UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA ELECTRÓNICA Y REDES DE COMUNICACIÓN

"ADMINISTRACIÓN Y GESTIÓN DE USUARIOS PARA ACCESO A LA RED INALÁMBRICA DE LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS BASADO EN EL PROTOCOLO 802.1x"

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

AUTOR: Carlos Patricio Bosmediano Cárdenas

DIRECTOR: Ing. Fabián Cuzme, Msc

Ibarra, 2017

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

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 determina 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	1003487954
Apellidos y Nombres	Bosmediano Cárdenas Carlos Patricio
Dirección	La Victoria, Rosa Andrade y pasaje M
Email	cpbosmedianoc@utn.edu.ec
Teléfono Móvil	0959167887
DATOS DE LA OBRA	
Título	ADMINISTRACIÓN Y GESTIÓN DE USUARIOS PARA ACCESO A LA RED INALÁMBRICA DE LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS BASADO EN EL PROTOCOLO 802.1x
Autor	Bosmediano Cárdenas Carlos Patricio
Fecha	Julio de 2017
Programa	Pregrado
Título por el que se aspira	Ingeniero en Electrónica y Redes de Comunicación
Director	Ing. Fabián Cuzme Rodríguez, Msc.

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Bosmediano Cárdenas Carlos Patricio, con cédula de identidad Nro. 1003487954, 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 forma 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 de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 144.

3. CONSTANCIAS

Yo, BOSMEDIANO CÁRDENAS CARLOS PATRICIO, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que éste no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo los 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 Ibarra, julio de 2017.

Bosmediano Cárdenas Carlos Patricio
100348795-4

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE.

Yo, **Bosmediano Cárdenas Carlos Patricio**, con cedula de identidad Nro. 1003487954, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador artículos 4, 5 y 6, en calidad de autor del trabajo de grado con el tema: **ADMINISTRACIÓN Y GESTIÓN DE USUARIOS PARA ACCESO A LA RED INALÁMBRICA DE LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS BASADO EN EL PROTOCOLO 802.1x**. Que ha sido desarrollado con propósito de obtener el título de Ingeniero en Electrónica y Redes de Comunicación de la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Bosmediano Cárdenas Carlos Patricio
100348795-4

Ibarra, julio de 2017

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

INGENIERO FABIÁN CUZME, MSC. DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN,

CERTIFICA:

Que el presente trabajo de titulación: "**ADMINISTRACIÓN Y GESTIÓN DE USUARIOS PARA ACCESO A LA RED INALÁMBRICA DE LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS BASADO EN EL PROTOCOLO 802.1x**" fue desarrollado por el estudiante BOSMEDIANO CÁRDENAS CARLOS PATRICIO, portador de la cedula de identidad 100348795-4, bajo mi supervisión.

Es todo cuanto puedo certificar en honor a la verdad.

Ing. Fabián Cuzme, Msc.
DIRECTOR DEL PROYECTO

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

A mi madre Mónica P. Cárdenas Estrella, por todo el amor, cariño y paciencia que me ha brindado toda su vida, pero sobre todo por estar ahí cuando la necesitaba.

A mi padre Carlos R. Bosmediano Padilla, por cuidarme y apoyarme siempre.

A mis hermanos Jonathan, Alexis y Nayeli, para demostrarles que el esfuerzo, la constancia, el sacrificio y la perseverancia son valores necesarios para alcanzar una meta.

A mi esposa María José Noboa M. y mi hija Dominique, quienes me han acompañado en mis situaciones más difíciles, dándome fuerzas para no caer vencido frente a las adversidades; pero sobre todo brindarme ese amor y cariño para lograr ser el esposo y padre más feliz del planeta.

Carlos P. Bosmediano C

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTOS

A la familia por ser el pilar fundamental para emprender el largo camino hacia el éxito.

Al Msc. Fabián Cuzme, Msc Jaime Michilena, Msc Mauricio Domínguez, docentes de la Facultad de Ingeniería en Ciencias Aplicadas FICA, quienes fueron los guías para lograr el desarrollo del proyecto.

A la Universidad Técnica del Norte, donde me formé como ser humano con valores y principios para lograr ser alguien en la vida.

RESUMEN

El proyecto planteado consiste en el diseño e implementación de un esquema de red que proporcione el servicio de Autenticación, Autorización y Auditoría (AAA) en la Facultad de ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte, para el control de acceso y administración de recursos de red, empleando soluciones basadas en software libre.

Para el desarrollo del sistema AAA se realiza un estudio sobre métodos de autenticación EAP (TLS, TTLS o PEAP) soportados por el estándar IEEE 802.1x, el protocolo LDAP y RADIUS, seguido de un análisis de la situación actual referente a todos los equipos que forman la red inalámbrica, se verificará cuáles son los dispositivos con los que se podrá trabajar. Una vez recolectada la información necesaria, se procede a diseñar el sistema de autentificación AAA, en la cual se crea una base de datos en OpenLdap para el almacenamiento de credenciales de todos los usuarios que comprenda la facultad.

Por último, se procederá a implementar el servicio de autentificación en la red inalámbrica de la facultad de Ingeniería en Ciencias Aplicadas denominada “ficawifi” con equipos marca Mikrotik, para brindar un acceso seguro a la red y un control centralizado de todos los usuarios.

ABSTRACT

The proposed project consists of the design and implementation of a scheme of network that provide authentication, authorization, and accounting service (AAA) in the Facultad de ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte, for the control of access and administration of network resources, using solutions based on software free.

For the development of the system AAA is a study on methods of EAP authentication (TLS, TTLS, or PEAP) supported by the IEEE standard 802. 1 x, the Protocol LDAP and RADIUS, followed by an analysis of the current situation relating to all the teams that make up the wireless network, is to verify what are the devices that will work. Once collected the necessary information, proceed to design the system of AAA authentication, which creates a database in OpenLdap for the storage of credentials for all users.

Finally, will proceed to implement the service's authentication on the wireless network of the Facultad de Ingeniería en Ciencias Aplicadas (FICA) called “ficawifi” with the trademark Mikrotik equipment to give an access and control of the users that connect to the wireless network of the Faculty to provide a secure network access and centralized control of all users.

ÍNDICE

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

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE. ..... ¡ERROR! MARCADOR NO DEFINIDO.

CERTIFICACIÓN ..... ¡ERROR! MARCADOR NO DEFINIDO.

DEDICATORIA VI

AGRADECIMIENTOS..... VII

RESUMEN VIII

ABSTRACT IX

ÍNDICE..... X

ÍNDICE DE ILUSTRACIONES Y ECUACIONES XIV

CAPÍTULO I: ANTECEDENTES..... 1

1.1 PROBLEMA 1
1.2 OBJETIVOS 2
1.2.1 Objetivo general *2*
1.2.2 Objetivos específicos *2*
1.3 ALCANCE 3
1.4 JUSTIFICACIÓN 4

CAPÍTULO II: MARCO TEÓRICO 5

2.1 ADMINISTRACIÓN 5
2.1.1 Administración de redes *5*
2. 1.2 Objetivos principales de la administración de redes *7*
2.2 GESTIONAR *7*
2.2.1 Gestión de redes *7*
2.2.2 Elementos de la gestión de red *8*
2.3 INTRODUCCIÓN A LAS REDES INALÁMBRICAS 9
2.3.1 Ventajas de las redes inalámbricas *10*
2.4 ESTÁNDAR IEEE 802.15 - BLUETOOTH 10
2.4.1 Estándar IEEE 802.16 - WiMAX *11*
2.4.2 Estándar IEEE 802.11 - WIFI *12*
2.5 MODIFICACIONES DEL ESTÁNDAR 802.11 13
2.6 SEGURIDAD 14
2.6.1 Principios de seguridad *15*
2.6.2 Confidencialidad *15*
2.6.3 Integridad *16*
2.6.4 Disponibilidad *16*
2.6.5 Otros aspectos relacionados *17*
2.7 AMENAZAS Y VULNERABILIDADES 18
2.7.1 Amenazas *18*
2.7.1.1 Fuentes de amenaza 18
2.7.2 Vulnerabilidades *22*
2.7.2.1 Tipos de vulnerabilidades 22

2.8 SEGURIDADES EN LAS REDES INALÁMBRICAS 23
2.9 MÉTODOS DE CIFRADO 24
2.9.1 WEP (Wired Equivalent Privacy) *24*
2.9.2 Autenticación WEP *25*
2.9.3 WPA/WPA2 WPA *26*
2.9.3.1 Características WPA 26
2.9.3.2 Mejoras de WPA con respecto a WEP 27
2.9.3.3 Métodos de funcionamiento de WPA 28
2.9.3.4 Debilidades de WPA 28
2.9.3.5 Características WPA2 y mejoras 28
2.9.3.6 Debilidades de WPA2 29
2.10 IEE 802.1X 29
2.11 SISTEMA DE CONTROL DE ACCESO AAA 33
2.11.1 Beneficios AAA *35*
2.11.2 Protocolo AAA: Diameter *36*
2.11.3 Protocolo AAA: TACACS+ *37*
2.11.3.1 Arquitectura TACACS+ 38
2.11.4 Protocolo AAA: RADIUS *38*
2.11.4.1 Arquitectura RADIUS 39
2.11.4.2 Principales características 39
2.12 MÉTODO DE AUTENTIFICACIÓN 41
2.13 TIPOS DE SERVIDORES DE AUTENTIFICACIÓN 42
2.13.2 FREERADIUS (Radius server para Software Libre) *44*
2.13.2.1 Ficheros FreeRADIUS 45
2.14 SERVICIO DE DIRECTORIOS 46
2.14.1 BASE DE DATOS LDAP *46*
2.15 SOFTWARE LIBRE 47
2.15.1 Sistema Operativo Debian GNU/Linux *48*
2.15.2 Sistema operativo servidor (Ubuntu Server) *48*
2.15.3 Sistema operativo CentOs *49*
2.15.4 Sistema operativo Zeroshell *50*
2.15.5 Sistema operativo Pfsence *51*

