x	Laboratorios	Fa0/25	Si/B01	Disponible	B01	-	-
access	x	Laboratorios	Fa0/26	Si/B02	Activado	B02	PCFICA-369	172.17.X.X
access	x	Laboratorios	Fa0/27	Si/B03	Activado	B03	PCFICA-367	172.17.X.X
access	x	Laboratorios	Fa0/28	Si/B04	Activado	B04	PCFICA-368	172.17.X.X
access	x	Laboratorios	Fa0/29	Si/B05	Disponible	B05	-	-
access	x	Laboratorios	Fa0/30	Si/B06	Disponible	B06	-	-
access	x	Laboratorios	Fa0/31	Si/B07	Activado	B07	PCFICA-375	172.17.X.X
access	x	Laboratorios	Fa0/32	Si/B08	Activado	B08	PCFICA-373	172.17.X.X
access	x	Laboratorios	Fa0/33	Si/B09	Activado	B09	PCFICA-374	172.17.X.X
access	x	Laboratorios	Fa0/34	Si/B10	Activado	B10	PCFICA-379	172.17.X.X
access	x	Laboratorios	Fa0/35	Si/B11	Activado	B11	PCFICA-381	172.17.X.X
access	x	Laboratorios	Fa0/36	Si/B12	Activado	B12	PCFICA-380	172.17.X.X
access	x	Laboratorios	Fa0/37	Si/B13	Disponible	B13	-	-
access	x	Laboratorios	Fa0/38	Si/B14	Activado	B14	PCFICA-386	172.17.X.X
access	x	Laboratorios	Fa0/39	Si/B15	Activado	B15	PCFICA-387	172.17.X.X
access	x	Laboratorios	Fa0/40	Si/B16	Activado	B16	PCFICA-385	172.17.X.X
access	x	Laboratorios	Fa0/41	Si/B17	Disponible	B17	-	-
access	x	Laboratorios	Fa0/42	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/43	Si/B19	Disponible	B19	-	-
access	x	Laboratorios	Fa0/44	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/45	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/46	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/47	NO	Disponible	-	-	-
access	x	Administrativos	Fa0/48	NO	Disponible	-	-	-
trunk			G1/0	-	-	-	-	-
			G2/0	-	-	-	-	-

Fuente: (Espinosa,2017)

1.2.1.3 Laboratorio 4.

El laboratorio 4 se encuentra en la primera planta de la FICA como se muestra en la Figura 23, los equipos de telecomunicaciones presentes como se muestra en la Tabla 22 y su mapeo de puerto como se muestra en las Tabla 23.

Tabla 22: Equipos Lab.4 – FICA

Equipos de Telecomunicaciones	Nombre	Marca	Dirección IP	Cantidad
Rack de 19" de ancho – 24 UR	-----	Panduit	-----	1
Patch Panel De 24 Puertos Cat. 6.	-----	Newlink	-----	3
Switch De 48 Puertos	WS-C2960-48TC-L	SW-EUCLIDES	172.17.X.X	1
Switch De 48 Puertos	WS-C2960-48TC-L	SW-EULER	172.17.X.X	1

Fuente: Adaptado de Laboratorio 4 – FICA

Tabla 23: Mapeo de red Lab.4 – FICA

Switch Catalyst 2960 Laboratorio 4							Equipo conectado	
Modo VLAN	VAN	Descripción	Puerto	Punto Red/N°	Estado	PatchPanel	Nombre	IP
access	x	Laboratorios	Fa0/1	Si/A01	Disponible	A01	-	-
access	x	Laboratorios	Fa0/2	Si/A02	Disponible	A02	-	-
access	x	Laboratorios	Fa0/3	Si/A03	Disponible	A03	-	-
access	x	Laboratorios	Fa0/4	Si/A04	Disponible	A04	-	-
access	x	Laboratorios	Fa0/5	Si/A05	Activado	A05	PCFICA-350	172.17.X.X
access	x	Laboratorios	Fa0/6	Si/A06	Activado	A06	PCFICA-352	172.17.X.X
access	x	Laboratorios	Fa0/7	Si/A07	Disponible	A07	-	-
access	x	Laboratorios	Fa0/8	Si/A08	Activado	A08	PCFICA-351	172.17.X.X
access	x	Laboratorios	Fa0/9	Si/A09	Disponible	A09	-	-
access	x	Laboratorios	Fa0/10	Si/A10	Activado	A10	PCFICA-357	172.17.X.X
access	x	Laboratorios	Fa0/11	Si/A11	Activado	A11	PCFICA-356	172.17.X.X
access	x	Laboratorios	Fa0/12	Si/A12	Disponible	A12	-	-
access	x	Laboratorios	Fa0/13	Si/A13	Activado	A13	PCFICA-342	172.17.X.X
access	x	Laboratorios	Fa0/14	Si/A14	Activado	A14	PCFICA-181	172.17.X.X
access	x	Laboratorios	Fa0/15	Si/A15	Activado	A15	PCFICA-341	172.17.X.X
access	x	Laboratorios	Fa0/16	Si/A16	Disponible	A16	-	-
access	x	Laboratorios	Fa0/17	Si/A17	Activado	A17	PCFICA-347	172.17.X.X
access	x	Laboratorios	Fa0/18	Si/A18	Activado	A18	PCFICA-346	172.17.X.X
access	x	Laboratorios	Fa0/19	Si/A19	Disponible	A19	-	-
access	x	Laboratorios	Fa0/20	Si/A20	Disponible	A20	-	-
access	x	Laboratorios	Fa0/21	Si/A21	Disponible	A21	-	-
access	x	Laboratorios	Fa0/22	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/23	Si/A23	Disponible	A23	-	-
access	x	Laboratorios	Fa0/24	Si/A24	Disponible	A24	-	-
access	x	Laboratorios	Fa0/25	Si/B01	Disponible	B01	-	-
access	x	Laboratorios	Fa0/26	Si/B02	Disponible	B02	-	-
access	x	Laboratorios	Fa0/27	Si/B03	Activado	B03	PCFICA-344	172.17.X.X
access	x	Laboratorios	Fa0/28	Si/B04	Activado	B04	PCFICA-343	172.17.X.X
access	x	Laboratorios	Fa0/29	Si/B05	Activado	B05	PCFICA-345	172.17.X.X
access	x	Laboratorios	Fa0/30	Si/B06	Activado	B06	PCFICA-348	172.17.X.X
access	x	Laboratorios	Fa0/31	Si/B07	Disponible	B07	-	-
access	x	Laboratorios	Fa0/32	Si/B08	Disponible	B08	-	-
access	x	Laboratorios	Fa0/33	Si/B09	Activado	B09	PCFICA-349	172.17.X.X
access	x	Laboratorios	Fa0/34	Si/B10	Disponible	B10	-	-
access	x	Laboratorios	Fa0/35	Si/B11	Activado	B11	PCFICA-353	172.17.X.X
access	x	Laboratorios	Fa0/36	Si/B12	Activado	B12	PCFICA-355	172.17.X.X
access	x	Laboratorios	Fa0/37	Si/B13	Disponible	B13	-	-
access	x	Laboratorios	Fa0/38	Si/B14	Activado	B14	PCFICA-354	172.17.X.X
access	x	Laboratorios	Fa0/39	Si/B15	Activado	B15	PCFICA-360	172.17.X.X
access	x	Laboratorios	Fa0/40	Si/B16	Activado	B16	PCFICA-198	172.17.X.X
access	x	Laboratorios	Fa0/41	Si/B17	Disponible	B17	-	-
access	x	Laboratorios	Fa0/42	Si/B18	Disponible	B18	-	-
access	x	Laboratorios	Fa0/43	Si/B19	Disponible	B19	-	-
access	x	Laboratorios	Fa0/44	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/45	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/46	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/47	NO	Disponible	-	-	-
access	x	Administrativos	Fa0/48	NO	Disponible	-	-	-
trunk			G1/0	-	-	-	-	-
			G2/0	-	-	-	-	-

Fuente: (Espinosa,2017)

1.2.1.4 Laboratorio 5.

El laboratorio 5 se encuentra en el segundo piso de la FICA como se muestra en la Figura 24, en el cual se ubican dos switch 3COM 4200 y su mapeo de puerto como se muestra en la Tabla 24.

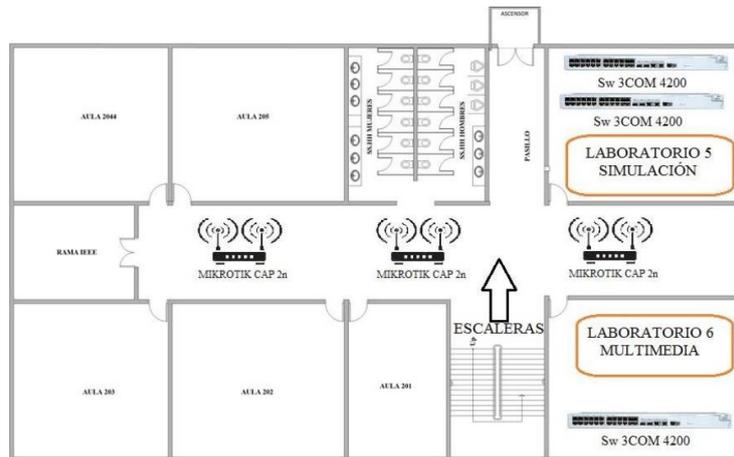


Figura 24: Segunda planta FICA-UTN
Fuente: DDTI - UTN

Tabla 24: Mapeo de red Lab.5 – FICA

Switch 3COM Laboratorio 5							Equipo conectado	
Modo VLAN	VAN	Descripción	Puerto	Punto Red/Nº	Estado	PatchPanel	Nombre	IP
access	x	Laboratorios	Fa0/1	NO	Disponible	NO	PCFICA-311	172.17.X.X
access	x	Laboratorios	Fa0/2	NO	Disponible	NO	PCFICA-312	172.17.X.X
access	x	Laboratorios	Fa0/3	NO	Disponible	NO	PCFICA-313	172.17.X.X
access	x	Laboratorios	Fa0/4	NO	Disponible	NO	PCFICA-314	172.17.X.X
access	x	Laboratorios	Fa0/5	NO	Activado	NO	PCFICA-315	172.17.X.X
access	x	Laboratorios	Fa0/6	NO	Activado	NO	PCFICA-316	172.17.X.X
access	x	Laboratorios	Fa0/7	NO	Activado	NO	PCFICA-317	172.17.X.X
access	x	Laboratorios	Fa0/8	NO	Activado	NO	PCFICA-318	172.17.X.X
access	x	Laboratorios	Fa0/9	NO	Activado	NO	-	-
access	x	Laboratorios	Fa0/10	NO	Activado	NO	-	-
access	x	Laboratorios	Fa0/11	NO	Activado	NO	-	-
access	x	Laboratorios	Fa0/12	NO	Activado	NO	-	-
access	x	Laboratorios	Fa0/13	NO	Activado	NO	PCFICA-319	172.17.X.X
access	x	Laboratorios	Fa0/14	NO	Activado	NO	PCFICA-320	172.17.X.X
access	x	Laboratorios	Fa0/15	NO	Activado	NO	PCFICA-321	172.17.X.X
access	x	Laboratorios	Fa0/16	NO	Activado	NO	PCFICA-322	172.17.X.X
access	x	Laboratorios	Fa0/17	NO	Activado	NO	PCFICA-323	172.17.X.X
access	x	Laboratorios	Fa0/18	NO	Activado	NO	PCFICA-324	172.17.X.X
access	x	Laboratorios	Fa0/19	NO	Activado	NO	PCFICA-325	172.17.X.X
access	x	Laboratorios	Fa0/20	NO	Activado	NO	PCFICA-326	172.17.X.X
access	x	Laboratorios	Fa0/21	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/22	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/23	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/24	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/1	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/2	NO	Activado	NO	PCFICA-327	172.17.X.X
access	x	Laboratorios	Fa0/3	NO	Activado	NO	PCFICA-328	172.17.X.X
access	x	Laboratorios	Fa0/4	NO	Activado	NO	PCFICA-329	172.17.X.X
access	x	Laboratorios	Fa0/5	NO	Activado	NO	PCFICA-330	172.17.X.X
access	x	Laboratorios	Fa0/6	NO	Activado	NO	PCFICA-331	172.17.X.X
access	x	Laboratorios	Fa0/7	NO	Activado	NO	PCFICA-332	172.17.X.X
access	x	Laboratorios	Fa0/8	NO	Activado	NO	PCFICA-333	172.17.X.X
access	x	Laboratorios	Fa0/9	NO	Activado	NO	PCFICA-334	172.17.X.X
access	x	Laboratorios	Fa0/10	NO	Activado	NO	PCFICA-335	172.17.X.X
access	x	Laboratorios	Fa0/11	NO	Activado	NO	PCFICA-336	172.17.X.X
access	x	Laboratorios	Fa0/12	NO	Activado	NO	PCFICA-337	172.17.X.X
access	x	Laboratorios	Fa0/13	NO	Activado	NO	PCFICA-338	172.17.X.X
access	x	Laboratorios	Fa0/14	NO	Activado	NO	PCFICA-338	172.17.X.X
access	x	Laboratorios	Fa0/15	NO	Activado	NO	PCFICA-340	172.17.X.X
access	x	Laboratorios	Fa0/16	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/17	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/18	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/19	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/20	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/21	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/22	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/23	NO	Disponible	NO	-	-

access	x	Administrativos	Fa0/24	NO	Disponible	NO	-	-
trunk			G1/0	-	-	-	-	-
			G2/0	-	-	-	-	-

Fuente: (Espinosa,2017)

1.2.1.5 Laboratorio 6.

El laboratorio 6 se ubica en el segundo piso de la FICA como se muestra en la figura 24, en el cual se encuentran un switch 3COM 4200 y su mapeo de puerto como se muestra en la Tabla 25.

Tabla 25: Mapeo de red Lab.6 – FICA

Switch 3COM Laboratorio 6							Equipo conectado	
Modo VLAN	VAN	Descripción	Puerto	Punto Red/N°	Estado	PatchPanel	Nombre	IP
access	x	Laboratorios	Fa0/1	NO	Disponible	NO	PCFICA-311	172.17.X.X
access	x	Laboratorios	Fa0/2	NO	Disponible	NO	PCFICA-312	172.17.X.X
access	x	Laboratorios	Fa0/3	NO	Disponible	NO	PCFICA-313	172.17.X.X
access	x	Laboratorios	Fa0/4	NO	Disponible	NO	PCFICA-314	172.17.X.X
access	x	Laboratorios	Fa0/5	NO	Activado	NO	PCFICA-315	172.17.X.X
access	x	Laboratorios	Fa0/6	NO	Activado	NO	PCFICA-316	172.17.X.X
access	x	Laboratorios	Fa0/7	NO	Activado	NO	PCFICA-317	172.17.X.X
access	x	Laboratorios	Fa0/8	NO	Activado	NO	PCFICA-318	172.17.X.X
access	x	Laboratorios	Fa0/9	NO	Activado	NO	-	-
access	x	Laboratorios	Fa0/10	NO	Activado	NO	-	-
access	x	Laboratorios	Fa0/11	NO	Activado	NO	-	-
access	x	Laboratorios	Fa0/12	NO	Activado	NO	-	-
access	x	Laboratorios	Fa0/13	NO	Activado	NO	PCFICA-319	172.17.X.X
access	x	Laboratorios	Fa0/14	NO	Activado	NO	PCFICA-320	172.17.X.X
access	x	Laboratorios	Fa0/15	NO	Activado	NO	PCFICA-321	172.17.X.X
access	x	Laboratorios	Fa0/16	NO	Activado	NO	PCFICA-322	172.17.X.X
access	x	Laboratorios	Fa0/17	NO	Activado	NO	PCFICA-323	172.17.X.X
access	x	Laboratorios	Fa0/18	NO	Activado	NO	PCFICA-324	172.17.X.X
access	x	Laboratorios	Fa0/19	NO	Activado	NO	PCFICA-325	172.17.X.X
access	x	Laboratorios	Fa0/20	NO	Activado	NO	PCFICA-326	172.17.X.X
access	x	Laboratorios	Fa0/21	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/22	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/23	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/24	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/25	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/26	NO	Activado	NO	PCFICA-327	172.17.X.X
access	x	Laboratorios	Fa0/27	NO	Activado	NO	PCFICA-328	172.17.X.X
access	x	Laboratorios	Fa0/28	NO	Activado	NO	PCFICA-329	172.17.X.X
access	x	Laboratorios	Fa0/29	NO	Activado	NO	PCFICA-330	172.17.X.X
access	x	Laboratorios	Fa0/30	NO	Activado	NO	PCFICA-331	172.17.X.X
access	x	Laboratorios	Fa0/32	NO	Activado	NO	PCFICA-332	172.17.X.X
access	x	Laboratorios	Fa0/32	NO	Activado	NO	PCFICA-333	172.17.X.X
access	x	Laboratorios	Fa0/33	NO	Activado	NO	PCFICA-334	172.17.X.X
access	x	Laboratorios	Fa0/34	NO	Activado	NO	PCFICA-335	172.17.X.X
access	x	Laboratorios	Fa0/35	NO	Activado	NO	PCFICA-336	172.17.X.X
access	x	Laboratorios	Fa0/36	NO	Activado	NO	PCFICA-337	172.17.X.X
access	x	Laboratorios	Fa0/37	NO	Activado	NO	PCFICA-338	172.17.X.X
access	x	Laboratorios	Fa0/38	NO	Activado	NO	PCFICA-338	172.17.X.X
access	x	Laboratorios	Fa0/39	NO	Activado	NO	PCFICA-340	172.17.X.X
access	x	Laboratorios	Fa0/40	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/41	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/42	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/43	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/44	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/45	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/46	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/47	NO	Disponible	NO	-	-
access	x	Administrativos	Fa0/48	NO	Disponible	NO	-	-
trunk			G1/0	-	-	-	-	-
			G2/0	-	-	-	-	-

Fuente: SuperPutty

1.2.1.6 Laboratorio 9.

Este laboratorio se encuentra en el último piso de la FICA como se muestra en la Figura 25. En el laboratorio 9 se alojan los equipos de telecomunicaciones y desde ahí se da acceso a la red también al laboratorio 8, que solo cuenta con puntos de red identificados con la inicial “B” más el número correspondiente del puerto. Los equipos de telecomunicaciones presentes como se muestra en la Tabla 26 y su mapeo de puerto como se muestra en la Tabla 27.

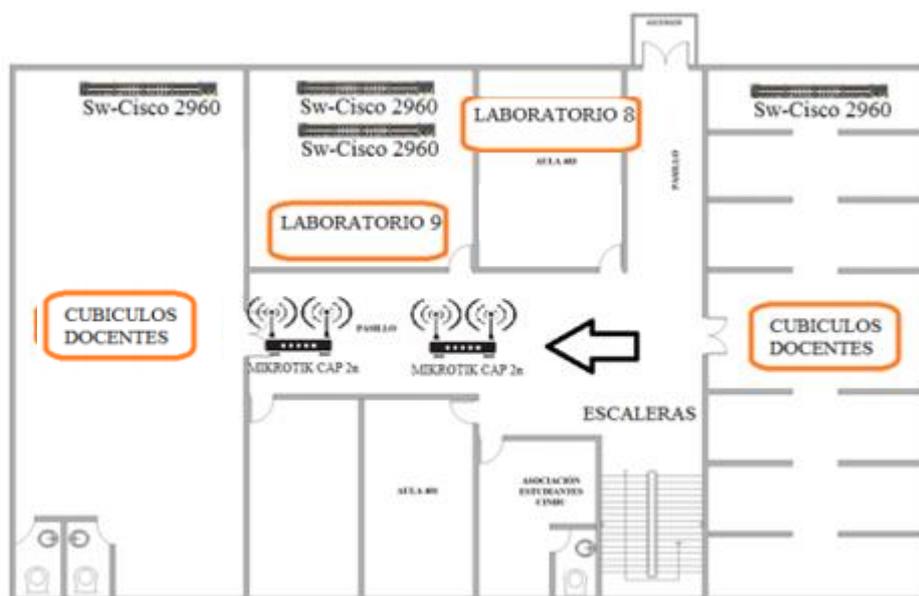


Figura 25: Cuarta planta FICA-UTN
Fuente: DDTI - UTN

Tabla 26: Equipos Lab.9 – FICA

Equipos de Telecomunicaciones	Marca	Nombre	Dirección IP	Cantidad
Rack De 19" de ancho-36 UR	Panduit	-----	-----	1
Patch Panel De 24 Puertos Cat. 6.	Newlink	-----	-----	4
Switch De 48 Puertos	Cisco Catalyst 2960	-----	172.20.X.X	1
Switch De 48 Puertos	Cisco Catalyst 2960	-----	172.20.X.X	1

Fuente: Adaptado de Laboratorio 9 – FICA

Tabla 27: Mapeo de red Lab.9 – FICA

Switch Catalyst 2960 Laboratorio 9							Equipo conectado	
Modo VLAN	VAN	Descripción	Puerto	Punto Red/N°	Estado	PatchPanel	Nombre	IP
access	x	Laboratorios	Fa0/1	PPA01	Activado	A01	PCFICA-175	172.17.X.X
access	x	Laboratorios	Fa0/2	PPA02	Activado	A02	PCFICA-176	172.17.X.X
access	x	Laboratorios	Fa0/3	PPA03	Activado	A03	PCFICA-177	172.17.X.X
access	x	Laboratorios	Fa0/4	PPA04	Activado	A04	PCFICA-178	172.17.X.X
access	x	Laboratorios	Fa0/5	PPA05	Activado	A05	PCFICA-170	172.17.X.X
access	x	Laboratorios	Fa0/6	PPA06	Activado	A06	PCFICA-171	172.17.X.X
access	x	Laboratorios	Fa0/7	PPA07	Activado	A07	PCFICA-172	172.17.X.X
access	x	Laboratorios	Fa0/8	PPA08	Activado	A08	PCFICA-174	172.17.X.X
access	x	Laboratorios	Fa0/9	PPA09	Activado	A09	PCFICA-165	172.17.X.X
access	x	Laboratorios	Fa0/10	PPA10	Activado	A10	PCFICA-166	172.17.X.X
access	x	Laboratorios	Fa0/11	PPA11	Activado	A11	PCFICA-167	172.17.X.X
access	x	Laboratorios	Fa0/12	PPA12	Activado	A12	PCFICA-168	172.17.X.X
access	x	Laboratorios	Fa0/13	PPA13	Disponible	A13	-	-
access	x	Laboratorios	Fa0/14	PPA14	Disponible	A14	-	-
access	x	Laboratorios	Fa0/15	PPA15	Disponible	A15	-	-
access	x	Laboratorios	Fa0/16	PPA16	Disponible	A16	-	-
access	x	Laboratorios	Fa0/17	PPA17	Activado	A17	PCFICA-163	172.17.X.X
access	x	Laboratorios	Fa0/18	PPA18	Activado	A18	PCFICA-162	172.17.X.X
access	x	Laboratorios	Fa0/19	PPA19	Activado	A19	PCFICA-161	172.17.X.X
access	x	Laboratorios	Fa0/20	PPA20	Activado	A20	PCFICA-160	172.17.X.X
access	x	Laboratorios	Fa0/21	PPA21	Disponible	A21	-	-
access	x	Laboratorios	Fa0/22	PPA22	Disponible	A22	-	-
access	x	Laboratorios	Fa0/23	PPA23	Disponible	A23	-	-
access	x	Laboratorios	Fa0/24	PPA24	Disponible	A24	-	-
access	x	Laboratorios	Fa0/25	PPB01	Disponible	B01	-	-
access	x	Laboratorios	Fa0/26	PPB02	Disponible	B02	-	-
access	x	Laboratorios	Fa0/27	PPB03	Disponible	B03	-	-
access	x	Laboratorios	Fa0/28	PPB04	Activado	B04	PCFICA-263	172.17.X.X
access	x	Laboratorios	Fa0/29	PPB05	Activado	B05	PCFICA-264	172.17.X.X
access	x	Laboratorios	Fa0/30	PPB06	Activado	B06	PCFICA-265	172.17.X.X
access	x	Laboratorios	Fa0/31	PPB07	Activado	B07	PCFICA-267	172.17.X.X
access	x	Laboratorios	Fa0/32	PPB08	Disponible	B08	-	-
access	x	Laboratorios	Fa0/33	PPB09	Disponible	B09	-	-
access	x	Laboratorios	Fa0/34	PPB10	Activado	B10	PCFICA-253	-
access	x	Laboratorios	Fa0/35	PPB11	Activado	B11	PCFICA-269	172.17.X.X
access	x	Laboratorios	Fa0/36	PPB12	Disponible	B12	-	-
access	x	Laboratorios	Fa0/37	PPB13	Disponible	B13	-	-
access	x	Laboratorios	Fa0/38	PPB14	Activado	B14	PCFICA-270	172.17.X.X
access	x	Laboratorios	Fa0/39	PPB15	Activado	B15	PCFICA-273	172.17.X.X
access	x	Laboratorios	Fa0/40	PPB16	Disponible	B16	-	-
access	x	Laboratorios	Fa0/41	PPB17	Disponible	B17	-	-
access	x	Laboratorios	Fa0/42	PPB18	Activado	B18	PCFICA-274	172.17.X.X
access	x	Laboratorios	Fa0/43	PPB19	Activado	B19	PCFICA-250	172.17.X.X
access	x	Laboratorios	Fa0/44	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/45	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/46	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/47	NO	Disponible	-	-	-
access	x	Administrativos	Fa0/48	NO	Disponible	-	-	-
trunk			G1/0	-	-	-	-	-
			G2/0	-	-	-	-	-

Fuente: SuperPutty

1.2.1.7 Cubículos docentes 1.

Esta dependencia se encuentra en el último piso de la FICA como se muestra en la Figura 25, los equipos de telecomunicaciones presentes como se muestra en la Tabla 28 y su mapeo de puerto como se muestra en la Tabla 29.

Tabla 28: Equipos Cubículos docentes 1 – FICA

Equipos de Telecomunicaciones	Marca	Nombre	Dirección IP	Cantidad
Rack De PARED 19"	Panduit	-----	-----	1
Patch Panel De 24 Puertos Cat. 6.	Newlink	-----	-----	1
Switch De 48 Puertos	WS-C2960-24TC-L	SW-Galileo	172.20.X.XX	1

Fuente: Adaptado de cubículos de docentes 1 – FICA

Tabla 29: Mapeo de red cubículos docentes 1

Switch Catalyst 2960 Sala de Profesores							Equipo conectado	
Modo VLAN	VAN	Descripción	Puerto	Punto Red/N°	Estado	PatchPanel	Nombre	IP
access	x	Laboratorios	Fa0/1	Si/A01	Disponible	A01	-	-
access	x	Laboratorios	Fa0/2	Si/A02	Disponible	A02	-	-
access	x	Laboratorios	Fa0/3	Si/A03	BBDisponible	A03	-	-
access	x	Laboratorios	Fa0/4	Si/A04	Disponible	A04	-	-
access	x	Laboratorios	Fa0/5	Si/A05	Disponible	A05	-	-
access	x	Laboratorios	Fa0/6	Si/A06	Disponible	A06	-	-
access	x	Laboratorios	Fa0/7	Si/A07	Disponible	A07	-	-
access	x	Laboratorios	Fa0/8	Si/A08	Disponible	A08	-	-
access	x	Laboratorios	Fa0/9	Si/A09	Disponible	A09	-	-
access	x	Laboratorios	Fa0/10	Si/A10	Disponible	A10	-	-
access	x	Laboratorios	Fa0/11	Si/A11	Disponible	A11	-	-
access	x	Laboratorios	Fa0/12	Si/A12	Disponible	A12	-	-
access	x	Laboratorios	Fa0/13	Si/A13	Disponible	A13	-	-
access	x	Laboratorios	Fa0/14	Si/A14	Disponible	A14	-	-
access	x	Laboratorios	Fa0/15	Si/A15	Disponible	A15	-	-
access	x	Laboratorios	Fa0/16	Si/A16	Disponible	A16	-	-
access	x	Laboratorios	Fa0/17	Si/A17	Disponible	A17	-	-
access	x	Laboratorios	Fa0/18	Si/A18	Disponible	A18	-	-
access	x	Laboratorios	Fa0/19	Si/A19	Disponible	A19	-	-
access	x	Laboratorios	Fa0/20	Si/A20	Disponible	A20	-	-
access	x	Laboratorios	Fa0/21	Si/A21	Disponible	A21	-	-
access	x	Laboratorios	Fa0/22	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/23	Si/A23	Disponible	A23	-	-
access	x	Laboratorios	Fa0/24	Si/A24	Disponible	A24	-	-
access	x	Laboratorios	Fa0/25	Si/B01	Disponible	B01	-	-
access	x	Laboratorios	Fa0/26	Si/B02	Disponible	B02	-	-
access	x	Laboratorios	Fa0/27	Si/B03	Disponible	B03	-	-
access	x	Laboratorios	Fa0/28	Si/B04	Disponible	B04	-	-
access	x	Laboratorios	Fa0/29	Si/B05	Disponible	B05	-	-
access	x	Laboratorios	Fa0/30	Si/B06	Disponible	B06	-	-
access	x	Laboratorios	Fa0/31	Si/B07	Disponible	B07	-	-
access	x	Laboratorios	Fa0/32	Si/B08	Disponible	B08	-	-
access	x	Laboratorios	Fa0/33	Si/B09	Disponible	B09	-	-
access	x	Laboratorios	Fa0/34	Si/B10	Disponible	B10	-	-
access	x	Laboratorios	Fa0/35	Si/B11	Disponible	B11	-	-
access	x	Laboratorios	Fa0/36	Si/B12	Disponible	B12	-	-
access	x	Laboratorios	Fa0/37	Si/B13	Disponible	B13	-	-
access	x	Laboratorios	Fa0/38	Si/B14	Disponible	B14	-	-
access	x	Laboratorios	Fa0/39	Si/B15	Disponible	B15	-	-
access	x	Laboratorios	Fa0/40	Si/B16	Disponible	B16	-	-
access	x	Laboratorios	Fa0/41	Si/B17	Disponible	B17	-	-
access	x	Laboratorios	Fa0/42	Si/B18	Disponible	B18	-	-
access	x	Laboratorios	Fa0/43	Si/B19	Disponible	B19	-	-
access	x	Laboratorios	Fa0/44	NO	Disponible	-	-	-
trunk			G1/0	-	-	-	-	-
			G2/0	-	-	-	-	-

Fuente: SuperPutty

1.2.1.8 Cubículos docentes 2.

Los cubículos se encuentran en el último piso de la FICA como se muestra en la Figura 25, los equipos de telecomunicaciones presentes como se muestra en la Tabla 30 y su mapeo de puerto como se muestra en la Tabla 31.

Tabla 30: Equipos cubículos docentes 2 – FICA

Equipos de Telecomunicaciones	Marca	Nombre	Dirección IP	Cantidad
Rack de pared 19"	Panduit	-----	-----	1
Patch Panel De 24 Puertos Cat. 6.	Newlink	-----	-----	2
Switch De 48 Puertos	WS-C2960-48TC-L	SW-Fourier	172.20.X.X	1

Fuente: Adaptado de Cubículos de docentes 2 – FICA

Tabla 31: Mapeo de red cubículos docentes 2

Switch Catalyst 2960 de Cubículos de Profesores						Equipo conectado		
Modo VLAN	VAN	Descripción	Puerto	Punto Red/N°	Estado	PatchPanel	Nombre	IP
access	x	Laboratorios	Fa0/1	NO	Activado	A01	-	-
access	x	Laboratorios	Fa0/2	NO	Activado	A02	-	172.17.X.X
access	x	Laboratorios	Fa0/3	NO	Disponibile	A03	-	-
access	x	Laboratorios	Fa0/4	NO	Disponibile	A04	-	-
access	x	Laboratorios	Fa0/5	NO	Activado	A05	-	172.17.X.X
access	x	Laboratorios	Fa0/6	NO	Disponibile	A06	-	172.17.X.X
access	x	Laboratorios	Fa0/7	NO	Activado	A07	-	-
access	x	Laboratorios	Fa0/8	NO	Disponibile	A08	-	172.17.X.X
access	x	Laboratorios	Fa0/9	NO	Disponibile	A09	-	-
access	x	Laboratorios	Fa0/10	NO	Disponibile	A10	-	172.17.X.X
access	x	Laboratorios	Fa0/11	NO	Disponibile	A11	-	172.17.X.X
access	x	Laboratorios	Fa0/12	NO	Disponibile	A12	-	-
access	x	Laboratorios	Fa0/13	NO	Disponibile	A13	-	172.17.X.X
access	x	Laboratorios	Fa0/14	NO	Disponibile	A14	-	172.17.X.X
access	x	Laboratorios	Fa0/15	NO	Disponibile	A15	-	172.17.X.X
access	x	Laboratorios	Fa0/16	NO	Activado	A16	-	-
access	x	Laboratorios	Fa0/17	NO	Disponibile	A17	-	172.17.X.X
access	x	Laboratorios	Fa0/18	NO	Disponibile	A18	-	172.17.X.X
access	x	Laboratorios	Fa0/19	NO	Activado	A19	-	-
access	x	Laboratorios	Fa0/20	NO	Disponibile	A20	-	-
access	x	Laboratorios	Fa0/21	NO	Disponibile	A21	-	-
access	x	Laboratorios	Fa0/22	NO	Activado	-	-	-
access	x	Laboratorios	Fa0/23	NO	Activado	A23	-	-
access	x	Laboratorios	Fa0/24	NO	Disponibile	A24	-	-
access	x	Laboratorios	Fa0/25	NO	Disponibile	B01	-	-
access	x	Laboratorios	Fa0/26	NO	Disponibile	B02	-	-
access	x	Laboratorios	Fa0/27	NO	Disponibile	B03	-	172.17.X.X
access	x	Laboratorios	Fa0/28	NO	Disponibile	B04	-	172.17.X.X
access	x	Laboratorios	Fa0/29	NO	Disponibile	B05	-	172.17.X.X
access	x	Laboratorios	Fa0/30	NO	Disponibile	B06	-	172.17.X.X
access	x	Laboratorios	Fa0/31	NO	Disponibile	B07	-	-
access	x	Laboratorios	Fa0/32	NO	Disponibile	B08	-	-
access	x	Laboratorios	Fa0/33	NO	Disponibile	B09	-	172.17.X.X
access	x	Laboratorios	Fa0/34	NO	Activado	B10	-	-
access	x	Laboratorios	Fa0/35	NO	Disponibile	B11	-	172.17.X.X
access	x	Laboratorios	Fa0/36	NO	Disponibile	B12	-	172.17.X.X
access	x	Laboratorios	Fa0/37	NO	Disponibile	B13	-	-
access	x	Laboratorios	Fa0/38	NO	Disponibile	B14	-	172.17.X.X

access	x	Laboratorios	Fa0/39	NO	Disponible	B15	-	172.17.X.X
access	x	Laboratorios	Fa0/40	NO	Disponible	B16	-	172.17.X.X
access	x	Laboratorios	Fa0/41	NO	Disponible	B17	-	-
access	x	Laboratorios	Fa0/42	NO	Disponible	B18	-	-
access	x	Laboratorios	Fa0/43	NO	Disponible	B19	-	-
access	x	Laboratorios	Fa0/44	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/45	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/46	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/47	NO	Disponible	-	-	-
access	x	Administrativos	Fa0/48	NO	Disponible	-	-	-
trunk			G1/0	-	Activado	-	-	-
			G2/0	-	-	-	-	-

Fuente: SuperPutty

3.2.2 FICAYA.

Los switch de distribución de esta facultad se encuentran distribuidos en varias locaciones unos dentro de la universidad, otros repartidos por el campus forestal “Yuyucocha” y la granja experimental “La Pradera”. Estos últimos se conectan por enlaces de radio a la casona universitaria, la topología física como se muestra en la Figura 26, los equipos de telecomunicaciones como se muestra en la Tabla 32.

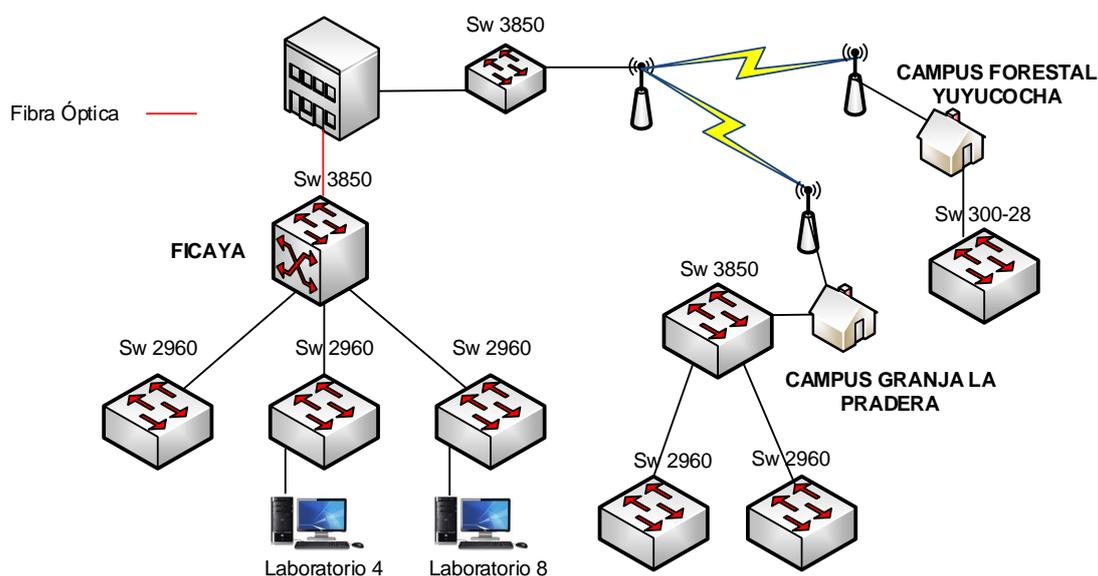


Figura 26: Topología física FICAYA-UTN

Fuente: DDTI-UTN

Tabla 32: Equipos de Telecomunicaciones – FICAYA

Ubicación	Equipos	Nombre	# Puertos
Cuarto de Equipos	WS-C3850-48T-S	SW3850-FICAYA	48
Cuarto de Equipos	WS-C2960X-48TS-L	SW2960-FICAYA-01	48

Cuarto de Equipos	WS-C2960X-48TS-L	SW2960-FICAYA-02	48
Cuarto de Equipos	WS-C2960X-48TS-L	SW2960-FICAYA-03	48
Yuyucocha	SG 300-28	SW-Ghost-Rider	28
La Pradera	WS-C3850-48T-S	SW-Falcon	48
La Pradera	WS-C2960X-48TS-L	SW-Aulas	48
La Pradera	WS-C2960X-48TS-L	SW-Oficinas	48

Fuente: Adaptado DDTI - UTN

3.2.3 FACAE.

Esta facultad presenta la siguiente topología física como se muestra en la Figura 27 y los equipos de telecomunicaciones como se muestra en la Tabla 33.