CAPÍTULO III: SITUACIÓN ACTUAL DE LA RED INALÁMBRICA DE LA FICA 52

3.1 UBICACIÓN 52
3.2 FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS (FICA) 52
3.3 METODOLOGÍA DE LA INVESTIGACIÓN 53
3.3.1 Tipo de investigación *53*
3.3.2. Área de estudio *53*
3.3.3 Universo *54*
3.3.4 Cálculo de la muestra *54*
3.3.5 Criterio de inclusión *55*
3.3.6 Criterios de encuesta y entrevista *55*
3.3.7 Técnicas e instrumentos a utilizar *56*
3.4 INTERPRETACIÓN Y ANÁLISIS DE RESULTADOS 56
3.5 DESCRIPCIÓN DE LA RED INALÁMBRICA 56
3.6 EQUIPAMIENTO 58
3.6.1 Infraestructura de la red inalámbrica en Data Center FICA *58*
3.6.2 Configuración inicial de equipos CAP y CAPsMAN *59*

3.7 DESCRIPCIÓN TÉCNICA DE EQUIPOS 61
3.7.1 Access point MikroTik cAP – 2n *61*
3.7.2 QP-COM switch 24 puertos – 1240R *62*
3.7.2.1 Características 62
3.7.3 Router MIKROTIK RB1100AHx2 ..... *63*
3.8 DISTRIBUCIÓN DE AP'S PARA LA RED INALÁMBRICA 64
3.9 DISTRIBUCIÓN DE CANALES EN LA RED INALÁMBRICA 65
3.10 DIRECCIONAMIENTO IP DE LA RED INALÁMBRICA. 67

CAPÍTULO IV: DISEÑO DE LA INFRAESTRUCTURA CON SOPORTE AAA 68

4.1 DESCRIPCIÓN DE LA PROBLEMÁTICA EXISTENTE 68
4.2 REQUERIMIENTOS DEL SISTEMA 68
4.3 SELECCIÓN DEL SOFTWARE Y HARDWARE PARA EL SERVICIO DE AUTENTIFICACIÓN. 75
4.3.1 Selección de Software *75*
4.3.2 Selección de Hardware *78*
4.3.3 Diseño del Sistema *80*
4.4 ESTRUCTURA JERÁRQUICA BASE DE DATOS LDAP FICA 80
4.5 DIAGRAMA DE FUNCIONAMIENTO DEL SISTEMA 82
4.5.1 Bloque 1 (Petición) *83*
4.5.2 Bloque 2 (Autentificación) *83*
4.5.3 Bloque 3 (Autorización) *83*
4.5.4 Bloque 4 (Registro) *83*
4.6 TOPOLOGÍA FÍSICA Y LÓGICA DEL SISTEMA 83

CAPÍTULO V: IMPLEMENTACIÓN SERVIDOR RADIUS 85

5.1 INSTALACIÓN DEL SISTEMA OPERATIVO DEBIAN 8.6 85
5.2 CONFIGURACIÓN DE RED 86
5.3 INSTALACIÓN LDAP 87
5.3.1 Reconfiguración LDAP *88*
5.3.2 Schema para usuarios FICA *90*
5.3.3 Añadir esquema al Directorio LDAP *91*
5.3.4 Ingreso de datos para LDAP *92*
5.3.4.1 Formato de unidades organizativas 93
5.3.4.2 Formato de grupos o dependencias 94
5.3.4.3 Usuarios 95
5.4 INSTALACIÓN FREERADIUS 97
5.4.1 Configuración FreeRADIUS *97*
5.4.1.1 Fichero radius.conf 97
5.4.1.2 Ficheros sites enabled / /inner-tunnel 98
5.4.1.3 Fichero eap.conf 100
5.4.1.4 Fichero LDAP 101
5.4.1.5 Fichero clients.conf 101
5.5 RECONFIGURACIÓN DE LOS PUNTOS DE ACCESO (CAP Y CAPSMAN) 102
5.5.1 Configuración CAP *102*
5.5.2 Configuración CAPsMAN *105*
5.5.3 Control de ancho de banda (QUEUE - PCQ) *107*
5.6 WLAN SSID 107
5.7. PRUEBAS DE FUNCIONAMIENTO 108

5.7.1 Difusión de SSID con seguridad 802.1x y verificación de canales dentro de las instalaciones FICA. *109*
5.7.2 Pruebas de conexión entre cliente y servidor utilizando radtest (local) y NTRadPing (remota). *110*
5.7.3 Pruebas de conexión de estudiantes, docentes (FICA) en diferentes dispositivos (laptops – Celulares – Tablets). *113*
5.7.4 Asignación de IP dinámicas, control de ancho de banda - test de velocidad *117*
5.8 OPTIMIZACIÓN DE LA RED "FICAWIFI" 122
5.8.1 Amarre IP/MAC para Docentes y personal administrativo *123*
5.8.2 Reasignación de rango IP en DHCP-SERVER *126*
5.8.3 Reconfiguración DNS para servicios internos (Portal UTN, portafolios, biblioteca, repositorio) *127*

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES 128

6.1 CONCLUSIONES 128
6.2 RECOMENDACIONES 129

GLOSARIO DE TÉRMINOS 131

REFERENCIAS BIBLIOGRÁFICAS 135

ANEXOS 140

ANEXO A – FORMATOS DE ENCUESTAS 140

ANEXO B – FORMATO DE ENTREVISTA 144

ANEXO C – INTERPRETACIÓN Y ANÁLISIS DE RESULTADOS DE ENCUESTAS 146

ANEXO D – CONFIGURACIONES FREERADIUS + LDAP + DEBIAN 8.6 + EQUIPOS MIKROTIK 159

ANEXO E – CONFIGURACIONES DE EQUIPOS FINALES (WINDOWS – ANDROID) 186

ANEXO F: DATASHEET 1 - MIKROTIK CAP – 2N 195

ANEXO H: DATASHEET 3 –MIKROTIK RB1100 AX 197

ÍNDICE DE ILUSTRACIONES Y ECUACIONES

ILUSTRACIÓN 1. ELEMENTOS DE GESTIÓN DE REDES..... 8
ILUSTRACIÓN 2. INTERACCIÓN BLUETOOTH (802.15) 11
ILUSTRACIÓN 3. LOGOTIPO WIMAX..... 12
ILUSTRACIÓN 4. LOGOTIPO DISPOSITIVO CON WIFI 13
ILUSTRACIÓN 5. CONFIDENCIALIDAD 16
ILUSTRACIÓN 6. INTEGRIDAD 16
ILUSTRACIÓN 7. DISPONIBILIDAD..... 17
ILUSTRACIÓN 8: FUNCIONAMIENTO WEP 25
***ILUSTRACIÓN* 9.** COMPARATIVA WPA/WPA2..... 29
ILUSTRACIÓN 10. AUTENTIFICACIÓN 802.1X..... 30
ILUSTRACIÓN 11. AUTENTIFICACIÓN TACACS+..... 38
ILUSTRACIÓN 12. COMPONENTES RADIUS 39
ILUSTRACIÓN 13. FUNCIONAMIENTO RADIUS. 42
ILUSTRACIÓN 14. FICHEROS FREERADIUS. 45
ILUSTRACIÓN 15. FUNCIONAMIENTO LDAP..... 47
ILUSTRACIÓN 16. VERSIONES SOFTWARE LIBRE 48
ILUSTRACIÓN 17. CAMPUS UTN "EL OLIVO"..... 52
ECUACIÓN 1. DETERMINACIÓN DE LA MUESTRA..... 54
ILUSTRACIÓN 18. SSID "FICAWIFI" 57
ILUSTRACIÓN 19. HOTSPOT "FICAWIFI"..... 57
ILUSTRACIÓN 20: TEST DE VELOCIDAD 58
ILUSTRACIÓN 21. INFRAESTRUCTURA RED INALÁMBRICA "FICAWIFI"..... 59
ILUSTRACIÓN 22. CONFIGURACIÓN INICIAL CAP 60
ILUSTRACIÓN 23. CONFIGURACIÓN INICIAL CAPSMAN 61
***ILUSTRACIÓN* 24.** CAP - 2N..... 61
ILUSTRACIÓN 25. QPCOM SWITCH 24 PUERTOS 62
ILUSTRACIÓN 26. ROUTERBOARD MIKROTIK 1100AH. 64
ILUSTRACIÓN 27. DISTRIBUCIÓN CAP-2N 65
ILUSTRACIÓN 28. DISTRIBUCIÓN DE CANALES..... 66
ILUSTRACIÓN 29. DIRECCIONAMIENTO IP – "FICAWIFI" 67
ILUSTRACIÓN 30. ESTRUCTURA JERÁRQUICA DE LA BASE DE DATOS LDAP FICA..... 81
ILUSTRACIÓN 31. DIAGRAMA DE FUNCIONAMIENTO DEL SISTEMA. 82
***ILUSTRACIÓN* 32** TOPOLOGÍA FINAL DEL SISTEMA. 84
***ILUSTRACIÓN* 33.** ENTORNOS DE INSTALACIÓN DEBIAN 8.6. 85
***ILUSTRACIÓN* 34.** CONTRASEÑA ROOT. 86
ILUSTRACIÓN 35. INSTALACIÓN LDAP-SERVER..... 87
ILUSTRACIÓN 36. CONTRASEÑA ADMINISTRADOR LDAP. 87
ILUSTRACIÓN 37. OBJETOS LDAP..... 88
ILUSTRACIÓN 38. FICHERO PHPLDAPADMIN/CONFIG.PHP..... 88
ILUSTRACIÓN 39. VERIFICACIÓN ÁRBOL LDAP. 89
ILUSTRACIÓN 40. FICHERO SCHEMA. 90
ILUSTRACIÓN 41. FICHERO USUARIOSLDAPFICA.CONF. 90
ILUSTRACIÓN 42. ESQUEMA LDIF. 91
ILUSTRACIÓN 43. ADICIÓN DE ESQUEMA PARA EL DIRECTORIO LDAP. 91
ILUSTRACIÓN 44. VERIFICACIÓN 1. 92
ILUSTRACIÓN 45. VERIFICACIÓN 2. 92
ILUSTRACIÓN 46. DIRECTORIO DE FICHEROS LDIF. 93
***ILUSTRACIÓN* 47.** FORMATO DE OU PARA CIERCOM 93

ILUSTRACIÓN **48**. FORMATO DE OU PARA CIERCOM 94
ILUSTRACIÓN **49.** FORMATO DE DEPENDENCIAS DENTRO DE CADA UNIDAD ORGANIZATIVA. 95
ILUSTRACIÓN **50**. FORMATO DE ID USUARIO..... 96
ILUSTRACIÓN 51. INSTALACIÓN FREERADIUS..... 97
ILUSTRACIÓN **52.** FICHERO RADIUSD. CONF..... 98
ILUSTRACIÓN 53. FICHERO RADIUS.CONF: PROXY..... 98
ILUSTRACIÓN **54.** FICHERO SITES-ENABLED..... 99
ILUSTRACIÓN **55.** FICHERO SITES-ENABLE / INNER-TUNNEL..... 99
ILUSTRACIÓN **56.** FICHERO EAP.CONF: EAP-TLS..... 100
ILUSTRACIÓN **57.** FICHERO EAP.CONF: CACHE – TTLS..... 100
ILUSTRACIÓN **58.** CONFIGURACIÓN MÓDULO LDAP..... 101
ILUSTRACIÓN **59.** FICHERO CLIENTS.CONF..... 101
ILUSTRACIÓN 60. VENTANA PRINCIPAL WINBOX. 102
ILUSTRACIÓN 61. CONFIGURACIÓN IP ESTÁTICA..... 103
ILUSTRACIÓN 62. IDENTIFICACIÓN DE INTERFACES 103
ILUSTRACIÓN 63. CONFIGURACIÓN BRIDGE 104
ILUSTRACIÓN 64. CONFIGURACIÓN CAP..... 104
ILUSTRACIÓN 65. RADIUS- MIKROTIK..... 105
ILUSTRACIÓN 66. ACTIVACIÓN MANAGER CAPSMAN 106
ILUSTRACIÓN 67. CONFIGURACIÓN DE INTERFACES EN CAPSMAN 107
ILUSTRACIÓN 68. CONTROL AB 107
ILUSTRACIÓN 69. SSID FACULTAD. 108
ILUSTRACIÓN 70. PRUEBA 1: DIFUSIÓN SSID..... 109
ILUSTRACIÓN 71. VERIFICACIÓN DE USUARIOS LDAP. 110
ILUSTRACIÓN 72. FORMATO RADTEST. 111
ILUSTRACIÓN 73. PRUEBA 2: LOCAL CON EL COMANDO RADTEST 111
ILUSTRACIÓN 74. PRUEBA REMOTA DE USUARIOS 112
ILUSTRACIÓN 75. PESTAÑA DE SEGURIDAD RED INALÁMBRICA. 113
ILUSTRACIÓN 76. PRUEBA 3: CONEXIÓN EAP-TTLS. 114
ILUSTRACIÓN **77.** PRUEBA 4: CONEXIÓN SMARTPHONE..... 115
ILUSTRACIÓN 78. LOG LDAP 116
ILUSTRACIÓN 79. CONFIGURACIÓN DHCP-SERVER 117
ILUSTRACIÓN 80. ANCHO DE BANDA GRUPO DOCENTES-ADMINISTRATIVOS..... 118
ILUSTRACIÓN 81. ANCHO DE BANDA GRUPO ESTUDIANTES..... 118
ILUSTRACIÓN 82. PRUEBA 5 - SUBRED DOCENTES/ADMINISTRATIVOS..... 119
ILUSTRACIÓN 83. PRUEBA 6: SUBRED ESTUDIANTES..... 120
ILUSTRACIÓN **84**. CONFIGURACIÓN ARP..... 124
ILUSTRACIÓN **85.** TABLA ARP 124
ILUSTRACIÓN **86.** ASIGNACIÓN IP POR DHCP..... 125
ILUSTRACIÓN **87.** VERIFICACIÓN DHCP-SERVER..... 126
ILUSTRACIÓN **88.** RANGO IP..... 126
ILUSTRACIÓN **89.** REDIRECCIONAMIENTO DNS..... 127
ILUSTRACIÓN **90.** FICHERO DE CONFIGURACIÓN INTERFAZ..... 159
ILUSTRACIÓN 91. SCRIPT IPTABLES. 160
ILUSTRACIÓN 92. FICHERO EJECUTABLE CON IPTABLES. 160
ILUSTRACIÓN 93. EJECUCIÓN DEL COMANDO UPDATE..... 161
ILUSTRACIÓN 94. ACTUALIZACIÓN DE FICHEROS Y PAQUETES. 161
ILUSTRACIÓN 95. INSTALACIÓN FREERADIUS..... 162
ILUSTRACIÓN 96. INSTALACIÓN LDAP. 162

ILUSTRACIÓN 97. CONTRASEÑA ADMINISTRADORA LDAP. 163
ILUSTRACIÓN 98. CONFIRMACIÓN CONTRASEÑA ADMIN LDAP. 163
ILUSTRACIÓN 99. FINALIZACIÓN DEL PROCESO LDAP. 163
ILUSTRACIÓN 100. OMITIR CONFIGURACIÓN INICIAL LDAP. 164
ILUSTRACIÓN 101. INGRESO DEL DOMINIO LOCAL. 164
ILUSTRACIÓN 102. INGRESO DE NOMBRE DE ORGANIZACIÓN PARA BASE DE DATOS LDAP. 165
ILUSTRACIÓN 103. CONTRASEÑA DE ADMINISTRADOR LDAP. 165
ILUSTRACIÓN 104. SELECCIÓN DE MOTOR DE BÚSQUEDA. 165
ILUSTRACIÓN 105. PURGAR PAQUETE SLAPD. 166
ILUSTRACIÓN 106. ELIMINACIÓN DE BASES DE DATOS ANTIGUAS. 166
ILUSTRACIÓN 107. ELECCIÓN DE LA VERSIÓN PARA EL PROTOCOLO LDAP. 166
ILUSTRACIÓN 108. FINALIZACIÓN DE CONFIGURACIÓN LDAP. 167
ILUSTRACIÓN 109. LÍNEA DE COMANDO QUE PERMITE COPIAR SCHEMA A OTRO DIRECTORIO. 167
ILUSTRACIÓN 110. INGRESO DE ESQUEMA CREADO PREVIAMENTE. 168
ILUSTRACIÓN 111. BÚSQUEDA DE ESQUEMAS EXISTENTES. 168
ILUSTRACIÓN 112. LÍNEA DE COMANDO PARA CREAR ESTRUCTURA LDIF. 169
ILUSTRACIÓN 113. ARCHIVOS DE CONFIGURACIÓN CREADOS A PARTIR DE SLAPCAT. 169
ILUSTRACIÓN 114. MODIFICACIÓN ARCHIVO RADIUS.LDIF. 169
ILUSTRACIÓN 115. ADICIÓN DE SCHEMA AL DIRECTORIO LDAP. 170
ILUSTRACIÓN 116. COMPROBACIÓN DEL SCHEMA AGREGADO. 170
ILUSTRACIÓN 117. REINICIO DE OPENLDAP. 171
ILUSTRACIÓN 118. CONFIGURACIÓN MÓDULO LDAP. 171
ILUSTRACIÓN 119. FICHEROS DEFAULT E INNER-TUNEL. 172
ILUSTRACIÓN 120. FICHERO DE CONFIGURACIÓN PHPLDAPADMIN. 173
ILUSTRACIÓN 121. CONFIGURACIÓN DE CLIENTES RADIUS. 173
ILUSTRACIÓN 122. FICHERO DE CERTIFICADOS. 174
ILUSTRACIÓN 123. FICHERO CA.CNF. 174
ILUSTRACIÓN 124. FICHERO SERVER.CNF. 174
ILUSTRACIÓN 125. FICHERO CLIENT.CNF. 174
ILUSTRACIÓN 126. GENERACIÓN DE CERTIFICADOS. 175
ILUSTRACIÓN 127. ENLACE SIMBÓLICO DE CERTIFICADOS. 175
ILUSTRACIÓN 128. VENTANA PRINCIPAL WINBOX.EXE. 176
***ILUSTRACIÓN* 129**. CONFIGURACIÓN IP FIJA CAP 177
***ILUSTRACIÓN* 130.** INTERFACES CAP 177
***ILUSTRACIÓN* 131.** BRIDGE CAP 178
***ILUSTRACIÓN* 132.** PUERTOS BRIDGE 178
***ILUSTRACIÓN* 133**. ACTIVACIÓN CAP 179
***ILUSTRACIÓN* 134**. VERIFICACIÓN CAP 179
***ILUSTRACIÓN* 135.** CAPSMAN ENABLE 180
***ILUSTRACIÓN* 136.** VERIFICACIÓN CAPSMAN 180
***ILUSTRACIÓN* 137.** CONFIGURACIÓN CHANNELS 181
***ILUSTRACIÓN* 138**.CONFIGURACIÓN DATAPATH 181
***ILUSTRACIÓN* 139.** CONFIGURACIÓN SEGURIDADES 182
***ILUSTRACIÓN* 140.** SOLAPA CONFIGURATIONS 182
***ILUSTRACIÓN* 141.** INTERFACES CAPSMAN 183
***ILUSTRACIÓN* 142**. SERVICIO RADIUS 184
***ILUSTRACIÓN* 143.** ECUALIZADORES PCQ 184
***ILUSTRACIÓN* 144.** ENTRADAS QUEUE 185

***ILUSTRACIÓN* 145.** CONFIGURACIÓN AVANZADA QUEUE 185
***ILUSTRACIÓN* 146.** ASISTENTE DE INSTALACIÓN SECUREW2. 186
***ILUSTRACIÓN* 147.** ACUERDOS DE LICENCIA. 187
ILUSTRACIÓN 148. SELECCIÓN DE COMPONENTES A INSTALAR. 187
ILUSTRACIÓN 149. FINALIZACIÓN DE INSTALACIÓN. 188
ILUSTRACIÓN 150. CONFIGURACIÓN MANUAL DE RED. 188
ILUSTRACIÓN 151. ELECCIÓN DEL TIPO DE CONEXIÓN. 189
ILUSTRACIÓN 152. CONFIGURACIÓN DE RED. 189
ILUSTRACIÓN 153. VERIFICACIÓN DE RED. 190
ILUSTRACIÓN 154. PROPIEDADES DE RED INALÁMBRICA. 190
ILUSTRACIÓN 155. PERFIL POR DEFECTO SECUREW2. 191
ILUSTRACIÓN 156. CONFIGURACIÓN DE CONEXIÓN. 191
ILUSTRACIÓN 157. CONFIGURACIÓN DE CERTIFICADOS. 192
ILUSTRACIÓN 158. CONFIGURACIÓN DE AUTENTIFICACIÓN. 192
ILUSTRACIÓN 159. CONFIGURACIÓN DE CUENTA. 193
ILUSTRACIÓN 160. VERIFICACIÓN DE RED. 193
ILUSTRACIÓN 161. CONFIGURACIÓN SMARTPHONE 194
ILUSTRACIÓN 162. CONEXIÓN EXITOSA SMARTPHONE. 194