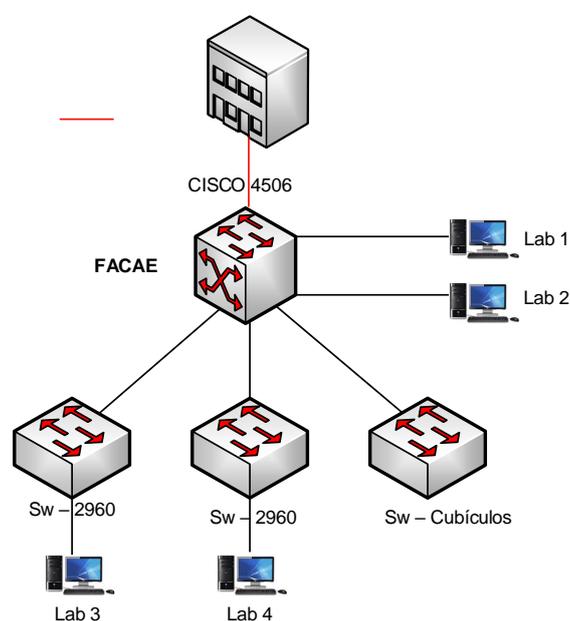


Figura 27: Topología física FACAE-UTN
Fuente: DDTI-UTN

Tabla 33: Equipos de Telecomunicaciones – FACAE

Ubicación	Equipos	Nombre	# Puertos
Cuarto de Equipos	WS-C4506-E L3	-	144
Cuarto de Equipos	WS-C2960X-48TS-L	-	48
Laboratorio IV	WS-C2960G-248TC-L	Elizabeth	48

3.2.4 FECYT.

Esta facultad presenta la siguiente topología física como se muestra en la Figura 28 y los equipos de telecomunicaciones como se muestra en la Tabla 34.

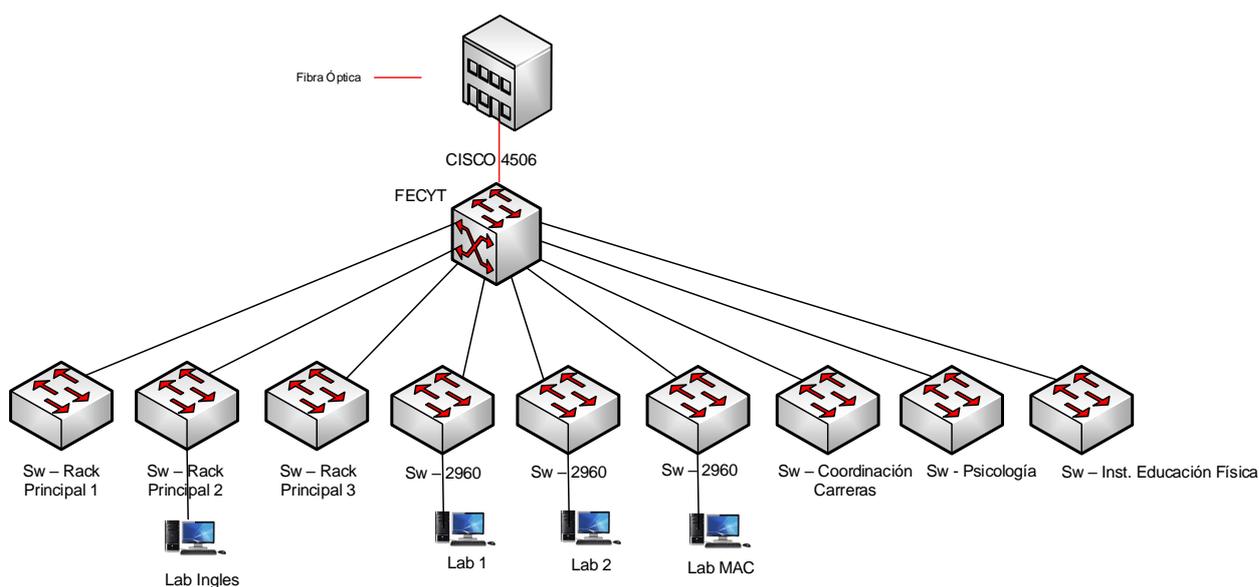


Figura 28: Topología física FECYT -UTN
Fuente: DDTI-UTN

Tabla 34: Equipos de Telecomunicaciones – FECYT

Ubicación	Equipos	Nombre	# Puertos
Cuarto de Equipos	WS-C3850-48T-S		48
Cuarto de Equipos	WS-C2960-48TC-L	SW-AC-DC	48
Cuarto de Equipos	WS-C2960-48TC-L	SW- Aerosmith	48
Cuarto de Equipos	WS-C2960-24TC-L	SW-Beatles	24
Laboratorio 1	WS-C2960-48TC-L	SW-Chicago	48
Laboratorio 2	WS-C2960-48TC-L	SW-Cinderella	48
Laboratorio MAC	WS-C2960-48TC-L	SW-Europe	48
Coordinación de Carreras	WS-C2960-48TC-L	SW-Jackson	48

Inst. Educación Física	WS-C2960-24TC-L	SW-Kiss	24
Psicología	WS-C2960-48TC-L	SW-SOAD	48

Fuente: Adaptado DDTI - UTN

3.2.5 FCCSS.

Esta facultad posee equipos de telecomunicaciones dentro de la casona universitaria, a su vez en el antiguo hospital San Vicente de Paul; estos últimos están enlazados por radio enlaces. La facultad presenta la siguiente topología física como se muestra en la Figura 29 y los equipos de telecomunicaciones como se muestra en la Tabla 35.

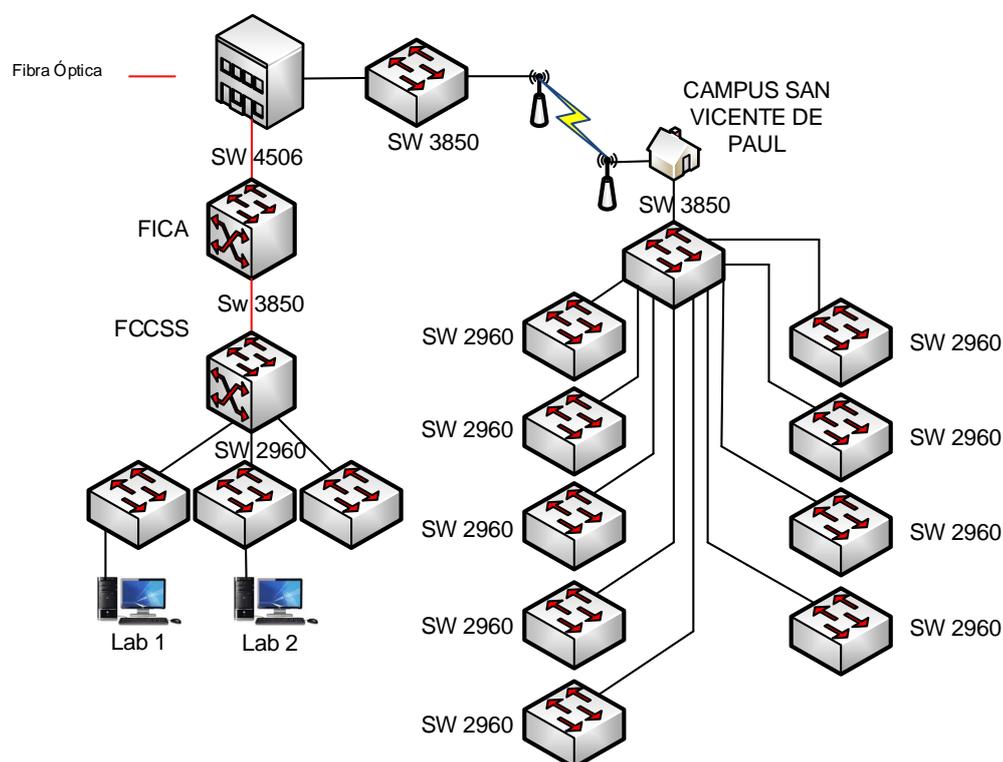


Figura 29: Topología física FCCSS -UTN
Fuente: DDTI-UTN

Tabla 35: Equipos de Telecomunicaciones – FCCSS

Ubicación	Equipos	Nombre	# Puertos
Cuarto de Equipos	WS-C3850-48T-S		48
Cuarto de Equipos	WS-C2960X-48TS-LL	SW- Pasteur	48

Planta Alta 4	WS-C2960X-48TS-LL	SW-PASILLO	48
Planta Alta 4	WS-C2960X-48TS-LL	SW-LAB1	48
Planta Alta 4	WS-C2960X-48TS-LL	SW-LAB2	28
Antiguo hospital San Vicente de Paul			
Planta Alta	WS-C3850-48T-S	SW1-R1	48
Planta Alta	WS-C2960-48TC-L	SW2-R1	48
Planta Alta	WS-C2960-48TC-L	SW1-R2	48
Planta Baja	WS-C2960-48TC-L	SW1-R3	48
Planta Baja	WS-C2960-48TC-L	SW1-R4	48
Planta Baja	WS-C2960-48TC-L	SW2-R4	48
Planta Baja	WS-C2960-48TC-L	SW1-R5	48
Planta Baja	WS-C2960-48TC-L	SW1-R6	48
Planta Baja	WS-C2960-48TC-L	SW1-R7	48
Planta Baja	WS-C2960-48TC-L	SW2-R7	48

Fuente: Adaptado DDTI - UTN

3.3 Descripción de la red en otras dependencias

3.3.1 Edificio central.

Este edificio cuenta con siguiente la topología física como se muestra en la Figura 30 y los equipos de telecomunicaciones como se muestra en la Tabla 36.

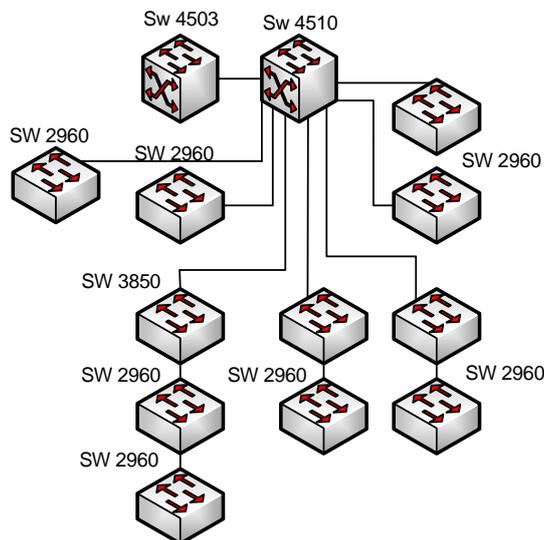


Figura 30: Topología física Edificio Central - UTN
Fuente: DDTI-UTN

Tabla 36: Equipos de Telecomunicaciones – Edificio Central

Ubicación	Equipos	Nombre	# Puertos
Datacenter	WS-C3750G-12S-S	SW-IPS-PUBLICAS	
Datacenter	WS-C4510R+E	SW-Zeus-Primario	
Datacenter	WS-C4503-E L3	SW-Zeus-Secundario	
Datacenter	Nexus 5548	SW-Nexus	
Datacenter Chasis Blade	WS-CBS3020-HPQ	SW-Afrodita	
Datacenter Chasis Blade	WS-CBS3020-HPQ	SW-Apolo	
Planta Baja	WS-C2960-48TC-L	SW-ATENEA	48
Planta Alta 1	WS-C2960-48TC-L	SW-CRATOS	48
Planta Alta1	WS-C2960-24TC-L	SW-CRONOS	24
Auditorio José Martí	WS-C2960-48TC-L	SW-ERIS	48
Auditorio José Martí	WS-C2960-48TC-L	SW-EROS	48
Canal Universitario	WS-C2960-48TC-L	SW-HADES	48
Planta Alta 4	WS-C3850-48T	SW-ANDROMEDA	48
Planta Alta 4	WS-C2960X-48TS-L	SW-ARTEMISA	48
Planta Alta 4	WS-C2960-48TC-L	SW-HERA	48
Entrada Principal	WS-C2960-24TC-L	SW-ACCESO	24

Fuente: Adaptado DDTI - UTN

3.3.2 Edificio posgrados.

La locación presenta la siguiente topología física como se muestra en Figura 31 y los equipos de telecomunicaciones como se muestra en la Tabla 37.

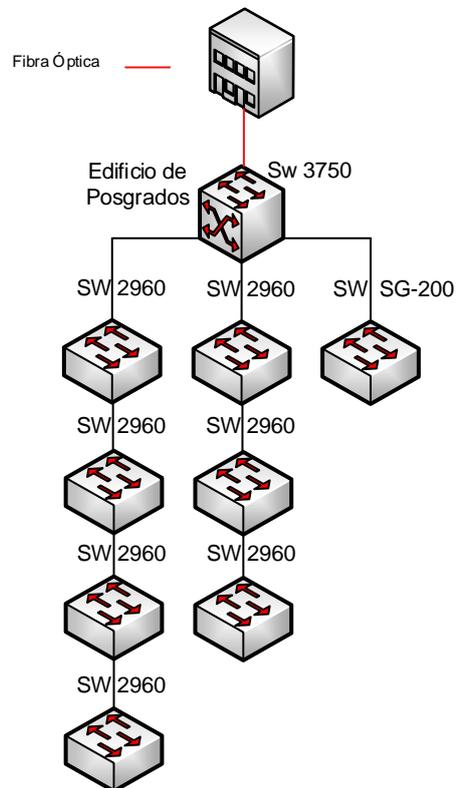


Figura 31: Topología física Edificio Posgrados - UTN
Fuente: DDTI-UTN

Tabla 37: Equipos de Telecomunicaciones – Edificio de Posgrado

Ubicación	Equipos	Nombre	# Puertos
Cuarto de Equipos	WS-C3750X-24	SW-Ares	24
Cuarto de Equipos	WS-C2960-24TC-L	Postgrado2	24
Cuarto de Equipos	WS-C2960-24TC-L	Postgrado3	24
Cuarto de Equipos	WS-C2960S-48TS-S	SW-Bills	48
Cuarto de Equipos	WS-C2960S-48TS-S	SW-Boo	48
Primer Piso	WS-C2960S-48TD-L	SW-Broly	48
Primer Piso	WS-C2960S-48TS-S	SW-Bulma	48
Primer Piso	WS-C2960S-48TS-S	SW-Cell	48

3.3.3 U. EMPRENDE, CAI.

El edificio presenta la siguiente topología física como se muestra en Figura 32 y los equipos de telecomunicaciones como se muestra en la Tabla 38.

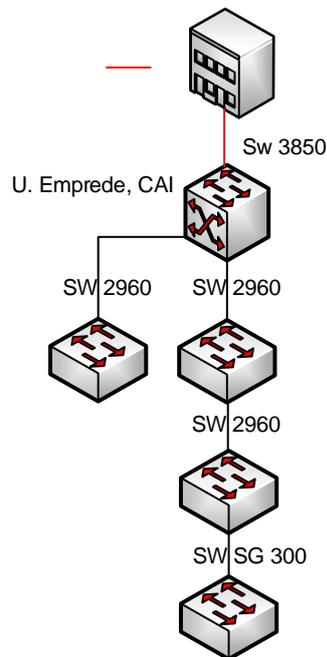


Figura 32: Topología física U Emprede, CAI - UTN
Fuente: DDTI-UTN

Tabla 38: *Equipos de Telecomunicaciones – U. EMPRENDE, CAI*

Ubicación	Equipos	Nombre	# Puertos
Planta Baja	WS-C3850-48T-S	SW3850-CAI	48
Planta Baja	WS-C2960X-48TS-L	CAI-SW2-R1	48
Segundo Piso	WS-C2960X-48TS-L	CAI-SW1-R2	48
Segundo Piso	SRW2048	CAI-SW2-R2	
	WS-C2960-48TC-L	CAI-SW3-R2	48

Fuente: Adaptado DDTI - UTN

3.3.4 Biblioteca.

El edificio posee la siguiente distribución física y los equipos de telecomunicaciones como se muestra en la Figura 33 y Tabla 39.

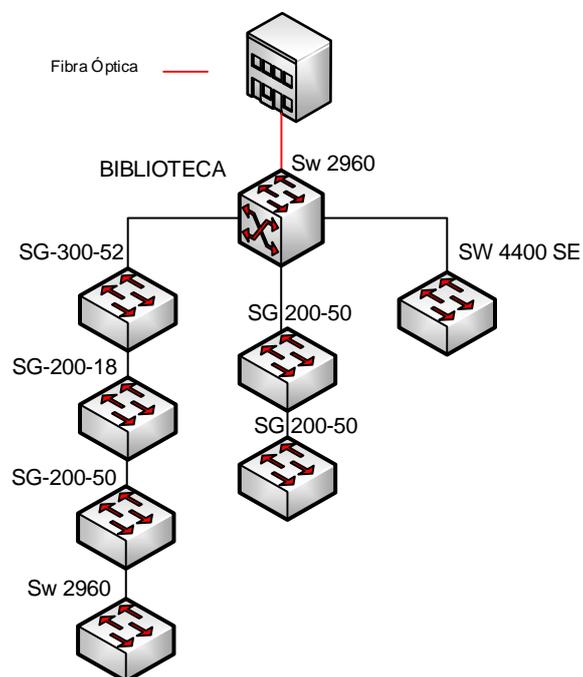


Figura 33: Topología física Biblioteca - UTN
Fuente: DDTI-UTN

Tabla 39: *Equipos de Telecomunicaciones – Biblioteca*

Ubicación	Equipos	Nombre	# Puertos
Cuarto de equipos	WS-C2960X-48TS-L	SW-BIBLIOTECA-01	48
Cuarto de equipos	SG-300-52	Alan-Poe	48
Cuarto de equipos	SG-200-18	Almagro	48
IC3	SG 200-50	Berne	48
IC3	SG 200-50	Borges	48
Cuarto de equipos	WS-C2960-48TS-LL	SW-Cámaras	48
Segundo piso	SS3 SW 4400 SE		

Fuente: Adaptado DDTI - UTN

3.3.5 Bienestar universitario.

Este edificio presenta la siguiente topología física como se muestra en la Figura 34 y los equipos de telecomunicaciones como se muestra en la Tabla 40.

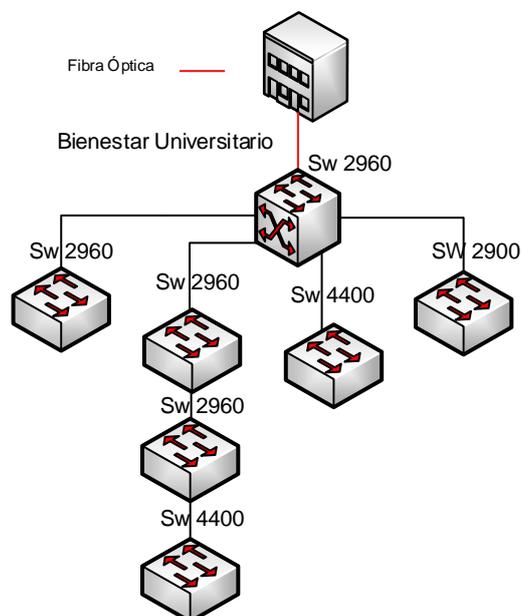


Figura 34: Topología física Biblioteca- UTN
Fuente: DDTI-UTN

Tabla 40: Equipos de Telecomunicaciones – Bienestar Universitario

Ubicación	Equipos	Nombre	# Puertos
Planta Baja	WS-C2960X-48TS-LL	SW-IRIS	48
Planta Baja	WS-C2960X-48TS-LL	SW-MORFEO	48
Planta Alta 2	WS-C2960X-48TS-LL	SW-NEMESIS	48
Planta Alta 2	WS-C2960X-48TS-LL	SW-NIX	48
Planta Alta 2	SS3 SW 4400 SE	SW-ODIN	
Planta Alta 4	SS3 SW 4400	SW-MOMO	
Garita		SW-PERSEO	

Fuente: Adaptado DDTI - UTN

3.3.6 Complejo acuático.

Este edificio presenta la siguiente topología física como se muestra en la Figura 35 y los sucesivos equipos de telecomunicaciones como se muestra en la Tabla 41.

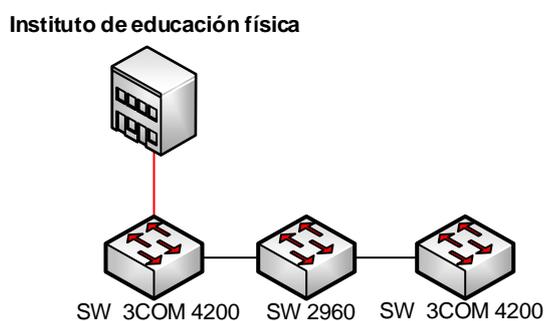


Figura 35: Topología física Complejo Acuático - UTN
Fuente: DDTI-UTN

Tabla 41: *Equipos de Telecomunicaciones – Complejo Acuático*

Ubicación	Equipos	Nombre	# Puertos
Piscina	SS3 SW 4200	SW-Metallica	
Clubes UTN	WS-C2960X-48TS-L	-	48
Gimnasio	SS3 SW 4400 SE	SW-Metallica	

Fuente: Adaptado DDTI - UTN

3.3.7 Auditorio Agustín Cueva.

Esta locación presenta los siguientes equipos de telecomunicaciones como se muestra en la Tabla 42.

Tabla 42: *Equipos de Telecomunicaciones – Auditorio Agustín Cueva*

Ubicación	Equipos	Nombre	# Puertos
Planta Alta 1	WS-C2960X-48TS-L	SW-POSEIDON	48

Fuente: Adaptado DDTI - UTN

3.3.8 Colegio universitario.

Los equipos de telecomunicaciones en este edificio como se muestra en la Tabla 43.

Tabla 43: *Equipos de Telecomunicaciones – Colegio Universitario*

Ubicación	Equipos	Nombre	# Puertos
Planta Baja	WS-C2960S-48TS-S	SW-CALDERON	48

Fuente: Adaptado DDTI – UTN

3.4 Switch compatibles con el protocolo 802.1X

Los equipos de conmutación distribuidos en todo el territorio que integra la Universidad Técnica del Norte y su compatibilidad con el protocolo 802.1x, como se muestra en la Tabla 44.

Tabla 44: *Listado de switch UTN*

DEPENDENCIA	UBICACIÓN	MODELO	802.1X
Edificio Central	Data center	WS-C3750G-12S-S	✓
	Data center	WS-C4510R+E	✓
	Data center	WS-C4503-E L3	✓
	Data center	NEXUS 5548	X
	Data center Chasis Blade	WS-CBS3020-HPQ	✓
	Data center Chasis Blade	WS-CBS3020-HPQ	✓
	Planta Baja	WS-C2960-48TC-L	✓
	Planta Alta 1	WS-C2960-48TC-L	✓
	Planta Alta 1	WS-C2960-24TC-L	✓
	Auditorio José Martí	WS-C2960-48TC-L	✓
	Auditorio José Martí	WS-C2960-48TC-L	✓
	Canal Universitario	WS-C2960-48TC-	✓
	Planta Alta 4	WS-C3850-48T	✓
	Planta Alta 4	WS-C2960X-48TS-L	✓
	Planta Alta 4	WS-C2960-48TC-L	✓
	Entrada Principal	WS-C2960-24TC-L	✓
	Cuarto de Equipos	WS-C4506-E L3	✓
FICA	Laboratorio I	WS-C2960-48TC-L	✓
	Laboratorio II	WS-C2960-48TC-L	✓
	Laboratorio III	WS-C2960-48TC-L	✓
	Laboratorio III	WS-C2960-24TC-L	✓
	Laboratorio IV	WS-C2960-48TC-L	✓
	Laboratorio IV	WS-C2960-48TC-L	✓
	Laboratorio V	SW 3COM	✓
	Laboratorio V	SW 3COM	✓
	Laboratorio VI	SW 3COM	✓
	Laboratorio VII	WS-C2950-24	✓
	Laboratorio VII	WS-C2950-24	✓
	Cubículos	WS-C2960-48TC-L	✓
	Sala de profesores	WS-C2960-24TC-L	✓
	FICAYA	Cuarto de Equipos	WS-C3850-48T-S
Cuarto de Equipos		WS-C2960X-48TS-L	✓
Cuarto de Equipos		WS-C2960X-48TS-L	✓
Cuarto de Equipos		WS-C2960X-48TS-L	✓
Yuyucocha		SG 300-28	✓
La Pradera		WS-C3850-48T-S	✓
La Pradera		WS-C2960X-48TS-L	✓
La Pradera		WS-C2960X-48TS-L	✓
Cuarto de Equipos		WS-C3850-48T-S	✓
Cuarto de Equipos		WS-C2960X-48TS-L	✓
Cuarto de Equipos		WS-C2960X-48TS-L	✓
Cuarto de Equipos		WS-C2960X-48TS-L	✓
Yuyucocha		SG 300-28	✓
Cuarto de Equipos		WS-C3850-48T-S	✓
Cuarto de Equipos	WS-C2960-48TC-L	✓	
Cuarto de Equipos	WS-C2960-48TC-L	✓	
Cuarto de Equipos	WS-C2960-24TC-L	✓	
Laboratorio 1	WS-C2960-48TC-L	✓	
Laboratorio 2	WS-C2960-48TC-L	✓	

FECYT	Laboratorio MAC	WS-C2960-48TC-L	✓
	Coordinación de Carreras	WS-C2960-24TC-L	✓
	Inst. Educación Física	WS-C2960S-24TS-S	✓
	Psicología	WS-C2960-48TC-L	✓
	Cuarto de Equipos	WS-C3850-48T-S	✓
FACAE	Cuarto de Equipos	WS-C4506-E L3	✓
	Cuarto de Equipos	WS-C2960X-48TS-L	✓
	Laboratorio IV	WS-C2960G-248TC-L	✓
	Cubículos Docentes	DLINK	
FCCSS	Cuarto de Equipos	WS-C3850-48T-S	✓
	Cuarto de Equipos	WS-C2960X-48TS-LL	✓
	Planta Alta 4	WS-C2960X-48TS-LL	✓
	Planta Alta 4	WS-C2960X-48TS-LL	✓
	Planta Alta 4	WS-C2960X-48TS-LL	✓
Postgrado	Cuarto de Equipos	WS-C3750X-24	✓
	Cuarto de Equipos	WS-C2960-24TC-L	✓
	Cuarto de Equipos	WS-C2960-24TC-L	✓
	Cuarto de Equipos	WS-C2960S-48TS-S	✓
	Cuarto de Equipos	WS-C2960S-48TS-S	✓
	Primer Piso	WS-C2960S-48TD-L	✓
	Primer Piso	WS-C2960S-48TS-S	✓
U Emprende	Primer Piso	WS-C2960S-48TS-S	✓
	Tercer Piso	SG-200-26	✓
	Planta Baja	WS-C3850-48T-S	✓
	Planta Baja	WS-C2960X-48TS-L	✓
	Segundo Piso	WS-C2960X-48TS-L	✓
Biblioteca	Segundo Piso	SRW2048	✓
	Segundo Piso	WS-C2960-48TC-L	✓
	Cuarto de equipos	WS-C2960X-48TS-L	✓
	Cuarto de equipos	SG-300-52	✓
	Cuarto de equipos	SG-200-18	✓
	IC3	SG 200-50	✓
Bienestar Universitario	IC3	SG 200-50	✓
	Cuarto de equipos	WS-C2960-48TS-LL	✓
	Planta Baja	WS-C2960X-48TS-LL	✓
	Planta Baja	WS-C2960X-48TS-LL	✓
	Planta Alta 2	WS-C2960X-48TS-LL	✓
	Planta Alta 2	WS-C2960X-48TS-LL	✓
	Planta Alta 4	3COM SS3 SW 4400	✓
Complejo Acuático	Planta Alta 4	3COM SS3 SW 4400	✓
	Garita	WS-C2960-24TC-L	✓
	Piscina	SS3 SW 4200	✓
Auditorio Agustín Cueva	Clubes UTN	WS-C2960X-48TS-L	✓
	Gimnasio	SS3 SW 4400 SE	✓
Colegio Universitario	Planta Alta	WS-C2960S-48TS-S	✓
	Planta Baja	WS C2960S-48TS-S	✓
Centro Infantil	Centro Infantil	3COM	✓
Campus San Vicente de Paúl	Planta Alta	WS-C3850-48T-S	✓
	Planta Alta	WS-C2960-48TC-L	✓
	Planta Alta	WS-C2960-48TC-L	✓
	Planta Baja	WS-C2960-48TC-L	✓
	Planta Baja	WS-C2960-48TC-L	✓
	Planta Baja	WS-C2960-48TC-L	✓
	Planta Baja	WS-C2960-48TC-L	✓
	Planta Baja	WS-C2960-48TC-L	✓
	Planta Baja	WS-C2960-48TC-L	✓

Fuente: Adaptado DDTI - UTN

A través de la tabla se puede observar que todos los switch presentes en las dependencias de la Universidad Técnica del Norte son compatibles con el protocolo 802.1X, con excepción del equipo NEXUS 5548.

Capítulo IV

Diseño del Sistema de Seguridad

4.1 Diseño en capa de acceso por facultades

Para realizar el diseño en las facultades y dependencias presentes en la casona universitaria, se tiene en cuenta que el servidor RADIUS-LDAP se encuentra alojado en la DMZ de la red, como se muestra en la Figura 36.

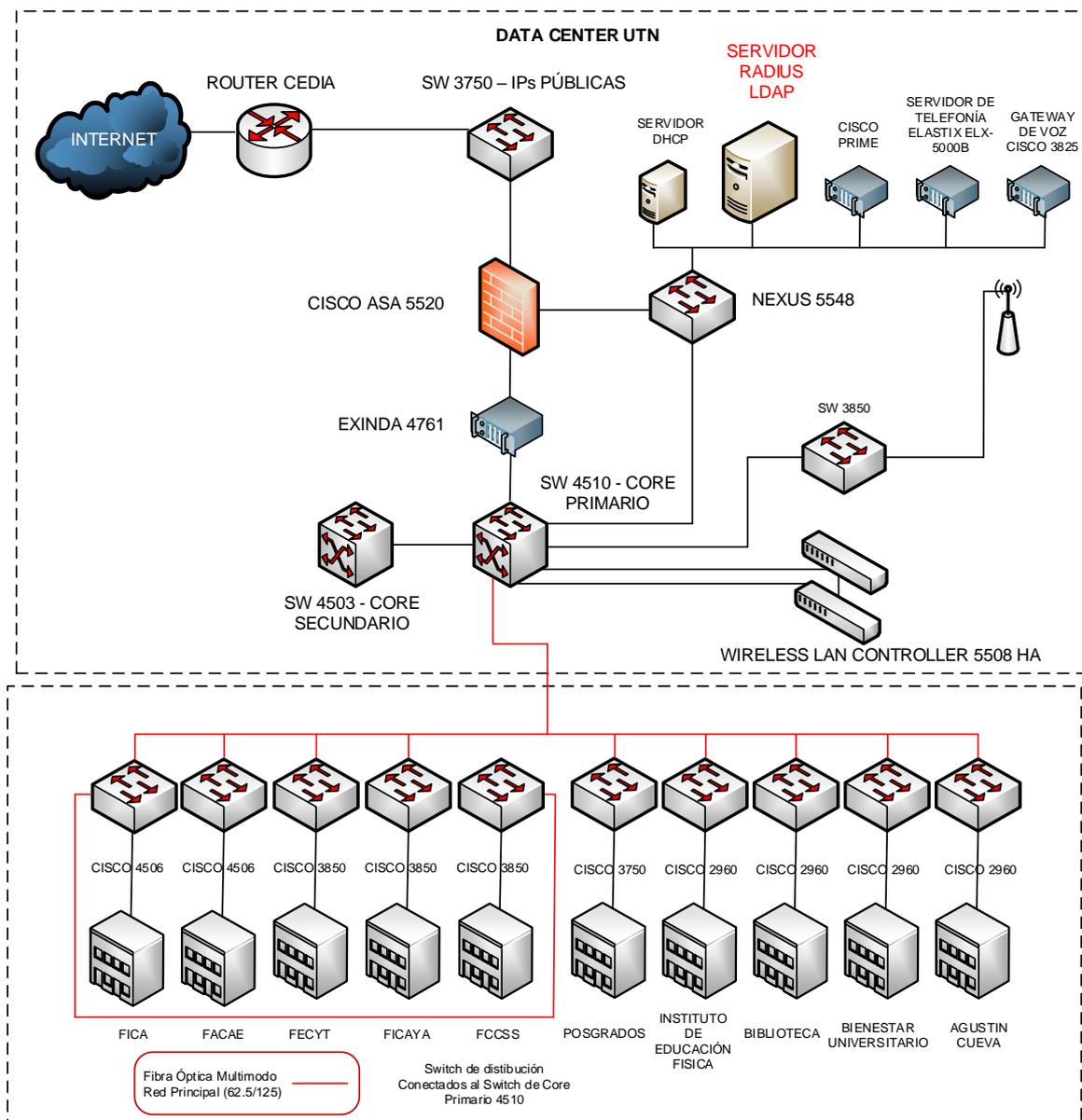


Figura 36: Ubicación del servidor RADIUS – LDAP

Fuente: Adaptado DDTI

4.1.1 FICA.

En este apartado se realiza el diseño de seguridad teniendo en cuenta cada uno de los switch de acceso contenidos en la facultad, considerando el número de computadoras presentes en los laboratorios y los puntos de red en la parte de los cubículos de los docentes. Todos los laboratorios están segmentados en una vlan llamada FICA-LABORATORIOS y docentes en la vlan FICA-ADMINISTRATIVOS. En la Figura 37 se tiene la topología general del diseño, a partir de aquí los demás diseños se toma en cuenta de una forma nombrada la DMZ del edificio central.

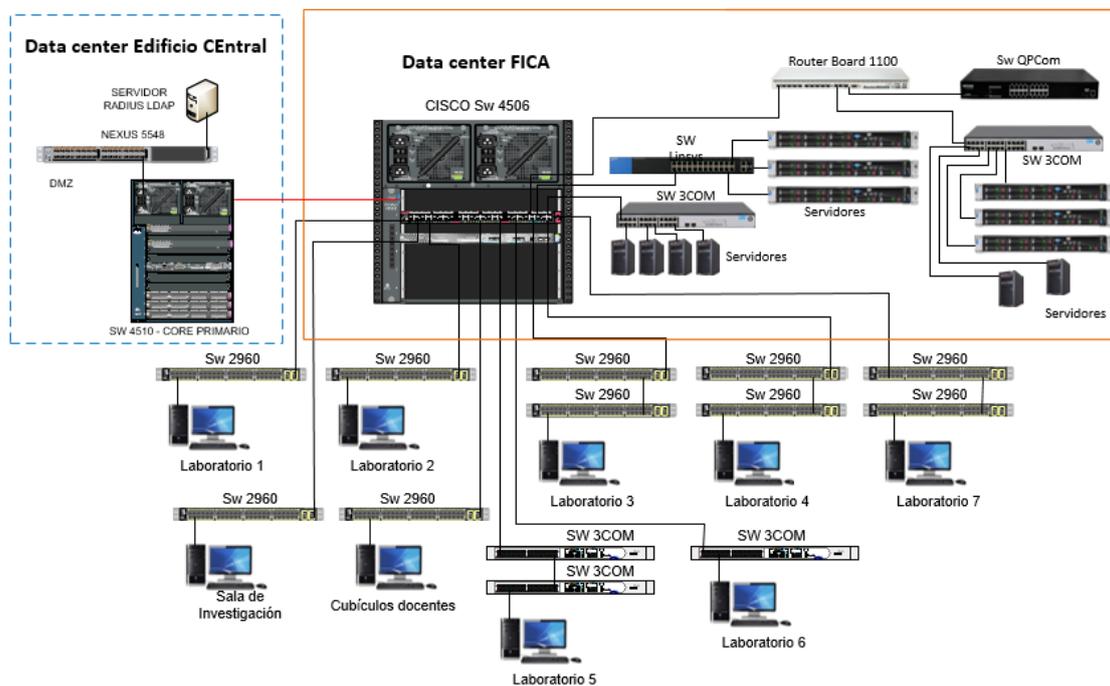


Figura 37: Diseño sistema de seguridad facultad FICA
Fuente: Programa Visio

4.1.1.1 Laboratorio 1.

El laboratorio se encuentra ubicado en la primera planta de la facultad, cuenta con 26 computadoras conectadas al switch de acceso, este último enlazado al switch de distribución

que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 38.

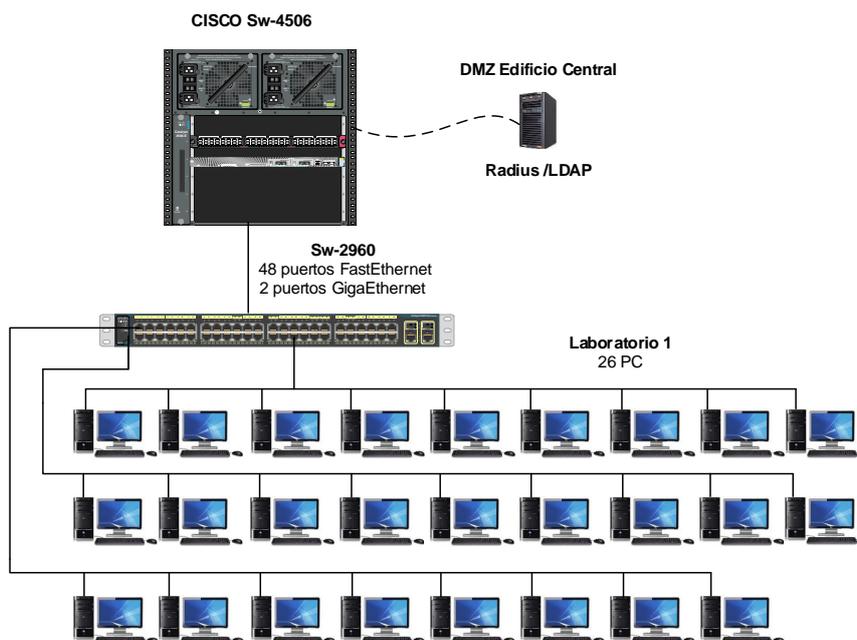


Figura 38: Diagrama capa acceso FICA – Laboratorio 1
Fuente: Programa Visio

La configuración del protocolo 802.1X para todos los switch cisco 2960, como se muestra en la Tabla 45. Los pasos indicados siguen un orden de secuencia y a partir de aquí las configuraciones para este modelo de switch se encuentra en el anexo II A.

Tabla 45: *Habilitar y configurar protocolo 802.1X switch cisco 2960*

Descripción	Comando
Habilita el modo EXEC privilegiado	enable
Entra en modo de configuración global	configure terminal
Habilita AAA	aaa new-model
El comando configura la autorización de la red a través de RADIUS	aaa authorization network default group radius
Especifica RADIUS como el método para la autenticación basada en puerto 802.1X	aaa authentication dot1x default group radius

Habilita la contabilidad de sesiones de autenticación 802.1X	aaa accounting dot1x default start-stop group radius
La IP del servidor RADIUS, contraseña y puertos de trabajo.	radius-server host ip-servidor auth-port 1812 acct-port 1813 key “ ”
Habilita globalmente la autenticación basada en puerto 802.1X.	dot1x system-auth-control
Asignación de interfaces	Range interface f1/3 - 10
Trabajar en modo acceso	switch mode access
Habilita la autenticación en un puerto.	dot1x port-control auto
Coloca el puerto controlado en el estado no autorizado hasta que se lleva a cabo la autenticación entre el cliente y el servidor de autenticación. Una vez que el cliente pasa la autenticación, el puerto se autoriza.	

Fuente: Adaptado CISCO

4.1.1.2 Laboratorio 2.

Esta dependencia está situada en la primera planta de la facultad, posee 20 computadoras conectadas al switch de acceso; este último enlazado al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 39. La configuración del protocolo 802.1 X se muestra en el anexo II A.