ÍNDICE DE TABLAS

TABLA 1. *ELEMENTOS DE GESTIÓN* 9
TABLA 2. *COMPARACIÓN DE ESTÁNDARES 802.11* 14
TABLA 3. FUENTES DE AMENAZAS 19
TABLA 4. *FUENTE DE VULNERABILIDADES* 22
TABLA 5. *COMPARATIVA EAP* 33
TABLA 6. *COMPARACIÓN ENTRE SERVIDORES DE AUTENTICACIÓN* 42
TABLA 7. DESCRIPCIÓN DE FICHEROS FREERADIUS 45
TABLA 8. *USUARIOS FICA EN EL PERIODO MARZO 2017 – AGOSTO 2017* 53
TABLA 9. OBJETIVOS DE ENCUESTA Y ENTREVISTA 55
TABLA 10. *EQUIPOS PARA WLAN FICA* 58
TABLA 11. *ESPECIFICACIONES TÉCNICAS CAP - 2N* 62
TABLA 12. ESPECIFICACIONES TÉCNICAS SWITCH QPCOM 63
TABLA 13. *ESPECIFICACIONES TÉCNICAS ROUTERBOARD MIKROTIK 1100AH* 64
TABLA 14. *REQUERIMIENTOS INICIALES DEL SISTEMA* 70
TABLA 15. *REQUERIMIENTOS DE ARQUITECTURA* 72
TABLA 16. *REQUERIMIENTOS DE STAKEHOLDERS* 74
TABLA 17. *SELECCIÓN DE SOFTWARE* 76
TABLA 18. *REQUERIMIENTOS PARA LA INSTALACIÓN DEL SISTEMA OPERATIVO DEBIAN JESSIE* 76
TABLA 19. *REQUERIMIENTOS PARA LA INSTALACIÓN DE FREERADIUS* 77
TABLA 20. *SERVIDORES DISPONIBLES DATACENTER FICA* 78
TABLA 21. *SELECCIÓN DEL HARDWARE* 79
TABLA 22. *TABLA DE PRUEBAS* 108
TABLA 23. FALLAS EN LA RED 123

Capítulo I: Antecedentes

1.1 Problema

Cuando se considera un sin número de requisitos de seguridad en aplicaciones distribuidas, la autorización y control aparece como un elemento clave para el diseño del sistema de seguridad completo. Álvarez (s.f) menciona que “algunas propiedades que definen a la seguridad están determinadas por flexibilidad, confiabilidad y expresividad de un esquema para autorización, por tanto, el control de acceso viene a ser el mecanismo primordial que permitirá a los propietarios de los recursos definir, gestionar y hacer buen uso de los servicios que se ofrecen.”.

Actualmente, la tarea más demandada para administradores de la red es asegurar que todo dispositivo que se conecte a la red por cualquier método de acceso, cumpla con un modelo de seguridad establecido por la entidad, controlando de esta manera el acceso de intrusos o personal no autorizado, utilizando mecanismos de autentificación que garanticen el acceso solo a usuarios que pertenezcan a la entidad. La Facultad de Ingeniería en Ciencias Aplicadas no cuenta con un control de acceso seguro de autentificación, esto representaría un gran problema si se habla de salvaguardar la información y la confidencialidad de los mensajes de cada individuo, ya que cualquier persona mal intencionada podría acceder a los servicios internos y obtener información valiosa de ella.

Además, se ha visto que la infraestructura interna de la Facultad de Ingeniería en Ciencias Aplicadas no cuenta con mecanismos de control para la navegación de internet, dando como resultado que cada estudiante (usuario) pueda utilizar este recurso descontroladamente, indefinidamente y sin medida, causando un malestar y lentitud a otros equipos que necesiten desarrollar sus labores, como por ejemplo, el acceso a los

portafolios estudiantiles, correo institucional, entre otros servicios. Y de igual manera, no existe un control de usuarios que acceden desde las redes LAN a servicios no referenciados al ámbito laboral o estudiantil como por ejemplo descargas de música, videos, películas, entre otros, dando como resultado el mal uso de la red en sí.

1.2 Objetivos

1.2.1 Objetivo general

Diseñar e Implementar un sistema de seguridad y autentificación de usuarios para permitir al administrador una gestión centralizada de la red inalámbrica de la Facultad de Ingeniería en Ciencias Aplicadas.

1.2.2 Objetivos específicos

- Analizar y comprender los conceptos relacionados con servicios de autentificación en redes inalámbricas para determinar la o las alternativas más apropiadas que soporten autentificación segura.
- Identificar los parámetros necesarios para montar un servicio de autentificación y seguridad con los dispositivos que comprenden la parte de la red inalámbrica, existentes actualmente el DataCenter de la Facultad de Ingeniería en Ciencias Aplicadas
- Realizar pruebas de funcionamiento de los equipos con los cuales se va a trabajar, con el fin de brindar las mejores prestaciones del servidor de autentificación a elegirse en toda la red inalámbrica de la facultad.
- Seleccionar el servidor de autentificación más eficaz de acuerdo a requerimientos establecidos en la fase de diseño para su posterior implementación dentro de las instalaciones de la Facultad de Ingeniería en Ciencias Aplicadas.

1.3 Alcance

El proyecto tiene como finalidad una administración centralizada de todos los usuarios de la red inalámbrica de la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte, a través de la implementación de un servidor o software de autentificación seguro que permita la integración de métodos de acceso seguro, para poder proteger la red inalámbrica de intrusos. Para la ejecución de este tema planteado, se investigará el modo de funcionamiento de los servicios de autentificación que se encuentren en el mercado y estén basados en software libre, así como también sus configuraciones respectivas, los protocolos utilizados y sobre todo datos técnicos de requerimientos tanto de software como hardware; posteriormente se realizara el análisis de la situación actual de la red y de los equipos que lo conforman, los cuales se encuentran en las instalaciones de la Facultad de Ingeniería en Ciencias Aplicadas, para poder acoplarlos al sistema de autentificación, como puede ser un servidor Radius AAA basados en el protocolo IEE 802.1X, o cualquier otro software o servicio que proteja a la red inalámbrica y brinde autentificación segura.

Una vez recolectada la información necesaria, se procederá a configurar un servidor OpenLdap como directorio de almacenamiento de credenciales de todos los usuarios que comprenda la facultad, luego se realizara pruebas de configuración del servicio AAA con los equipos que conforman la red inalámbrica y con determinados parámetros, para el buen funcionamiento de la misma, como por ejemplo, en el tipo de acceso al medio; que personas pueden ingresar (Docente, Estudiantes, Personal Administrativo de la Facultad), delimitación de banda, entre otros. El servidor AAA valida a los usuarios que intentan acceder a la infraestructura de la institución, consultando la base de datos de usuarios LDAP, si el usuario no es encontrado o la contraseña es incorrecta, el servidor rechazaría la petición de acceso del usuario, y no le permitirá hacer uso del recurso.

Por último, se procederá a implementar el servicio de autentificación probado en el punto anterior, dentro de las instalaciones de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) para poder cubrir el objetivo planteado sobre el acceso y administración de los usuarios en la red inalámbrica de la Facultad.

1.4 Justificación

La administración y gestión de usuarios en redes inalámbricas es de suma importancia debido a que las redes se encuentran propensas a vulnerabilidades; con la aparición de herramientas y softwares altamente sofisticadas para generar ataques informáticos o a su vez se podría generar un mal uso del recurso, por lo que se ve la necesidad de contar con un sistema seguro capaz de mitigar este tipo de tráfico malicioso que amenaza los recursos de la red por usuarios no autorizados.

Con el planteamiento de este proyecto lo que se pretenderá es elevar los niveles de seguridad en el intercambio de información dentro de la red inalámbrica, de esta forma se centra en dar paso al usuario que cuente con la debida autorización para que acceda a los diferentes servicios; al mismo tiempo se podrá mantener un control estricto y directo de los usuarios conectados a esta red, se lograra dar la correcta distribución de la red inalámbrica y de esta manera evitar el mal uso del servicio, los cuales causan un malestar a las demás usuario que se encuentran conectados a la misma, debido a la indisponibilidad de red.

Además, aprovechando la variedad de herramientas que actualmente software libre brinda se podrá diseñar un sistema de administración y gestión seguro para que pueda ser adaptado a la Facultad de Ingeniería en Ciencias Aplicadas, esto debido a que no se tendrá que pagar las licencias por el software a usar.

Capítulo II: Marco Teórico

En este capítulo se analizará los conceptos relacionados a la administración y gestión de usuarios en una red inalámbrica centralizada con soporte AAA, utilizando un servidor LDAP como base de datos. También se abordarán los temas de seguridad con protocolos de acceso, los métodos de cifrado y autenticación de datos, el estándar IEEE 802.11, así como también los diferentes tipos de protocolos de autentificación AAA existentes en software libre.

2.1 Administración

De manera concreta, se puede mencionar que administrar es planear, organiza, dirigir y controlar los recursos de un ente económico para alcanzar objetivos claramente determinados. Administración “es el acto de administrar, gestionar o dirigir empresas, negocios u organizaciones, personas y recursos, con el fin de alcanzar los objetivos definidos." (Significados.com, 2013). La manera en la que las organizaciones son administradas o gestionadas determinará si tendrán éxito en la utilización de sus recursos para alcanzar los objetivos propuestos. Debido a esto, el rol del administrador posee un fuerte impacto en el rendimiento de las organizaciones.

2.1.1 Administración de redes

La administración de una red de datos es considerada muy compleja dado que involucra una combinación de distintos servicios como voz, video y datos; la interconexión de diferentes tipos de redes LAN, MAN y WAN; la utilización de diversos medios de comunicación como par trenzado, cable coaxial, fibra óptica, satelital, microondas; distintos protocolos de comunicación en los que se incluyen TCP/IP, SPX/IPX, SNA; el empleo de muchos sistemas operativos como DOS, Windows, UNIX y diferentes arquitecturas de red tales como: Ethernet, Token Ring, entre otras (Caicedo, 2013)

Los elementos involucrados en la administración de la red son:

- Objetos: Constituyen los aparatos que se administran, se consideran los elementos de más bajo nivel.
- Agentes: Los agentes son el programa o el conjunto de los mismos que almacenan la información de administración del sistema en un nodo o elemento de la red. El agente tiene como objetivo el transmitir información al administrador central acerca de:
    - Notificación de problemas
    - Datos de diagnóstico
    - Identificador del nodo
    - Características del nodo (Caicedo, 2013)
- Administrador del Sistema: Es la unión de programas que se ubican en un punto central, al cual llegan los mensajes que necesitan acción o que poseen información solicitada por el administrador al programa agente. (Caicedo, 2013)
- Usuarios: Los usuarios son el conjunto de personas, los clientes que utilizan el dispositivo físico con el cual acceden a la red de datos o al internet. (Caicedo, 2013)

Los administradores de red tienen como función mantener el hardware y software de la red; esto incluye el despliegue, mantenimiento y monitoreo del engranaje de la red: switches, routers, cortafuegos, etc. La asignación de direcciones, asignación de protocolos de ruteo y configuración de tablas de ruteo así como, configuración de autenticación y autorización de los servicios, son actividades que se encuentran incluidas en la administración de una red. (ECURED, 2012). Los analistas y especialistas de red trabajan en el diseño y seguridad de la red, además de la resolución de problemas o

depuración de inconvenientes relacionados con la red. Su trabajo incluye también el mantenimiento de la infraestructura de autorización a la red.

2. 1.2 Objetivos principales de la administración de redes

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Mejorar la utilización de los recursos y hacer un uso eficiente de la red.
- Disminuir los costos mediante el control de gastos y mejorando los mecanismos de cobro.
- Proteger a la red contra el acceso no autorizado, volviéndola más segura e imposibilitando que personas ajenas entiendan la información que circula en dicha red.
- Controlar los cambios y actualizaciones que se susciten en la red, de tal manera que interrumpan lo menos posible en el servicio a los usuarios.
- Proporcionar servicios de soporte (ECURED, 2012)

2.2 Gestionar

El término “gestionar” involucra la aplicación de reglas, procedimientos y métodos operativos con el fin de que ciertas actividades sean llevadas a cabo con eficacia. (Pymes.com, 2011). La gestión consiste en poner en práctica las acciones planificadas y estudiar las desviaciones que se puedan producir sobre el plan trazado.

2.2.1 Gestión de redes

En sus inicios, la gestión de red estableció como objetivo el monitoreo del tráfico de red y el establecimiento de lo que se conoce como “Calidad de Servicio” (DoS), además de la detección de los errores que pudiesen producirse en la red, la identificación y

solvencia. (Molero, 2010). En concordancia, la gestión de red fue conocida anteriormente como gestión integrada, ya que ofrecían una gestión de red autónoma, la cual establecía las habilidades de cada administrador de red sobre cada uno de los nodos en la red en función de que cada uno poseía su propio sistema de gestión local. De igual manera, evolucionó hacia los sistemas heterogéneos, trayendo consigo la necesidad de sistemas de gestión de red de diversas naturalezas.

En virtud de lo anteriormente mencionado, la gestión de red heterogénea ha planteado y desarrollado diversos modelos, de entre los cuales destacan la Gestión de Red OSI y la Gestión Internet, este último ampliamente utilizado en la actualidad. (Molero, 2010). Como ya es conocido, existe una gran variedad de sistemas heterogéneos, debido a lo cual se exige la existencia de un marco de elementos (protocolos, estándares, entre otros) que faciliten el control permanente de la red, motivo por el cual, se desarrolló el protocolo SNMP que junto con otros protocolos de TCP/IP permite una gestión de red consolidada y marcada hasta la fecha el punto final en materia de protocolos de gestión.

2.2.2 Elementos de la gestión de red

Los elementos de la gestión de red son los siguientes: agentes, gestores y dispositivo administrativo; como se puede observar en la ilustración 1:

Ilustración 1. Elementos de gestión de redes
Fuente: (Molero, 2010)

Partiendo del gráfico anterior, se describen los elementos de la gestión de red mencionados en la tabla 1:

Tabla 1. *Elementos de Gestión*

Agentes	Gestores	Dispositivo administrativo
Se definen como un software de administración de redes que se ubican en un nodo administrado.	Se conocen también como "Sistema de Gestión de Redes NMS". Son utilizados para ejecutar aplicaciones que supervisan y controlan permanentemente todos los dispositivos administrados. **Ejemplo:** Aplicaciones de consola que permiten establecer vistas y control remoto de dispositivos tales como router, switch y hasta impresoras.	Es cualquier nodo en la red que contiene un agente SNMP y reside en una red administrada. Se encargan de recoger y almacenar información de control y monitoreo, que se pone a disposición de los gestores utilizando protocolos de administración de red. **Ejemplos:** Computadores o impresoras Routers Servidores de acceso Hubs Switches Bridges

Fuente: (Molero, 2010)

2.3 Introducción a las redes inalámbricas

Las redes inalámbricas pueden encontrarse en todo lugar, para computadores, dispositivos portátiles, conexiones de área amplia, entre otros. Con el objetivo de instalar y resolver problemas de redes inalámbricas, se deben entender los conceptos elementales de las comunicaciones inalámbricas, además de poseer conocimiento de los dispositivos, estándares, frecuencias y métodos de seguridad. Los dispositivos inalámbricos permiten la conexión central de computadores y dispositivos portátiles, también ofrecen una extensión de conectividad a una red inalámbrica que ya existe, esto puede utilizarse para conectar redes de área local a internet. También, algunos dispositivos inalámbricos se pueden conectar directamente entre sí de manera punto a punto. (Microsoft Official Academic Course, 2014). El punto de acceso inalámbrico o WAP es el dispositivo inalámbrico más conocido. En muchas ocasiones, este dispositivo actúa como un router,

firewall y proxy IP. Permite la conectividad de diferentes dispositivos inalámbricos tales como laptops, PDAs, computadoras portátiles, mediante la realización de conexiones vía ondas de radio en frecuencias específicas.

2.3.1 Ventajas de las redes inalámbricas

Entre las ventajas de las redes inalámbricas a corto y largo plazo, se incluyen:

- Accesibilidad: En la actualidad, todos los equipos portátiles y a mayoría de teléfonos móviles cuentan con la tecnología Wi-Fi, que es necesaria para realizar la conexión directa a una LAN inalámbrica. Se puede acceder de manera segura a los recursos de la red desde cualquier ubicación dentro de su área de cobertura.
- Movilidad: Permite que los usuarios permanezcan conectados a la red inclusive cuando no se encuentren en un punto determinado. Facilita el acceso a documentos y aplicaciones, además se puede consultar la red para obtener información importante desde cualquier ubicación.
- Escalabilidad: Las redes inalámbricas se pueden ampliar con el equipo existente, mientras que una red cableada suele necesitar equipo físico adicional.
- Seguridad: Debido a que el control y la administración del acceso a una red inalámbrica es importante, la tecnología Wi-Fi proporciona protecciones de seguridad sólidas para que los datos solo se encuentren disponibles para las personas a las que se les haya permitido el acceso. (CISCO, 2012)

2.4 Estándar IEEE 802.15 - Bluetooth

Bluetooth es una tecnología de comunicaciones inalámbricas que fue establecida para corto alcance, admitiendo transmisión de voz y datos creando una red de área personal. Éste es un sistema que ensancha el espectro por saltos de frecuencia, trabajando en las bandas ISM de disponibilidad internacional a 2,4 GHz. La especificación 2.0 de

Bluetooth aplicó una velocidad de transmisión mejorada (EDR) de hasta 3 Mbits/s; además, ésta tecnología sigue la tendencia a la reducción del consumo de energía. (Rohde & Schwarz, 2016)

Ilustración 2. Interacción Bluetooth (802.15)
Fuente:https://www.ohvava.com/media/catalog/product/cache/1/image/9df78eab33525d08d6e5fb8d27136e95/0/8/08_1_12.jpg

Como muestra la ilustración anterior, Bluetooth se encuentra incorporado en la mayoría de dispositivos móviles, permitiendo la conectividad de auriculares inalámbricos o entre teléfonos móviles u otros dispositivos para su sincronización. También, la mayoría de automóviles nuevos cuentan con el sistema de manos libres basado en Bluetooth®, como un equipamiento estándar u opcional. Debido al bajo valor de consumo de esta tecnología de baja energía está dirigida al mercado de sensores de uso deportivo, sanitario y de condición física. (Rohde & Schwarz, 2016) Además, la posibilidad de conectar dispositivos de baja energía a los terminales móviles permite el diseño de nuevas aplicaciones.

2.4.1 Estándar IEEE 802.16 - WiMAX

"Interoperabilidad Mundial para Acceso por Microondas", comúnmente llamado "WiMAX", consiste en un estándar inalámbrico metropolitano que fue creado por las

empresas Intel y Alvarion en el año 2002, y fue ratificado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), denominado IEEE-802.16. (CCM, 2016).

Con exactitud, WiMAX es la denominación comercial que el Foro WiMAX les da a dispositivos que cumplen con el estándar IEEE 802.16, garantizando un alto nivel de interoperabilidad entre estos dispositivos. Se les ha permitido llevar el logotipo que se muestra la ilustración 3 a los dispositivos certificados por el Foro WiMAX (CCM, 2016).