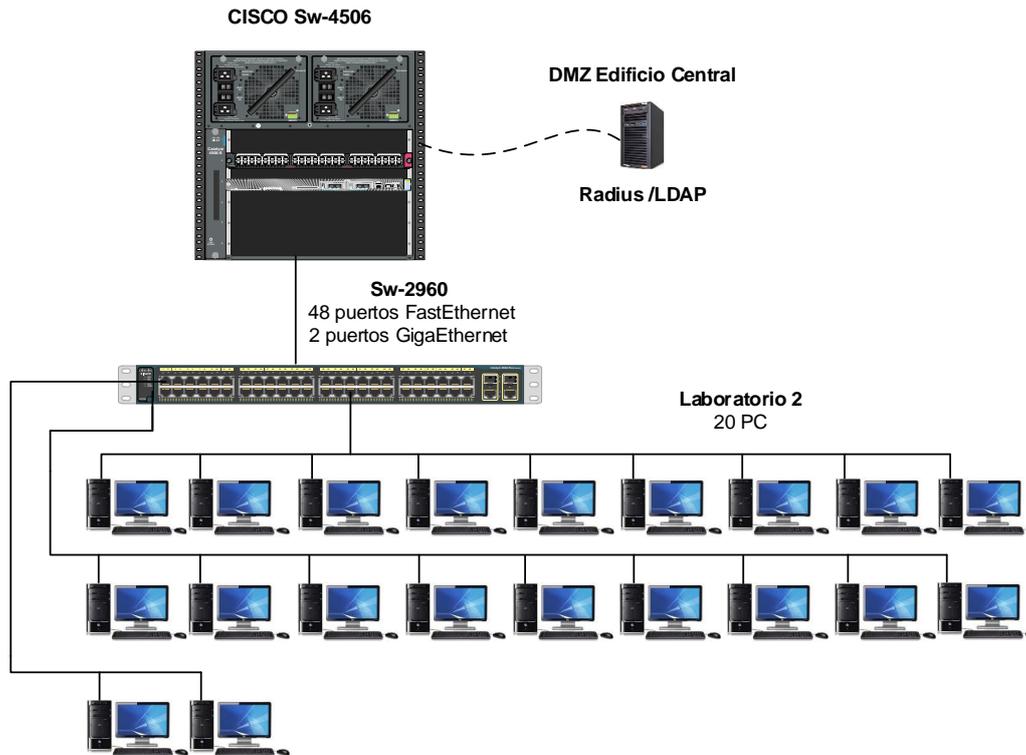


Figura 39: Diagrama capa acceso FICA – Laboratorio 2
Fuente: Programa Visio

4.1.1.3 Laboratorio 3.

La locación se ubica en la primera planta del edificio, contiene 30 computadoras conectadas a 2 switch de acceso en cascada; estos últimos enlazados al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 40. La configuración del protocolo 802.1 X se muestra en el anexo II A.

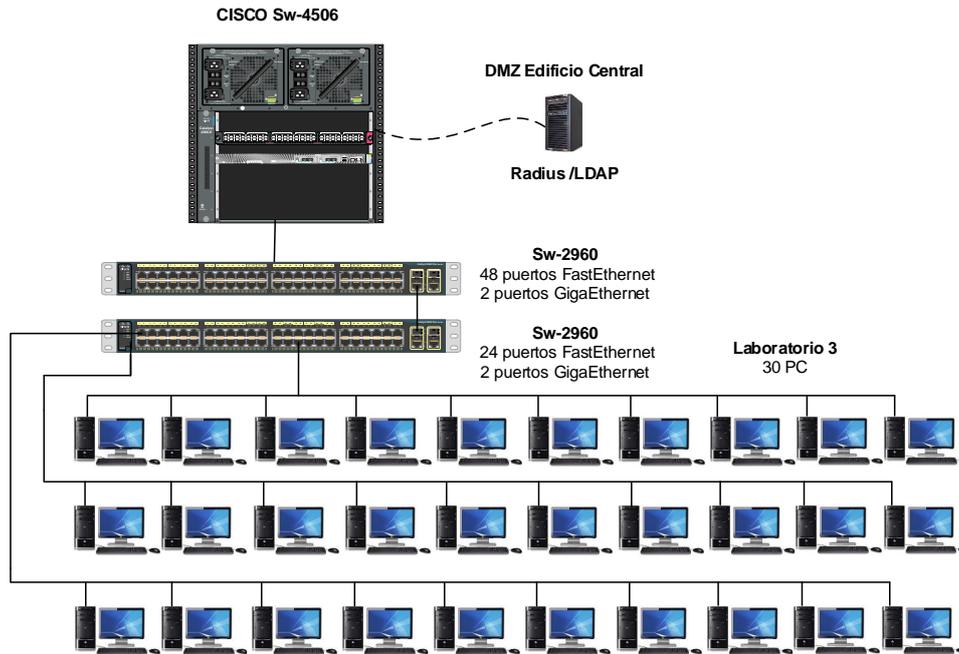


Figura 40: Diagrama capa acceso FICA – Laboratorio 3
Fuente: Programa Visio

4.1.1.4 Laboratorio 4.

La estancia se ubica en la primera planta de la facultad, tiene 20 computadoras conectadas a 2 switch de acceso en cascada; estos últimos enlazados a switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 41. La configuración del protocolo 802.1 X se muestra en el anexo II A.

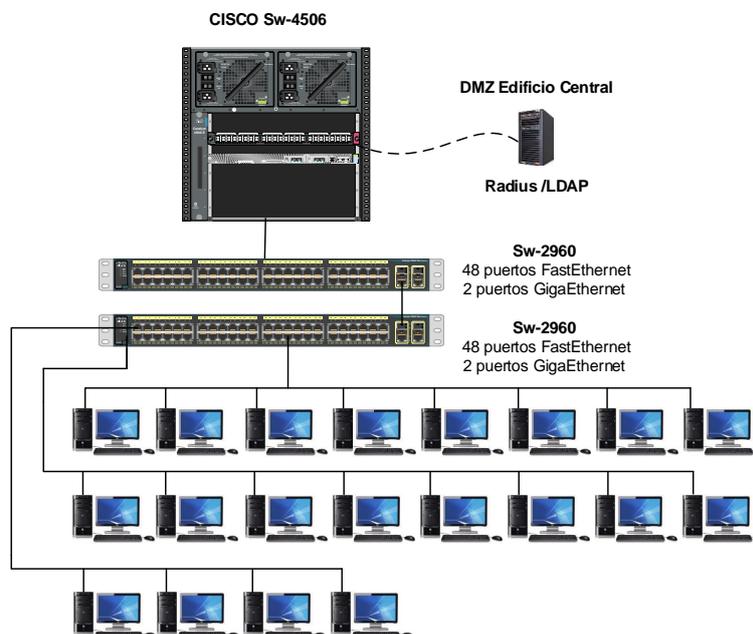


Figura 41: Diagrama capa acceso FICA – Laboratorio 4
Fuente: Programa Visio

4.1.1.5 Laboratorio 5.

El laboratorio se encuentra en la segunda planta de la facultad, cuenta con 30 computadoras conectadas a 2 switch de acceso en cascada; estos últimos enlazados al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 42.

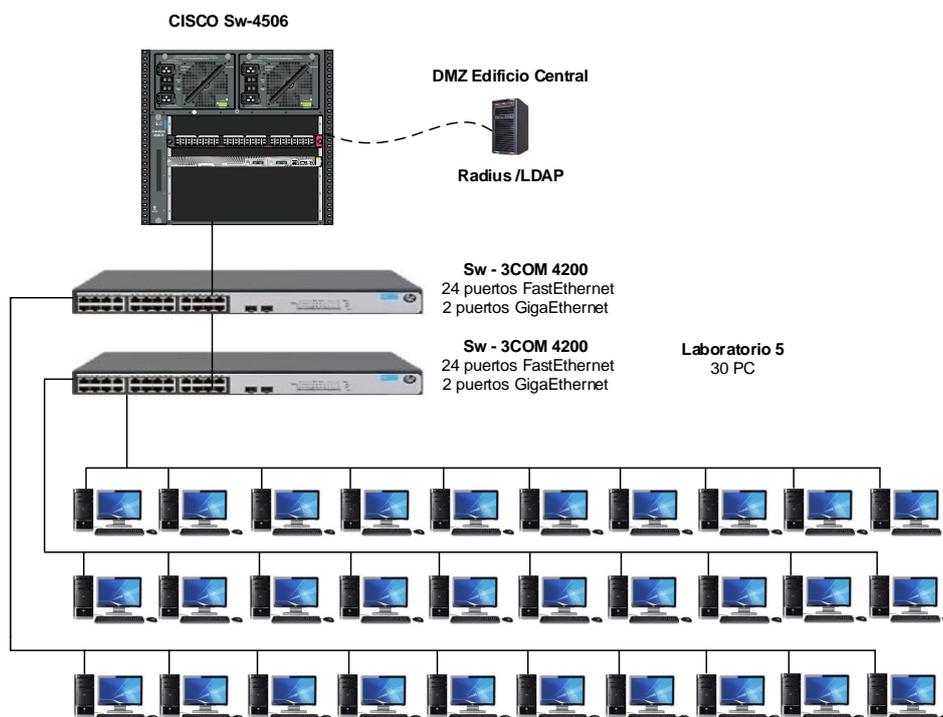


Figura 42: Diagrama capa acceso FICA – Laboratorio 5
Fuente: Programa Visio

La configuración del protocolo 802.1X para todos los switch de las series 3COM 4200,4400; como se muestra en la Tabla 46. Los pasos indicados siguen un orden de secuencia y a partir de aquí las configuraciones para este modelo de switch se encuentra en el anexo II G.

Tabla 46: *Habilitar y configurar protocolo 802.1X switch 3COM 4200,4400*

Descripción	Comando
Entrar en la vista del sistema.	system-view
Agregar usuario local de acceso local.	local-user localuser service-type lan-access

Habilitar la función de corte inactivo y establecer el intervalo de corte inactivo.

password simple localpass

attribute idle-cut 20

quit

Configure las direcciones IP de los servidores RADIUS de autenticación y contabilidad primarios.

primary authentication IP servidor

primary accounting IP servidor

Especifique la clave compartida para que el dispositivo intercambie paquetes con el servidor de autenticación.

key authentication ""

Especifique la clave compartida para que el dispositivo intercambie paquetes con el servidor de contabilidad.

key accounting ""

Configure el intervalo para que el dispositivo retransmita paquetes al Servidor RADIUS y el número máximo de intentos de transmisión.

timer response-timeout 5

retry 5

Configure el intervalo para que el dispositivo envíe paquetes de contabilidad en tiempo real al servidor RADIUS.

timer realtime-accounting 15

Especifique el dispositivo para eliminar el nombre de dominio de cualquier nombre de usuario antes de pasar el nombre de usuario al servidor de RADIUS.

user-name-format without-domain

quit

Crea un dominio "" e ingresa su vista.

domain ""

Establezca radius1 como el esquema authentication default radius-scheme radius1 local RADIUS para los usuarios del dominio authorization default radius-scheme radius1 local y especifique Usar autenticaciones locales accounting default radius-scheme radius1 local como esquema secundario.

Establece el número máximo de usuarios access-limit enable 30 para el dominio en 30.

Active la función de corte inactivo y idle-cut enable 20 establezca el intervalo de corte inactivo. quit

Configure “ ” como el dominio domain default enable “ ” predeterminado.

Habilitar 802.1X globalmente. dot1x

Habilite 802.1X para el puerto interface GigabitEthernet “ ” GigabitEthernet “ ”. dot1x quit

Fuente: Adaptado <https://www.manualslib.com/manual/575168/3com-4210g.html?page=557#manual>

4.1.1.6 Laboratorio 6.

Esta dependencia se sitúa en la segunda planta de la facultad, posee 26 computadoras conectadas a un switch de acceso; este último enlazado al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 43. La configuración del protocolo 802.1 X se muestra en el anexo II G.

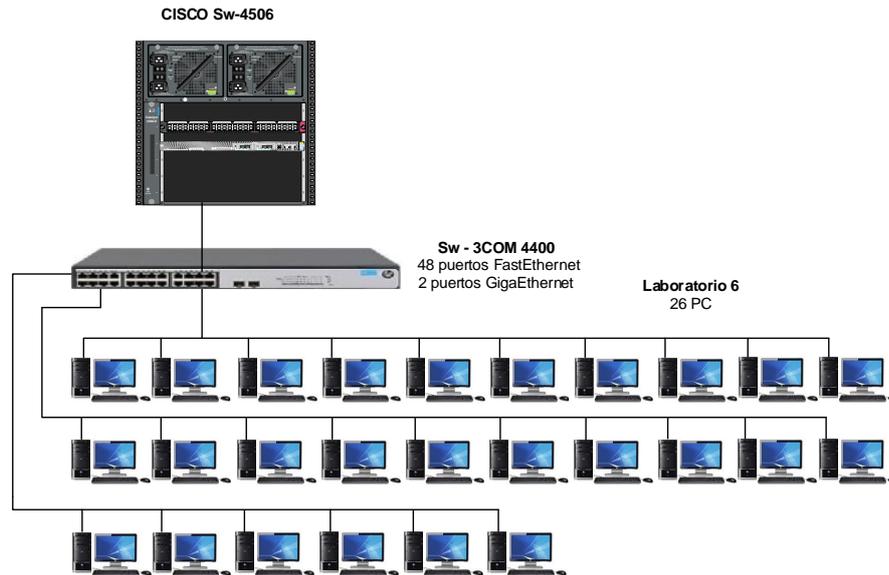


Figura 43: Diagrama capa acceso FICA – Laboratorio 6
Fuente: Programa Visio

4.1.1.7 Laboratorio 9.

La locación está ubicada en la última planta de la facultad, posee 30 computadoras conectadas a 2 switch de acceso en cascada que a su vez da puntos de red al laboratorio 8 con 15 computadoras; los switch están enlazados al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 44. La configuración del protocolo 802.1 X se muestra en el anexo II A.

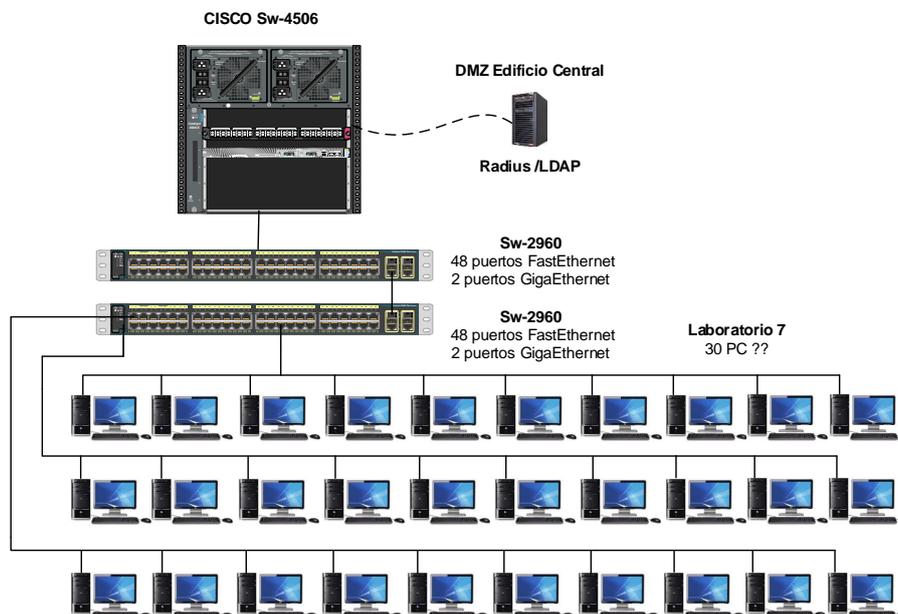


Figura 44: Diagrama capa acceso FICA – Laboratorio 9
Fuente: Programa Visio

4.1.1.8 Cubículos docentes 1.

Esta dependencia se establece en la última planta del edificio, posee puntos de red designados para cada uno de los docentes distribuidos en sus cubículos. Los puntos de red están conectados a un switch de acceso, este último enlazado al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 45. La configuración del protocolo 802.1 X se muestra en el anexo II A.

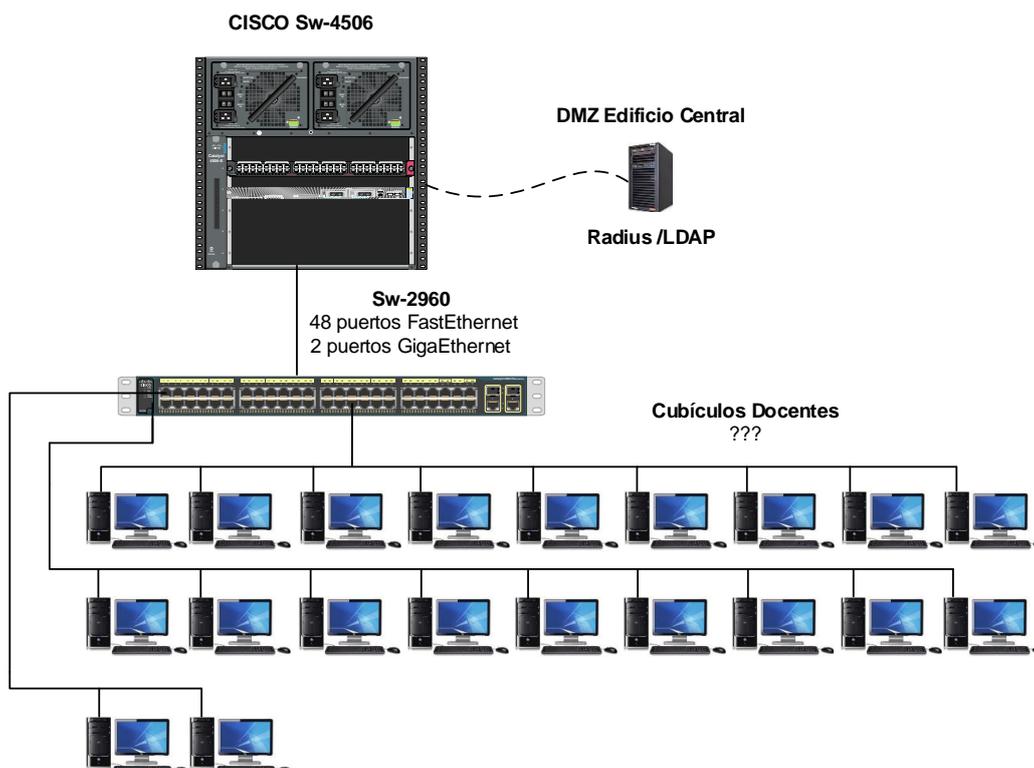


Figura 45: Diagrama capa acceso FICA – Cubículos 1
Fuente: Programa Visio

4.1.1.9 Cubículos docentes 2

Esta estancia se ubica en la última planta de la facultad, posee puntos de red conectadas al switch de acceso, este último enlazado al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 46. La configuración del protocolo 802.1 X se muestra en el anexo II A.

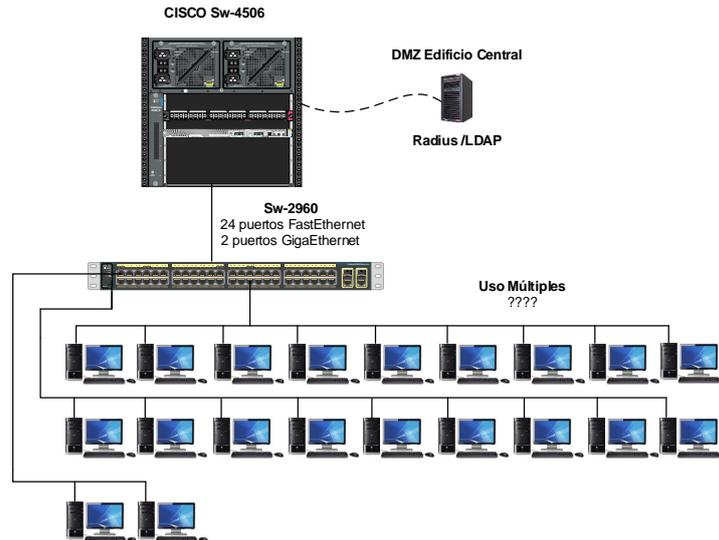


Figura 46: Diagrama capa acceso FICA – Cubículos 2
Fuente: Programa Visio

4.1.2 FICAYA.

En esta facultad se plantea el diseño de los switch de acceso contenidos en la misma, teniendo en cuenta el número de computadoras presentes en los laboratorios. En el edificio los puntos de red de la planta baja están conectados directamente al switch de acceso cisco 2960, para todas las dependencias se emplea la vlan FICAYA–ADMINISTRATIVOS y en cuanto a los laboratorios se emplea la vlan FICAYA-LABORATORIOS. En el diseño de esta capa se establece la ubicación de las distintas estancias como se muestra en la Figura 47. La configuración del protocolo 802.1 X se muestra en el anexo II A.

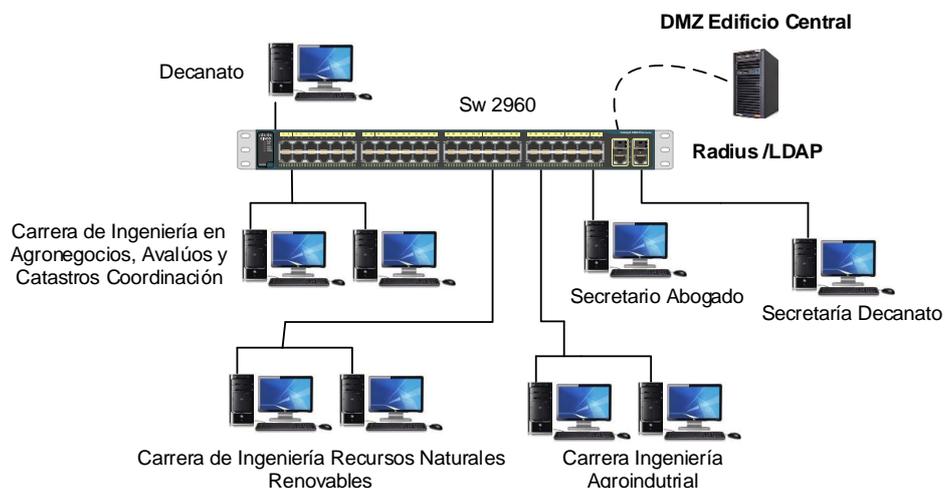


Figura 47: Diagrama capa acceso FICAYA – Planta Baja
Fuente: Programa Visio

4.1.2.1 Laboratorio 4.

El laboratorio posee 26 computadoras conectadas a un switch de acceso, este último enlazado al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 48. La configuración del protocolo 802.1 X se muestra en el anexo II A.

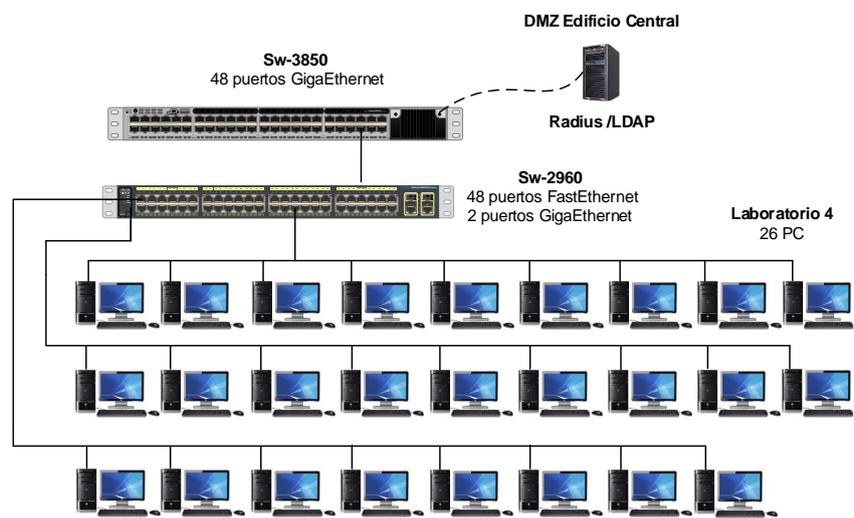


Figura 48: Diagrama capa acceso FICAYA – Laboratorio 4
Fuente: Programa Visio

4.1.2.2 Laboratorio 8.

La estancia posee 30 computadoras conectadas a un switch de acceso, este último enlazado al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 49. La configuración del protocolo 802.1 X se muestra en el anexo II A.

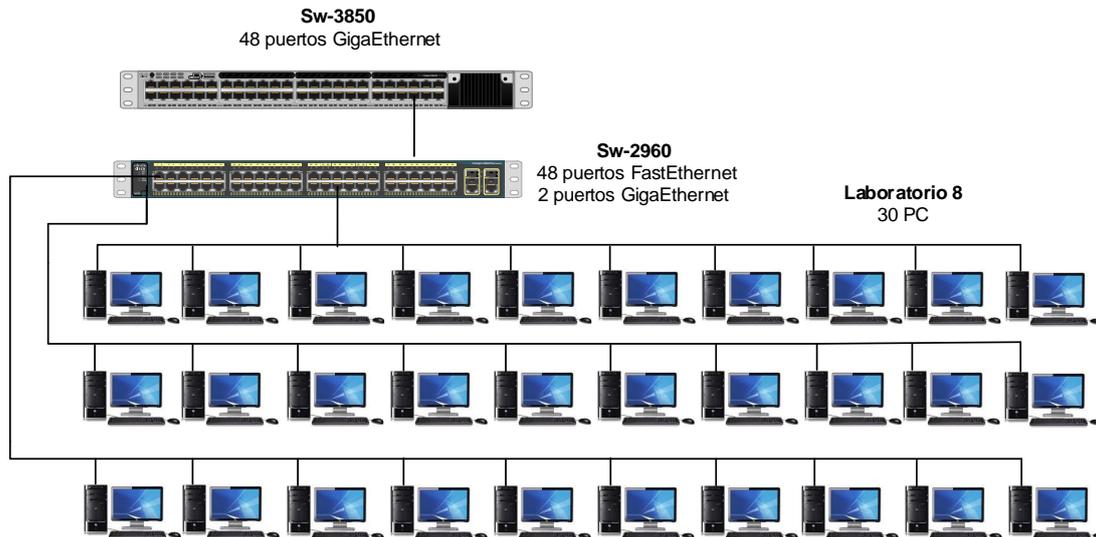


Figura 49: Diagrama capa acceso FICAYA – Laboratorio 8
Fuente: Programa Visio

4.1.3 FACAE.

En esta facultad establece el diseño de cada uno de los switch de acceso contenidos en la misma, teniendo en cuenta la cantidad de computadoras presentes en los laboratorios y la vlan a la que pertenecen (FACE-LABORATORIOS).

4.1.3.1 Laboratorio 3.

Esta dependencia posee 41 computadoras conectadas a un switch de acceso; este último enlazado al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 50. La configuración del protocolo 802.1 X se muestra en el anexo II A.

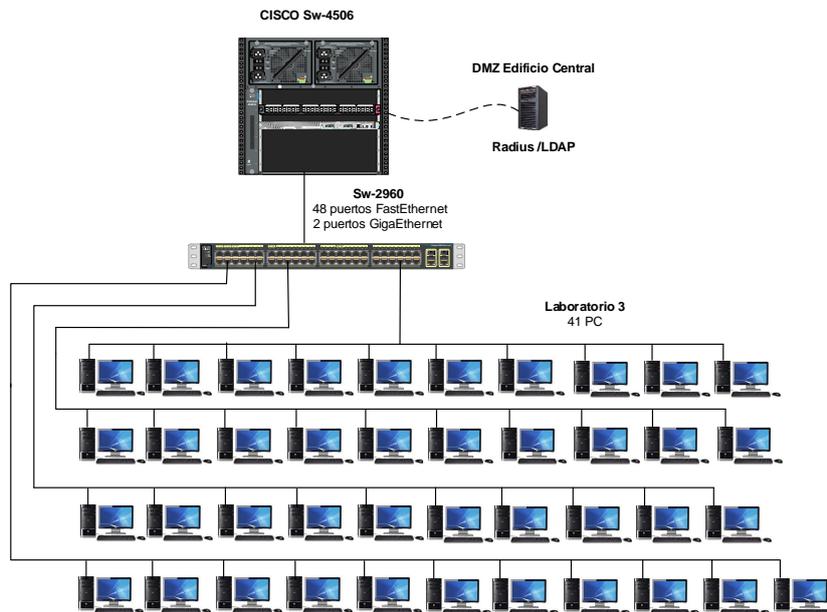


Figura 50: Diagrama capa acceso FACA E – Laboratorio 3
Fuente: Programa Visio

4.1.3.1 Laboratorio 4.

El laboratorio posee 26 computadoras conectadas al switch de acceso, este último enlazado al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 51. La configuración del protocolo 802.1 X se muestra en el anexo II A.

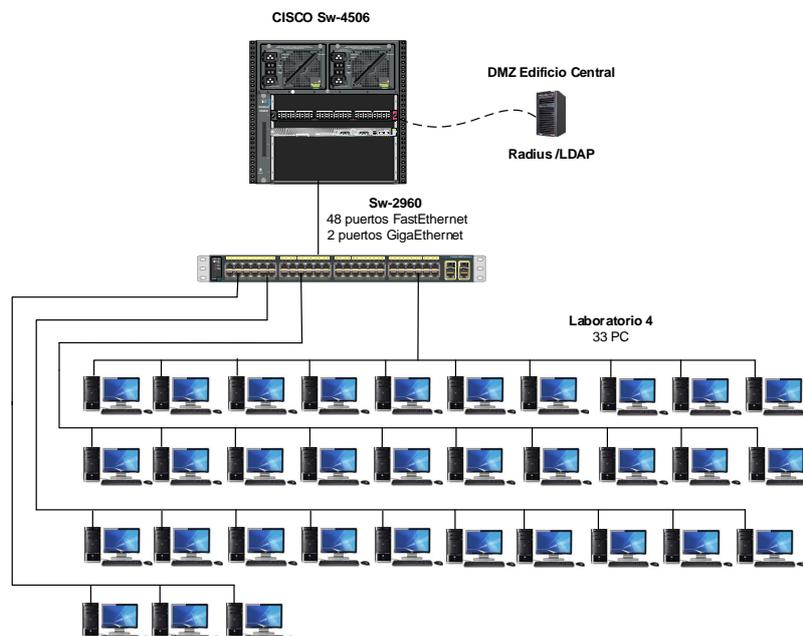


Figura 51: Diagrama capa acceso FACA E – Laboratorio 4
Fuente: Programa Visio

4.1.4 FECYT.

En esta locación se realiza el diseño de cada uno de los switch de acceso contenidos en la misma, teniendo en cuenta el número de computadoras ubicadas en los laboratorios y la vlan en la que se encuentran (FECYT-LABORATORIOS).

4.1.4.1 Laboratorio 1.

Esta dependencia tiene 30 computadoras conectadas al switch de acceso; este último enlazado al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 52. La configuración del protocolo 802.1 X se muestra en el anexo II A.

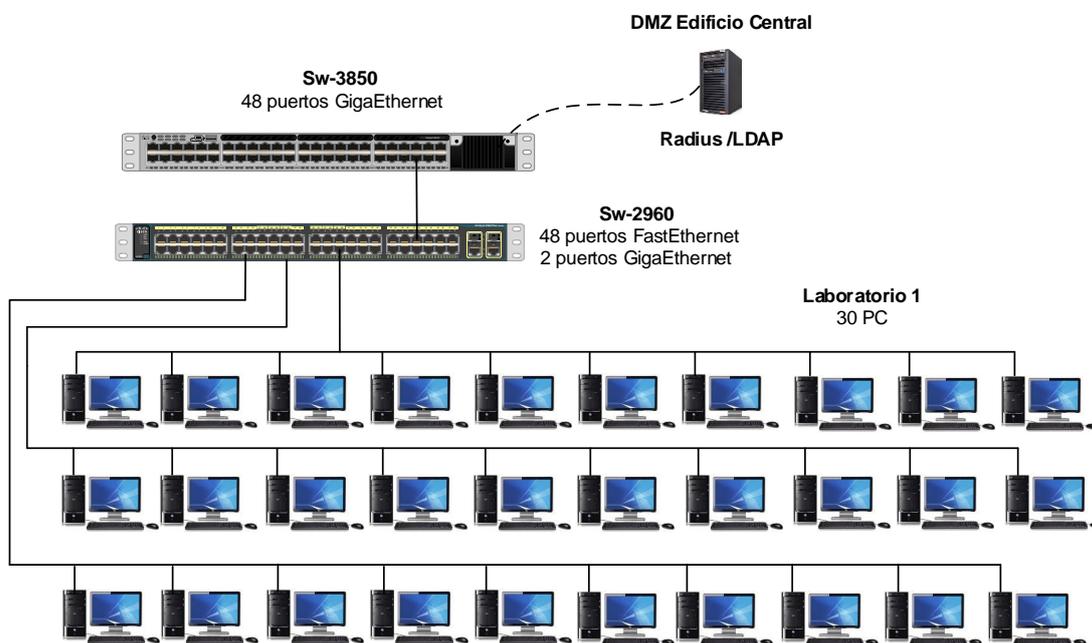


Figura 52: Diagrama capa acceso FECYT – Laboratorio 1
Fuente: Programa Visio

4.1.4.2 Laboratorio 2.

La locación contiene 30 computadoras conectadas a un switch de acceso; este último enlazado al switch de distribución que interconecta con el edificio central y permite la conexión

con la DMZ, como muestra la Figura 53. La configuración del protocolo 802.1 X se muestra en el anexo II A.

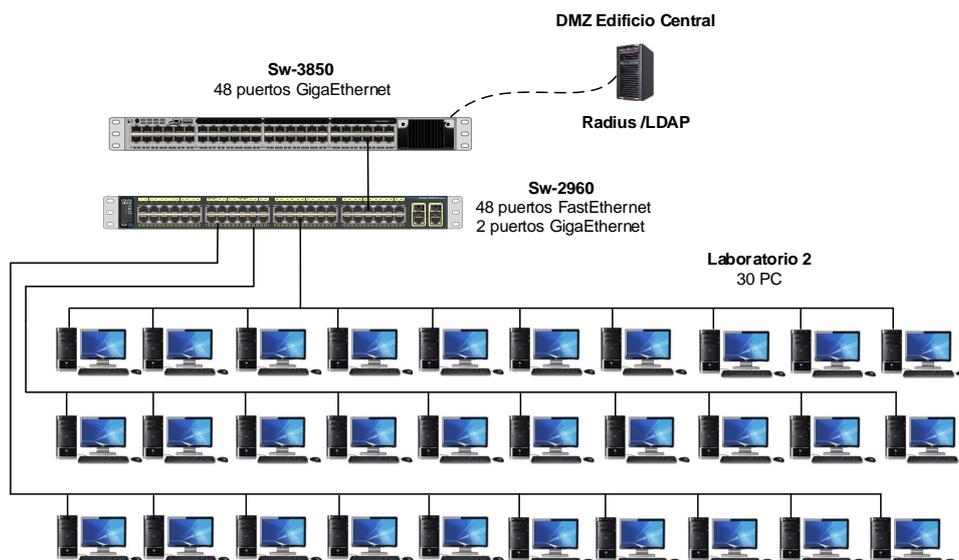


Figura 53: Diagrama capa acceso FECYT – Laboratorio 2
Fuente: Programa Visio

4.1.4.3 Laboratorio MAC.

El laboratorio contiene 38 computadoras conectadas un a switch de acceso; este último enlazado al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 54. La configuración del protocolo 802.1 X se muestra en el anexo II A.

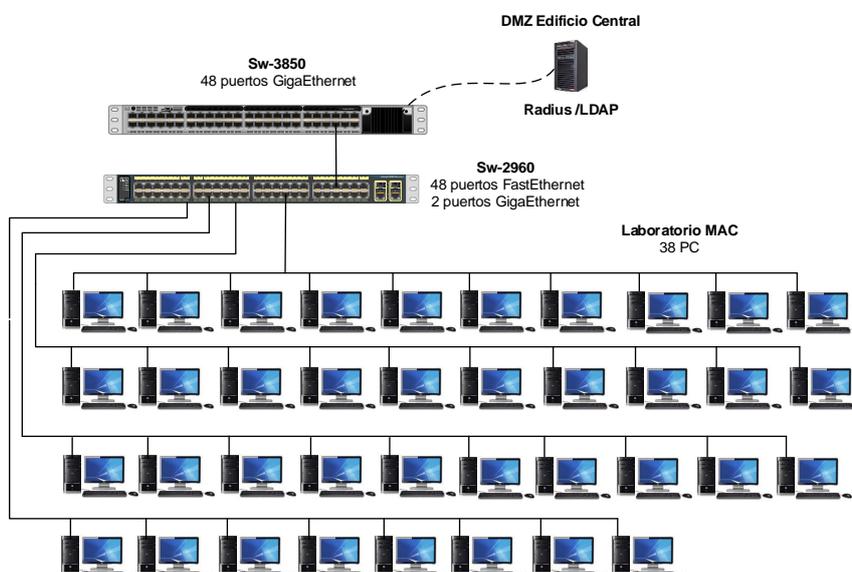


Figura 54: Diagrama capa acceso FECYT – Laboratorio MAC
Fuente: Programa Visio

4.1.4.4 Laboratorio Inglés.

Esta dependencia tiene 34 computadoras conectadas al switch de acceso; este último enlazado al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 55. La configuración del protocolo 802.1 X se muestra en el anexo II A.

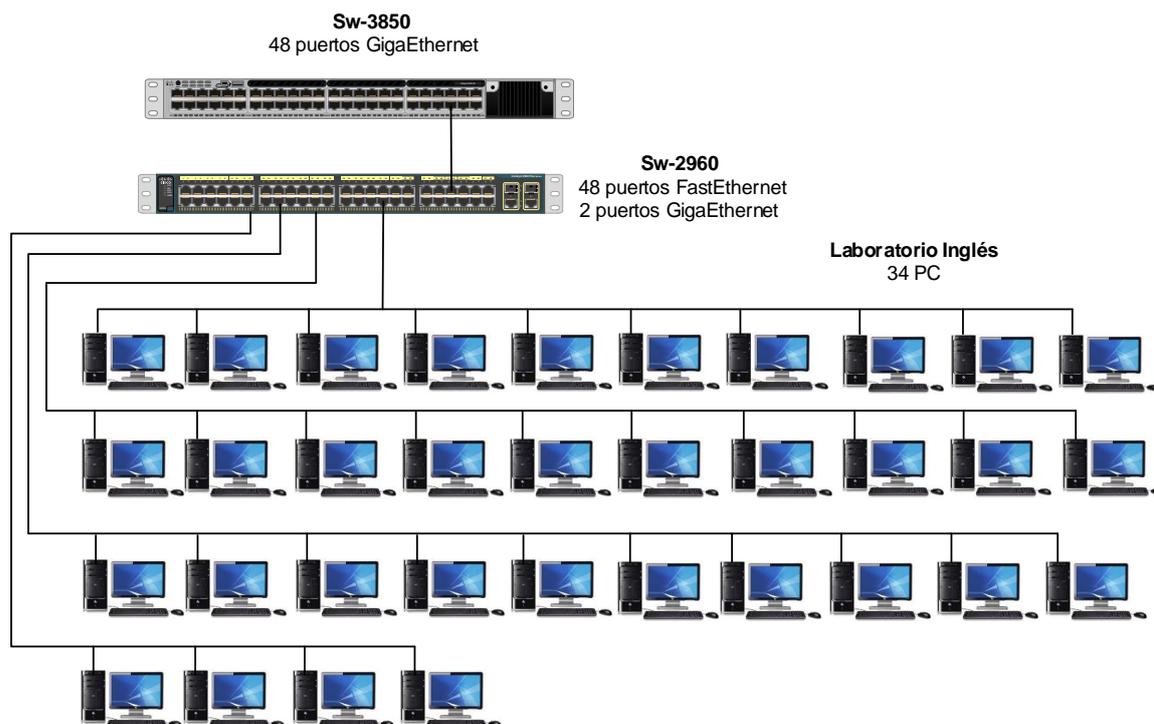


Figura 55: Diagrama capa acceso FECYT – Laboratorio Inglés
Fuente: Programa Visio

4.1.5 FCCSS.

En este apartado se efectúa el diseño de los switch de acceso incluidos en la facultad, teniendo en cuenta el número de computadoras presentes en los laboratorios y la vlan a la que pertenecen (VLAN-FCCSS).