Ilustración 3. Logotipo Wimax
Fuente: http://static.commentcamarche.net/es.kioskea.net/pictures/wimax-images-wimax-logo.png

WiMAX tiene como objetivo el proporcionar acceso a internet de alta velocidad en un rango de cobertura con varios kilómetros de radio. En teoría, se menciona que WiMAX proporciona velocidades de aproximadamente 70 Mbps en un rango de 50 kilómetros.

Como ventaja, WiMAX permite conexiones inalámbricas entre un *transceptor de la estación base* (BTS) y miles de abonados sin que éstos tengan que estar en línea de visibilidad (LOS) directa con esa estación. Esta tecnología es llamada NLOS, o "sin línea de visibilidad". La tecnología WiMAX elude obstáculos pequeños, como árboles o una casa, pero no atraviesa montañas ni edificios altos, en estos casos, el rendimiento total real puede ser inferior a 20 Mbps. (CCM, 2016)

2.4.2 Estándar IEEE 802.11 - WIFI

La especificación IEEE 802.11 (ISO/IEC 8802-11), consiste en un estándar internacional que tiene por objetivo definir las características de una red de área local inalámbrica (WLAN). Wi-Fi, cuyo significado es "fidelidad inalámbrica", es el nombre de la certificación que fue otorgada por la Wi-Fi Alliance, antes denominada "Wireless

Ethernet Compatibility Alliance", grupo que se encarga de garantizar la compatibilidad entre los dispositivos que usan el estándar 802.11. Debido a la inadecuada utilización de los términos, además de razones de marketing, el nombre del estándar es confundido con el nombre de la certificación, por lo que una red Wi-Fi, es en realidad una red que está cumpliendo con el estándar 802.11. (CCM, 2016).

A los dispositivos que han sido certificados por la Wi-Fi Alliance se les permite utilizar el logotipo que se muestra la ilustración 4.

Ilustración 4. Logotipo dispositivo con Wifi
Fuente: (CCM, 2016)

El estándar 802.11 ha establecido los subniveles del modelo OSI para las conexiones inalámbricas que se realizan mediante ondas electromagnéticas, por ejemplo:

- La capa física, también abreviada capa "PHY", ofrece tres tipos de codificación de información.
- La subcapa de control de enlace lógico (LLC) y la subcapa de control de acceso al medio (MAC) conforman la capa de enlace de datos

2.5 Modificaciones del estándar 802.11

En conjunto, los estándares inalámbricos IEEE 802.11a, 802.11b, 802.11g y 802.11n son denominados tecnologías Wi-Fi. Un sinnúmero de productos, como los teléfonos inteligentes o los enrutadores inalámbricos, usan las tecnologías 802.11 como un estándar

para la implementación de redes de área local inalámbricas (WLAN) rápido y ultra rápidas. (buffalo-technology, 2015). En la tabla 2 se evidencia la comparación entre los distintos tipos de estándares 802.11:

Tabla 2. *Comparación de estándares 802.11*

Estándar	Velocidad (teórica)	Velocidad (práctica)	Banda	AB	Detalles	Año
802.11	2 Mbps	1 Mbps				1997
802.11a	54 Mbps	22 Mbps	5.4 Ghz			1999
802.11b	11 Mbps	6 Mbps	2.4 Ghz			1999
802.11g	54 Mbps	22 Mbps	2.4 Ghz	20 MHz		2003
802.11n	600 Mbps	100 Mbps	2.4 Ghz y 5.4 Ghz	40 MHz	Disponible en la mayoría de los dispositivos modernos. Puede configurarse para usar solo 20 MHz de ancho y así prevenir interferencias en una zona congestionada.	2009
802.11ac	6.93 Gbps	100 Mbps	5.4 Ghz	80 o hasta 160 MHz	Nuevo estándar sin interferencia pero con menos alcance, aunque hay tecnologías que lo amplían.	2012
802.11ad	7.12 Gbps					2012

Fuente: http://ieeestandards.galeon.com/aficiones1573579.html

2.6 Seguridad

La seguridad se define como la característica imprescindible de cualquier sistema (sea informático o no), el cual nos advierte que aquel sistema se encuentra libre de peligro, riesgo o daño y que de una cierta manera es considerada infalible. Si se detalla el caso de sistemas o redes informáticas, se vuelve un tema muy difícil de conseguir, por lo cual se pasa a hablar lo que comúnmente se conoce en el mundo de las redes como fiabilidad (Probabilidad de que un sistema trabaje tal y como fue programado) más que seguridad; por tanto cabe recalcar que los sistemas informáticos serían más fiables para la empresa que seguros (Huerta, 2014).

La seguridad informática garantiza que ningún curioso pueda leer o modificar los mensajes destinados a otras personas; es decir la seguridad se enfoca en la gente o individuos que intentan acceder a servicios no autorizados. (Bertolín, 2010). Además, la seguridad se ocupa del resolver el problema de plagio y captura de información legitima, como de aquellos que intentan negar la disponibilidad del servicio.

2.6.1 Principios de seguridad

Se entiende por servicio de seguridad como aquel que mejora la seguridad de un sistema informativos y la relación con el flujo de información que posee la misma. Estos servicios están encaminados a evitar ataques de seguridad y se utiliza uno o más mecanismos de seguridad para facilitar el servicio. (UNAM, 2009). Una clasificación utilizada muy a menudo comprende:

- Confidencialidad
- Disponibilidad
- Integridad
- No repudio
- Autenticidad

2.6.2 Confidencialidad

Al hablar por confidencialidad se hace referencia a un servicio de seguridad, el cual establece que la información no estará disponible o estará oculta para otras personas, entidades o procesos no autorizados. (tecno.unsl.edu.ar, 2008). La confidencialidad, es comúnmente denominada como secreto o reserva, que se refiere a la capacidad de un sistema para evitar intrusos en información almacenada.

Ilustración 5. Confidencialidad
Fuente: http://www.albaceteinnova.org/wp-content/uploads/2012/02/myviaje_confidencial-300x215.jpg

2.6.3 Integridad

López (2014) afirma que "La integridad se entiende como el servicio que garantiza que la información solo podría ser modificada, eliminada o borrada solo por aquel personal que tiene el acceso total al mismo." Suelen integrarse varios conceptos semejantes en este aspecto de seguridad como por ejemplo la precisión y la autenticidad.

En el área de redes y comunicaciones, la integridad viene dada por la autenticidad, el cual trata de brindar los medios para validad que el origen de los datos es el adecuado, así como aquel o aquellos que la enviaron y cuando fueron enviados o recibidos. (tecno.unsl.edu.ar, 2008)

Ilustración 6. Integridad
Fuente: http://www.pcworld.com.mx/postsGenPic.aspx?i=25313

2.6.4 Disponibilidad

La disponibilidad se entiende como:

- El grado de rapidez en la que un dato es entregado cuando se es pedido por un usuario autorizado.

- El menor tiempo en la que un usuario puede acceder a un sistema operativo.

Según (tecno.unsl.edu.ar, 2008) se habla de disponibilidad cuando "cualquier sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo."

Según (apser, 2015) se hace referencia a este término cuando se habla del "acceso de personas u organismos a los datos con los que se trabaja. Es clave que el sistema garantice que se pueda acceder tanto a estos datos como a procesos en sí en cualquier momento de forma rápida y sencilla y solucionar posibles problemas cuando puedan surgir."

Ilustración 7. Disponibilidad
Fuente: http://www.manas-ti.com/wp-content/themes/novus/images/-Almacenamiento.jpg

2.6.5 Otros aspectos relacionados

Existe dos aspectos más de seguridad que influyen indirectamente a los tres aspectos fundamentales de seguridad, tales como:

- **Autenticidad:** Esta propiedad asegura el origen de la información, en la cual la identidad del emisor puede ser validada demostrando ser un usuario de confianza. (tecno.unsl.edu.ar, 2008). Con esta propiedad se asegura que la información sea legítima y no sea algún intento de plagio o programas con archivos maliciosos.
- **Imposibilidad de rechazo (no-repudio):** Con esta propiedad se asegura de que cualquier entidad pública o privada, persona o individuo que envié o reciba información, no podrá alegar ante la ley o a terceros que no realizo o recibió

aquella información. (tecno.unsl.edu.ar, 2008). Esta propiedad, así como la anterior son de vital importancia en sectores bancarios y el uso de comercio digital.

2.7 Amenazas y vulnerabilidades

Para emplear los controles adecuados de seguridad, se debe comprender dos parámetros fundamentales, primero quien es la amenaza o qué será lo que amenazara dicho entorno, y en segundo lugar es el conocer los riesgos asociados a dichos escenarios una vez que llegue a concretarse. Los problemas de seguridad están divididos en:

2.7.1 Amenazas

Las amenazas son considerados como cualquier agente exterior al sistema, donde es posible establecer medidas se seguridad, pero prácticamente son incontrolables y jamás se las podrá eliminar del mismo. (Tutorial de Seguridad Informatica, 2013). Las amenazas en si son acontecimientos que causan alteraciones a la información que circula en el sistema, las cuales pueden ocasionar graves pérdidas materiales, de información y económicas a cualquier organización.

2.7.1.1 Fuentes de amenaza

Las amenazas son aquellas causantes de la destrucción parcial o total de un sistema, las cuales pueden dividirse en varias categorías para su posterior investigación. La tabla 3 presenta un breve resumen de los 5 tipos que son:

Tabla 3. Fuentes de Amenazas

FACTOR	CARACTERÍSTICAS	TIPOS	DEFINICIÓN
FACTOR HUMANO	La principal fuente de amenaza que existe en todo sistema informático son las personas y a su vez es el tipo de amenaza en el cual se invierte la mayoría de recursos para tratar de mitigarlos o por otro lado contrarrestar los efectos. Este tipo de factor abarca todas las falencias de medidas de seguridad por la falta de controles adecuados para el mismo.	Curiosos	Es todo aquel individuo que entra sin aviso previo a un sistema (en algunos casos de manera esporádica), impulsado por el deseo de investigar, aprender o simplemente por curiosidad.
		Intrusos remunerados	Encargados de infiltrarse de cualquier manera a un sistema a cambio de una remuneración monetaria o cualquier tipo de pago.
		Personal enterado	En este caso es el propio personal interno o quizá exempleados los que producen daños severos en el sistema impulsados por motivaciones personales que van desde una simple mal entendido o en otros casos remuneraciones de otras organizaciones.
		Robo, Sabotaje, Fraude	Extracción de información confidencial para fines lucrativos, interrupción de operaciones para dañar los equipos, aprovechar recursos para beneficio ajeno
		Ingeniería social	Hace referencia a la obtención de información confidencial a través de la manipulación de personal autorizado, los cuales son llevados a revelar o violar las políticas de seguridad establecidos.
HARDWARE	Son todas aquellas amenazas que vienen dadas por fallas físicas del sistema que se represente en cualquier elemento del mismo. Todos estos defectos pueden ser causados por defectos de fábrica o mal diseño del hardware, pero no se descarta el mal uso o descuido del mismo	Mal diseño	Son todos los componentes del sistema que no cumplen con requerimientos necesarios de funcionamiento, es decir, dicho componente o pieza no fue diseñado para trabajar correctamente en el sistema
		Errores de fabricación	Hace referencia a todas aquellas piezas que vienen con defectos de fábrica y por obvias razones fallaran en su operación al intentar usarlas. Aun sabiendo que la calidad de las piezas son de estricto compromiso del fabricante, la organización es la más afectada en este tipo de amenazas

		Suministro de energía	Cualquier variación fuera de los rangos normales de voltaje podrían dañar los dispositivos, por eso se debe tomar en cuenta que todo el suministro de energía funcione dentro de esos parámetros, pues existen cierta cantidad de componentes que necesitan una energía exacta para ser energizados sin que se agote su vida útil más rápidamente.
		Descuido y mal uso	Cualquier dispositivo o componente que forme parte de un sistema debe estar dentro de parámetros impuestos por el fabricante, incluyendo el tiempo de uso, así como los tiempos adecuados de mantenimiento y almacenamiento. Al no seguir estas instrucciones sobre el bueno uso de componentes se provocaría un desgaste acelerado del mismo que traerá como consecuencia la reducción de vida útil de los recursos.
RED DE DATOS	Esta amenaza se presenta cuando la red de comunicación no está disponible para su uso, esto puede ser provocado por un ataque deliberado por parte de un intruso o un error físico o lógico del sistema mismo. Las dos principales amenazas que se presentan en una red de datos son, la no disponibilidad de la red, y la extracción lógica de información a través de ésta	Topología seleccionada:	De acuerdo a los recursos que comparten en la red o el alcance del mismo, puede ser más conveniente seleccionar una topología sobre otra, siempre y cuando teniendo en cuenta que las desventajas de cada arquitectura pueden dejar fuera de servicio a toda la red.
		Sistema operativo	Teniendo en cuenta que el modelo de referencia OSI permite la interacción entre equipos con diferentes SO, se observa algunos casos en las que ciertas operaciones no son compatibles entre sistemas operativos, lo cual hace que el recurso quede divido.
		Incumplimiento de las normas de instalación de la red	Graves problemas de trasmisión de datos, pérdida de información, indisponibilidad de recursos entre otros
		Software de desarrollo	Se trata de software personalizado que es creado con el fin de atacar a un sistema por completo, o a su vez aprovecharse de las características que posee para poder penetrar en su seguridad.
		Software de aplicación	

SOFTWARE	Las amenazas en el software son aquellos fallos que ocurren dentro del sistema operativo, este puede ser causado por un mal desarrollo de software, un mal diseño o un mal acople, además de que coexiste un tipo de software malicioso que representaría un amenaza directa contra un sistema		A pesar de que no es creado para realizar ataques específicos sobre el software, estas aplicaciones pueden ser usadas de manera maligna para atacar al sistema.
		Código malicioso	Se trata de cualquier software (infectado) que ingresa al sistema operativo sin ser intersectado, además intenta romper a como dé lugar las reglas se seguridad. Estos códigos maliciosos incluyen caballos de Troya, los gusanos informáticos, bots, hacker de sombrero negro, entre otras amenazas pre programado como las bombas lógicas
		Virus	Se trata de un tipo de código malicioso el cual tiene la capacidad de duplicarse a sí mismo utilizando los recursos del mismo sistema infectado, propagando su infección en todos los componentes que forman dicho sistema rápidamente
		Troyanos y Gusanos	Son un tipos de virus que se infiltran en una red de datos y afectan a los computadores y en general a la red, el uno es encargado de abrir puertas traseras en los programas legítimos, por otra parte el gusano aprovecha todos los recursos de los objetos infectados y hace que cada infección genere otro gusano para lograrse esparcir más rápidamente.
DESASTRES NATURALES	Son aquellos eventos que se originan por las fuerzas naturales. Estos desastres afectan tanto a la información contenida en el sistema, así como también toda la integridad del sistema (infraestructura) el cual puede dejar inoperable por completo al sistema.	Inundaciones, los terremotos, incendios, huracanes, tormentas eléctricas	
		Los cuales provocan cortos circuitos, destrucción total o parcial de los equipos de cómputo, o alteraciones físicas de las localidades, causando que ya no sean apropiadas para albergar un equipo de cómputo.	

Fuente: (Tutorial de Seguridad Informatica, 2013)

2.7.2 Vulnerabilidades

La vulnerabilidad informática se define como el elemento de un sistema informático que puede ser utilizado por un atacante para violar la seguridad, de igual manera pueden causar daños por sí mismos sin tratarse de un ataque intencionado. (Tutorial de Seguridad Informatica, 2013). Las vulnerabilidades son consideradas un elemento interno del sistema, por lo cual es responsabilidad de los administradores y usuarios el detectarlos, valorarlos y reducirlos.

2.7.2.1 Tipos de vulnerabilidades

Las vulnerabilidades se producen como resultado a errores de programación (bugs), fallos en el diseño del sistema, además, las limitaciones tecnológicas pueden ser utilizadas por los atacantes.

En la presente investigación, se han clasificado las vulnerabilidades en seis tipos: físicas, naturales, de hardware, de software, de red y de factor humano.

Tabla 4. *Fuente de Vulnerabilidades*

TIPOS	DEFINICIÓN	EJEMPLOS
FÍSICA	Se relaciona con el acceso físico al sistema, se refiere a las instalaciones donde se encuentran los equipos de cómputo, mismos que contienen la información o forman parte de los procesos importantes del sistema.	Este tipo de vulnerabilidades se presentan en forma de malas prácticas de las políticas de acceso a los sistemas y la utilización de los medios físicos de almacenamiento de información, permitiendo así la extracción de datos del sistema sin autorización.
NATURALES	Principalmente se presentan como deficiencias de las medidas tomadas para afrontar desastres, por ejemplo, la ausencia de reguladores, mal sistema de ventilación o calefacción, etc.	Debido a que los fenómenos naturales son inevitables, es necesaria la instalación de medidas de seguridad que protejan al sistema de ese tipo de eventos.
HARDWARE Y SOFTWARE	Las vulnerabilidades de hardware están representadas por la posibilidad de fallo de	Cada programa puede ser utilizado como un medio para atacar a un sistema más grande, utilizando los

	las piezas físicas del sistema debido a diversas causas, mal uso, descuido, mal diseño, entre otras. Además, trata acerca de las maneras en las que el hardware puede ser utilizado para atacar la seguridad del sistema.	errores de programación o debido a que en el diseño no fueron tomados en cuenta ciertos aspectos, como controles de acceso, seguridad, implantación, entre otros. Ambos factores vuelven susceptible al sistema a recibir amenazas de software.
RED	Dado que se trata de una serie de equipos conectados entre sí compartiendo recursos, las redes son sistemas muy vulnerables, por lo que es posible atacar a toda la red invadiendo primero uno de los equipos y por medio de éste expandirse al resto.	La transmisión de la información es la prioridad de la red, por lo que todas las vulnerabilidades se relacionan a la intercepción de dicha información por personas sin autorización y con fallas en la disponibilidad del servicio. Ambos puntos logran que las vulnerabilidades de las redes sean una combinación de vulnerabilidades de hardware, software, físicas e incluso naturales.
FACTOR HUMANO	La más frecuente es la falta de capacitación y concienciación, lo que desencadena en la negligencia en el cumplimiento de las políticas de seguridad y la mala utilización del equipo de cómputo.	El robo de información o la destrucción de los sistemas pueden ser el resultado de una vulnerabilidad humana, quizás un usuario reveló accidentalmente las contraseñas de acceso o no realiza una revisión periódica de las bitácoras de actividades de los equipo de cómputo con el objetivo de buscar actividades sospechosas.

Fuente: (Tutorial de Seguridad Informatica, 2013)

Es importante además entender que es posible reducir, controlar o eliminar las vulnerabilidades, contrarrestando entonces la posibilidad de que una amenaza avance y se convierta en un ataque.

2.8 Seguridades en las redes inalámbricas

La red inalámbrica es evidentemente más insegura que una red cableada, debido a que la señal no se encuentra confinada a un medio de transmisión delimitado y con protección física contra el acceso de cualquier atacante potencial. Por el contrario, cualquier atacante pasivo que se encuentre al alcance de la red inalámbrica y que cuente con un receptor de

radio adecuado puede interceptar y decodificar la señal si es que no se han tomado medidas para evitarlo. Por otro lado, los ataques activos, especialmente los de degeneración de servicio, pueden resultar más complicados de prevenir, inclusive en la práctica pueden ser inevitables, debido a la falta de aislamiento del medio de transmisión o de autenticidad en los mensajes correspondientes al protocolo definido en el estándar 802.11 (Navarro, 2013)

2.9 Métodos de cifrado

La autenticación es el proceso mediante el cual se verifica y asegura la identidad de los participantes en una transacción. Si este proceso no se llevase a cabo, existiese la posibilidad de que cualquier individuo asuma una identidad falsa, poniendo en peligro la privacidad y la integridad de la información. (Torres, 2010). Dentro del contexto de las redes WLAN, la autenticación es una medida que se ha diseñado con el fin de establecer la validez de una transmisión entre estaciones inalámbricas o puntos de acceso.