4.1.5.1 Laboratorio 1.

El laboratorio contiene 27 computadoras conectadas un a switch de acceso; este último enlazado al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 56. La configuración del protocolo 802.1 X se muestra en el anexo II A.

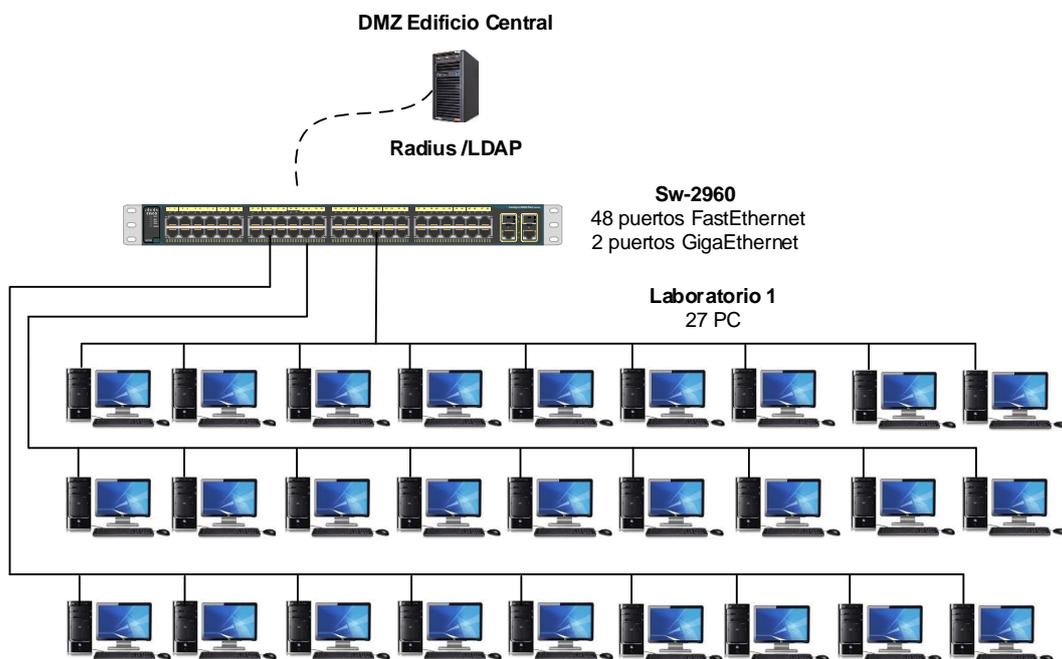


Figura 56: Diagrama capa acceso FCCSS – Laboratorio 1

Fuente: Programa Visio

4.1.5.2 Laboratorio 2.

La dependencia posee 30 computadoras conectadas un a switch de acceso; este último enlazado al switch de distribución que interconecta con el edificio central y permite la conexión con la DMZ, como muestra la Figura 57. La configuración del protocolo 802.1 X se muestra en el anexo II A.

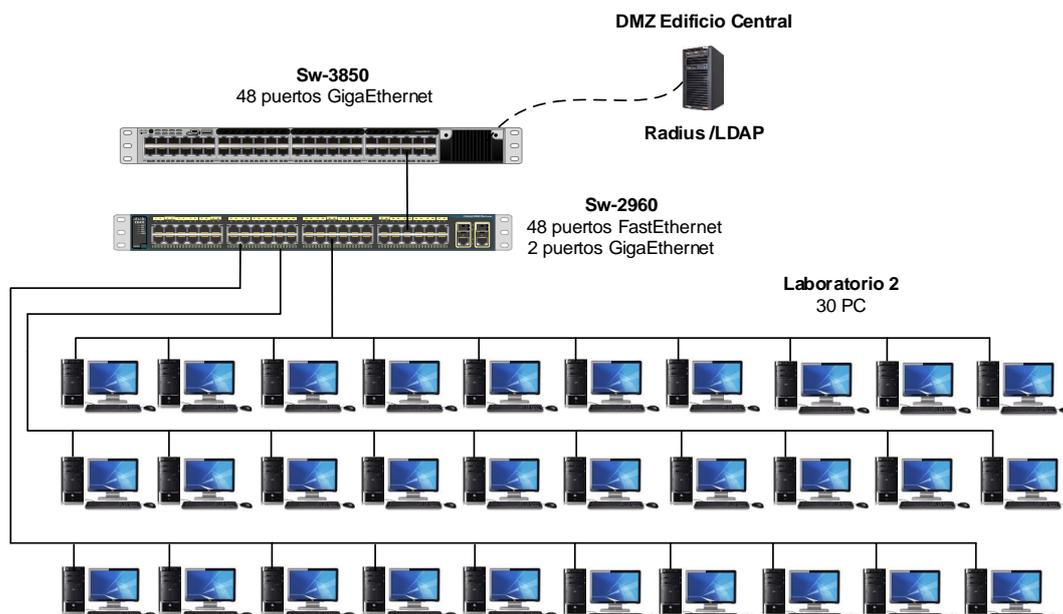


Figura 57: Diagrama capa acceso FCCSS – Laboratorio 2
Fuente: Programa Visio

4.2 Diseño en otras dependencias

4.2.1 Edificio central.

En esta sección se efectúa el diseño de cada uno de los switch de acceso contenidos en el edificio, teniendo en cuenta las dependencias existentes en el mismo. Cada departamento para acceder a la red está segmentado en distintas vlans según su función; (vlan AUTORIDADES, vlan COMUNICACION-ORGANIZACIONAL y la gran mayoría en la vlan ADMINISTRATIVOS).

Los switch de acceso con sus respectivas locaciones distribuidas por pisos, como se muestra en las Figuras 58, 59, 60, 61 y 62. La configuración del protocolo 802.1X en el switch 3850 se muestra en la Tabla 47 y a partir de aquí en el anexo II E.

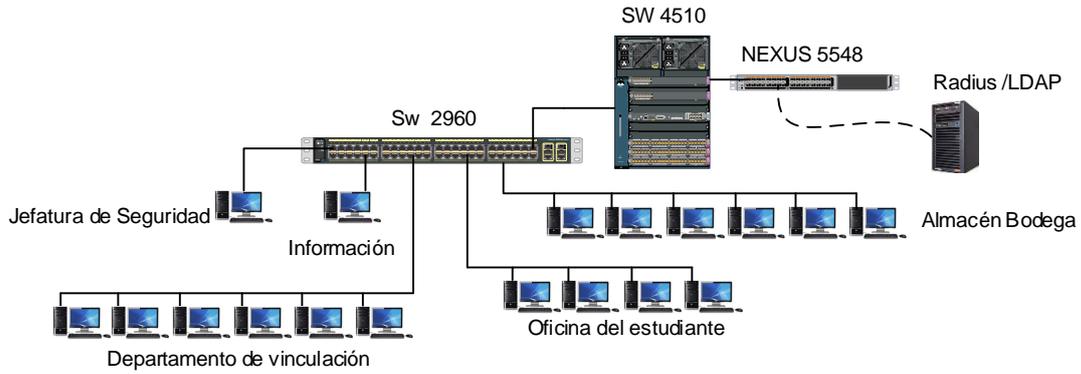


Figura 58: Diagrama capa acceso Edificio Central - Planta Baja
Fuente: Programa Visio

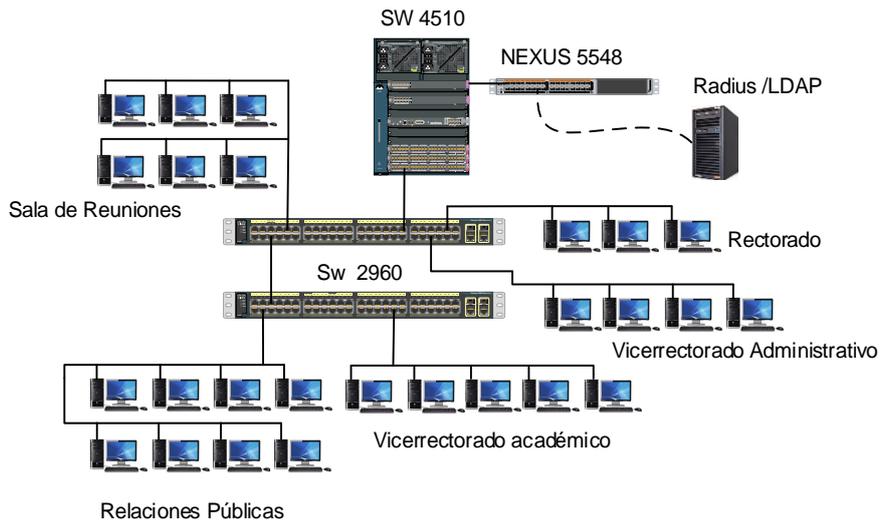


Figura 59: Diagrama capa acceso Edificio Central - Primera planta
Fuente: Programa Visio

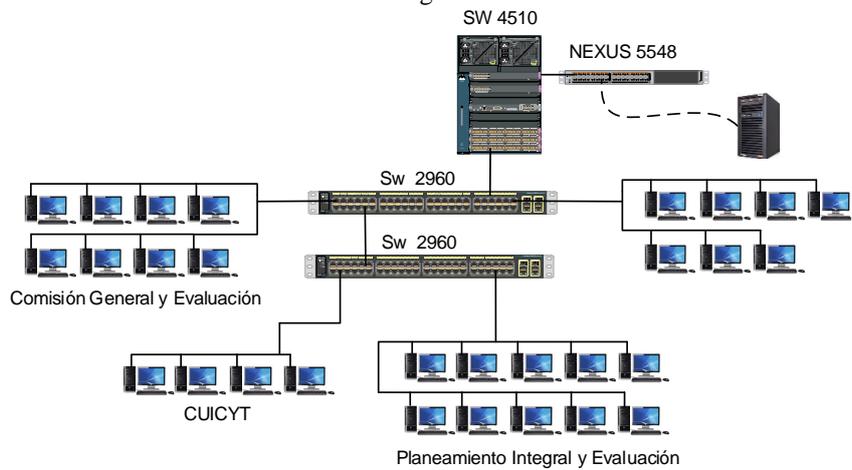


Figura 60: Diagrama capa acceso Edificio Central - Segunda planta
Fuente: Programa Visio

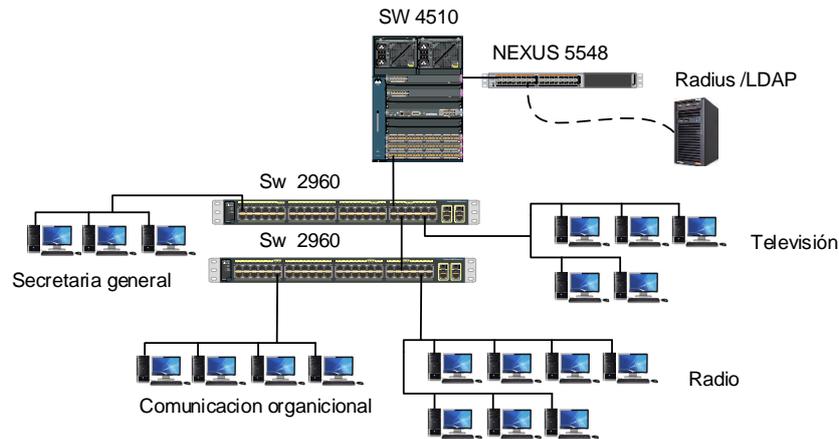


Figura 61: Diagrama capa acceso Edificio Central - Tercera planta
Fuente: Programa Visio

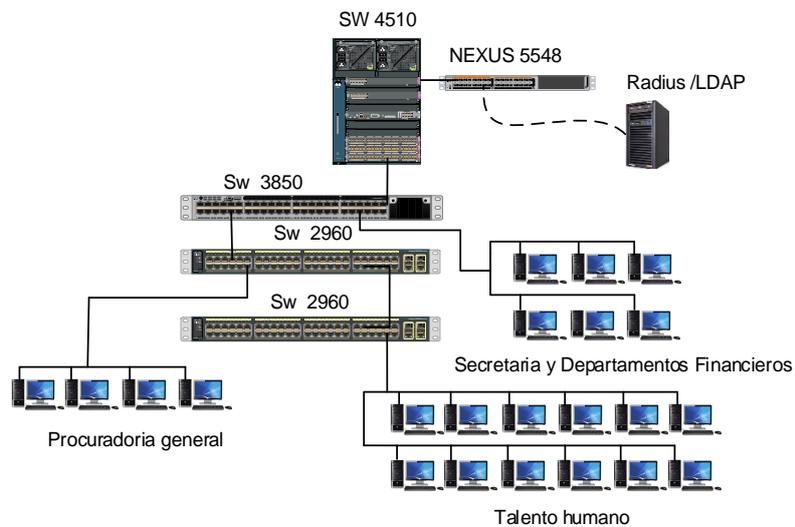


Figura 62: Diagrama capa acceso Edificio Central - Cuarta planta
Fuente: Programa Visio

Tabla 47: *Habilitar y configurar protocolo 802.1X switch cisco 3850*

Descripción	Comando
Habilita el modo EXEC privilegiado	enable
Entra en modo de configuración global	configure terminal
Habilita AAA	aaa new-model
El comando configura la autorización de la red a través de RADIUS	aaa authorization network default group radius

Especifica RADIUS como el método para la autenticación basada en puerto 802.1X	<code>aaa authentication dot1x default group radius</code>
Habilita la contabilidad de sesiones de autenticación 802.1X	<code>aaa accounting dot1x default start-stop group radius</code>
La IP del servidor RADIUS, contraseña y puertos de trabajo.	<code>radius-server host ip-servidor auth-port 1812 acct-port 1813 key “ ”</code>
Habilita globalmente la autenticación basada en puerto 802.1X.	<code>dot1x system-auth-control</code>
Asignación de interfaces	<code>Range interface f1/3 - 10</code>
Trabajar en modo acceso	<code>switch mode access</code>
Habilita la autenticación en un puerto.	<code>dot1x port-control auto</code>
Coloca el puerto controlado en el estado no autorizado hasta que se lleva a cabo la autenticación entre el cliente y el servidor de autenticación. Una vez que el cliente pasa la autenticación, el puerto se autoriza.	

Fuente: Adaptado CISCO

4.2.2 Edificio de posgrado.

En este apartado se realiza el diseño de los switch de acceso contenidos en el edificio, teniendo en cuenta las dependencias existentes. La red se encuentra segmentada en dos vlans; (VLAN ADMINISTRATIVOS Y VLAN LABORATORIOS). El switch de acceso en la planta baja, como se muestra en la figura 63. La configuración del protocolo 802.1 X se muestra en el anexo II A.

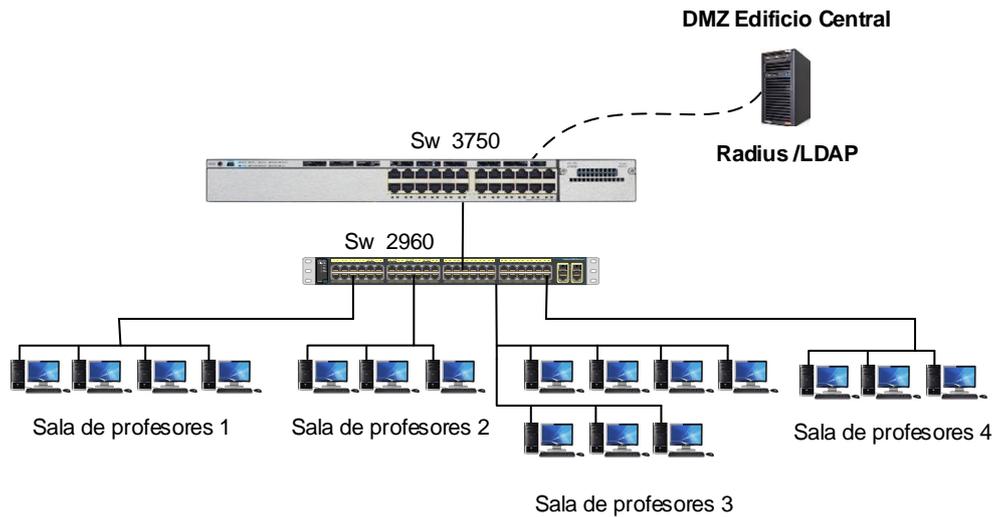


Figura 63: Diagrama capa acceso Edificio de Posgrados
Fuente: Programa Visio

4.2.3 U. EMPRENDE, CAI.

En esta sección se realiza el diseño de cada uno de los switch de acceso contenidos en el edificio, teniendo en cuenta las dependencias existentes en el mismo. Cada departamento para acceder a la red está segmentado en distintas vlans según su función; (vlan U-EMPRENDE, vlan CAI-LABORATORIOS y la vlan CAI-ADMINISTRATIVOS).

Los switch de acceso con sus respectivas locaciones distribuidas por pisos, como se muestra en las Figuras 64, 65, 66, 67 y 68. La configuración del protocolo 802.1 X se muestra en el anexo II A.

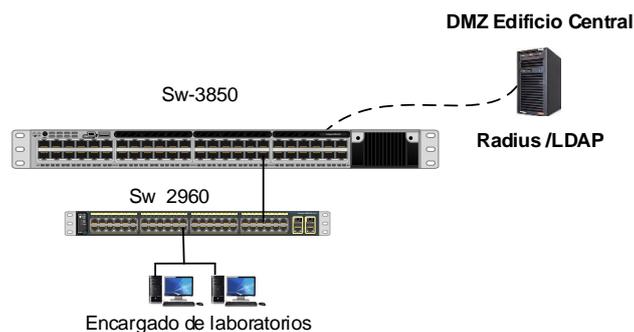


Figura 64: Diagrama capa acceso– Planta baja
Fuente: Programa Visio

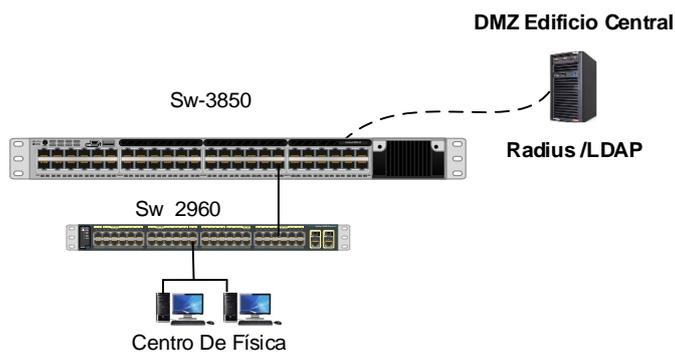


Figura 65: Diagrama capa acceso– Primer Piso
Fuente: Programa Visio

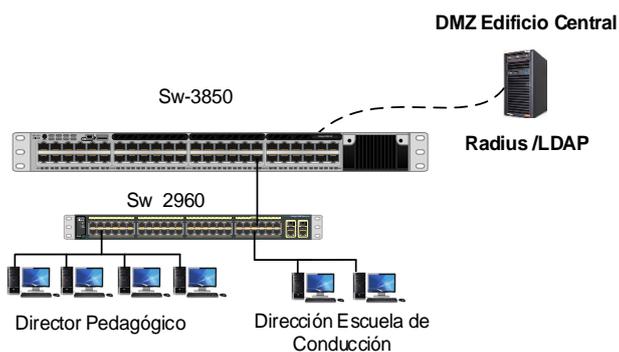


Figura 66: Diagrama capa acceso Escuela de Conducción – Segundo Piso
Fuente: Programa Visio

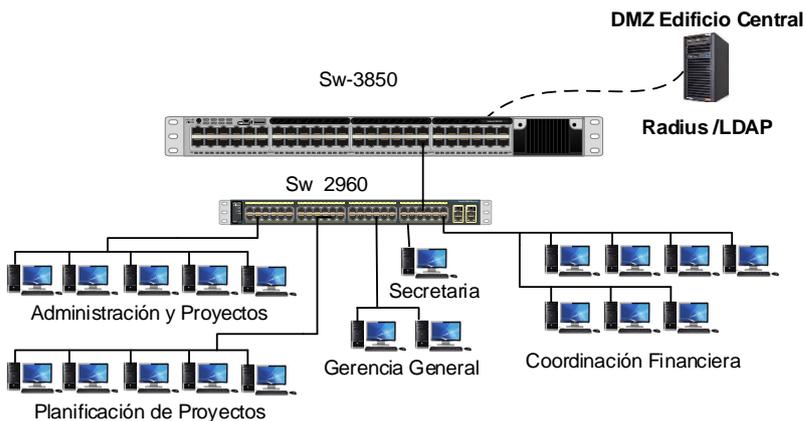


Figura 67: Diagrama capa acceso U. EMPRENDE – Tercer Piso
Fuente: Programa Visio

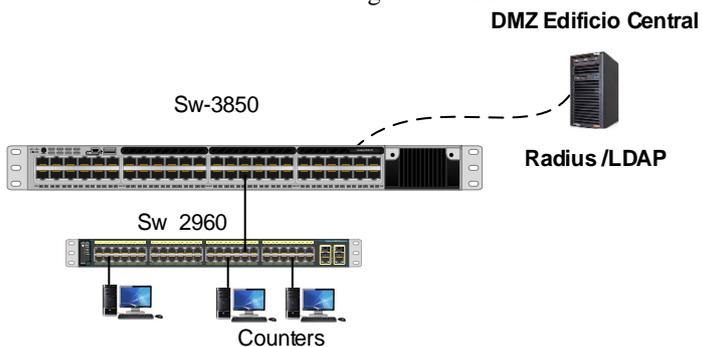


Figura 68: Diagrama capa acceso CAI – Cuarto Piso

Fuente: Programa Visio

4.2.4 Biblioteca.

Este edificio cuenta con tres vlans, BIBLIOTECA-LABORATORIOS, BIBLIOTECA-DOCENTES y BIBLIOTECA-ADMINISTRATIVOS; repartidos por los switch de acceso. El diseño se efectúa según las dependencias presentes en los distintos pisos de la edificación como se muestra las Figuras 69, 70, y 71. La configuración del protocolo 802.1 X se muestra en el anexo II A.

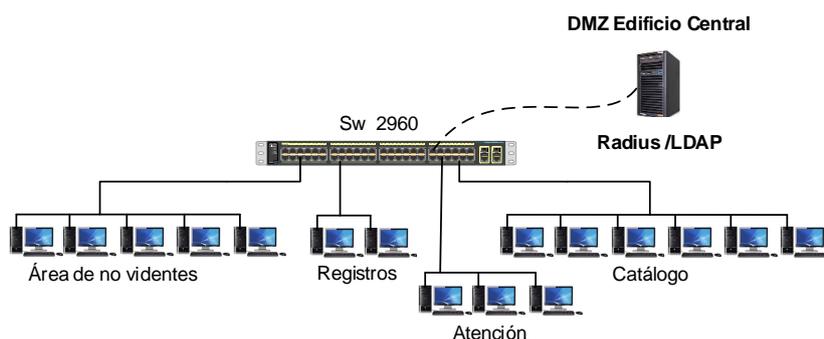


Figura 69: Diagrama capa acceso Biblioteca – Planta Baja
Fuente: Programa Visio

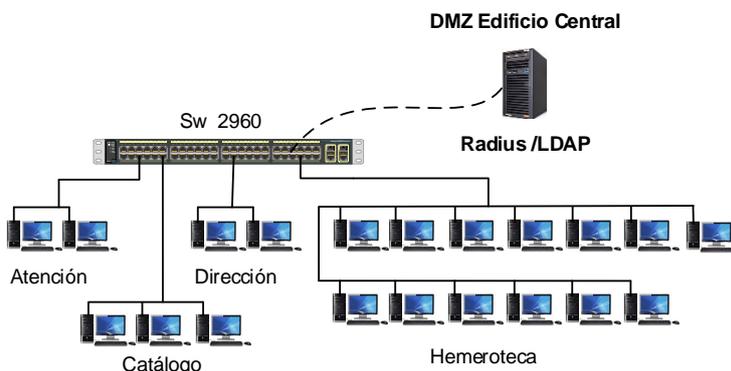


Figura 70: Diagrama capa acceso Biblioteca – Primer Piso
Fuente: Programa Visio

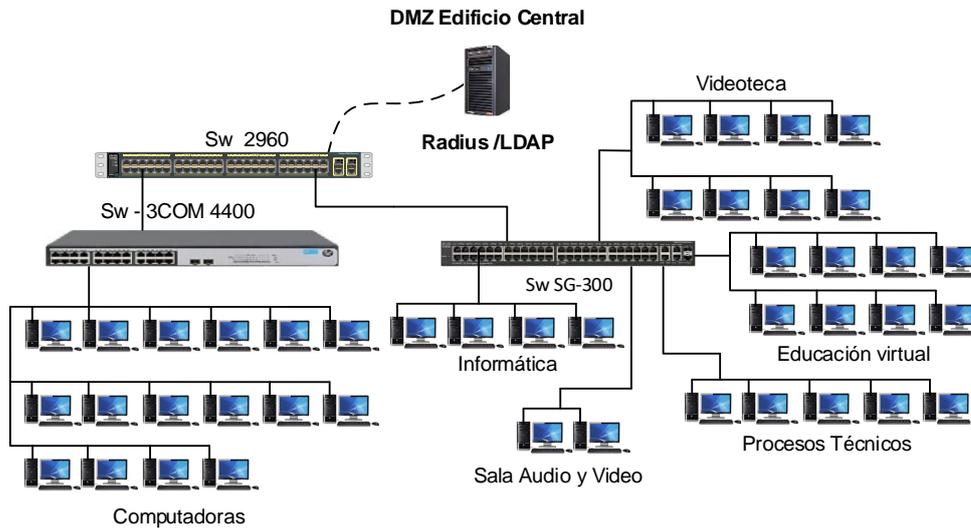


Figura 71: Diagrama capa acceso Biblioteca – Segundo Piso
Fuente: Programa Visio

4.2.5 Bienestar Universitario.

En este apartado se realiza el diseño de los switch de acceso contenidos en el edificio, teniendo en cuenta las dependencias existentes. La red se encuentra segmentada en dos vlans; (BIENESTAR-DOCENTES Y BIENESTAR-ADMINISTRATIVOS). Los switch de acceso con sus respectivas locaciones distribuidas por pisos, como se muestra en las Figuras 72 y 73. La configuración del protocolo 802.1 X se muestra en el anexo II A y G.

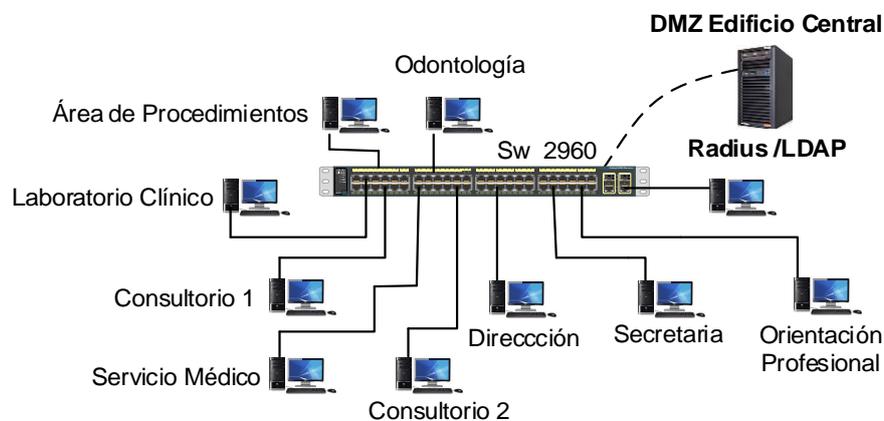


Figura 72: Diagrama capa acceso Bienestar Universitario – Planta Baja
Fuente: Programa Visio

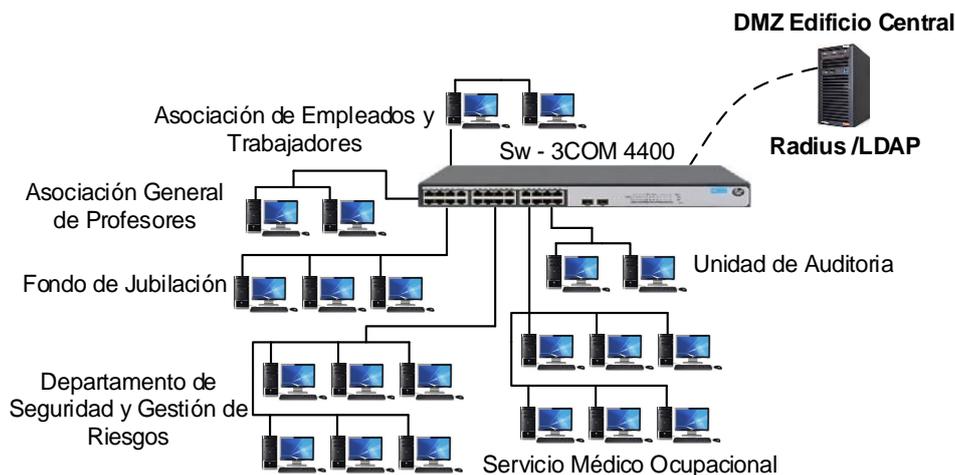


Figura 73: Diagrama capa acceso Bienestar Universitario – Cuarto Piso
Fuente: Programa Visio

4.2.6 Complejo Acuático.

En esta dependencia existen dos switch de acceso de la marca 3COM que están enlazados al switch cisco 2960 de distribución; que interconecta con el edificio central y permite la conexión con la DMZ a través de la vlan CLUBES-UTN, como muestra la Figura 74. La configuración del protocolo 802.1 X se muestra en el anexo II G.

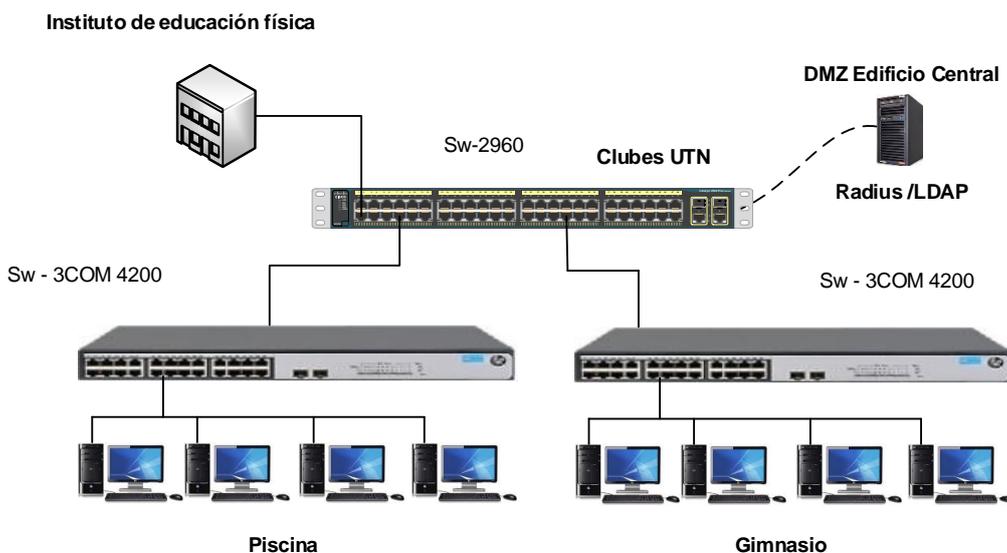


Figura 74: Diagrama capa acceso Complejo Acuático
Fuente: Programa Visio

4.2.7 Auditorio Agustín Cueva.

En esta ubicación existe un switch que cumple la función de acceso y distribución; que interconecta con el edificio central y permite la conexión con la DMZ usando la vlan AGUSTIN-CUEVA, como muestra la Figura 75. La configuración del protocolo 802.1 X se muestra en el anexo II A.

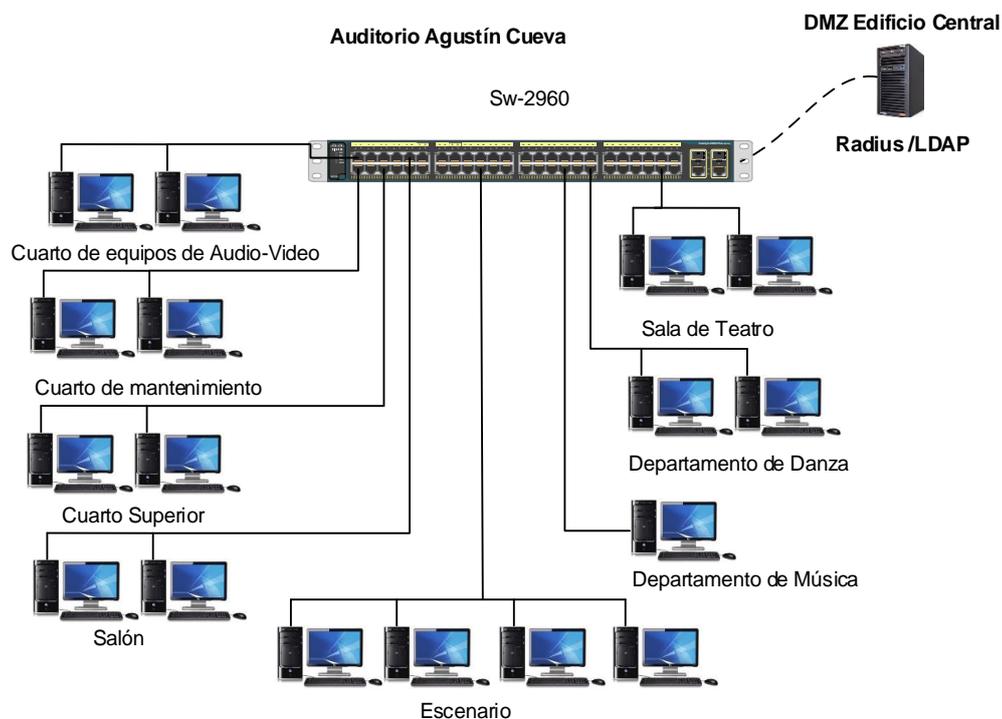


Figura 75: Diagrama capa acceso Auditorio Agustín Cueva
Fuente: Programa Visio

4.3 Diseño en capa de distribución y núcleo.

4.3.1 FICA.

En la facultad los puntos de red de la planta baja van conectados directamente al switch de distribución cisco 4506, para todos los habitáculos se emplea la vlan FICA-ADMINISTRATIVOS. En el diseño de esta capa se tiene en cuenta la ubicación de las distintas dependencias como se muestra en la Figura 76 y los puertos usados del switch para la vlan

administrativos como se muestra en la Tabla 48. La configuración del protocolo 802.1 X en el switch 4506 como se muestra en la Tabla 49 y a partir de aquí en el anexo II C.

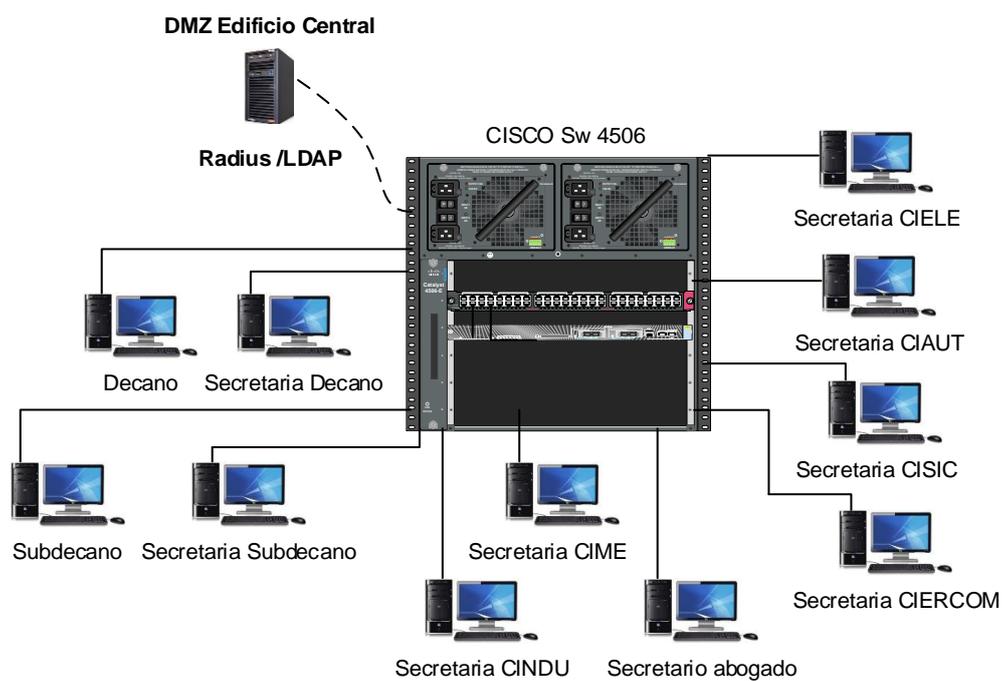


Figura 76: Diagrama capa distribución - FICA

Fuente: Autoría

Tabla 48: Puertos vlan FICA-ADMINISTRATIVOS activos SW-4506

# Vlan	Nombre	Puerto Activo
44	FICA-ADMINISTRATIVOS	Fa4/1, Fa4/2, Fa4/3, Fa4/6 Fa4/7, Fa4/8, Fa4/12, Fa4/13 Fa4/15, Fa4/16, Fa4/19, Fa4/21 Fa4/28, Fa5/1, Fa5/2, Fa5/3 Fa5/4, Fa5/5, Fa5/6, Fa5/7 Fa5/8, Fa5/9, Fa5/10, Fa5/11 Fa5/12, Fa5/13, Fa5/14, Fa5/15 Fa5/16, Fa5/17, Fa5/18, Fa5/19 Fa5/20, Fa5/21, Fa5/22, Fa5/24 Fa5/25, Fa5/26, Fa5/27, Fa5/28 Fa5/29, Fa5/31, Fa5/33, Fa5/34 Fa5/35, Fa5/36, Fa5/37, Fa5/38 Fa5/39, Fa5/40, Fa5/41, Fa5/43 Fa5/44, Fa5/45, Fa5/46, Fa5/47 Fa5/48, Fa6/1, Fa6/2, Fa6/3 Fa6/4, Fa6/5, Fa6/6, Fa6/7 Fa6/8, Fa6/9, Fa6/10, Fa6/11

Fa6/12, Fa6/13, Fa6/14, Fa6/15
 Fa6/16, Fa6/17, Fa6/18, Fa6/19
 Fa6/20, Fa6/21, Fa6/22, Fa6/23
 Fa6/24, Fa6/25, Fa6/26, Fa6/27
 Fa6/28, Fa6/29, Fa6/30, Fa6/31
 Fa6/32, Fa6/33, Fa6/34, Fa6/35
 Fa6/36, Fa6/37, Fa6/38, Fa6/39
 Fa6/40, Fa6/41, Fa6/42, Fa6/43
 Fa6/44, Fa6/45, Fa6/47, Fa6/48

Fuente: Recuperado DDTI

Tabla 49: *Habilitar y configurar protocolo 802.1X switch cisco 4506*

Descripción	Comando
Habilita el modo EXEC privilegiado	enable
Entra en modo de configuración global	configure terminal
Habilita AAA	aaa new-model
El comando configura la autorización de la red a través de RADIUS	aaa authorization network default group radius
Especifica RADIUS como el método para la autenticación basada en puerto 802.1X	aaa authentication dot1x default group radius
Habilita la contabilidad de sesiones de autenticación 802.1X	aaa accounting dot1x default start-stop group radius
La IP del servidor RADIUS, contraseña y puertos de trabajo.	radius-server host ip-servidor auth-port 1812 acct-port 1813 key “ ”
Habilita globalmente la autenticación basada en puerto 802.1X.	dot1x system-auth-control
Asignación de interfaces	Range interface f1/3 - 10
Trabajar en modo acceso	switch mode access
Habilita la autenticación en un puerto.	dot1x port-control auto
Coloca el puerto controlado en el estado no	

autorizado hasta que se lleva a cabo la autenticación entre el cliente y el servidor de autenticación. Una vez que el cliente pasa la autenticación, el puerto se autoriza.

Fuente: Adaptado CISCO

4.3.2 FICAYA.

En esta locación no se efectúa el diseño, ya que al switch de distribución 3850 no se encuentra conectado a ninguna dependencia del edificio. Solo cumple la función de interconexión entre el edificio central y cada uno de los switch de acceso presentes en la facultad.

4.3.3 FACAE.

En esta facultad los puntos de red de la planta baja al igual que los del laboratorio 1 y laboratorio 2 están conectados directamente al switch de distribución cisco 4506. Para las dependencias se emplea la vlan FACAE – ADMINISTRATIVOS y en cuanto a los laboratorios la vlan FACAE – LABORATORIOS. En el diseño de esta capa se tiene en cuenta la ubicación de las distintas locaciones como se muestra en la Figura 77. y los puertos usados del switch para la vlan administrativos y vlan laboratorios como se muestra en la Tabla 50. La configuración del protocolo 802.1 X se muestra en el anexo II C.

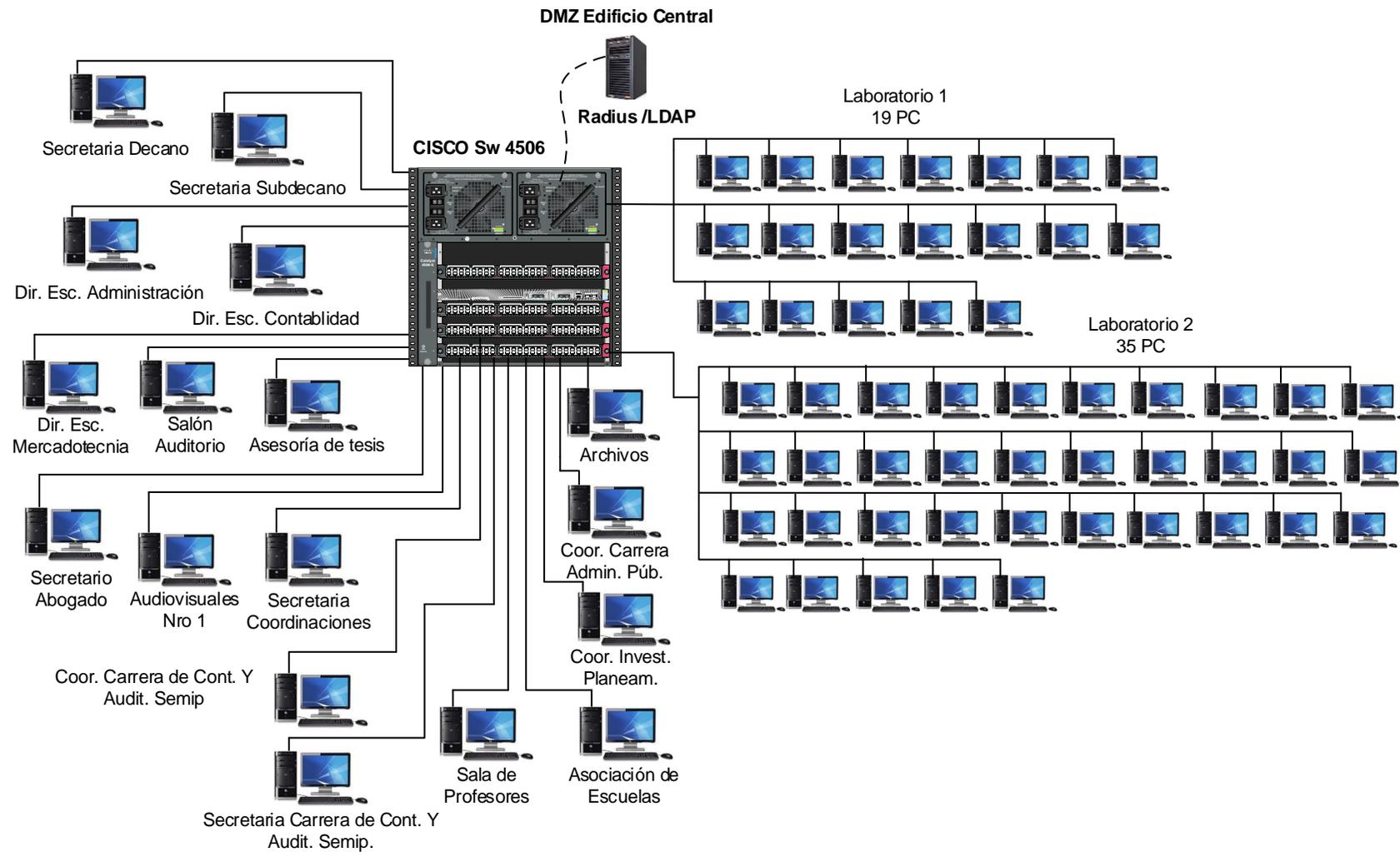


Figura 77: Diagrama capa distribución - FACAE
Fuente: Programa Visio

Tabla 50: *Puertos vlan ADMINISTRATIVOS, LABORATORISO activos FACAE SW-4506*

# Vlan	Nombre	Puerto Activo
68	FACAE-ADMINISTRATIVOS	Fa4/2, Fa4/3, Fa4/4, Fa4/5 Fa4/8, Fa4/9, Fa4/25, Fa6/19 Fa6/20, Fa6/21, Fa6/22, Fa6/23 Fa6/37, Fa6/38, Fa6/39, Fa6/40 Fa6/41, Fa6/46
64	FACAE-LABORATORIOS	Fa4/1, Fa4/6, Fa4/7, Fa4/10 Fa4/11, Fa4/12, Fa4/13, Fa4/14 Fa4/15, Fa4/16, Fa4/17, Fa4/18 Fa4/19, Fa4/20, Fa4/21, Fa4/22 Fa4/23, Fa4/24, Fa4/26, Fa4/27 Fa4/28, Fa4/29, Fa4/30, Fa4/31 Fa4/32, Fa4/33, Fa4/34, Fa4/35 Fa4/36, Fa4/37, Fa4/38, Fa4/39 Fa4/40, Fa4/41, Fa4/42, Fa4/43 Fa4/44, Fa4/45, Fa4/46, Fa4/47 Fa4/48, Fa5/1, Fa5/2, Fa5/3 Fa5/4, Fa5/5, Fa5/6, Fa5/7 Fa5/8, Fa5/9, Fa5/10, Fa5/11 Fa5/12, Fa5/13, Fa5/14, Fa5/15 Fa5/16, Fa5/17, Fa5/18, Fa5/19 Fa5/20, Fa5/21, Fa5/22, Fa5/24 Fa5/25, Fa5/26, Fa5/27, Fa5/28 Fa5/29, Fa5/30, Fa5/31, Fa5/32 Fa5/33, Fa5/34, Fa5/35, Fa5/36 Fa5/37, Fa5/38, Fa5/39, Fa5/40 Fa5/41, Fa5/42, Fa5/43, Fa5/44 Fa5/45, Fa5/46, Fa5/47, Fa5/48 Fa6/1, Fa6/2, Fa6/3, Fa6/4 Fa6/5, Fa6/6, Fa6/7, Fa6/8 Fa6/9, Fa6/10, Fa6/11, Fa6/12 Fa6/13, Fa6/14, Fa6/15, Fa6/16 Fa6/17, Fa6/18, Fa6/24, Fa6/25 Fa6/26, Fa6/27, Fa6/32

Fuente: Recuperado DDTI

4.3.4 FECYT.

En este edificio los puntos de red de la planta baja van conectados directamente al switch de distribución cisco 3850, para todos los habitáculos se emplea la vlan FECYT - ADMINISTRATIVOS. En el diseño de esta capa se establece la ubicación de las distintas dependencias como se muestra en la Figura 78 y los puertos usados del switch para la vlan administrativos como se muestra en la Tabla 51. La configuración del protocolo 802.1 X se muestra en el anexo II E.

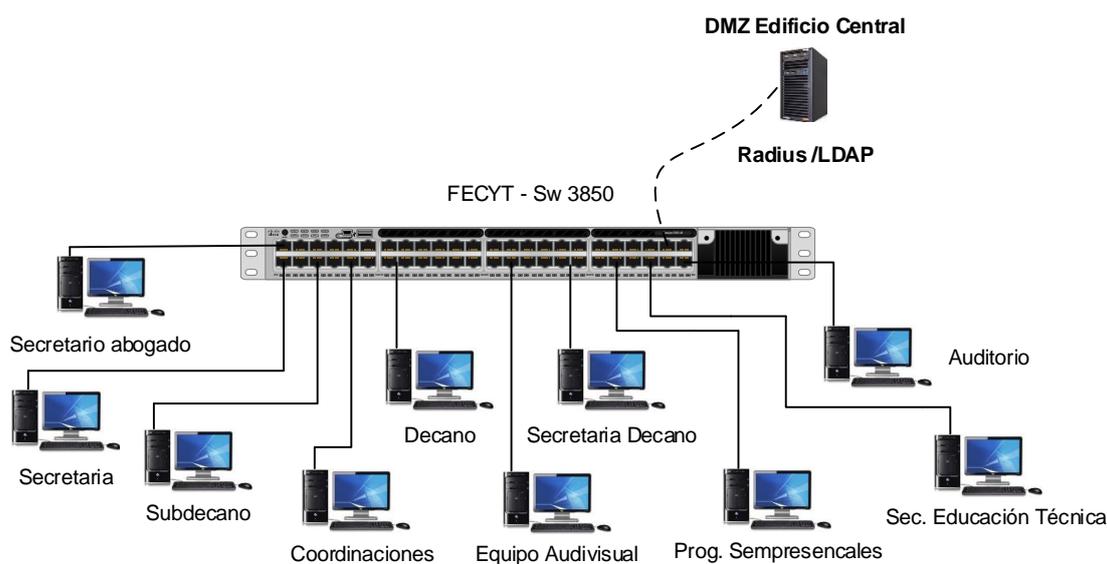


Figura 78: Diagrama capa distribución - FACAE
Fuente: Programa Visio

Tabla 51: Puertos vlan FECYT-ADMINISTRATIVOS activos SW-3850

# Vlan	Nombre	Puerto Activo
60	FECYT-ADMINISTRATIVOS	Gi1/0/13, Gi1/0/14, Gi1/0/15 Gi1/0/16, Gi1/0/17, Gi1/0/18 Gi1/0/19, Gi1/0/20

Fuente: Recuperado DDTI

4.3.5 FCCSS.

Dentro de la facultad los puntos de red de la planta baja van conectados directamente al switch de distribución cisco 3850, para todos los habitáculos se emplea la vlan FCCSS -

ADMINISTRATIVOS. En el diseño de esta capa se tiene en cuenta la ubicación de las distintas dependencias como se muestra en la Figura 79 y los puertos usados del switch para la vlan administrativos como se muestra en la Tabla 52. La configuración del protocolo 802.1 X se muestra en el anexo II E.

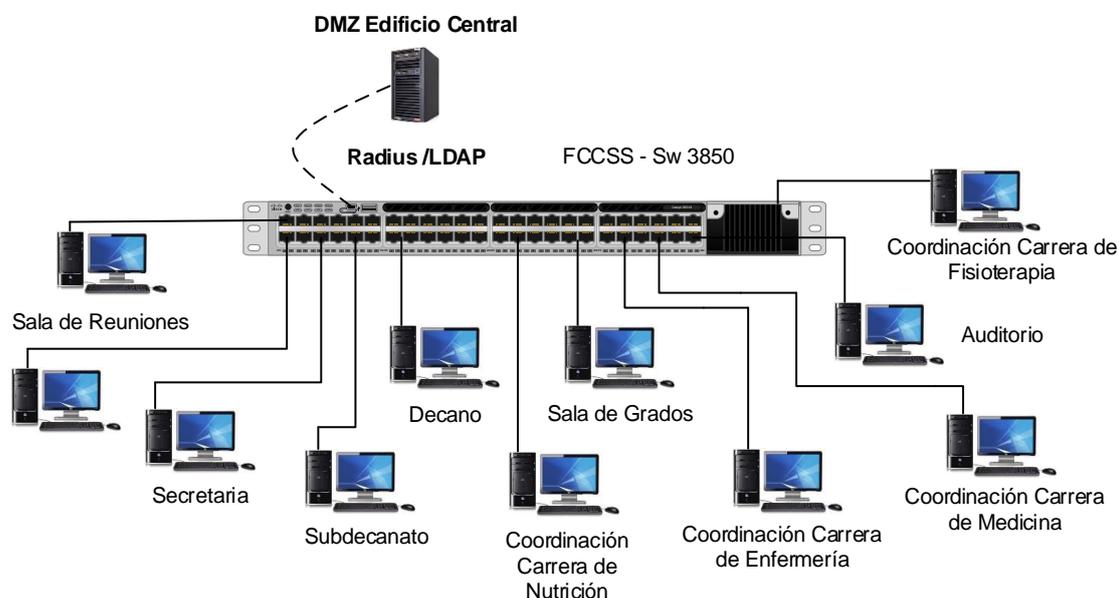


Figura 79: Diagrama capa distribución - FCCSS
Fuente: Programa Visio

Tabla 52: Puertos vlan FCCSS - ADMINISTRATIVOS activos SW-3850

# Vlan	Nombre	Puerto Activo
76	FECYT-ADMINISTRATIVOS	Gi1/0/4, Gi1/0/5, Gi1/0/6 Gi1/0/7, Gi1/0/8, Gi1/0/9 Gi1/0/10, Gi1/0/11, Gi1/0/23 Gi1/0/24, Gi1/0/25, Gi1/0/26 Gi1/0/27, Gi1/0/28, Gi1/0/29 Gi1/0/30, Gi1/0/31, Gi1/0/32 Gi1/0/33, Gi1/0/34, Gi1/0/35 Gi1/0/36, Gi1/0/37, Gi1/0/38 Gi1/0/39, Gi1/0/40, Gi1/0/41 Gi1/0/42, Gi1/0/44

Fuente: Recuperado DDTI

4.3.6 Edificio Central.

En este edificio; algunas de las locaciones de la planta baja; los puntos de red están conectados directamente al switch de Core Cisco 4510. Para las dependencias se emplean los vlans DDTI, FINANCIERO, ADMINISTRATIVOS y ADQUISICIONES. En el diseño de la capa de distribución se tiene en cuenta la ubicación de las distintas locaciones como se muestra en la Figura 80 y los puertos usados del switch para los vlans como se muestra en la Tabla 53. La configuración del protocolo 802.1 X en el switch 4510 se muestra en la Tabla 54 y de aquí en adelante en el anexo II C.

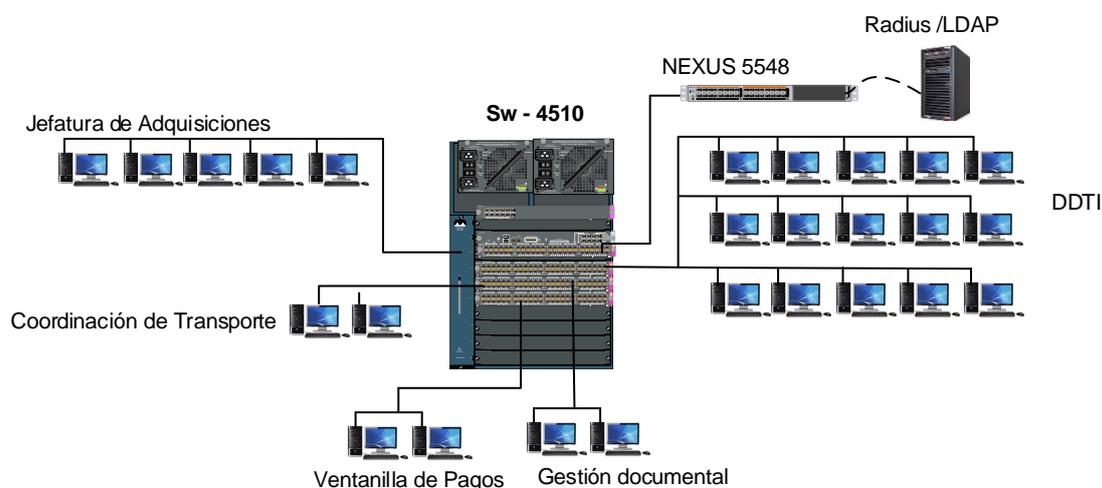


Figura 80: Diagrama capa distribución – Edificio Central
Fuente: Programa Visio

Tabla 53: Puertos vlans activos Edificio - Central SW-4510

# Vlan	Nombre	Puerto Activo
14	DDTI	Gi8/3, Gi8/4, Gi8/6, Gi8/7 Gi8/8, Gi8/10, Gi8/12, Gi8/14 Gi8/16, Gi8/17, Gi8/18, Gi8/19 Gi8/20, Gi8/21, Gi8/22, Gi8/23 Gi8/25, Gi8/26, Gi8/27, Gi8/28 Gi8/29, Gi8/30, Gi8/33, Gi8/34 Gi8/35, Gi8/37, Gi8/38, Gi8/40

		Gi8/41, Gi8/42, Gi8/43, Gi8/45 Gi9/1, Gi9/2, Gi9/3, Gi9/4 Gi9/5, Gi9/6, Gi9/12, Gi10/10 Gi10/35, Gi10/38
16	FINANCIERO	Gi9/25, Gi9/26, Gi9/27, Gi9/33
20	ADMINISTRATIVOS	Gi9/29, Gi9/30, Gi9/31, Gi9/32 Gi9/41, Gi10/1, Gi10/9, Gi10/11 Gi10/14, Gi10/15, Gi10/16 Gi10/17, Gi10/32
22	ADQUISICIONES	Gi10/3, Gi10/12, Gi10/13 Gi10/18, Gi10/19, Gi10/20 Gi10/21, Gi10/22, Gi10/23

Fuente: Recuperado DDTI

Tabla 54: *Habilitar y configurar protocolo 802.1X switch cisco 4510*

Descripción	Comando
Habilita el modo EXEC privilegiado	enable
Entra en modo de configuración global	configure terminal
Habilita AAA	aaa new-model
El comando configura la autorización de la red a través de RADIUS	aaa authorization network default group radius
Especifica RADIUS como el método para la autenticación basada en puerto 802.1X	aaa authentication dot1x default group radius
Habilita la contabilidad de sesiones de autenticación 802.1X	aaa accounting dot1x default start-stop group radius
La IP del servidor RADIUS, contraseña y puertos de trabajo.	radius-server host ip-servidor auth-port 1812 acct-port 1813 key “ ”
Habilita globalmente la autenticación basada en puerto 802.1X.	dot1x system-auth-control

Asignación de interfaces	Range interface f1/3 - 10
Trabajar en modo acceso	switch mode access
Habilita la autenticación en un puerto.	dot1x port-control auto
Coloca el puerto controlado en el estado no autorizado hasta que se lleva a cabo la autenticación entre el cliente y el servidor de autenticación. Una vez que el cliente pasa la autenticación, el puerto se autoriza.	

Fuente: Adaptado CISCO

4.4 Instalación del servidor RADIUS-LDAP-MYSQL

En esta sección se describe la instalación y configuración de los paquetes requeridos para el funcionamiento del servidor Radius. La parte de autenticación y autorización se realiza a través de un servidor LDAP y en cuanto a la contabilidad se efectúa mediante el uso de un servidor de base de datos MySQL. Se ha establecido para el diseño del sistema de seguridad la instalación del sistema operativo Ubuntu 16.04 ya que es un software libre, estable y actualizable periódicamente. A su vez es compatible e integrable con los paquetes de freeradius, Openldap y MySQL.

La instalación detallada del sistema operativo Ubuntu 16.04, los servidores (LDAP, MySQL) y la administración de los mismos, se muestran en los anexos III A, III B y III C . Para el desarrollo de la estructura del árbol de la LDAP se tuvo en cuenta la misma que está en funcionamiento en la Universidad Técnica del Norte, por lo tanto, se replicó su estructura como se muestra en la Figura 81.

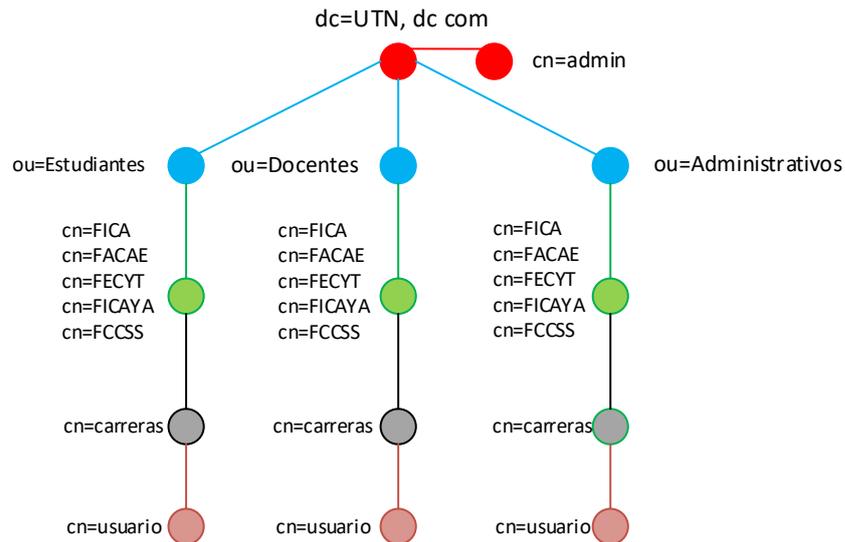


Figura 81: Árbol de distribución LDAP - UTN
Fuente: Adaptado DDTI

4.4.1 Instalación paquetes Freeradius

Previo a la instalación del servidor hay que actualizar los paquetes con el comando “apt-get update” e instalar las actualizaciones con la orden “apt-get upgrade”. A continuación, se instala los paquetes necesarios para el funcionamiento de freeradius, el módulo LDAP y MySQL (“apt-get install freeradius freeradius-ldap freeradius-mysql freeradius-utils”) como se muestra en la Figura 82.

```

root@ldap-radius:/home/mauri# apt-get install freeradius freeradius-ldap freeradius-mysql freeradius-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  freeradius-common libdbi-perl libfreeradius2 libltdl7 libmysqlclient20 libpython2.7 libpython2.7-minimal
  libpython2.7-stdlib mysql-common ssl-cert
Suggested packages:
  freeradius-postgresql freeradius-krb5 libclone-perl libmldbm-perl libnet-daemon-perl libsql-statement-perl
  openssl-blacklist
The following NEW packages will be installed:
  freeradius freeradius-common freeradius-ldap freeradius-mysql freeradius-utils libdbi-perl libfreeradius2
  libltdl7 libmysqlclient20 libpython2.7 libpython2.7-minimal libpython2.7-stdlib mysql-common ssl-cert
0 upgraded, 14 newly installed, 0 to remove and 4 not upgraded.
Need to get 5,827 kB of archives.
After this operation, 26.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] █
  
```

Figura 82: Instalación paquetes freeradius, módulos LDAP y Mysql
Fuente: Ubuntu-16.04

4.4.2 Confirmación de método de autenticación EAP-TTLS

El método EAP-TTLS tiene mejores prestaciones como se muestra en la Tabla 5. Al poseer un túnel SSL seguro aumenta los niveles de seguridad, ya que el túnel estará cifrado en los dos extremos. Otra ventaja es la posibilidad de usar métodos de autenticación heredados y la modificación dinámica; la identidad del usuario está protegida. Este método es el que se recomienda para el uso en una infraestructura de red ya que no se tiene que crear certificados por cada cliente, sino solo en la parte del servidor. Para configurar este método hay que buscar la carpeta de freeradius donde están los archivos a modificar, la ubicación del directorio es “cd /etc/freeradius/”. A continuación, se accede con un editor al archivo “eap.conf” y se hacen los cambios como se muestra en la Figura 83.

```
# common side effect of setting 'Auth-Type := EAP' is that the
# users then cannot use ANY other authentication method.
#
# EAP types NOT listed here may be supported via the "eap2" module.
# See experimental.conf for documentation.
#
eap (
    default_eap_type = ttls

    # A list is maintained to correlate EAP-Response
    # packets with EAP-Request packets. After a
    # configurable length of time, entries in the list
    # expire, and are deleted.
    #
    timer_expire     = 60
```

Figura 83: Elección método de autenticación EAP-TTLS
Fuente: Ubuntu-16.04 – Paquete freeradius

Al instalar freeradius se crea unos certificados por defecto para probar el funcionamiento del método, pero no es recomendable usar los mismos certificados en producción. Para ello se procede a crear una organización certificadora, el certificado del servidor y el certificado del cliente. Con la ayuda de archivos de configuración propios de freeradius se puede realizar la instalación de una forma efectiva mediante un script. Los archivos necesarios se encuentran en el directorio “cd /usr/share/doc/freeradius/examples/certs/”. Para crear la autoridad certificadora se modifica el archivo “ca.cnf” que es la plantilla, como se muestra en la Figura 84.

```

GNU nano 2.5.3 File: ca.cnf
[ req ]
prompt                = no
distinguished_name    = certificate_authority
default_bits          = 2048
input_password        = whatever
output_password       = whatever
x509_extensions       = v3_ca

[certificate_authority]
countryName           = EC
stateOrProvinceName   = Imbabura
localityName          = Ibarra
organizationName      = UTN
emailAddress          = emvallejos@utn.edu.com
commonName            = Autoridad Certificadora

```

Figura 84: Autoridad Certificadora
Fuente: Ubuntu-16.04 – Paquete freeradius

A continuación, se modifica las plantillas del certificado del servidor en el archivo “server.cnf” y el fichero “lient.cnf” para el cliente, como se muestra en las figuras 85 y 86 respectivamente.

```

GNU nano 2.5.3 File: server.cnf
countryName           = optional
stateOrProvinceName   = optional
localityName          = optional
organizationName      = optional
organizationalUnitName = optional
commonName            = supplied
emailAddress          = optional

[ req ]
prompt                = no
distinguished_name    = server
default_bits          = 2048
input_password        = 1234
output_password       = whatever

[server]
countryName           = EC
stateOrProvinceName   = Imbabura
localityName          = Ibarra
organizationName      = UTN
emailAddress          = emvallejos@ut.edu.ec
commonName            = Certificado Cerfidor

```

Figura 85: Certificado del servidor
Fuente: Ubuntu-16.04 – Paquete freeradius

```

GNU nano 2.5.3 File: client.cnf
[ req ]
prompt                = no
distinguished_name    = client
default_bits          = 2048
input_password        = whatever
output_password       = whatever

[client]
countryName           = EC
stateOrProvinceName   = Imbabura
localityName          = Ibarra
organizationName      = UTN
emailAddress          = user@example.com
commonName            = user@example.com

```

Figura 86: Servidor del usuario
Fuente: Ubuntu-16.04 – Paquete freeradius

Después de la edición de los tres archivos antes mencionados se corre el scrip “/bootstrap” y con ello se crea la nueva autoridad certificadora, certificados del servidor y cliente, como se muestra en la Figura 87.

```

Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'server.key'
-----
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'ca.key'
-----
Using configuration from ./server.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 1 (0x1)
  Validity
    Not Before: Jan  5 23:45:45 2019 GMT
    Not After  : Jan  5 23:45:45 2020 GMT
  Subject:
    countryName           = EC
    stateOrProvinceName   = Imbabura
    organizationName      = UTN
    commonName            = Certificado Servidor
    emailAddress          = emvallejos@ut.edu.ec
  X509v3 extensions:
    X509v3 Extended Key Usage:
      TLS Web Server Authentication
    X509v3 CRL Distribution Points:

    Full Name:
      URI:http://www.example.com/example_ca.crl
Certificate is to be certified until Jan  5 23:45:45 2020 GMT (365 days)

```

Figura 87: Creación CA y certificados
Fuente: Ubuntu-16.04 – Paquete freeradius

Finalmente, se desarrolla la comprobación de los archivos creados y copiados por el script con el comando “ls -l /etc/freeradius/certs/”, como se muestra en la Figura 88.

```

root@ldap-radius:/usr/share/doc/freeradius/examples/certs# ls -l /etc/freeradius/certs/
total 4
lrwxrwxrwx 1 root freerad  34 Jan  5 16:56 ca.pem -> /etc/ssl/certs/ca-certificates.crt
-rw-r--r-- 1 root freerad 245 Jan  5 16:56 dh
lrwxrwxrwx 1 root freerad  38 Jan  5 16:56 server.key -> /etc/ssl/private/ssl-cert-snakeoil.key
lrwxrwxrwx 1 root freerad  36 Jan  5 16:56 server.pem -> /etc/ssl/certs/ssl-cert-snakeoil.pem
root@ldap-radius:/usr/share/doc/freeradius/examples/certs# █

```

Figura 88: Comprobación de archivos creados
Fuente: Ubuntu-16.04 – Paquete freeradius

4.4.3 Integración Openldap a Freeradius.

En este apartado se procede a modificar el fichero “ldap” ubicado en la dirección /etc/freeradius/modules, con el fin de enlazar la ldap con el servicio freeradius. En el fichero se debe modificar la ip del servidor, la identidad, password y los parámetros de la base de datos, como se muestra en la Figura 89.

```
GNU nano 2.5.3 File: /etc/freeradius/modules/ldap
ldap {
    #
    # Note that this needs to match the name in the LDAP
    # server certificate, if you're using ldaps.
    server = "192.168.1.100"
    identity = "cn=admin,cd=utn,dc=com"
    password =
    basedn = "dc=utn,dc=com"
    filter = "(uid=%{Stripped-User-Name};-%{User-Name})"
    #base_filter = "(objectclass=radiusprofile)"
}
```

Figura 89: Parámetros LDAP
Fuente: Ubuntu 16.04 – Paquete Freeradius

Para realizar la autenticación a partir de la ldap se tiene que editar los ficheros “default” y “inner-tunnel” ubicados en la dirección /etc/freeradius/sites-available. Dentro de cada uno de los archivos se procede a comentar los parámetros relacionados con autenticación utilizando bases de datos, después descomentar la autorización y autenticación ldap, como se muestra en la Figura 90.

```
authorize {
    ldap
}

authenticate {
    Auth-Type LDAP {
        ldap
    }
}
```

Figura 90: Habilitar autorización y autenticación con LDAP
Fuente: Ubuntu 16.04 – Paquete Freeradius

A continuación, se procede a añadir el esquema Radius en la Ldap para poder trabajar con sus atributos. Freeradius posee una plantilla donde se encuentran todos los parámetros, se copia la misma desde la ubicación “/usr/share/doc/freeradius/examples/openldap.schema al directorio /etc/ldap/schema/radius.schema”.

Después se crea un archivo donde se llama a la ejecución de la plantilla “nano /tmp/schema.conf” con la siguiente información “include /etc/ldap/schema/radius.schema”. Para poder tener los datos en una tabla ldif se crea una carpeta contenedora con el comando “mkdir /tmp/salida” y se corre el comando “slaptest -f /tmp/schema.conf -F /tmp/salida/”, como se muestra en la Figura 91.

```
root@ldap-radius:/tmp/salida# slaptest -f /tmp/schema.conf -F /tmp/salida/
config file testing succeeded
root@ldap-radius:/tmp/salida# ls /tmp/salida/
cn=config  cn=config.ldif
root@ldap-radius:/tmp/salida#
```

Figura 91: Creación tabla ldif Radius
Fuente: Ubuntu 16.04 – Paquete ldap

Se continua con la modificación del archivo creado para poder agregar a la ldap y no de errores “nano /tmp/salida/cn=config/cn=schema/cn={0}radius.ldif”, los valores a modificar como se muestra en la Figura 92.

```
GNU nano 2.5.3 File: ...p/salida/cn=config/cn=schema/cn={0}radius.ldif Modified
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 344687e8
dn: cn=radius,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: radius
```

Figura 92: Asignar valores corrector Radius.ldif
Fuente: Ubuntu 16.04

Por último se agrega la tabla radius.ldif ldap “ldapadd -Q -Y EXTERNAL -H ldapi:/// -f /tmp/out/cn=config/cn=schema/cn={0}radius.ldif” y se verifica su existencia junto a las demás tablas ldif presentes ” ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config dn”, como se muestra en la Figura 93.

```
root@ldap-radius:/tmp/salida# ldapadd -Q -Y EXTERNAL -H ldapi:/// -f /tmp/salida/cn=config/cn=schema/cn={0}radius.ldif
adding new entry "cn=radius,cn=schema,cn=config"

root@ldap-radius:/tmp/salida# ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config dn
dn: cn=schema,cn=config

dn: cn={0}core,cn=schema,cn=config

dn: cn={1}cosine,cn=schema,cn=config

dn: cn={2}nis,cn=schema,cn=config

dn: cn={3}inetorgperson,cn=schema,cn=config

dn: cn={4}radius,cn=schema,cn=config
```

Figura 93: Agregar y comprobar Radius.ldif
Fuente: Ubuntu 16.04

4.4.4 Integración MySQL a Freeradius.

En el servidor hay que crear una base de datos con el nombre “Radius”, a su vez dar una contraseña y permitir que los cambios se realicen sin necesidad de reiniciar el servidor, como se muestra en la Figura 94.

```
mysql> CREATE DATABASE radius;
Query OK, 1 row affected (0.00 sec)

mysql> GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY "radius";
Query OK, 0 rows affected, 1 warning (0.01 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
```

Figura 94: Crear base de datos y configurar parámetros
Fuente: Ubuntu 16.04 – Paquete Mysql

Freeradius posee plantillas de Mysql para su funcionamiento para ello se efectúa la exportación de dichas plantillas a la base de datos Radius creada y su comprobación, como se muestra en la Figura 95.

```
root@ldap-radius:/home/mauri# mysql -u root -p radius < /etc/freeradius/sql/mysql/schema.sql;
Enter password:
root@ldap-radius:/home/mauri# mysql -u root -p radius < /etc/freeradius/sql/mysql/nas.sql;
Enter password:
root@ldap-radius:/home/mauri# mysql -u root -p -e "use radius;show tables;"
Enter password:
+-----+
| Tables_in_radius |
+-----+
| nas               |
| radacct           |
| radcheck          |
| radgroupcheck     |
| radgroupreply     |
| radpostauth       |
| radreply          |
| radusergroup      |
+-----+
```

Figura 95: Exportar plantillas y comprobación
Fuente: Fuente: Ubuntu 16.04 – Paquete Mysql

Después de tener la base de datos preparada para el funcionamiento en freeradius se procede a modificar el fichero “/etc/freeradius/radiusd.conf” para incluir la librería “sql”, como se muestra en la Figura 96.

```
# Include another file that has the SQL-related configuration.
# This is another file only because it tends to be big.
#
$INCLUDE sql.conf
```

Figura 96: Incluir librería “sql” en Freeradius
Fuente: Ubuntu 16.04 – Paquete Mysql

A continuación, en el archivo “sql.conf” ubicado en la carpeta “/etc/freeradius/” se establece las configuraciones el nombre de la base de datos, contraseña, permiso para usar los clientes e identificar los NAS, como se muestra en la Figura 97.

```
sql {
    database = "mysql"
    driver = "rlm_sql_${database}"
    # Connection info:
    server = "localhost"
    #port = 3306
    login = "radius"
    password = ""
    #
    #headclients = yes

    # Table to keep radius client info
    nas_table = "nas"
```

Figura 97: Enlazar base de datos y sus parámetros con Freradius
Fuente: Ubuntu 16.04 – Paquete Mysql

A su vez se modifica el archivo “/etc/freeradius/sites-enabled/default” y se establece como método “sql” la autorización, contabilidad, sesión y post-auth”, como se muestra en la Figura 98.

```

authorize {
...
    sql
...
}
accounting {
...
    sql
...
}
session {
    radutmp
    sql
}

post-auth {
...
    sql
...
}

```

Figura 98: Elegir método SQL para autorización, contabilidad, sesión post-auth
Fuente: Ubuntu 16.04 – Paquete Freeradius

Finalmente se reinicia el servicio freeradius y se verifica que no existen errores con los comandos “/etc/init.d/freeradius stop” y “freeradius -X”

4.4.5 Configuración de los clientes

Para definir los clientes hay que entrar en el fichero “clients.conf ” ubicado en el directorio “/etc/freeradius/”. En este archivo hay que definir todos los (NAS) que tienen acceso a usar freeradius y sus características (como todos los switch están en la vlan administrativa se define el segmento de red al que pertenecen todos), como se muestra en la Figura 99.

```

GNU nano 2.5.3 File: /etc/freeradius/clients.conf
#       client 192.168.3.4 {
#           secret = testing123
#       }
#)
client 192.168.1.0/24{
secret =
}

```

Figura 99: Definir segmento de red de switch
Fuente: Ubuntu 16.04 – Paquete Freeradius

Para comprobar si el servidor RADIUS – LDAP y los switch tienen acceso se emplea el comando “test aaa group radius “usuario” “contraseña” new-code”, como se muestra en la Figura 100.

```
ARISTOTELES#test aaa group radius emvallejos contraseña new-code  
User successfully authenticated
```

Figura 100: Comprobar acceso Radius-LDAP y NAS
Fuente: Ubuntu 16.04 – Paquete Freeradius

Capítulo V

5.1 Implementación en ambiente controlado y pruebas de funcionamiento

Una vez diseñado el sistema de seguridad basado en el protocolo 802.1X para toda la universidad, se establece un ambiente de prueba en la Facultad de Ingeniería en Ciencias Aplicadas (FICA). Con el fin de emular una DMZ el servidor se coloca en un puerto del switch cisco 4506 de distribución ubicado en el centro de datos de la facultad. Para la comprobación del protocolo se efectúa pruebas en clientes ubicados en la vlan FICA-LABORATORIOS y la vlan FICA-ADMINSITRATIVOS. Para el estudio del comportamiento del protocolo se emplea la herramienta de monitoreo de red Wireshark. La topología a implementar y probar como se muestra en la Figura 101. Para el funcionamiento del protocolo en el cliente se debe instalar el software SecureW2 y activar un servicio específico en el sistema. La instalación, configuración y habilitación del protocolo se muestra en el anexo IV.

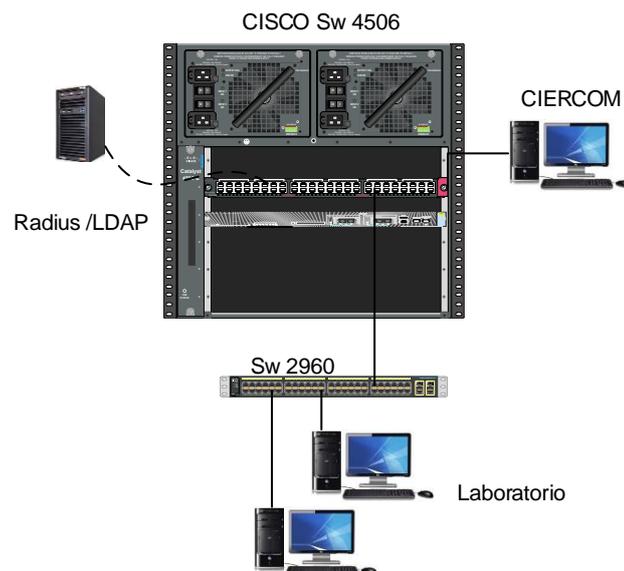


Figura 101: Topología FICA ambiente controlado
Fuente: Programa Visio

5.1.1 Interconexión del servidor al switch 4506.

En esta sección se procede a acceder al switch e identificar un puerto libre para el servidor. Así mismo agregar el puerto a la vlan FICA-ADMINISTRATIVOS, como se muestra en la Figura 102.

```
ARISTOTELES#v1
```

VLAN Name	Status	Ports
1 default	active	Fal/15
10 FICA-ADMINISTRATIVOS	active	Fal/3, Fal/4, Fal/5, Fal/6
20 FICA-LABORATORIOS	active	Fal/7, Fal/8, Fal/9, Fal/10

Figura 102: Asignación de puerto RADIUS - LDAP
Fuente: SuperPuTTY – Interfaz sw-4506

A continuación, se configura la tarjeta de red del servidor para que pertenezca a la vlan requerida (por seguridad se emplea otro direccionamiento). Editar el fichero “/etc/network/interfaces”, como se muestra en la Figura 103.

```
# The primary network interface
auto enp0s3
iface enp0s3 inet static
    address 192.168.130.85
    netmask 255.255.255.240
    network 192.168.130.0
    broadcast 192.168.130.255
    gateway 192.168.130.81
    # dns-* options are implemented by resolvconf, see
    dns-nameservers 8.8.8.8
```

Figura 103: Configurar interfaz de red servidor
Fuente: SuperPuTTY – Ubuntu 16.04

En el módulo ldap ubicado en la dirección “/etc/freeradius/modules/” se modifica la ip del servidor para enlazarlo al radius, como se muestra en la Figura 104.

```

ldap {
    server = "192.168.130.85"
    identity = "cn=admin,dc=utn,dc=com"
    password = █
    basedn = "dc=utn,dc=com"
    filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
    #base_filter = "(objectclass=radiusprofile)"
    ldap_connections_number = 5
    max_uses = 0
    # Port to connect on, defaults to 389. Setting this to
    # 636 will enable LDAPS if start_tls (see below) is not
    # able to be used.

```

Figura 104: Enlazar IP LDAP con Radius
Fuente: SuperPuTTY – Paquete Radius

Continuando con la configuración se realiza pruebas de conectividad entre las distintas vlans y el servidor, como se muestran en las Figuras 105, 106 y 107. Acto seguido iniciar servidor freeradius en modo depuración con el comando “freeradius -X”.

```

root@radius-ldap:/home/mauri# cd ..
root@radius-ldap:/home# cd ..
root@radius-ldap:/# ping 192.168.130.81
PING 192.168.130.81 (192.168.130.81) 56(84) bytes of data.
64 bytes from 192.168.130.81: icmp_seq=1 ttl=255 time=10.8 ms
64 bytes from 192.168.130.81: icmp_seq=2 ttl=255 time=6.22 ms
64 bytes from 192.168.130.81: icmp_seq=3 ttl=255 time=12.4 ms
64 bytes from 192.168.130.81: icmp_seq=4 ttl=255 time=9.44 ms
64 bytes from 192.168.130.81: icmp_seq=5 ttl=255 time=6.37 ms

```

Figura 105: Conectividad servidor y VLAN-ADMINISTRATIVOS
Fuente: SuperPuTTY – Ubuntu 16.04

```

root@radius-ldap:/# ping 192.168.130.97
PING 192.168.130.97 (192.168.130.97) 56(84) bytes of data.
64 bytes from 192.168.130.97: icmp_seq=1 ttl=255 time=10.1 ms
64 bytes from 192.168.130.97: icmp_seq=2 ttl=255 time=7.11 ms
64 bytes from 192.168.130.97: icmp_seq=3 ttl=255 time=3.13 ms
64 bytes from 192.168.130.97: icmp_seq=4 ttl=255 time=10.1 ms
64 bytes from 192.168.130.97: icmp_seq=5 ttl=255 time=7.90 ms

```

Figura 106: Conectividad servidor y VLAN-LABORATORIOS
Fuente: SuperPuTTY – Ubuntu 16.04

```

root@radius-ldap:/# ping 172.16.100.1
PING 172.16.100.1 (172.16.100.1) 56(84) bytes of data.
64 bytes from 172.16.100.1: icmp_seq=1 ttl=255 time=7.71 ms
64 bytes from 172.16.100.1: icmp_seq=2 ttl=255 time=4.07 ms
64 bytes from 172.16.100.1: icmp_seq=3 ttl=255 time=10.0 ms
64 bytes from 172.16.100.1: icmp_seq=4 ttl=255 time=6.16 ms
64 bytes from 172.16.100.1: icmp_seq=5 ttl=255 time=13.0 ms

```

Figura 107: Conectividad servidor y VLAN-ADMINISTRATIVA
Fuente: SuperPuTTY – Ubuntu 16.04

Finalmente, se accede a los modos de administración de la LDAP y MySQL ingresando las siguientes direcciones en el navegador `http://ip-servidor/phpldadmin/index.php` y `http://ip-servidor/phpmyadmin/index.php` respectivamente, como se muestra en las Figuras 108 y 109.

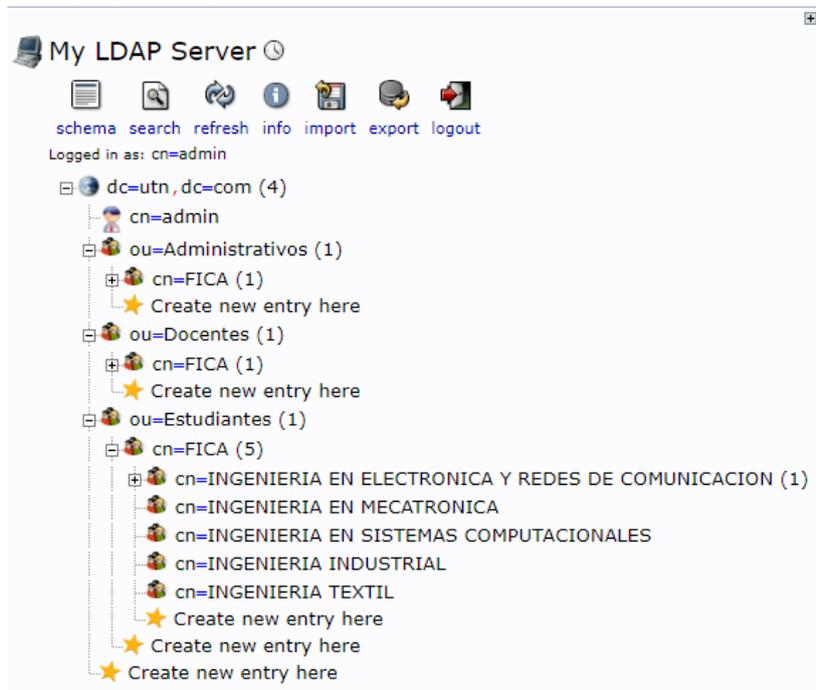


Figura 108: Administración LDAP
Fuente: Navegador Chrome

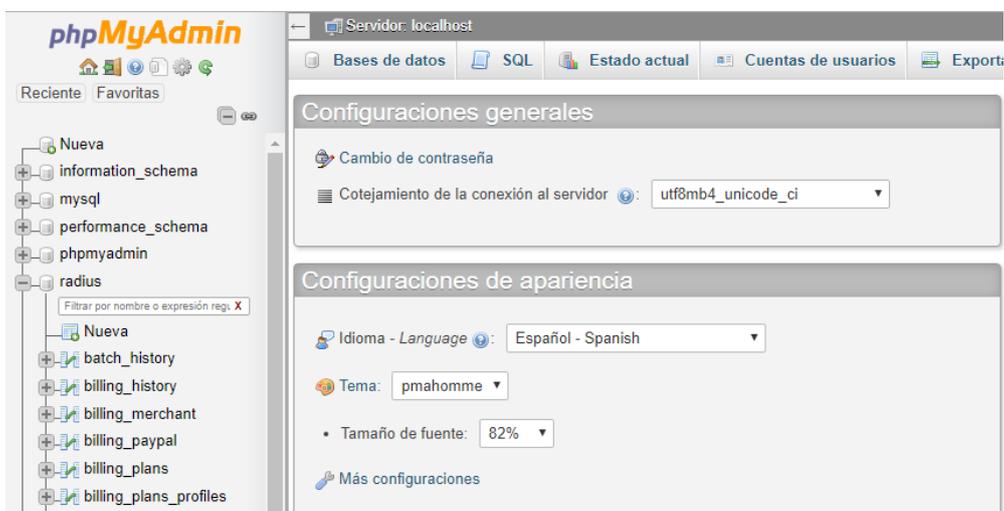


Figura 109: Administración MySQL
Fuente: Navegador Chrome

5.1.2 Configuración protocolo 802.1X Laboratorio 3.

Posteriormente, una vez comprobada la conectividad y el funcionamiento de los servidores, se procede a realizar la verificación del protocolo 802.1X. Para ello se emplea el laboratorio número 3 que contiene el SW-COPÉRNICO y el SW-COULOMB. Se accede a cada uno de los switch expuestos y se configura el protocolo, como se muestra en el anexo II A.

A continuación, se realiza la comprobación entre el NAS y la verificación de autenticación con el servidor LDAP, como se muestra en la Figura 100. Para finalizar la configuración dentro de los switch se identifica los puertos en los que el protocolo va a trabajar, pertenecientes a la VLAN-LABORATRIOS.

5.1.3 Pruebas de funcionamiento.

Dentro de este apartado se procede a describir de una forma detallada cómo funciona el protocolo dentro de distintos casos planteados. Para ello se identificó tres escenarios a la hora de intentar acceder a la red a través del servidor AAA desarrollado.

5.1.3.1 Acceso a la red sin credenciales.

En el primer escenario el usuario no ingresa sus credenciales en ningún momento y el puerto está activado para el funcionamiento de 802.1X en la interfaz FastEthernet 1/7 del SW-COPERNICO, como se muestra respectivamente en las Figuras 110 y 111.



Figura 110: Ingreso de credenciales
Fuente: Windows 10 – Programa SecureW2

```

Dot1x Info for FastEthernet1/7
-----
PAE                               = AUTHENTICATOR
PortControl                       = AUTO
ControlDirection                 = Both
HostMode                         = SINGLE_HOST
ReAuthentication                 = Disabled
QuietPeriod                      = 60
ServerTimeout                   = 30
SuppTimeout                      = 30
ReAuthPeriod                    = 3600 (Locally configured)
ReAuthMax                       = 2
MaxReq                          = 2
TxPeriod                        = 30
RateLimitPeriod                 = 0

Dot1x Authenticator Client List Empty

Port Status                      = UNAUTHORIZED

ARISTOTELES#

```

Figura 111: Estado del puerto dot1x FastEthernet 1/7
Fuente: SuperPuTTY – Interfaz SW-COPERNICO

Mediante el uso de la herramienta Wireshark se puede evidenciar que el NAS y el cliente empiezan la comunicación a través del protocolo EAP. El puerto se encuentra bloqueado y el switch para continuar con la negociación requiere credenciales para poder validar el puerto; por ello necesita una identidad; al no obtenerla sigue enviando el mensaje EAP del tipo Request Identity todo el tiempo, como se muestra en la Figura 112.

No.	Time	Source	Destination	Protocol	Length	Info
13	95.261408	c2:02:17:d4:f1:06	Nearest	EAP	60	Request, Identity
14	125.963637	c2:02:17:d4:f1:06	Nearest	EAP	60	Request, Identity
15	156.711562	c2:02:17:d4:f1:06	Nearest	EAP	60	Request, Identity
20	187.411737	c2:02:17:d4:f1:06	Nearest	EAP	60	Request, Identity
21	218.145052	c2:02:17:d4:f1:06	Nearest	EAP	60	Request, Identity
22	248.943744	c2:02:17:d4:f1:06	Nearest	EAP	60	Request, Identity


```

> Frame 13: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
< Ethernet II, Src: c2:02:17:d4:f1:06 (c2:02:17:d4:f1:06), Dst: Nearest (01:80:c2:00:00:03)
  > Destination: Nearest (01:80:c2:00:00:03)
  > Source: c2:02:17:d4:f1:06 (c2:02:17:d4:f1:06)
  Type: 802.1X Authentication (0x888e)
  Padding: 0000000000000000000000000000000000000000000000000000000000000000...
< 802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: EAP Packet (0)
  Length: 5
< Extensible Authentication Protocol
  Code: Request (1)
  Id: 30
  Length: 5
  Type: Identity (1)

```

Figura 112: Mensaje EAP del tipo Request, Identity
Fuente: Analizador de paquetes Wireshark

5.1.3.2 Acceso a la red con credenciales erróneas.

El segundo escenario consiste en el ingreso de credenciales erróneas por parte del usuario y evidenciar el funcionamiento del protocolo en dicho caso. Se analiza el envío de paquetes EAP entre el cliente al NAS y desde este último, paquete Radius al servidor AAA.

El cliente y el switch empiezan la negociación con el protocolo EAPOL start, que se emplea en conexiones cableadas del protocolo 802.1X, como se muestra en la Figura 113.

No.	Time	Source	Destination	Protocol	Length	Info
28	48.080992	02:00:4c:4f:4f:50	Nearest	EAPOL	19	Start


```

< Frame 28: 19 bytes on wire (152 bits), 19 bytes captured (152 bits) on interface 0
< Ethernet II, Src: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50), Dst: Nearest (01:80:c2:00:00:03)
  > Destination: Nearest (01:80:c2:00:00:03)
  > Source: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50)
  Type: 802.1X Authentication (0x888e)
< 802.1X Authentication
  Version: 802.1X-2001 (1)
  Type: Start (1)
  Length: 0
< VSS-Monitoring ethernet trailer, Source Port: 0
  Src Port: 0

```

Figura 113: Mensaje EAPOL del tipo Start
Fuente: Analizador de paquetes Wireshark

El NAS requiere una identidad para seguir con el proceso de autenticación por ello envía el mensaje EAP del tipo Request Identity, como se muestra en la figura 109. Acto seguido

el cliente envía una identidad la cual es anónima para la seguridad de la información que va a viajar, como se muestra en la Figura 114.

```

31 60.208566 02:00:4c:4f:4f:50 Nearest EAP 32 Response, Identity
-----
Frame 31: 32 bytes on wire (256 bits), 32 bytes captured (256 bits) on interface 0
Ethernet II, Src: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50), Dst: Nearest (01:80:c2:00:00:03)
802.1X Authentication
  Version: 802.1X-2001 (1)
  Type: EAP Packet (0)
  Length: 14
Extensible Authentication Protocol
  Code: Response (2)
  Id: 2
  Length: 14
  Type: Identity (1)
  Identity: anonymous

```

Figura 114: Mensaje EAP Response, Identity
Fuente: Analizador de paquetes Wireshark

A continuación, el switch encapsula el paquete (EAP Response Identity) en uno de formato Radius para pedir acceso al servidor AAA. Dentro de los parámetros importantes son la identidad, MAC, puerto al que está conectado y parámetros propios del NAS, como se muestra en la Figura 115.

```

424 381.579264 172.16.100.2 192.168.130.85 RADIUS 192 Access-Request id=9
-----
Frame 424: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits) on interface 0
Ethernet II, Src: c2:01:12:10:00:01 (c2:01:12:10:00:01), Dst: PcsCompu_ef:99:c6 (08:00:27:ef:99:c6)
Internet Protocol Version 4, Src: 172.16.100.2, Dst: 192.168.130.85
User Datagram Protocol, Src Port: 1645, Dst Port: 1812
RADIUS Protocol
  Code: Access-Request (1)
  Packet identifier: 0x9 (9)
  Length: 150
  Authenticator: f427b9e3cbf9837f543a4d765266bec0
  [The response to this request is in frame 425]
  Attribute Value Pairs
    > AVP: t=User-Name(1) l=11 val=anonymous
    > AVP: t=Service-Type(6) l=6 val=Framed(2)
    > AVP: t=Framed-MTU(12) l=6 val=1500
    > AVP: t=Called-Station-Id(30) l=19 val=C2-02-15-BC-F1-08
    > AVP: t=Calling-Station-Id(31) l=19 val=02-00-4C-4F-4F-50
    > AVP: t=EAP-Message(79) l=16 Last Segment[1]
    > AVP: t=Message-Authenticator(80) l=18 val=4b34fdc07bfacdfe972e3e3bb3844c
    > AVP: t=NAS-Port(5) l=6 val=8
    > AVP: t=NAS-Port-Id(87) l=17 val=FastEthernet1/8
    > AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)
    > AVP: t=NAS-IP-Address(4) l=6 val=172.16.100.2

```

Figura 115: Paquete RADIUS Access request Id=9
Fuente: Analizador de paquetes Wireshark

El siguiente proceso consiste en enviar el paquete (RADIUS Access-challenge) por parte del servidor; con la información del método de negociación EAP-TTLS; como muestra la Figura 116.

```

425 381.641747 192.168.130.85 172.16.100.2 RADIUS 106 Access-Challenge id=9
-----
Frame 425: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
Ethernet II, Src: PcsCompu_ef:99:c6 (08:00:27:ef:99:c6), Dst: c2:01:12:10:00:01 (c2:01:12:10:00:01)
Internet Protocol Version 4, Src: 192.168.130.85, Dst: 172.16.100.2
User Datagram Protocol, Src Port: 1812, Dst Port: 1645
RADIUS Protocol
  Code: Access-Challenge (11)
  Packet identifier: 0x9 (9)
  Length: 64
  Authenticator: 84a754cb8eadd820d224670de9c2ece3
  [This is a response to a request in frame 424]
  [Time from request: 0.062483000 seconds]
  Attribute Value Pairs
    AVP: t=EAP-Message(79) l=8 Last Segment[1]
      Type: 79
      Length: 8
      EAP fragment: 010300061520
    Extensible Authentication Protocol
      Code: Request (1)
      Id: 3
      Length: 6
      Type: Tunneled TLS EAP (EAP-TTLS) (21)
    > EAP-TLS Flags: 0x20
    > AVP: t=Message-Authenticator(80) l=18 val=b55e6458098dc9007580c8283f4f81e9
    > AVP: t=State(24) l=18 val=12b3672e12b072fa3f3d82c116fdb842

```

Figura 116: Paquete RADIUS Access-Challenge Id=9
Fuente: Analizador de paquetes Wireshark

Continuando con la negociación el switch envía al cliente un mensaje EAP Request con la elección del método, como se muestra en la Figura 117.

```

32 60.320963 c2:02:21:d8:f1:07 Nearest EAP 60 Request, Tunneled TLS EAP (EAP-TTLS)
-----
Frame 32: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: c2:02:21:d8:f1:07 (c2:02:21:d8:f1:07), Dst: Nearest (01:80:c2:00:00:03)
802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: EAP Packet (0)
  Length: 6
Extensible Authentication Protocol
  Code: Request (1)
  Id: 3
  Length: 6
  Type: Tunneled TLS EAP (EAP-TTLS) (21)
  > EAP-TLS Flags: 0x20

```

Figura 117: Mensaje EAP Request, Tunneled TLS EAP (EAP-TTLS)
Fuente: Analizador de paquetes Wireshark

El usuario inicia la negociación a través del protocolo TLSv1 con mensaje Client Hello, como se muestra en la Figura 118.

```

33 60.330386 02:00:4c:4f:4f:50 Nearest TLSv1 74 Client Hello
-----
Frame 33: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50), Dst: Nearest (01:80:c2:00:00:03)
802.1X Authentication
  Version: 802.1X-2001 (1)
  Type: EAP Packet (0)
  Length: 56
Extensible Authentication Protocol
  Code: Response (2)
  Id: 3
  Length: 56
  Type: Tunneled TLS EAP (EAP-TTLS) (21)
  > EAP-TLS Flags: 0x00
  > Secure Sockets Layer
    > TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 45
    > Handshake Protocol: Client Hello

```

Figura 118: Negociación del canal TLS
Fuente: Analizador de paquetes Wireshark

Después el switch encapsula el paquete Client Hello en uno del tipo Radius Access-Request y lo envía al servidor AAA, como se muestra en la Figura 119.

```

426 381.676905 172.16.100.2 192.168.130.85 RADIUS 252 Access-Request id=10
-----
Frame 426: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface 0
Ethernet II, Src: c2:01:12:10:00:01 (c2:01:12:10:00:01), Dst: PcsCompu_ef:99:c6 (08:00:27:ef:99:c6)
Internet Protocol Version 4, Src: 172.16.100.2, Dst: 192.168.130.85
User Datagram Protocol, Src Port: 1645, Dst Port: 1812
RADIUS Protocol
  Code: Access-Request (1)
  Packet identifier: 0xa (10)
  Length: 210
  Authenticator: c5b8f034eeddb72eb0e10d23f7bc5d3
  [The response to this request is in frame 427]
  > Attribute Value Pairs
    > AVP: t=User-Name(1) l=11 val=anonymous
    > AVP: t=Service-Type(6) l=6 val=Framed(2)
    > AVP: t=Framed-MTU(12) l=6 val=1500
      Type: 12
      Length: 6
      Framed-MTU: 1500
    > AVP: t=Called-Station-Id(30) l=19 val=C2-02-15-BC-F1-08
    > AVP: t=Calling-Station-Id(31) l=19 val=02-00-4C-4F-4F-50
    > AVP: t=EAP-Message(79) l=58 Last Segment[1]
      Type: 79
      Length: 58
      EAP fragment: 020300381500160301002d010000290301b713ca8ee555e5...
    > Extensible Authentication Protocol
      Code: Response (2)
      Id: 3
      Length: 56
      Type: Tunneled TLS EAP (EAP-TTLS) (21)
      > EAP-TLS Flags: 0x00
      > Secure Sockets Layer
        > TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
          Content Type: Handshake (22)
          Version: TLS 1.0 (0x0301)
          Length: 45
          Handshake Protocol: Encrypted Handshake Message

```

Figura 119: Paquete RADIUS Access request Id=10
Fuente: Analizador de paquetes Wireshark

Para continuar con el establecimiento del canal TLS el servidor comprueba la información enviada del cliente y responde con un mensaje RADIUS Access-Challenge al NAS con un certificado, los parámetros importantes como se muestra en la Figura 120.

```

427 381.743784 192.168.130.85 172.16.100.2 RADIUS 891 Access-Challenge id=10
Ethernet II, Src: PcsCompu_ef:99:c6 (08:00:27:ef:99:c6), Dst: c2:01:12:10:00:01 (c2:01:12:10:00:01)
Internet Protocol Version 4, Src: 192.168.130.85, Dst: 172.16.100.2
User Datagram Protocol, Src Port: 1812, Dst Port: 1645
RADIUS Protocol
  Code: Access-Challenge (11)
  Packet identifier: 0xa (10)
  Length: 849
  Authenticator: 43fd6aefc6b19914c015a366c0968cb4
  [This is a response to a request in frame 426]
  [Time from request: 0.066879000 seconds]
  Attribute Value Pairs
    > AVP: t=EAP-Message(79) l=255 Segment[1]
    > AVP: t=EAP-Message(79) l=255 Segment[2]
    > AVP: t=EAP-Message(79) l=255 Segment[3]
    > AVP: t=EAP-Message(79) l=28 Last Segment[4]
      Type: 79
      Length: 28
      EAP fragment: 3bc5aba97d3e55d2c443eddbace07cbe4016030100040e00...
    > Extensible Authentication Protocol
      Code: Request (1)
      Id: 4
      Length: 785
      Type: Tunnelled TLS EAP (EAP-TTLS) (21)
      > EAP-TLS Flags: 0x00
      EAP-TLS Length: 775
    > Secure Sockets Layer
      > TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
        Content Type: Handshake (22)
        Version: TLS 1.0 (0x0301)
        Length: 42
        Handshake Protocol: Encrypted Handshake Message
      > TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
        Content Type: Handshake (22)
        Version: TLS 1.0 (0x0301)
        Length: 714
        Handshake Protocol: Encrypted Handshake Message
      > TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
        Content Type: Handshake (22)
        Version: TLS 1.0 (0x0301)

```

Figura 120: Paquete RADIUS Access Challenged Id=10

Fuente: Analizador de paquetes Wireshark

El NAS envía un paquete EAP al cliente con información sobre el canal TLS, con los parámetros del certificado del servidor, como se muestra en la Figura 121.

```

61 397.782523 c2:02:15:bc:f1:08 Nearest TLSv1 803 Server Hello, Certificate, Server Hello Done
Frame 61: 803 bytes on wire (6424 bits), 803 bytes captured (6424 bits) on interface 0
Ethernet II, Src: c2:02:15:bc:f1:08 (c2:02:15:bc:f1:08), Dst: Nearest (01:80:c2:00:00:03)
802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: EAP Packet (0)
  Length: 785
Extensible Authentication Protocol
  Code: Request (1)
  Id: 14
  Length: 785
  Type: Tunnelled TLS EAP (EAP-TTLS) (21)
  > EAP-TLS Flags: 0x00
  EAP-TLS Length: 775
  > Secure Sockets Layer
    > TLSv1 Record Layer: Handshake Protocol: Server Hello
    > TLSv1 Record Layer: Handshake Protocol: Certificate
    > TLSv1 Record Layer: Handshake Protocol: Server Hello Done

```

Figura 121: Paquete EAP respuesta TLS

Fuente: Analizador de paquetes Wireshark

A continuación, el cliente intercambia la contraseña con la finalidad de cifrar el canal mediante un mensaje EAP TLSv1, como se muestra en la Figura 122.

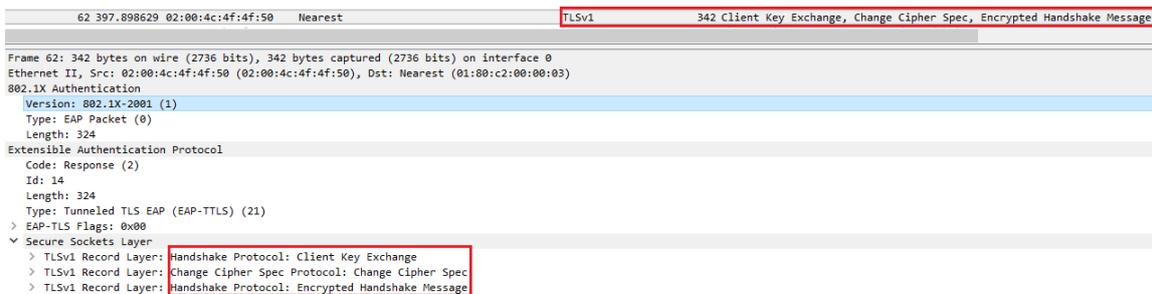


Figura 122: Paquete EAP TLSv1 cifrar canal
 Fuente: Analizador de paquetes Wireshark

Más adelante el NAS encapsula la trama anterior y la envía en formato Radius Access-Request al servidor AAA para validar en la LDAP, como se muestra en la figura 123.

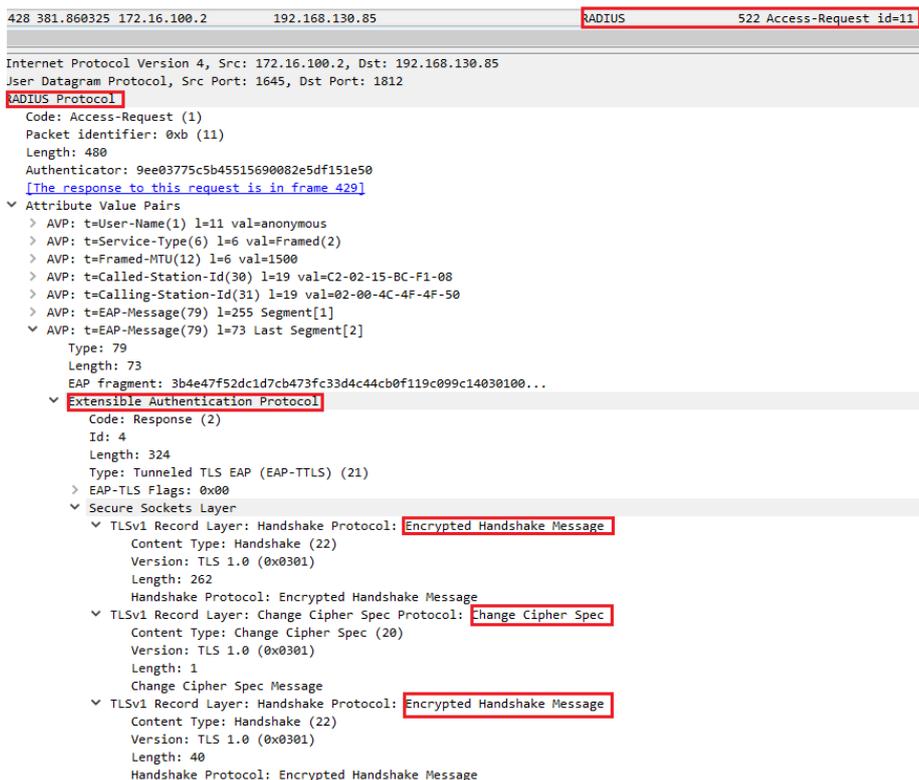


Figura 123: Paquete RADIUS Access request Id=11
 Fuente: Analizador de paquetes Wireshark

Ahora el servidor AAA manda un mensaje RADIUS Access-Challenge al NAS confirmando que el canal se encuentra cifrado con EAP-TTLS y del autenticador al cliente en formato EAP TLSv1, como muestran en las Figuras 124 y 125.

```

429 381.930834 192.168.130.85 172.16.100.2 RADIUS 161 Access-Challenge id=11
-----
Frame 429: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits) on interface 0
Ethernet II, Src: PcsCompu_ef:99:c6 (08:00:27:ef:99:c6), Dst: c2:01:12:10:00:01 (c2:01:12:10:00:01)
Internet Protocol Version 4, Src: 192.168.130.85, Dst: 172.16.100.2
User Datagram Protocol, Src Port: 1812, Dst Port: 1645
RADIUS Protocol
  Code: Access-Challenge (11)
  Packet identifier: 0xb (11)
  Length: 119
  Authenticator: ed9f90b6b1eac9f980d16d7f40e2dd5b
  [This is a response to a request in frame 428]
  [Time from request: 0.070509000 seconds]
  Attribute Value Pairs
    AVP: t=EAP-Message(79) l=63 Last Segment[1]
      Type: 79
      Length: 63
      EAP fragment: 0105003d158000000033140301000101160301002855ec3f...
    Extensible Authentication Protocol
      Code: Request (1)
      Id: 5
      Length: 61
      Type: Tunneled TLS EAP (EAP-TTLS) (21)
      EAP-TLS Flags: 0x80
      EAP-TLS Length: 51
    Secure Sockets Layer
      TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
        Content Type: Change Cipher Spec (20)
        Version: TLS 1.0 (0x0301)
        Length: 1
        Change Cipher Spec Message
      TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
        Content Type: Handshake (22)
        Version: TLS 1.0 (0x0301)
        Length: 40
        Handshake Protocol: Encrypted Handshake Message

```

Figura 124: Paquete RADIUS Access Challenged Id=11

Fuente: Analizador de paquetes Wireshark

```

63 398.075279 c2:02:15:bc:f1:08 Nearest TLSv1 79 Change Cipher Spec, Encrypted Handshake Message
-----
Frame 63: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Ethernet II, Src: c2:02:15:bc:f1:08 (c2:02:15:bc:f1:08), Dst: Nearest (01:80:c2:00:00:03)
802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: EAP Packet (0)
  Length: 61
Extensible Authentication Protocol
  Code: Request (1)
  Id: 15
  Length: 61
  Type: Tunneled TLS EAP (EAP-TTLS) (21)
  EAP-TLS Flags: 0x80
  EAP-TLS Length: 51
  Secure Sockets Layer
    TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message

```

Figura 125: Confirmación EAP-TTLS

Fuente: Analizador de paquetes Wireshark

Como el usuario ingresado no corresponde a ninguno registrado en la LDAP, el servidor notifica al NAS que no se pudo establecer la conexión correctamente, como se muestra en la Figura 126.

```

434 382.976248 192.168.130.85 172.16.100.2 RADIUS 86 Access-Reject id=12
-----
Frame 434: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: PcsCompu_ef:99:c6 (08:00:27:ef:99:c6), Dst: c2:01:12:10:00:01 (c2:01:12:10:00:01)
Internet Protocol Version 4, Src: 192.168.130.85, Dst: 172.16.100.2
User Datagram Protocol, Src Port: 1812, Dst Port: 1645
RADIUS Protocol
  Code: Access-Reject (3)
  Packet identifier: 0xc (12)
  Length: 44
  Authenticator: e1b13bbc2d1a95ef5b981e4944dd1820
  [This is a response to a request in frame 430]
  [Time from request: 1.008576000 seconds]
  Attribute Value Pairs
    AVP: t=EAP-Message(79) l=6 Last Segment[1]
      Type: 79
      Length: 6
      EAP fragment: 04050004
      Extensible Authentication Protocol
        Code: Failure (4)
        Id: 5
        Length: 4
    > AVP: t=Message-Authenticator(80) l=18 val=aca5df29559fb56319787993b2c4695a

```

Figura 126: Validación fallida RADIUS
Fuente: Analizador de paquetes Wireshark

Finalmente, se puede observar que la conexión en la parte del cliente no se pudo establecer ya que los parámetros de credenciales fueron erróneos. Por lo tanto, el puerto permanece bloqueado y no hay acceso a la red, como se muestra en la Figura 127.

```

65 399.131358 c2:02:15:bc:f1:08 Nearest EAP 60 Failure
-----
Frame 65: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: c2:02:15:bc:f1:08 (c2:02:15:bc:f1:08), Dst: Nearest (01:80:c2:00:00:03)
802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: EAP Packet (0)
  Length: 4
  Extensible Authentication Protocol
    Code: Failure (4)
    Id: 15
    Length: 4

```

Figura 127: Validación fallida cliente
Fuente: Analizador de paquetes Wireshark

5.1.3.3 Acceso a la red credenciales correctas.

En el último escenario de pruebas, se efectúa por parte del usuario el ingreso de credenciales correctas. La negociación del protocolo EAP-TTLS es igual a lo expuesto en el apartado anterior como se muestra desde las Figuras 113 a la 125 donde se detalla la conexión hasta el momento en que falla la autenticación con la LDAP. Por ello se inicia la explicación desde el punto en que las credenciales coinciden con las del servidor LDAP.

Como el cliente ha ingresado usuario y contraseña que corresponde al registrado en la LDAP, el servidor notifica al NAS que se pudo establecer la conexión correctamente, como se muestra en la Figura 128.

```

129 115.364417 192.168.130.85 172.16.100.2 RADIUS 213 Access-Accept id=4

Frame 129: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits) on interface 0
Ethernet II, Src: PcsCompu_ef:99:c6 (08:00:27:ef:99:c6), Dst: c2:01:12:10:00:01 (c2:01:12:10:00:01)
Internet Protocol Version 4, Src: 192.168.130.85, Dst: 172.16.100.2
User Datagram Protocol, Src Port: 1812, Dst Port: 1645
RADIUS Protocol
  Code: Access-Accept (2)
  Packet identifier: 0x4 (4)
  Length: 171
  Authenticator: 2b5364a4b5dd41f481954e976ea050fc
  [This is a response to a request in frame 128]
  [Time from request: 0.223365000 seconds]
  Attribute Value Pairs
    > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
    > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
    > AVP: t=EAP-Message(79) l=6 Last Segment[1]
      Type: 79
      Length: 6
      EAP fragment: 03060004
      Extensible Authentication Protocol
        Code: Success (3)
        Id: 6
        Length: 4
    > AVP: t=Message-Authenticator(80) l=18 val=b90c7dce0ea5dc091c6a56e35dfe3b28
    > AVP: t=User-Name(1) l=11 val=anonymous
      Type: 1
      Length: 11
      User-Name: anonymous

```

Figura 128: Validación correcta Radius
Fuente: Analizador de paquetes Wireshark

La conexión en la parte del cliente se pudo establecer ya que los parámetros de credenciales fueron correctos. Por lo tanto, el puerto se desbloquea con lo que hay acceso a la red, como se muestra en las Figuras 129 y 130.

```

10 61.143455 c2:02:1c:0c:f1:08 Nearest EAP 60 Success

Frame 10: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: c2:02:1c:0c:f1:08 (c2:02:1c:0c:f1:08), Dst: Nearest (01:80:c2:00:00:03)
802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: EAP Packet (0)
  Length: 4
Extensible Authentication Protocol
  Code: Success (3)
  Id: 6
  Length: 4

```

Figura 129: Validación correcta cliente
Fuente: Analizador de paquetes Wireshark

```

ARISTOTELES#show dot1x interface f1/8 details

Dot1x Info for FastEthernet1/8
-----
PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = SINGLE_HOST
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0

Dot1x Authenticator Client List
-----
Supplicant = 0200.4c4f.4f50
  Auth SM State = AUTHENTICATED
  Auth BEND SM Stat = IDLE
Port Status = AUTHORIZED

Authentication Method = Dot1x
Authorized By = Authentication Server
Vlan Policy = N/A

```

Figura 130: Validación puerto switch
Fuente: Analizador de paquetes Wireshark

Para finalizar con el análisis, se procede a explicar el proceso de la contabilidad que se efectúa entre el servidor y el NAS. Este último envía un mensaje del tipo Radius Accounting-Request al servidor AAA que contiene la petición de contabilidad, donde se identifica direccionamiento, puertos de comunicación y parámetros del protocolo RADIUS, como se muestra en la Figura 131.

```

75 60.321924 172.16.100.2 192.168.130.85 RADIUS 215 Accounting-Request
Frame 75: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface 0
Ethernet II, Src: c2:01:12:10:00:01 (c2:01:12:10:00:01), Dst: PcsCompu_ef:99:c6 (08:00:27:ef:99:c6)
Internet Protocol Version 4, Src: 172.16.100.2, Dst: 192.168.130.85
User Datagram Protocol, Src Port: 1646, Dst Port: 1813
RADIUS Protocol
Code: Accounting-Request (4)
Packet identifier: 0x1 (1)
Length: 173
Authenticator: c42e7ecf3c41a4b4f38e7f2e744086d8
[The response to this request is in frame 78]
Attribute Value Pairs
  > AVP: t=Called-Station-Id(30) l=19 val=C2-02-0B-00-F1-08
  > AVP: t=Calling-Station-Id(31) l=19 val=02-00-4C-4F-4F-50
  > AVP: t=Acct-Session-Id(44) l=51 val=172.16.100.2 anonymous 03/01/02 00:06:07 00000003
  > AVP: t=User-Name(1) l=11 val=anonymous
    Type: 1
    Length: 11
    User-Name: anonymous
  > AVP: t=Acct-Authentic(45) l=6 val=RADIUS(1)
    Type: 45
    Length: 6
    Acct-Authentic: RADIUS (1)
  > AVP: t=Acct-Status-Type(40) l=6 val=Start(1)
    Type: 40
    Length: 6
    Acct-Status-Type: Start (1)
  > AVP: t=NAS-Port(5) l=6 val=8
  > AVP: t=NAS-Port-Id(87) l=17 val=FastEthernet1/8
  > AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)
  > AVP: t=NAS-IP-Address(4) l=6 val=172.16.100.2
  > AVP: t=Acct-Delay-Time(41) l=6 val=0

```

Figura 131: Paquete Radius Accounting-Request
Fuente: Analizador de paquetes Wireshark

El servidor AAA envía un mensaje Radius del tipo Accounting-Response respondiendo al autenticador y dándole un valor al mismo, como se muestra en la Figura 132.

```

78 60.923494 192.168.130.85 172.16.100.2 RADIUS 62 Accounting-Response id=1
Frame 78: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: PcsCompu_ef:99:c6 (08:00:27:ef:99:c6), Dst: c2:01:12:10:00:01 (c2:01:12:10:00:01)
Internet Protocol Version 4, Src: 192.168.130.85, Dst: 172.16.100.2
User Datagram Protocol, Src Port: 1813, Dst Port: 1646
RADIUS Protocol
Code: Accounting-Response (5)
Packet identifier: 0x1 (1)
Length: 20
Authenticator: be8afeea19563c5d29bf218f89be844d

```

Figura 132: Paquete Radius Accounting-Response
Fuente: Analizador de paquetes Wireshark

Al realizar pruebas en distintas vlans presentes en la facultad, ya sea VLAN-LABORATORIOS Y VLAN-ADMINISTRATIVOS se determinó el correcto funcionamiento del diseño de seguridad. Con ello se ratifica que se puede usar el protocolo 802.1X junto al servidor AAA en cualquier segmento de la red de la Universidad y su comportamiento va ser el mismo como se describió en los casos anteriores con la salvedad del direccionamiento.

5.2 Conclusiones

Se cumplió los objetivos del proyecto ya que se evidenció el funcionamiento en todas las etapas del sistema de seguridad. Las pruebas con distintas vlans dentro de la Universidad Técnica del Norte demuestran el comportamiento del protocolo 802.1X y se determina que el diseño puede ser aplicado en cualquier locación de la red cableada.

El empleo del protocolo 802.1X sirve para mitigar las vulnerabilidades o amenazas tales como; robo de información, suplantación de identidad, denegación de servicios entre otras; que puede sufrir la red cableada de la casona universitaria. Por ello, con el uso de esta tecnología solo tendrán acceso los usuarios que posean credenciales válidas para ingresar a la red.

La universidad presenta un gran número de usuarios que requieren acceder a los servicios alojados en su red. Se estableció que el mejor mecanismo para la autenticación sea el EAP-TTLS PAP. Este método no tiene que crear certificados por cada cliente, sino solo en la parte del servidor. Por tanto, para la administración en un campus universitario su implementación es la mejor opción.

El método EAP-TTLS tiene mejores prestaciones, al poseer un túnel SSL seguro aumenta los niveles de seguridad, ya que el túnel estará cifrado en los dos extremos. Otra ventaja es la posibilidad de usar métodos de autenticación heredados y la modificación dinámica; la identidad del usuario está protegida.

El servidor Radius fue diseñado, para que en la parte de autenticación y autorización la ejecute a través de un servidor LDAP enlazado. El árbol LDAP se establece por estudiante, docente y administrativo. Por último, la contabilidad se efectúa mediante una base de datos MySQL. La administración del servidor AAA emplea varias interfaces gráficas para simplificar la misma.

La universidad cuenta en su infraestructura de red con equipos compatibles con el protocolo 802.1X tanto en la parte de acceso, distribución y Core. Estos switch se encuentran administrados a través de la VLAN-ADMINISTRATIVA, por ello activando el protocolo se tendrá acceso a las características del servidor AAA.

5.3 Recomendaciones

Por seguridad y para tener una red más robusta se recomienda la instalación de dos servidores AAA uno que funcione de una forma permanente y un secundario que sirva de respaldo. Al momento de la habilitación del protocolo en los switch se tiene la opción de este tipo de configuración.

El empleo de los log en la instalación y configuración del servidor AAA ayuda a encontrar errores. Con estos archivos se procede a depurar los posibles errores hasta llegar a establecer un correcto funcionamiento del servidor.

La estructura LDAP debe ser definida de una forma organizativa clara y diferenciada para facilitar la administración de los usuarios presentes en el servidor. Con ello se puede ubicar de una manera rápida usuarios para su modificación y también la eliminación de los mismos.

El administrador de la red debe usar contraseñas robustas para la administración del servidor AAA. A su vez debe realizar una metodología para asignar los parámetros de usuario y contraseña de cada uno de las personas que tendrán credenciales dentro de la Universidad Técnica del Norte.

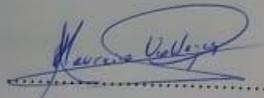
El protocolo 802.1X funciona en un rango de puertos o puertos seleccionados del switch. Con esta forma de trabajo se puede habilitar este tipo de seguridad según los requisitos del administrador, activando únicamente puertos que sean sensibles y dejando los demás de una forma predeterminada.

En un ambiente de producción, como es la Universidad Técnica del Norte se requiere cambiar los certificados que vienen instalados por defecto en los servidores. Estos deben ser

validados por una Autoridad Certificadora para mayor seguridad.

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD.

Yo, Edison Mauricio Vallejos Garzón, con cédula de identidad Nro.171807624-1, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.



Edison Mauricio Vallejos Garzón

CI: 171807624-1

Ibarra, 01 de abril 2019

Al instalar el servidor AAA se recomienda crear copias de seguridad de todos los archivos a modificar. Con ello se tiene un respaldo en caso de una configuración errónea al momento de levantar las características del servidor.

Para una futura implementación del protocolo 802.1X con autenticación EAP-TTLS PAP en redes cableadas e inalámbricas en la infraestructura de red de la Universidad Técnica. Se recomienda un análisis de tráfico previo con el fin de determinar las características de hardware y ancho de banda requerido para el correcto funcionamiento del servidor AAA.

BIBLIOGRAFÍA

- Kothaluru , T. R., & Shameel, M. Y. (Octubre de 2012). *FULLTEXT01 Evaluation of EAP Authentication Methods*. Obtenido de DIVA: <http://www.diva-portal.org/smash/get/diva2:831569/FULLTEXT01.pdf>
- Adler, T. (5 de Mayo de 2014). *Guide Version 1.0 TA UTAX 802.1X*. Obtenido de Triumph Adler: [http://www.triumph-adler.net/C125712200447418/vwLookupDownloads/FAQ_IEEE802.1x%20Deployment%20Guide_Version1.0_TA_UTAX.pdf/\\$FILE/FAQ_IEEE802.1x%20Deployment%20Guide_Version1.0_TA_UTAX.pdf](http://www.triumph-adler.net/C125712200447418/vwLookupDownloads/FAQ_IEEE802.1x%20Deployment%20Guide_Version1.0_TA_UTAX.pdf/$FILE/FAQ_IEEE802.1x%20Deployment%20Guide_Version1.0_TA_UTAX.pdf)
- Baheti, A. (2015). *Master's Projects. 425 Extensible Authentication Protocol Vulnerabilities*. Obtenido de San José State University: http://scholarworks.sjsu.edu/etd_projects/425
- Barker, K., & Wallace, K. (2015). *CompTIA Network+ N10-006 Cert Guide*. Indianapolis: Pearson.
- Barrett, D., Weiss, M., & Hausman, K. (2015). *CompTIA Security+ SYO-401 Exam Cram*. Pearson.
- Cisco. (2013). *C1 Network Security 802.11 Network Security Fundamentals*. Obtenido de Cisco: https://www.cisco.com/c/en/us/td/docs/wireless/wlan_adapter/secure_client/5-1/administration/guide/SSC_Admin_Guide_5_1/C1_Network_Security.pdf
- CISCO. (2014). *Introduction to Networks Companion Guide*. Indianapolis: Cisco Press.
- Deng, R., Weng, J., Ren, K., & Yegneswaran, V. (2016). *Security and Privacy in Communication Network*. Guangzhou: Springer.
- Elenkov, N. (2015). *Android Security Internals: An In-Depth Guide to Android's Security*. San Francisco: No Starch Press.

- Fuller, R., Jansen, D., & McPherson, M. (2013). *NX-OS and Cisco Nexus Switching: Next-Generation Data Center*. Indianapolis: Cisco Press.
- Funk, P., Software, F., Blake, S. W., & Industries, Inc, B. (Febrero de 2005). *eap-ttls-v1-00 EAP Tunneled TLS Authentication Protocol Version 1 (EAP-TTLSv1)*. Obtenido de IETF: <https://tools.ietf.org/html/draft-funk-eap-ttls-v1-00>
- Gnohz , C. (22 de Abril de 2015). *Colinz Cong*. Obtenido de Cisco TrustSec – ISE (Part 6) - 802.1X(AD): <https://colinzhong.blogspot.com/2015/04/cisco-trustsec-ise-part-6-8021xad.html>
- Howes, T., Smith, M., & Good, G. (2003). *Understanding and Deploying LDAP Directory Services*. Boston: Pearson Education, Inc.
- Huawei Technologies Co., L. (2016). *HCNA Networking Study Guide*. Shenzhen: Springer.
- Junipers, N. (12 de Mayo de 2016). *LA_802.1X_NAC Learn About 802.1X Network Access Control (NAC)*. Obtenido de JUNIPERS: https://www.juniper.net/documentation/en_US/learn-about/LA_802.1X_NAC.pdf
- Kim, D., & Solomon, M. G. (2018). *Fundamentals of Information Systems Security* (Third ed.). Burlington: Jones & Bartlett Learning.
- Kizza, J. M. (2015). *Guide to Computer Network Security*. Springer.
- Kocharians, N., & Vinson, T. (2015). *CCIE Routing and Switching v5.0 Official Cert Guide, Volume 2*. Indianapolis: Cisco Press.
- Magan , A. (2013). *Expanding a Digital Content Management System*. Burlington: Focal Press.

- Palekar, A., Simon, D., Microsoft Corporation, Salowey, J., Zhou, H., Zorn, G., . . . Josefsson, S. (15 de Octubre de 2004). *eap-tls-eap-10 Protected EAP Protocol (PEAP) Version 2*. Obtenido de IETF: <https://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-10>
- Porter, T., Kanclirz, A., Rosela, A., Cross, M., Chaffin, L., Baskin, B., & Shim, C. (2006). *Practical VoIP Security*. Canada: Syngress Publishing.
- Rigney, C., Rubens, A., Simpson, W. A., & Willens, S. (Junio de 2000). *rfc2865 Remote Authentication Dial In User Service (RADIUS)*. Obtenido de IETF: <https://www.rfc-editor.org/pdf/rfc/rfc2865.txt.pdf>
- Sandberg, B. (2015). *The complete reference Networking* . Chicago: McGraw-Hill Education.
- Sermersheim, J. (Junio de 2006). *rfc1823 The LDAP Application Program Interface*. Obtenido de IETF: <https://tools.ietf.org/html/rfc4511#page-3>
- Stallings, W. (2013). *Data And Computer Communications*. New Jersey: Pearson.
- Virtanen, T., & Curtis, B. (10 de Mayo de 2018). *ldaptor Ldaptor Documentation*. Obtenido de Read The Doc: <https://media.readthedocs.org/pdf/ldaptor/latest/ldaptor.pdf>
- Wright , J., & Cache, J. (2015). *Hacking Exposed - Wireless Security Secrets & Solutions*. McGraw Hill Professional.
- Wu, C.-H., & Irwin, D. (2013). *Introduction to Computer Networks and Cybersecurity*. Boca Ratón : Taylor & Francis Group.

ANEXO I

Ubicación de los puntos de red UTN

Ubicación de puntos de red – FICAYA

Departamento - Oficina	# Puntos	# Telf.
Decanato	8	2
Sub-Decanato	2	1
Secretaria Sub-Decanato	2	1
Secretario Abogado	2	2
Oficina De Agropecuaria	2	1
Oficina De Forestal	2	1
Oficina De Agroindustrial	2	1
Oficina De Agronegocios	4	1
Oficina De Recursos Naturales	2	1
Sala De Tutorías	5	No
Sala De Conferencias	1	No
Sala De Profesores	2	No
Laboratorio Sala A	26	1
Laboratorio Sala B	31	No
Laboratorio De Limnología	1	No
Laboratorio De Entomóloga	1	No
Laboratorio De Geología	1	No
Laboratorio De Uso Múltiple	2	No
Herbario	1	No
Museo	1	No
Club Ecológico	1	No
Aso. Est. Ing. Forestal	1	No
Aso. Est. Ing. Agroindustrial	1	No
Aso. Est. Ing. Recursos Naturales	1	No
Punto De Venta	2	No
Copiadora	2	No
Ap Internos	3	No
Total, Puntos De Red Y Teléfonos	109	12

Ubicación de puntos de red – FACAE

Departamento - Oficina	# Puntos	# Telf.
Decanato	1	1
Sub-Decanato	1	1
Secretaria Sub-Decanato	1	1
Secretario Abogado	3	1
Asesoría De Tesis	2	No
Coordinadora Mercadotecnia	3	1
Secretaria Ing. Mercadotecnia	1	1
Coordinador Contabilidad	1	1
Secretaria Ing. Contabilidad	1	1
Secretaria Ing. Contabilidad Semi-Presencial	1	1
Coordinador Economía	1	1
Secretaria Ing. Economía	1	1
Coordinador Comercial	1	1
Secretaria Ing. Comercial	1	1
Sala De Grados	1	No
Auditorio	2	No
Sala De Profesores	1	No
Oficina De Laboratorios	10	1
Laboratorio I	32	No
Laboratorio II	42	No
Laboratorio III	52	No
Laboratorio VI	36	No
Laboratorio De Publicidad I	5	No
Laboratorio De Publicidad II	5	No
Aula 103	2	No
Ap. Internos	3	No
Ap. Externos	2	No

Total, Puntos De Red Y Teléfonos	213	15
----------------------------------	-----	----

Ubicación de puntos de red – FECYT

Departamento - Oficina	# Puntos
Decanato	5
Secretaria Decanato	5
Sub-Decano	4
Secretaria Sub-Decanato	2
Secretario Abogado	4
Auditorio	4
Plan De Contingencia	8
Semipresencial	5
Coordinaciones	16
Oficina De Carreras	5
Secretarias De Carrera	3
Coor. Gestión Y Desarrollo	2
Coor. Contabilidad	2
Audiovisuales	10
Club De Turismo	2
Bodega	1
Lab. Psicología	4
Laboratorio 1	48
Laboratorio 2	32
Laboratorio 4	22
Laboratorio De Inglés	45
Ap. Interiores	3
Ap. Exteriores	1
Total, Puntos De Red Y Teléfonos	233

Ubicación de puntos de red – FCCSS

Departamento - Oficina	# Puntos
Decanato	2
Secretaria Decanato	2
Sub-Decano	2
Secretaria Sub-Decanato	2
Secretario Abogado	4
Sala Del HCD	4
Sala De Grados	2
Tutorías Enfermería (Pb)	4
Tutorías Nutrición	4
Tutorías Enfermería	2
Aula De Demostración	1
Proyectos Enfermería	2
Dirección Nutrición	6
Dirección Enfermería	2
Cubículos De Profesores	20
Sala De Internet	30
Laboratorio De Nutrición	1
Laboratorio De Estética	1
Laboratorio De Informática I	18
Laboratorio De Enfermería	2
Laboratorio De Morfo fisiología	3
Investigación Y Publicación	1
Archivo	2
FEUE	4
Aula 309	2
Aula 307	1
Aula 306	1
Aula Terraza	1

Aula Exterior	2
Ap. Exteriores	3
Total, Puntos De Red Y Teléfonos	127

Ubicación de puntos de red – Biblioteca

Departamento - Oficina	# Puntos
Cámaras	12
Prestamos Libros	16
Catálogo En Línea	6
Área Virtual	15
Equipos Portátiles	6
No Videntes	4
Hemeroteca	14
Dirección Biblioteca	10
Procesos Técnicos	6
Videoteca	8
Sala De Proyectos	2
Informática	4
Audio Y Video	2
Instituto De Altos Estudios	4
FII	4
Unidad Auditoria Interna	8
Ex Club De Robótica	2
Aso. General Profesores	4
Club Robótica	4
Área Ic3	14
Laboratorio Exámenes	8
Laboratorio 1	16
Laboratorio 2	16
Laboratorio 3	8
Archivo 1	16
Archivo 1	16
Total, Puntos De Red Y Teléfonos	227

Ubicación de puntos de red – Auditorio Agustín Cueva

Departamento - Oficina	# Puntos
Cuarto De Mantenimiento	2
Cuarto Superior (Switch De Energía)	2
Salón	2
Cuarto De Equipos De Audio-Video	2
Sala De Teatro	2
Sala Superior Izquierda (Asientos)	1
Departamento De Música	1
Departamento De Danza	2
Escenario	4
Ap Interno	1
Ap Externos	2
Total, Puntos De Red Y Teléfonos	21

Ubicación de puntos de red – Edificio Central planta baja

SECTOR	Puntos Red	Cámaras	# PC
DDTI	34	1	15
Departamento de vinculación	4		6
Oficina del estudiante	6	1	4
Información	2	1	2
Oficinas	11	1	2
Almacén Bodega	8	1	6
Jefatura de seguridad	2		1

Jefatura de adquisiciones	8		5
Coordinación de transporte	4		2
Departamento Financiero	10	1	1
Ventanilla de Pagos	4	1	2
Total	54	7	31

Ubicación de puntos de red – Edificio Central primer piso

SECTOR	Puntos Red	Cámaras	# PC
Vicerrectorado administrativo	6		4
Vicerrectorado académico	8		5
Relaciones publicas	9	1	8
Rectorado	8	1	3
Sala de reuniones	1	1	6
Total	32	3	26

Ubicación de puntos de red – Edificio Central segundo piso

SECTOR	Puntos Red	Cámaras	# PC
Pasillo			
Sala José Martí			
Sala Francisco de Orellana	2		
Sala de reuniones	8		
Comisión general y evaluación	12		8
Cubículos docentes	14		7
CUICYT	6		4
Planeamiento integral y evaluación	17		10
Total	59		29

Ubicación de puntos de red – Edificio Central tercer piso

SECTOR	Puntos Red	Cámaras	# PC
Radio	8		7
Televisión	19		5
Procuraduría	6		2
Sala José Martin	3		3
Total	36		17
Total	36		17

Ubicación de puntos de red – Edificio Central

Pisos	Puntos de Red	Dispositivos
Planta Baja	59	31
Primer Piso	46	26
Segundo Piso	59	29
Tercer Piso	36	17
Cuarto Piso	23	18
Total	223	92

ANEXO II

**Configuración del protocolo 802.1x según
modelo del switch.**

Anexo II A

Serie 2900

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Device> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Device# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>aaa new-model</p> <p>Example: Device(config)# aaa new-model</p>	<p>Enables AAA.</p>
Step 4	<p>aaa authentication dot1x {default listname} method1 [method2...]</p> <p>Example: Device(config)# aaa authentication dot1x default group radius</p>	<p>Creates a series of authentication methods that are used to determine user privilege to access the privileged command level so that the device can communicate with the AAA server.</p>
Step 5	<p>dot1x system-auth-control</p> <p>Example: Device(config)# dot1x system-auth-control</p>	<p>Globally enables 802.1X port-based authentication.</p>
Step 6	<p>identity profile default</p> <p>Example: Device(config)# identity profile default</p>	<p>Creates an identity profile and enters dot1x profile configuration mode.</p>
Step 7	<p>interface type slot/port</p> <p>Example: Device(config-identity-prof)# interface GigabitEthernet 1/0/1</p>	<p>Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.</p>
Step 8	<p>access-session port-control {auto force-authorized force-unauthorized}</p> <p>Example: Device(config-if)# access-session port-control auto</p>	<p>Enables 802.1X port-based authentication on the interface.</p> <ul style="list-style-type: none"> • auto—Enables IEEE 802.1X authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The Device requests the identity of the supplicant and begins relaying authentication messages between the supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the Device by using the supplicant MAC address. • force-authorized—Disables IEEE 802.1X authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1X-based authentication of the client. This is the default setting. • force-unauthorized—Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. The Device cannot provide authentication services to the supplicant through the port. <p>Note Effective with Cisco IOS Release 12.2(33)SX1, the authentication port-control command replaces the dot1xport-control command.</p>

Step 9	<code>dot1x pae [supplicant authenticator both]</code> Example: Device(config-if)# dot1x pae authenticator	Sets the Port Access Entity (PAE) type. <ul style="list-style-type: none">• supplicant—The interface acts only as a supplicant and does not respond to messages that are meant for an authenticator.• authenticator—The interface acts only as an authenticator and does not respond to any messages meant for a supplicant.• both—The interface behaves both as a supplicant and as an authenticator and thus does respond to all dot1x messages.
Step 10	<code>end</code> Example: Device(config-if)# end	Exits interface configuration mode and enters privileged EXEC mode.
Step 11	<code>show dot1x</code> Example: Device# show dot1x	Displays whether 802.1X authentication has been configured on the device.

Anexo II B

Serie 3750

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>aaa new-model</code>	Enable AAA.
Step 3	<code>aaa authentication dot1x { default } method1</code>	Create an 802.1x authentication method list. To create a default list to use when a named list is <i>not</i> specified in the authentication command, use the default keyword followed by the method to use in default situations. The default method list is automatically applied to all ports. For <i>method1</i> , enter the group radius keywords to use the list of all RADIUS servers for authentication. Note Though other keywords are visible in the command-line help string, only the group radius keywords are supported.
Step 4	<code>dot1x system-auth-control</code>	Enable 802.1x authentication globally on the switch.
Step 5	<code>aaa authorization network { default } group radius</code>	(Optional) Configure the switch to use user-RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment. For per-user ACLs, single-host mode must be configured. This setting is the default.
Step 6	<code>radius-server host ip-address</code>	(Optional) Specify the IP address of the RADIUS server.
Step 7	<code>radius-server key string</code>	(Optional) Specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.
Step 8	<code>interface interface-id</code>	Specify the port connected to the client to enable for 802.1x authentication, and enter interface configuration mode.
Step 9	<code>switchport mode access</code>	(Optional) Set the port to access mode only if you configured the RADIUS server in Step 6 and Step 7.
Step 10	<code>authentication port-control auto</code> or <code>dot1x port-control auto</code>	Enable 802.1x authentication on the port. For feature interaction information, see the "802.1x Authentication Configuration Guidelines" section.
Step 11	<code>end</code>	Return to privileged EXEC mode.
Step 12	<code>show authentication</code> or <code>show dot1x</code>	Verify your entries.
Step 13	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Anexo II C

Serie 4500

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# aaa new-model	Enables AAA.
Step 3	Switch(config)# aaa authentication dot1x {default} method1 [method2...]	Creates an 802.1X authentication method list. To create a default list that is used when a named list is not specified in the authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. Enter at least one of these keywords: <ul style="list-style-type: none"> • group radius—Use the list of all RADIUS servers for authentication. • none—Use no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.
Step 4	Switch(config)# aaa authorization network {default} group radius	(Optional) Configure the switch for user RADIUS authorization for all network-related service requests, such as VLAN assignment.
Step 5	Switch(config)# interface interface-id	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
Step 6	Switch(config-if)# dot1x port-control auto	Enables 802.1X authentication on the interface. For feature interaction information with trunk, dynamic, dynamic-access, EtherChannel, secure, and SPAN ports, see the "802.1X Configuration Guidelines" section.
Step 7	Switch(config-if)# end	Returns to privileged EXEC mode.
Step 8	Switch # show dot1x all	Verifies your entries. Check the Status column in the 802.1X Port Summary section of the display. An enabled status means that the port-control value is set either to auto or to force-unauthorized .
Step 9	Switch# show running-config	Verifies your entries.
Step 10	Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Anexo II D

CBS3020-HPQ

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa new-model	Enable AAA.
Step 3	aaa authentication dot1x (default) method1	<p>Create an IEEE 802.1x authentication method list.</p> <p>To create a default list that is used when a named list is <i>not</i> specified in the authentication command, use the default keyword followed by the method that is to be used in default situations. The default method list is automatically applied to all ports.</p> <p>For <i>method1</i>, enter the group radius keywords to use the list of all RADIUS servers for authentication.</p> <p>Note Though other keywords are visible in the command-line help string, only the group radius keywords are supported.</p>
Step 4	dot1x system-auth-control	Enable IEEE 802.1x authentication globally on the switch.
Step 5	aaa authorization network (default) group radius	<p>(Optional) Configure the switch to use user-RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment.</p> <p>Note For per-user ACLs, single-host mode must be configured. This setting is the default.</p>
Step 6	radius-server host ip-address	(Optional) Specify the IP address of the RADIUS server.
Step 7	radius-server key string	(Optional) Specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.
Step 8	interface interface-id	Specify the port connected to the client that is to be enabled for IEEE 802.1x authentication, and enter interface configuration mode.
Step 9	switchport mode access	(Optional) Set the port to access mode only if you configured the RADIUS server in Step 6 and Step 7.
Step 10	dot1x port-control auto	<p>Enable IEEE 802.1x authentication on the port.</p> <p>For feature interaction information, see the “IEEE 802.1x Authentication Configuration Guidelines” section on page 8-21.</p>
Step 11	end	Return to privileged EXEC mode.
Step 12	show dot1x	Verify your entries.
Step 13	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Anexo II E

Serie 3850

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Device(config)# aaa new-model	Enables AAA.
Step 4	aaa authentication dot1x {default listname} method1 [method2...] Example: Device(config)# aaa authentication dot1x default group radius	Creates a series of authentication methods that are used to determine user privilege to access the privileged command level so that the device can communicate with the AAA server.
Step 5	dot1x system-auth-control Example: Device(config)# dot1x system-auth-control	Globally enables 802.1X port-based authentication.
Step 6	identity profile default Example: Device(config)# identity profile default	Creates an identity profile and enters dot1x profile configuration mode.
Step 7	interface type slot/port Example: Device(config-identity-prof)# interface GigabitEthernet 1/0/1	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
Step 8	access-session port-control {auto force-authorized force-unauthorized} Example: Device(config-if)# access-session port-control auto	Enables 802.1X port-based authentication on the interface. <ul style="list-style-type: none"> • auto—Enables IEEE 802.1X authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The Device requests the identity of the supplicant and begins relaying authentication messages between the supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the Device by using the supplicant MAC address. • force-authorized—Disables IEEE 802.1X authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1X-based authentication of the client. This is the default setting. • force-unauthorized—Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. The Device cannot provide authentication services to the supplicant through the port. <p>Note Effective with Cisco IOS Release 12.2(33)SX1, the authentication port-control command replaces the dot1xport-control command.</p>

<p>Step 9</p>	<p>dot1x pae [supplicant authenticator both]</p> <p>Example: Device(config-if)# dot1x pae authenticator</p>	<p>Sets the Port Access Entity (PAE) type.</p> <ul style="list-style-type: none"> • supplicant—The interface acts only as a supplicant and does not respond to messages that are meant for an authenticator. • authenticator—The interface acts only as an authenticator and does not respond to any messages meant for a supplicant. • both—The interface behaves both as a supplicant and as an authenticator and thus does respond to all dot1x messages.
<p>Step 10</p>	<p>end</p> <p>Example: Device(config-if)# end</p>	<p>Exits interface configuration mode and enters privileged EXEC mode.</p>
<p>Step 11</p>	<p>show dot1x</p> <p>Example: Device# show dot1x</p>	<p>Displays whether 802.1X authentication has been configured on the device.</p>

Anexo II F

SG-200 y SG-300

Software Version

- 1.4.5.02 – Sx200 Series, Sx300 Series
- 1.1.0.14 – Sx220 Series

Host and Session Authentication

Step 1. Log in to the web-based utility and choose **Security > 802.1X > Host and Session Authentication**.

Note: The images below are taken from the SG220-26P Smart switch.



Step 2. Click the radio button of the port that you want to edit.

Host and Session Authentication Table						
Entry No.	Port	Host Authentication	Single Host			
			Action on Violation	Traps	Trap Frequency	Number of Violation
<input type="radio"/>	1 GE1	Multiple Host				
<input checked="" type="radio"/>	2 GE2	Multiple Host				
<input type="radio"/>	3 GE3	Multiple Host				
<input type="radio"/>	4 GE4	Multiple Host				
<input type="radio"/>	5 GE5	Multiple Host				
<input type="radio"/>	6 GE6	Multiple Host				
<input type="radio"/>	7 GE7	Multiple Host				

Note: In this example, Port GE2 is chosen.

Step 3. Click **Edit** to edit host and session authentication for the specified port.



Step 4. The Edit Port Authentication window will then pop up. From the Interface drop-down list, make sure the specified port is the one you chose in Step 2. Otherwise, click the drop-down arrow to choose the right port.

Interface: Port | GE2 ▾

Host Authentication: Single Host Multiple Host Multiple Sessions

Note: If you are using the 200 or 300 Series, the Edit Host and Session Authentication window appears.

Step 5. Click the radio button that corresponds to the desired authentication mode in the *Host Authentication* field. The options are:

- Single Host – The switch only grants a single authorized host access to the port.
- Multiple Host (802.1X) – Multiple hosts can gain access to the single port. This is the default mode. The switch requires only the first host to be authorized, thereafter all other clients that are connected to the port have access to the network. Should the authentication fail, the first host and all the attached clients are denied access to the network.
- Multiple Sessions – Multiple host can gain access to the single port, however each host must be authenticated.

Note: In this example, Single host is chosen.

Interface: Port GE2

Host Authentication: Single Host
 Multiple Host
 Multiple Sessions

Note: If you chose Multiple Host or Multiple Sessions, skip to **Step 9**.

Step 6. In the single Host Violation Settings area, click the radio button that corresponds to the desired Action on Violation. A violation occurs if packets arrive from a host who has a MAC address that does not match the MAC address of the original supplicant. When this occurs, the action determines what happens to packets that arrive from hosts that are not considered the original supplicant. The options are:

- Protect (Discard) – Drops the packets. This is the default action.
- Restrict (Forward) – Gives access and forwards the packets.
- Shutdown – Blocks the packets and shuts down the port. The port remains down until reactivated or until the switch is rebooted.

Note: In this example, Restrict (Forward) is chosen.

Single Host Violation Settings:

Action on Violation: Protect (Discard)
 Restrict (Forward)
 Shutdown

Step 7. (Optional) Check **Enable** in the *Traps* field to enable traps. Traps are generated Simple Network Management Protocol (SNMP) messages used to report system events. A trap is sent to the SNMP manager of the switch when a violation occurs.

Single Host Violation Settings:

Action on Violation: Protect (Discard)
 Restrict (Forward)
 Shutdown

Traps: Enable

Step 8. Enter the desired time allowed in seconds between sent traps in the *Trap Frequency* field. This defines how often traps are sent.

Note: In this example, 30 seconds is used.

Single Host Violation Settings:

Action on Violation: Protect (Discard)
 Restrict (Forward)
 Shutdown

Traps: Enable

Trap Frequency: sec (Range: 1 - 1000000, Default: 10)

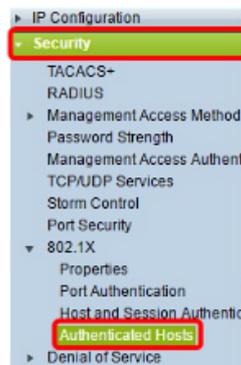
Apply Close

Step 9. Click **Apply**.

You should now have configured Host and Session Authentication on your switch.

Viewing Authenticated Hosts

Step 1. Log in to the web-based utility and choose **Security > 802.1X > Authenticated Host**.



The Authenticated Hosts Table displays the following information for authenticated hosts.

Authenticated Hosts					
Authenticated Host Table					
User Name	Port	Session Time (DD:HH:MM:SS)	Authentication Method	MAC Address	VLAN ID
0 results found.					

Anexo II G

3COM 4200,4400

Habilitar y configurar protocolo 802.1X switch 3COM 4200,4400

Descripción	Comando
Entrar en la vista del sistema.	system-view
Agregar usuario local de acceso local.	local-user localuser service-type lan-access password simple localpass
Habilitar la función de corte inactivo y establecer el intervalo de corte inactivo.	attribute idle-cut 20 quit
Configure las direcciones IP de los servidores RADIUS de autenticación y contabilidad primarios.	primary authentication IP servidor primary accounting IP servidor
Especifique la clave compartida para que el dispositivo intercambie paquetes con el servidor de autenticación.	key authentication ""
Especifique la clave compartida para que el dispositivo intercambie paquetes con el servidor de contabilidad.	key accounting ""
Configure el intervalo para que el dispositivo retransmita paquetes al Servidor RADIUS y el número máximo de intentos de transmisión.	timer response-timeout 5 retry 5
Configure el intervalo para que el dispositivo envíe paquetes de contabilidad en tiempo real al servidor RADIUS.	timer realtime-accounting 15

Especifique el dispositivo para eliminar el nombre de dominio de cualquier nombre de usuario antes de pasar el nombre de usuario al servidor de RADIUS.

```
user-name-format without-domain
quit
```

Crea un dominio “ ” e ingresa su vista.

```
domain “ ”
```

Establezca radius1 como el esquema RADIUS para los usuarios del dominio y especifique Usar autenticaciones locales como esquema secundario.

```
authentication default radius-scheme radius1 local
authorization default radius-scheme radius1 local
accounting default radius-scheme radius1 local
```

Establece el número máximo de usuarios para el dominio en 30.

```
access-limit enable 30
```

Active la función de corte inactivo y establezca el intervalo de corte inactivo.

```
idle-cut enable 20
```

Configure “ ” como el dominio predeterminado.

```
domain default enable “ ”
```

Habilitar 802.1X globalmente.

```
dot1x
```

Habilite 802.1X para el puerto GigabitEthernet “ ”.

```
interface GigabitEthernet “ ”
```

```
dot1x
```

```
quit
```

```
<swb1>
```

```
<swb1>sysconfig
```

```
[swb1]dot1x
```

```
[swb1]domain default enable test
```

```
[swb1]dot1x authentication-method eap
```

```
[swb1]radius scheme system
```

```
[swb1]radius scheme test
```

```
[swb1-radius-test]server-type standard
```

```
[swb1-radius-test]primary authentication IP SERVIDOR
```

```
[swb1-radius-test]primary accounting IP SERVIDOR
```

```
[swb1-radius-test]key authentication CLAVE
```

```
[swb1-radius-test]key accounting CLAVE
[swb1-radius-test]user-name-format without-domain
[swb1]interface GigabitEthernet 1/0/3
[swb1-GigabitEthernet1/0/3]dot1x port-method portbased
[swb1-GigabitEthernet1/0/3]dot1x
```

ANEXO III

**Instalación del sistema operativo Ubuntu 16,
servidor LDAP-MySQL y administración.**

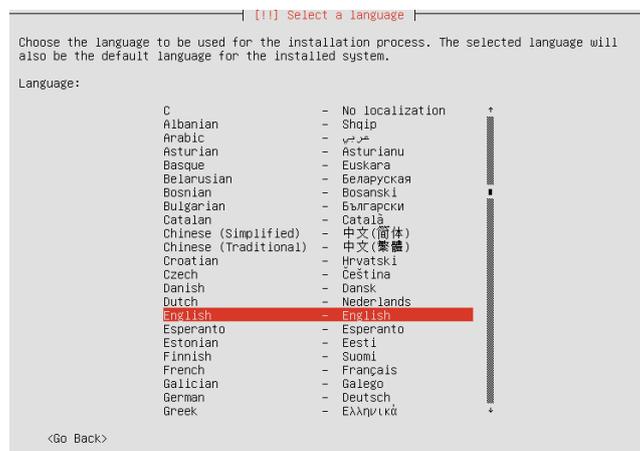
Anexo III A

Instalación sistema operativo Ubuntu

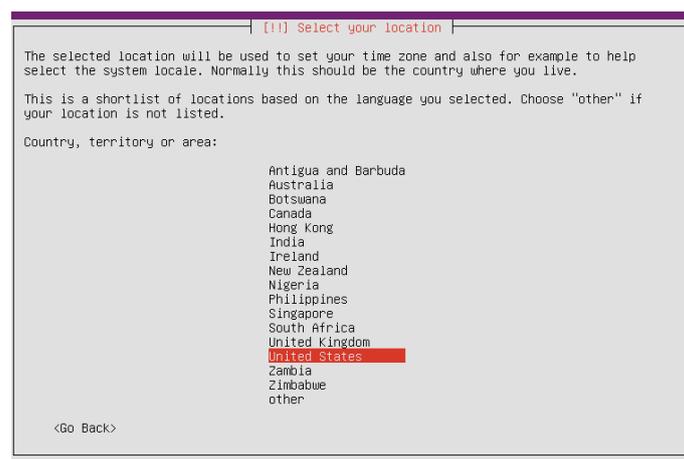
1. Menú de instalación del sistema operativo Ubuntu 16



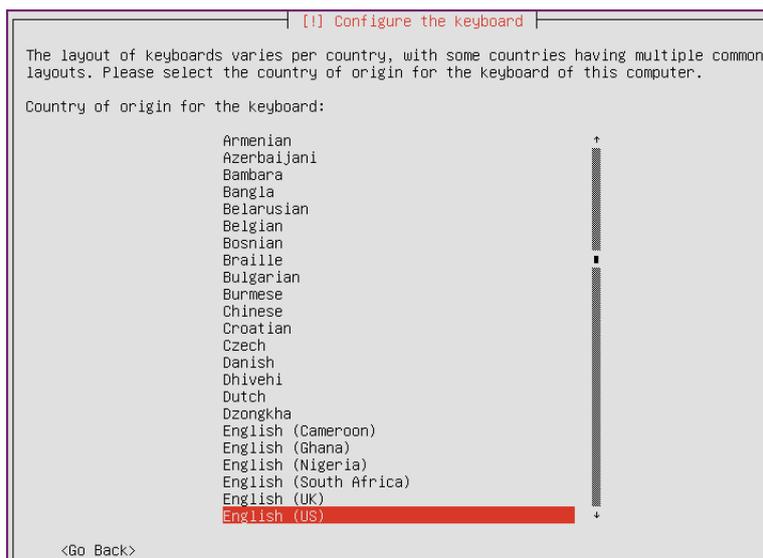
2. Elegir idioma de la instalación.



3. Escoger la ubicación para la determinación de la zona horaria.



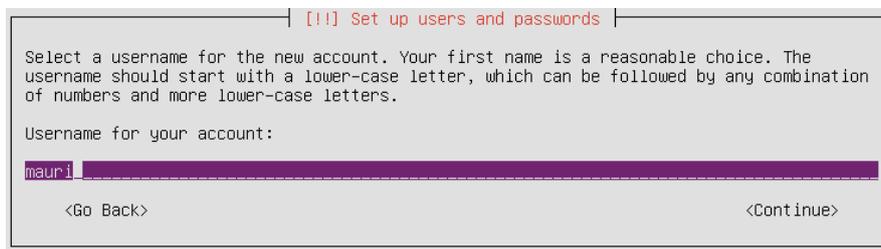
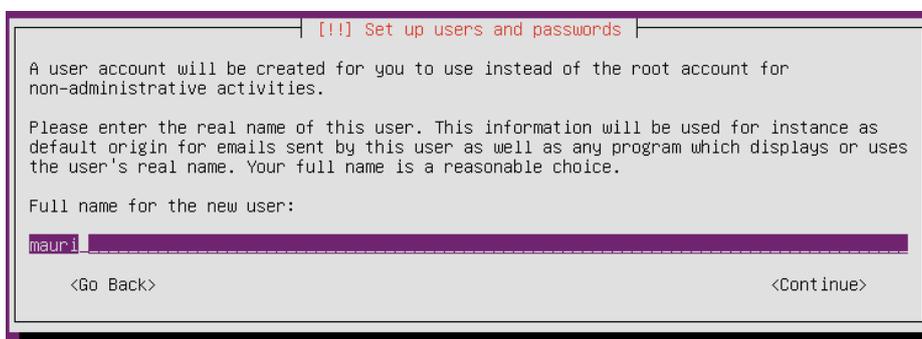
4. Seleccionar la configuración del teclado.



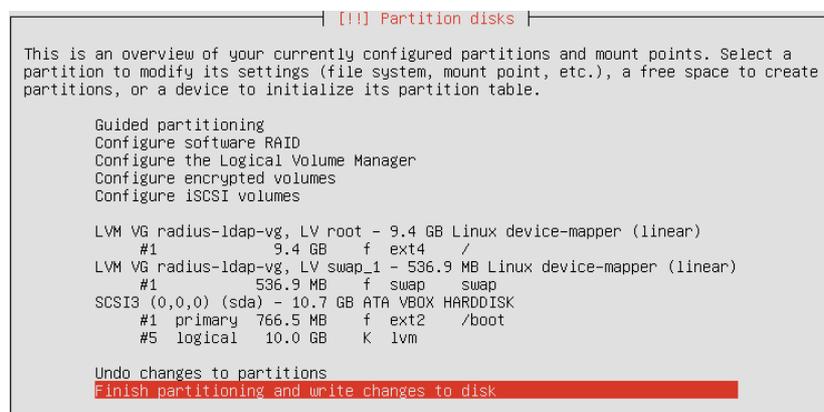
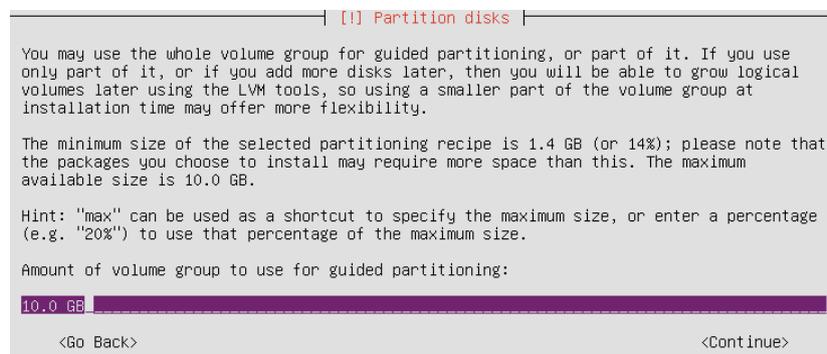
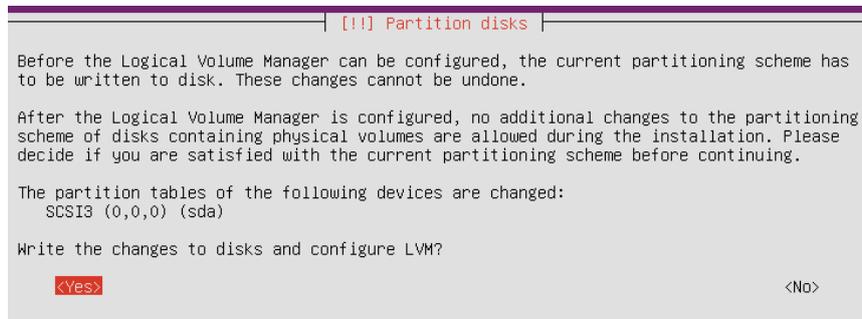
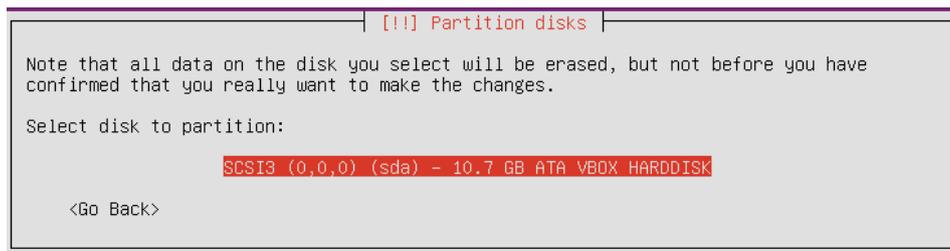
5. Determinar el nombre para el sistema.

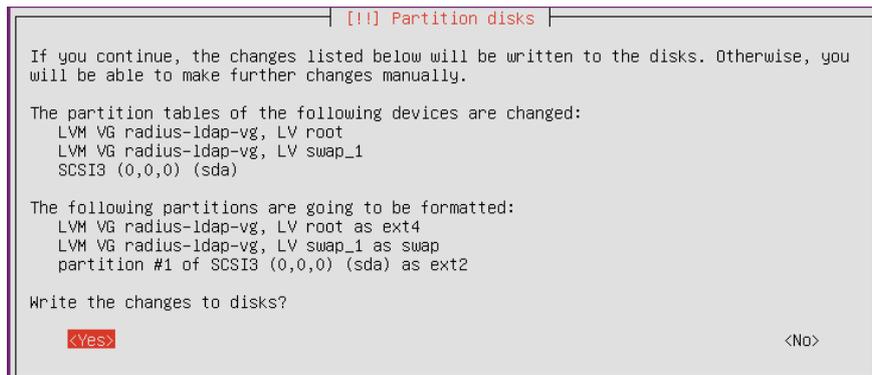


6. Elegir el nombre de usuario y contraseña

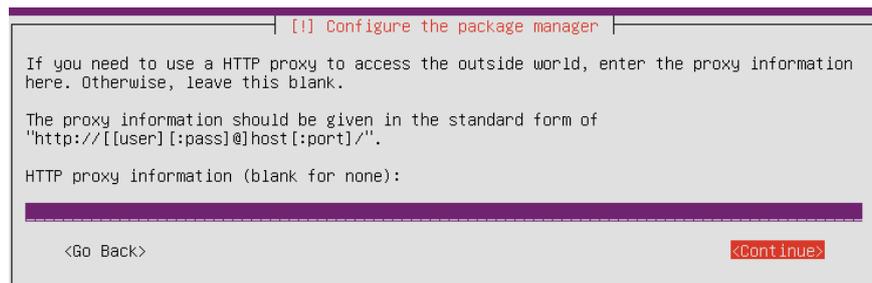


9. Escoger la partición y dar formato.

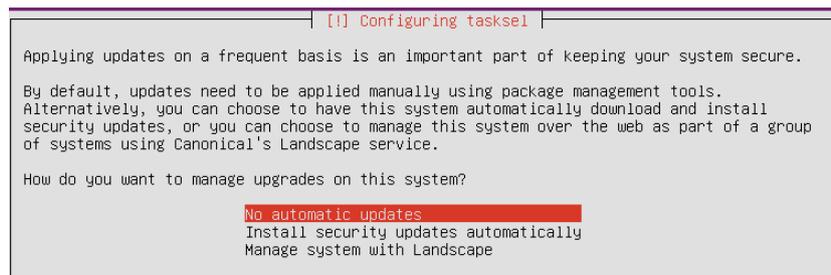




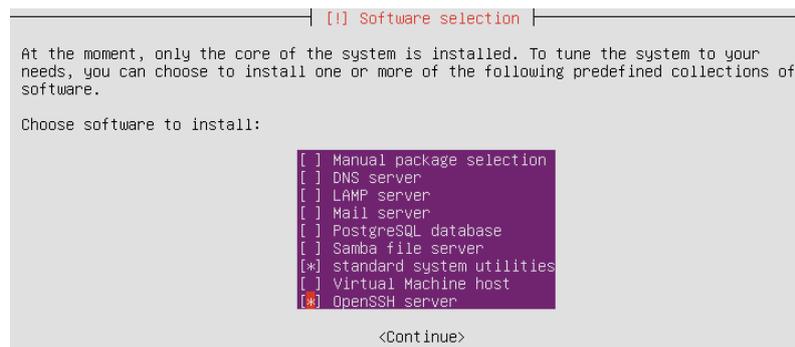
10. Establecer proxy si se posee.



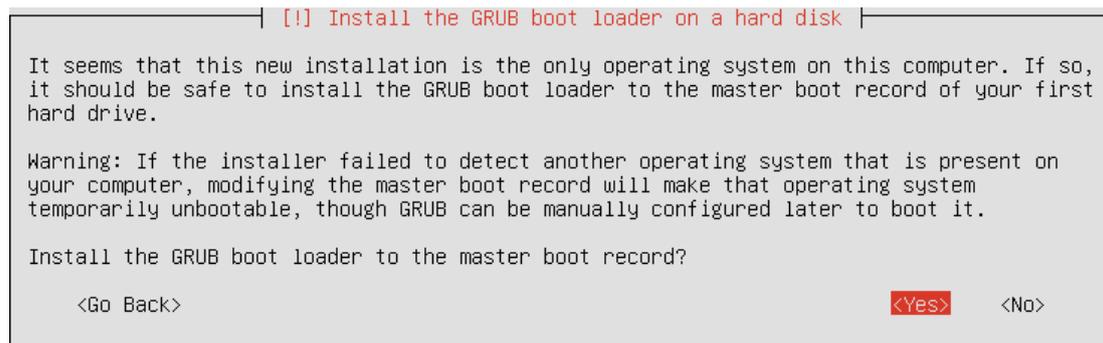
11. Deshabilitar las actualizaciones automáticas.



12. Instalar OpenSSH server en el sistema



13. Determinar el inicio con GRUB boot.



6. Establecer el nombre de la organización

```

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa Configuring slapd aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Please enter the name of the organization to use in the base DN of your LDAP directory.

Organization name:

utn

<Ok>

```

7. Ingresar contraseña administrador

```

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa Configuring slapd aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Please enter the password for the admin entry in your LDAP directory.

Administrator password:

*****

<Ok>

```

8. Confirmación contraseña administrador

```

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa Configuring slapd aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Please enter the admin password for your LDAP directory again to verify that you have typed it
correctly.

Confirm password:

*****

<Ok>

```

9. Determinar el motor de base de datos a utilizar

```

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa Configuring slapd aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
HDB and BDB use similar storage formats, but HDB adds support for subtree renames. Both support the
same configuration options.

The MDB backend is recommended. MDB uses a new storage format and requires less configuration than BDB
or HDB.

In any case, you should review the resulting database configuration for your needs. See
/usr/share/doc/slapd/README.Debian.gz for more details.

Database backend to use:

BDB
HDB
MDB

<Ok>

```

10. Borrar base de datos

```

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa Configuring slapd aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Do you want the database to be removed when slapd is purged?

<Yes> <No>

```

11. Mover la base de datos anterior

```

##### Configuring slapd #####
There are still files in /var/lib/ldap which will probably break the configuration process. If you
enable this option, the maintainer scripts will move the old database files out of the way before
creating a new database.

Move old database?

<Yes> <No>

```

12. Desactivar el protocolo LDAPv2 manual

```

##### Configuring slapd #####
The obsolete LDAPv2 protocol is disabled by default in slapd. Programs and users should upgrade to
LDAPv3. If you have old programs which can't use LDAPv3, you should select this option and 'allow
bind_v2' will be added to your slapd.conf file.

Allow LDAPv2 protocol?

<Yes> <No>

```

13. Inicializar el servicio OPENLDAP

```

root@radius-ldap:/home/mauri# dpkg-reconfigure slapd
Moving old database directory to /var/backups:
There are leftover files in /var/lib/ldap. This will probably break
creating the initial directory. If that's the case please move away
stuff in there and retry the configuration.
Creating initial configuration... done.
Creating LDAP directory... done.
root@radius-ldap:/home/mauri# █

```

Instalación administración LDAP “PhpLdapAdmin”

Para una administración más robusta y clara se usa la herramienta phpldapadmin dentro de un servidor LDAP. Con el comando `apt-get install phpldapadmin` se efectúa la instalación del paquete. Después de su establecimiento hay que enlazar con el servicio Openldap, para ello hay que editar el archivo `/etc/phpldapadmin/config.php` donde se procede a modificar los dominios según nuestras configuraciones establecidas.

```

GNU nano 2.5.3 File: /etc/phpldapadmin/config.php

'cookie', 'session' or 'sasl' auth types, LEAVE THE LOGIN_DN AND LOGIN_PASS
BLANK. If you specify a login_attr in conjunction with a cookie or session
auth_type, then you can also specify the bind_id/bind_pass here for searching
the directory for users (ie, if your LDAP server does not allow anonymous
binds. */
servers->setValue('login', 'bind_id', 'cn=admin,dc=utn,dc=com');
# servers->setValue('login', 'bind_id', 'cn=Manager,dc=example,dc=com');

```

```

GNU nano 2.5.3 File: /etc/phpldapadmin/config.php
auto-detect it for you. */
$servers->setValue('server','base',array('dc=utn,dc=com'));

```

Configurar unidades organizativas, grupos y usuarios

Método I. Ingresar tablas por comandos.

1. Crear directorio contenga ficheros “ldif”.

mkdir LDAP

2. Crear ficheros:

nano unidadesorganizativas.ldif

```

GNU nano 2.5.3 File: unidadesorganizativas.ldif
dn: ou=fica,dc=utn,dc=com
objectClass: top
objectClass: organizationalUnit
ou: fica

dn: ou=biblioteca,dc=utn,dc=com
objectClass: top
objectClass: organizationalUnit
ou: biblioteca

```

nano grupos.ldif

```

GNU nano 2.5.3 File: grupos.ldif
dn: cn=Administrativos,ou=Fica,dc=utn,dc=com
objectClass: top
objectClass: posixGroup
gidNumber: 2000
cn: Administrativos

dn: cn=Docentes,ou=Fica,dc=utn,dc=com
objectClass: top
objectClass: posixGroup
gidNumber: 2000
cn: Docentes

dn: cn=Estudiantes,ou=Fica,dc=utn,dc=com
objectClass: top
objectClass: posixGroup
gidNumber: 2000
cn: Estudiantes

```

nano usuarios.ldif

```

GNU nano 2.5.3 File: usuarios.ldif
cn: cn=Mauricio Vallejos,cn=Estudiantes,ou=Fica,dc=utn,dc=com
cn: Mauricio Vallejos
gidnumber: 2000
givenname: Mauricio
homedirectory: /home/users/mvallejos
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: top
sn: Vallejos
uid: mvallejos
uidnumber: 1000
userpassword: {SSHA}5UXKqiSQ/1lr4ocl2pumiHpBMWsl0heK

```

3. Cargamos la configuración de los ficheros

```
ldapadd -x -D 'cn=admin,dc=utn,dc=com' -W -f unidadesorganizativas.ldif
```

```
ldapadd -x -D 'cn=admin,dc=utn,dc=com' -W -f grupos.ldif
```

```
ldapadd -x -D 'cn=admin,dc=utn,dc=com' -W -f usuarios.ldif
```

Método II. Administración por “PhpLdapAdmin”

1. Ingresar a la administración “IP del servidor”/phpldapadmin/index.php



2. Colocar dominio y contraseña

Login DN:

Password:

Anonymous

3. Acceso a panel de administración.

The screenshot shows the phpLDAPadmin interface. At the top left, there's a navigation menu with options like 'Home', 'Purge caches', and 'Show Cache'. Below that, there's a 'My LDAP Server' section with a tree view showing the directory structure: 'dc=utn, dc=com (1)' containing 'cn=admin'. A 'Delete DN' notification banner at the top right states 'Successfully deleted DN ou=ESTUDIANTES,dc=utn,dc=com'. The main content area features the phpLDAPadmin logo and a message: 'Use the menu to the left to navigate'. At the bottom, there are links for 'Credits', 'Documentation', and 'Donate'.

4. Desplegar opción importar

The screenshot displays the 'Import' page. The title 'Import' is centered in a dark blue header, with 'Server: My LDAP Server' below it. The main content area has two options: 'Select an LDIF file' with a 'Seleccionar archivo' button and the text 'Ningún archivo seleccionado' and 'Maximum file size 2M'; and 'Or paste your LDIF here' with a large text area containing three LDIF entries for 'Estudiantes', 'Docentes', and 'Administrativos'. At the bottom, there is a checkbox for 'Don't stop on errors' and a 'Proceed >>' button.

5. Cargar tablas LDIF de organización

This screenshot shows the 'Import' page after a successful import. The title 'Import' is in the dark blue header, followed by 'Server: My LDAP Server File: STDIN 318 bytes (LDIF Import)'. The main content area displays three lines of green text indicating success: 'Adding ou=Estudiantes,dc=utn,dc=com Success', 'Adding ou=Docentes,dc=utn,dc=com Success', and 'Adding ou=Administrativos,dc=utn,dc=com Success'.

6. Importar y cargar tablas de FICA

Import
 Server: My LDAP Server

Select an LDIF file
 Ningún archivo seleccionado
Maximum file size 2M

Or paste your LDIF here

```

dn: cn=FICA,ou=Estudiantes,dc=utn,dc=com
objectclass: posixGroup
objectclass: top
cn: FICA
gidNumber: 20000

dn: cn=FICA,ou=Docentes,dc=utn,dc=com
objectclass: posixGroup
objectclass: top
cn: FICA
gidNumber: 20001

dn: cn=FICA,ou=Administrativos,dc=utn,dc=com
objectclass: posixGroup
objectclass: top
cn: FICA
gidNumber: 20002
          
```

Don't stop on errors

Import
 Server: My LDAP Server File: STDIN 355 bytes (LDIF Import)

Adding cn=FICA,ou=Estudiantes,dc=utn,dc=com Success

Adding cn=FICA,ou=Docentes,dc=utn,dc=com Success

Adding cn=FICA,ou=Administrativos,dc=utn,dc=com Success

7. Importar y cargar tablas carreras FICA

Import
 Server: My LDAP Server

Select an LDIF file
 Ningún archivo seleccionado
Maximum file size 2M

Or paste your LDIF here

```

dn: cn=INGENIERIA EN ELECTRONICA Y REDES DE COMUNICACION,cn=FICA,ou=Estudiantes,dc=utn,dc=com
cn: INGENIERIA EN ELECTRONICA Y REDES DE COMUNICACION
gidNumber: 20000
objectclass: posixGroup
objectclass: top

dn: cn=INGENIERIA EN MECATRONICA,cn=FICA,ou=Estudiantes,dc=utn,dc=com
cn: INGENIERIA EN MECATRONICA
gidNumber: 20000
objectclass: posixGroup
objectclass: top

dn: cn=INGENIERIA EN SISTEMAS COMPUTACIONALES,cn=FICA,ou=Estudiantes,dc=utn,dc=com
cn: INGENIERIA EN SISTEMAS COMPUTACIONALES
gidNumber: 20000
objectclass: posixGroup
objectclass: top

dn: cn=INGENIERIA INDUSTRIAL,cn=FICA,ou=Estudiantes,dc=utn,dc=com
          
```

Import

Server: **My LDAP Server** File: **STDIN 886 bytes (LDIF Import)**

```

Adding cn=INGENIERIA EN ELECTRONICA Y REDES DE COMUNICACION,cn=FICA,ou=Estudiantes,dc=utn,dc=com
Success
Adding cn=INGENIERIA EN MECATRONICA,cn=FICA,ou=Estudiantes,dc=utn,dc=com Success
Adding cn=INGENIERIA EN SISTEMAS COMPUTACIONALES,cn=FICA,ou=Estudiantes,dc=utn,dc=com Success
Adding cn=INGENIERIA INDUSTRIAL,cn=FICA,ou=Estudiantes,dc=utn,dc=com Success
Adding cn=INGENIERIA TEXTIL,cn=FICA,ou=Estudiantes,dc=utn,dc=com Success

```

8. Importar y cargar tablas usuarios

Import

Server: **My LDAP Server**

Select an LDIF file Ningún archivo seleccionado

Maximum file size 2M

Or paste your LDIF here

```

dn: cn=Edison Mauricio Vallejos Garzon,cn=INGENIERIA EN ELECTRONICA Y REDES DE
COMUNICACION,cn=FICA,ou=Estudiantes,dc=utn,dc=com
cn: Edison Mauricio Vallejos Garzon
description: Ingeniería En Electrónica Y Redes De Comunicación
mail: emvallejos@utn.edu.ec
objectClass: person
objectClass: uidObject
objectClass: top
objectClass: radiusprofile
objectClass: inetOrgPerson
radiusTunnelMediumType: IEEE-802
radiusTunnelPrivateGroupId:
radiusTunnelType: VLAN
sn: Vallejos Garzón
uid: emvallejos
userPassword: 12345678

```

Don't stop on errors

Import

Server: **My LDAP Server** File: **STDIN 542 bytes (LDIF Import)**

```

Adding cn=Edison Mauricio Vallejos Garzon,cn=INGENIERIA EN ELECTRONICA Y REDES DE
COMUNICACION,cn=FICA,ou=Estudiantes,dc=utn,dc=com Success

```

9. Panel de administración

phpLDAPadmin

Home | Purge caches | Show Cache

My LDAP Server 🕒









[schema](#)
[search](#)
[refresh](#)
[info](#)
[import](#)
[export](#)
[logout](#)

Logged in as: cn=admin

- 🌐 dc=utn,dc=com (4)
 - 👤 cn=admin
 - 👤 ou=Administrativos (1)
 - 👤 cn=FICA (1)
 - 👤 cn=Admin1
 - ★ Create new entry here
 - 👤 ou=Docentes (1)
 - 👤 cn=FICA (1+)
 - 👤 cn=Docente1
 - ★ Create new entry here
 - 👤 ou=Estudiantes (1)
 - 👤 cn=FICA (5)
 - 👤 cn=INGENIERIA EN ELECTRONICA Y REDES DE COMUNICACION (1)
 - 👤 cn=Edison Mauricio Vallejos Garzon
 - 👤 cn=INGENIERIA EN MECATRONICA
 - 👤 cn=INGENIERIA EN SISTEMAS COMPUTACIONALES
 - 👤 cn=INGENIERIA INDUSTRIAL
 - 👤 cn=INGENIERIA TEXTIL
 - ★ Create new entry here
 - ★ Create new entry here
 - ★ Create new entry here

Anexo III C

Instalación servidor de base de datos Mysql y administración

1. Instalar los paquetes necesarios:

```
sudo apt-get install mysql-server mysql-common mysql-client
```

```
root@ldap-radius:/home/mauri# sudo apt-get install mysql-server mysql-common mysql-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
mysql-common is already the newest version (5.7.24-0ubuntu0.16.04.1).
mysql-common set to manually installed.
The following additional packages will be installed:
  libaiol libcgi-fast-perl libcgi-pm-perl libencode-locale-perl libevent-core-2.0-5 libfcgi-perl libhtml-parser-perl
  libhtml-tagset-perl libhtml-template-perl libhttp-date-perl libhttp-message-perl libio-html-perl liblwp-mediatypes-perl
  libtimedate-perl liburi-perl mysql-client-5.7 mysql-client-core-5.7 mysql-server-5.7 mysql-server-core-5.7
Suggested packages:
  libdata-dump-perl libipc-sharedcache-perl libwww-perl mailx tinyca
The following NEW packages will be installed:
  libaiol libcgi-fast-perl libcgi-pm-perl libencode-locale-perl libevent-core-2.0-5 libfcgi-perl libhtml-parser-perl
  libhtml-tagset-perl libhtml-template-perl libhttp-date-perl libhttp-message-perl libio-html-perl liblwp-mediatypes-perl
  libtimedate-perl liburi-perl mysql-client mysql-client-5.7 mysql-client-core-5.7 mysql-server mysql-server-5.7
  mysql-server-core-5.7
0 upgraded, 21 newly installed, 0 to remove and 11 not upgraded.
Need to get 19.0 MB of archives.
After this operation, 162 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

2. Configurar la contraseña de MySQL de usuario ROOT

```

##### Configuring mysql-server-5.7 #####
While not mandatory, it is highly recommended that you set a password for the MySQL administrative "root" user.

If this field is left blank, the password will not be changed.

New password for the MySQL "root" user:
*****
<Ok>

```

3. Confirmar la contraseña

```

##### Configuring mysql-server-5.7 #####

Repeat password for the MySQL "root" user:
*****
<Ok>

```

4. Ingresar a la base de datos con usuario "root" y contraseña.

```

root@ldap-radius:/home/mauri# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.24-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>

```

5. Crear base de datos de Radius.

```
mysql> CREATE DATABASE radius;
Query OK, 1 row affected (0.00 sec)
```

6. Identificar a la base de datos con una contraseña.

```
mysql> GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY " ";
Query OK, 0 rows affected, 1 warning (0.00 sec)
```

Administración MySQL

PhPMyAdmin

7. Instalar el paquete apt-get install phpmymadmin

```
root@ldap-radius:/home/mauri# apt-get install phpmymadmin
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package phpmymadmin
root@ldap-radius:/home/mauri# apt-get install phpmymadmin
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  dbconfig-common dbconfig-mysql fontconfig-config fonts-dejavu-core javascript-common libfontconfig1 libgd3 libjpeg8
  libjpeg-turbo8 libjpeg8 libjs-jquery libjs-sphinxdoc libjs-underscore libmcrypt4 libtiff5 libvpx3 libxpm4 php-gd php-gettext
  php-mbstring php-mcrypt php-mysql php-pear php-phpseclib php-tcpdf php7.0-gd php7.0-mbstring php7.0-mcrypt php7.0-mysql
Suggested packages:
  libgd-tools libmcrypt-dev mcrypt php-libsodium php-gmp php-imagick www-browser
The following NEW packages will be installed:
  dbconfig-common dbconfig-mysql fontconfig-config fonts-dejavu-core javascript-common libfontconfig1 libgd3 libjpeg8
  libjpeg-turbo8 libjpeg8 libjs-jquery libjs-sphinxdoc libjs-underscore libmcrypt4 libtiff5 libvpx3 libxpm4 php-gd php-gettext
  php-mbstring php-mcrypt php-mysql php-pear php-phpseclib php-tcpdf php7.0-gd php7.0-mbstring php7.0-mcrypt php7.0-mysql
  phpmymadmin
0 upgraded, 30 newly installed, 0 to remove and 11 not upgraded.
Need to get 16.3 MB of archives.
After this operation, 61.3 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

8. Elegir servidor web para configurar phpMyAdmin

```

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa* Configuring phpmymadmin aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Please choose the web server that should be automatically configured to run phpMyAdmin.

Web server to reconfigure automatically:

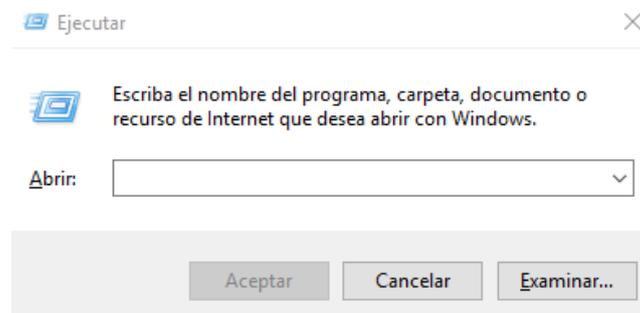
[*] apache2
[ ] lighttpd

<Ok>
```

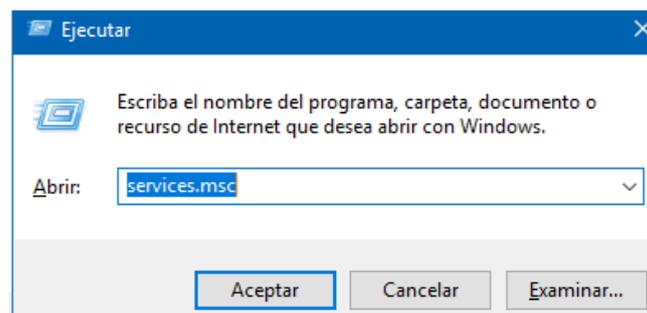

ANEXO IV

Habilitar protocolo 802.1X en Windows, instalación del programa SecureW2 y su configuración.

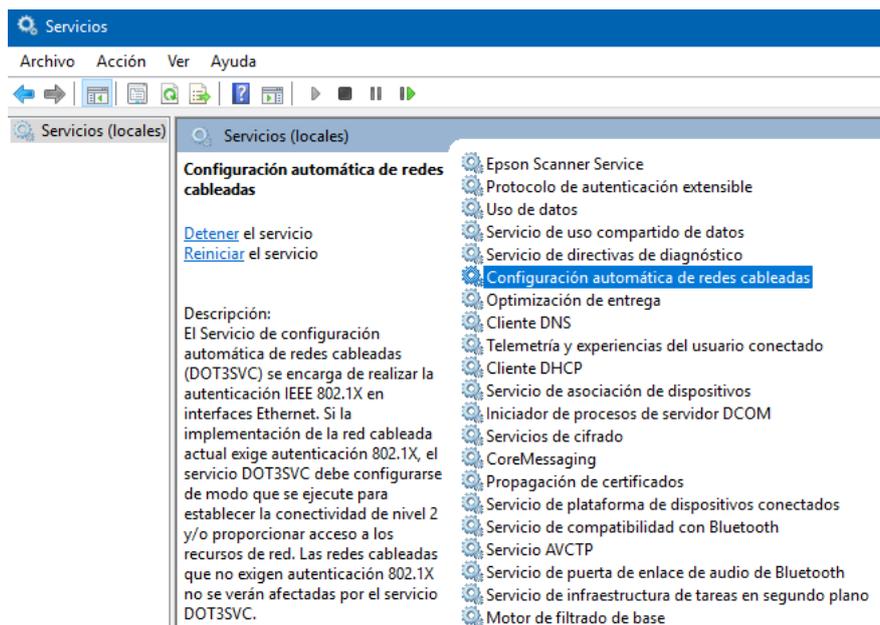
1. Ingresar a la ventana ejecutar con el comando Windows+r



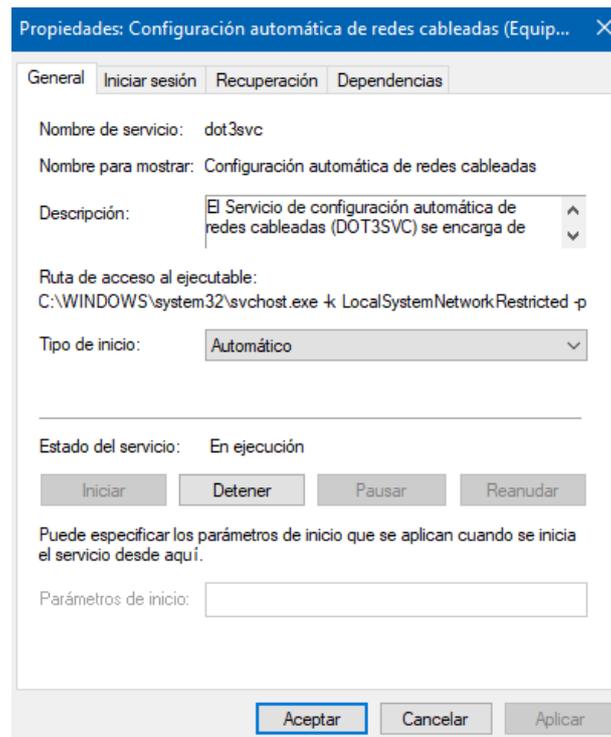
2. Escribir “services.msc” e ingresar a los servicios de Windows.



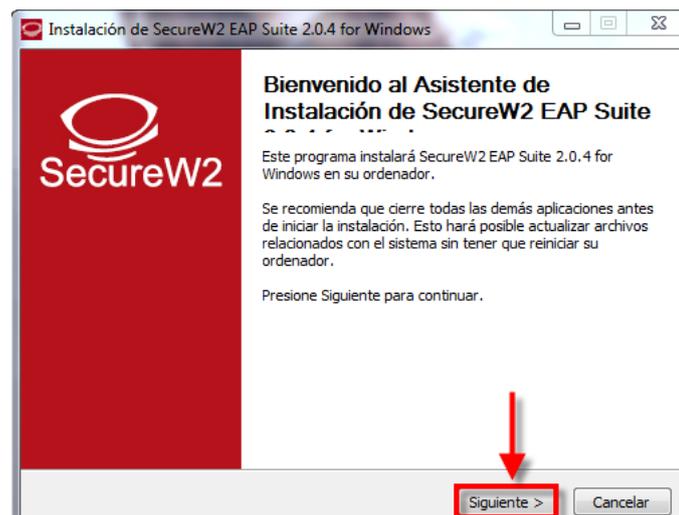
3. Elegir el servicio “Configuración automática de redes cableadas”.

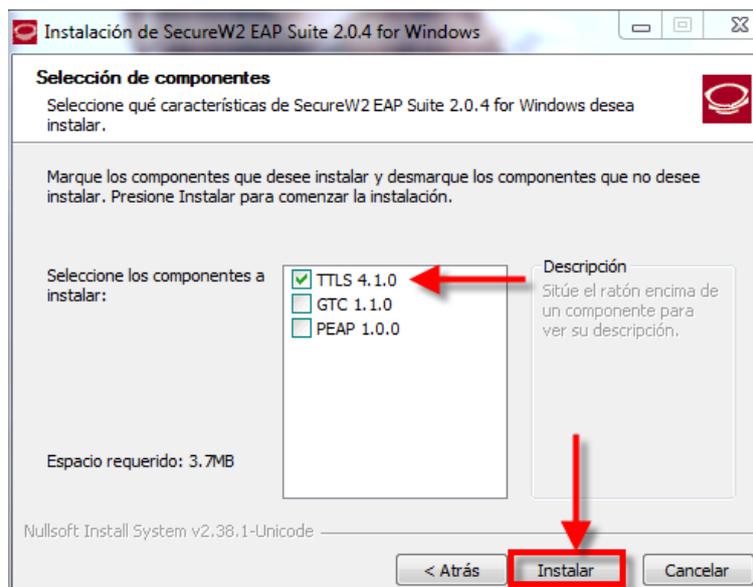
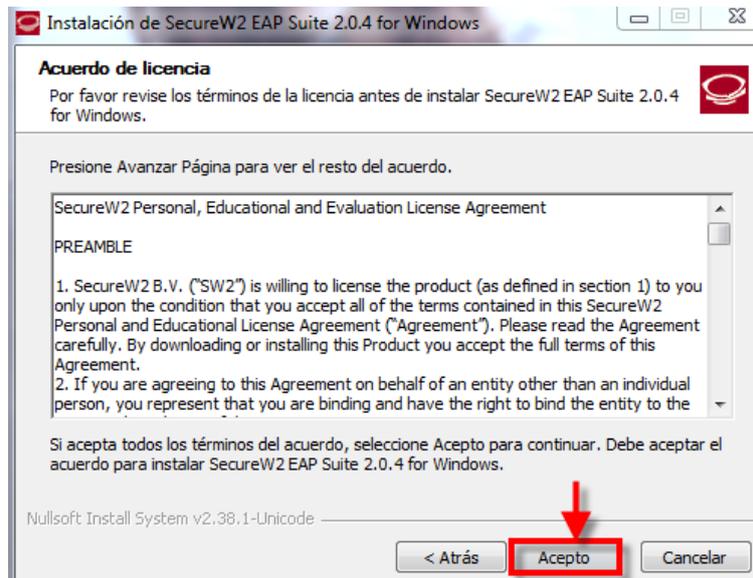


4. Establecer el servicio como automático.

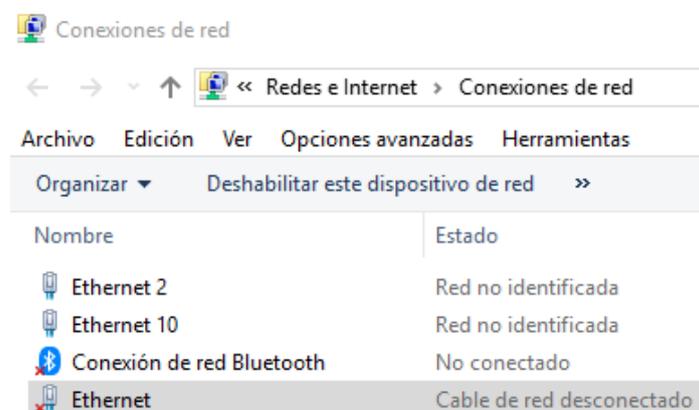


5. Instalar el programa SecureW2

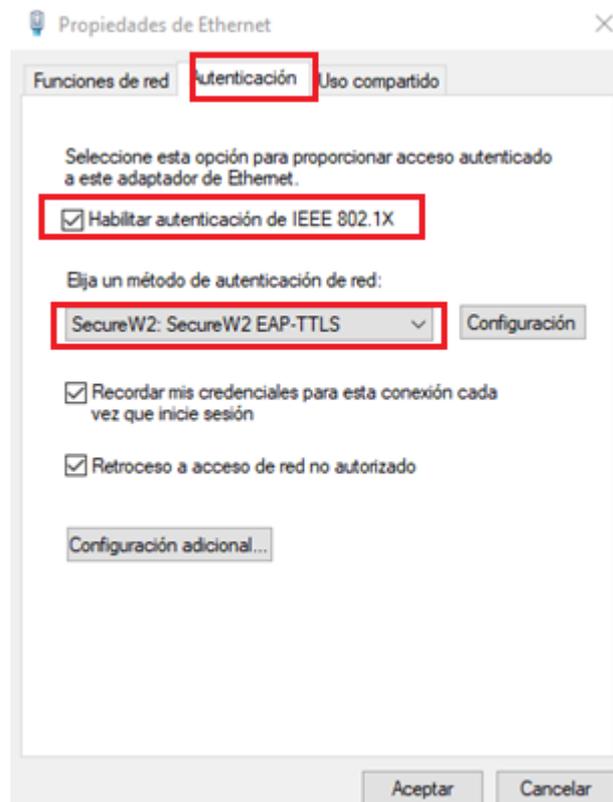




6. Ingresar a Conexiones de red.



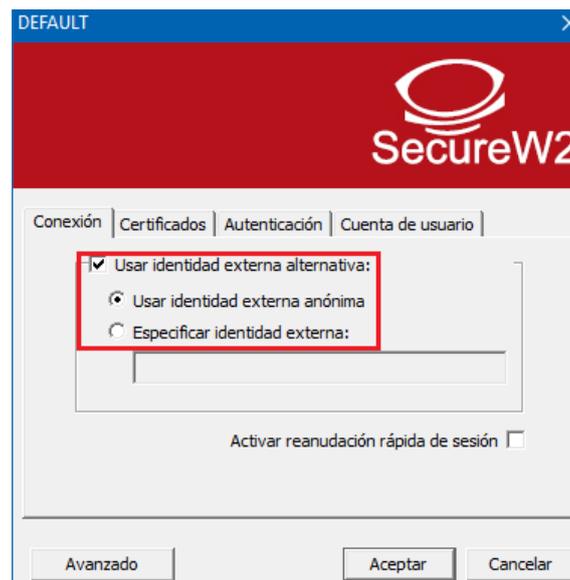
7. Dentro de propiedades de Ethernet elegir la pestaña autenticación, habilitar autenticación IEEE 802.1x y en método de autenticación de red señalar SecureW2 EAP-TTLS.



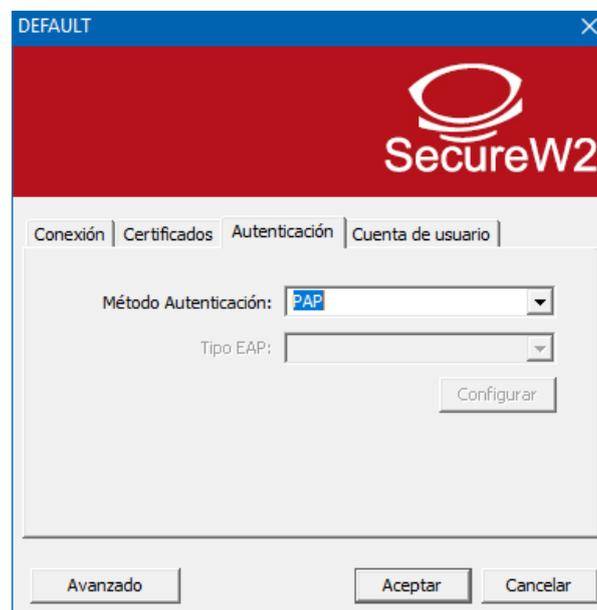
8. En la pestaña configuración se establece el perfil del usuario.



9. En el apartado conexión, seleccionar la identidad externa anónima.



10. Continuando con la configuración, en el apartado autenticación seleccionar método “PAP”.



11. Finalmente, en cuenta de usuario señalar pedir credenciales de usuario.