2.9.1 WEP (Wired Equivalent Privacy)

Wired Equivalente Privacy fue el método de seguridad original del protocolo 802.11 y el único existente durante sus primeros cinco años. (Torres, 2010). En la publicación realizada por WEP, se establecieron un conjunto de objetivos que pretendían ser cumplidos:

- Al poseer una clave relativamente larga y un vector de inicialización cambiante en cada paquete, se vuelve razonablemente fuerte.
- Poseer la capacidad de encriptarse y des encriptarse por sí solo, requerimiento imprescindible en una WLAN, dado que los paquetes perdidos representan un alto porcentaje.
- Ser eficiente y poderse implementar en hardware o software.

- Ser exportable, es decir, que pueda utilizarse en todo el mundo.
- Ser opcional

Las redes Wi-Fi se volvieron populares a partir del año 2000, razón por la cual atrajeron la atención de la comunidad criptográfica, mismas que descubrieron grietas de seguridad en WEP, por lo que a finales del año 2001 ya existían herramientas en internet para derrotarlo.

2.9.2 Autenticación WEP

Este tipo de autenticación utiliza una clave secreta que se utiliza sobre un algoritmo para encriptar y des encriptar mensajes, entonces, para poder enviar un mensaje, hay que saber cómo encriptarlo, demostrando así que es un usuario autorizado. La autenticación tiene como base la posesión de una clave. En la autenticación WEP existe un proceso de intercambio de cuatro mensajes; el punto de acceso envía un mensaje al cliente para que se efectúe una transformación sobre él. El mensaje de prueba, o challenge text, es un número aleatorio con una longitud de 128 bits; sobre este mensaje se efectúa un proceso de encriptado WEP usando la clave secreta compartida, el resultado obtenido se compara en el AP con lo que se esperaba obtener, y así concluir este proceso. (Torres, 2010)

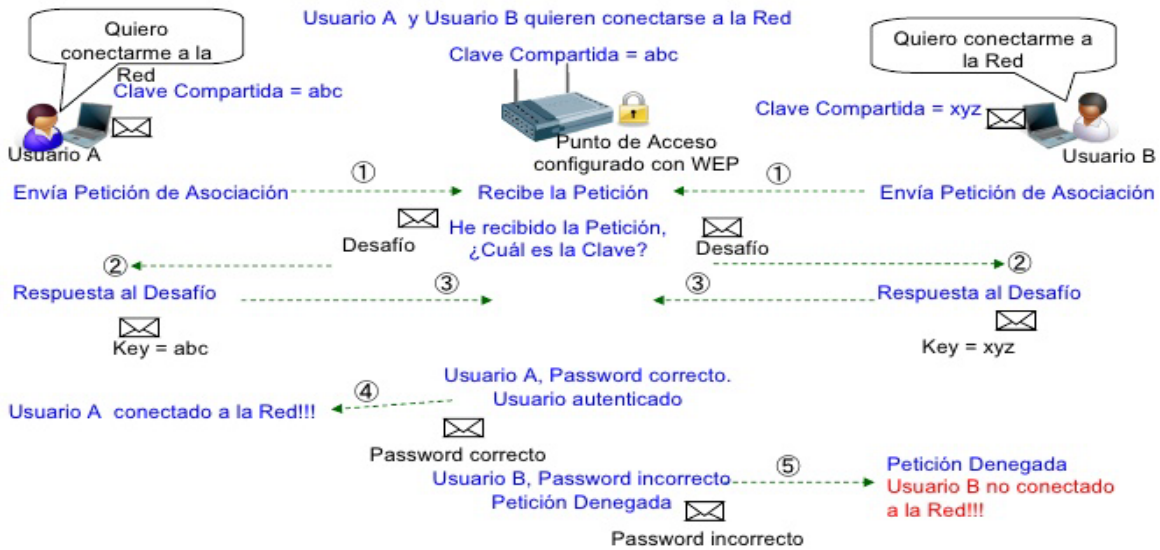


Ilustración 8: Funcionamiento WEP

Fuente: Curso de Seguridad Informática de la Universidad de Salamanca 2012

De esta manera, el usuario demuestra su conocimiento de una clave secreta sin ser necesario que ésta viaje por el medio, así no peligra su confidencialidad durante el proceso, aunque existiese un dispositivo no autorizado realizando una escucha o sniffing. (Torres, 2010). Uno de los inconvenientes que presenta este proceso, es que en ningún momento el AP se identifica, es decir que la autenticación no es mutua; otro problema es que un sniffer si podría llegar a descubrir la clave observando el intercambio entre texto plano y texto cifrado.

2.9.3 WPA/WPA2 WPA

Wifi Protect Access, también conocida como Transition Security Network (TSN), es el mecanismo de control de acceso a una red inalámbrica. El gran número d vulnerabilidades existentes en WEP obligaron a Wi-Fi Alliance a desarrollar una alternativa, denominada Wi-Fi Protected Access (WPA), con el fin de cerrar la brecha hasta que el nuevo estándar 802.11i oferte mecanismos de seguridad más fuertes. WEP es del año 1999 y las principales vulnerabilidades de seguridad fueron encontradas en 2001; en 2004 IEEE tenía casi listos los trabajos del nuevo estándar para reemplazar a WEP, publicados en la norma IEEE 802.11i, pero debido a la tardanza, Wi-Fi decidió colaborar con el IEEE tomando las partes del nuevo estándar que ya se encontraban listas y así publicar WPA, que es un compromiso entre WEP y el más reciente WPA2. (Torres, 2010)

2.9.3.1 Características WPA

La utilización más fuerte del vector de inicialización, la distribución dinámica de claves y nuevas técnicas de integridad y autentificación son las principales características de WPA, que incluye las siguientes tecnologías:

- ***IEEE 802.1X:*** Estándar de 2001 que proporciona un control de acceso en redes con base en puertos.
- ***EAP:*** Definido en la RFC 2284, de inicio fue diseñado para el Point to Point Protocol, aunque es utilizado por WPA entre la estación y el servidor RADIUS. Éste es un protocolo de autentificación extensible, efectúa las tareas de autentificación, autorización y contabilidad.
- ***Temporal Key Integrity Protocol:*** TKPI es el protocolo que se encarga de generar la clave dinámica utilizada en cada trama, mejorando así de manera notable el cifrado de datos, incluyendo el vector de inicialización.
- ***Message Integrity Code:*** MIC es el código que verifica la identidad de los datos de las tramas. (Torres, 2010)

2.9.3.2 Mejoras de WPA con respecto a WEP

Al incluir vectores de 48 bits de longitud y especificando reglas de secuencia, WPA soluciona la debilidad del vector de inicialización de WEP. Los 48 bits de longitud permiten generar innumerables claves diferentes, evitando así la existencia de duplicados. El algoritmo de cifrado usado por WPA es RC4, el mismo que en WEP, aunque ya se ha demostrado que es inseguro. La secuencia de los vectores de inicialización, conocida por ambos extremos de la comunicación, puede ser utilizada para evitar ataques de repetición de tramas. Se ha incluido el nuevo código denominado MIC para conservar la integridad de los mensajes o Integrity Check Value (ICV), eliminando así el CRC-32, que ya demostró ser inservible en WEP. (Torres, 2010)

Actualmente, las claves se generan de forma dinámica y se distribuyen automáticamente, por lo que se evita la modificación manual en cada elemento de red cada cierto tiempo, como sucedía en WEP. Para la autentificación se modificaron los métodos de autenticación y cifrado, proporcionando más seguridad; los usuarios usan

claves que han sido compartidas previamente, o en el caso de grandes redes LAN inalámbricas, se utiliza un servidor RADIUS para asociarse con el punto de acceso. Posterior a la autenticación, el usuario y el punto de acceso negocian una clave de acceso individual de 128 bits, con el fin de evitar que otras estaciones en la WLAN rastreen el tráfico de datos. Para añadir más seguridad a la WPA estándar, se realiza una renegociación periódica de la clave entre el usuario y el punto de acceso, de esta manera se elimina la posibilidad de que un intruso inicie un ataque de fuerza. (Torres, 2010)

2.9.3.3 Métodos de funcionamiento de WPA

WPA puede trabajar de dos maneras:

- **Enterprise Mode:** El modo corporativo cuenta con servidor AAA y RADIUS, precisa de un servidor configurado para realizar las tareas de autentificación, autorización y contabilidad.

- **Home Mode:** Para usuarios domésticos o redes pequeñas, utiliza una clave que se ha compartido en las estaciones y puntos de acceso, clave que se utiliza únicamente para la autentificación, mas no para el cifrado de datos. (Torres, 2010)

2.9.3.4 Debilidades de WPA

Al utilizar WPA como mecanismo de seguridad, los puntos de acceso aceptan únicamente la autenticación y cifrado WPA, impidiendo la conexión de usuarios sin WPA. Por otra parte, un usuario configurado para utilizar WPA no puede conectarse a puntos de acceso sin WPA. (Torres, 2010). El problema que se mantiene con WPA es que tiene como base el algoritmo de cifrado RC4, que posee varias vulnerabilidades.

2.9.3.5 Características WPA2 y mejoras

Presentado en 2004, WPA2 vuelve a las WLAN más seguras. Se han dejado atrás ciertas características de seguridad, sustituyendo el algoritmo RC4 por el Advanced

Encryption Standard (AES); además se incorporaron los métodos de autenticación y el cifrado WPA. (Torres, 2010). Debido a estas mejoras, ya no es posible para los atacantes hacer el rastreo de una WLAN ni ejecutar ataques de fuerza bruta contra los resultados.

WPA2 permite, al igual que WPA, dos maneras de llevar a cabo la autenticación: si el ámbito de aplicación es empresarial (IEEE 802.11i/EAP) o personal (PSK). Pese a que esta variante ofrece las características de seguridad más populares, no es compatible con el beneficio de autenticación a través de un servidor RADIUS; al contrario de la versión Enterprise WPA2 que abarca todo el estándar 802.11i y si permite la autenticación RADIUS. (Torres, 2010)

La ilustración 9 muestra una comparación entre WPA y WPA2

		WPA	WPA2
Modo Corporativo	Autenticación	802.1X / EAP	802.1X / EAP
	Cifrado	TKIP/MIC	AES-CCMP
Modo Personal	Autenticación	PSK	PSK
	Cifrado	TKIP/MIC	AES-CCMP

***Ilustración* 9.** Comparativa WPA/WPA2
Fuente: (Torres, 2010)

2.9.3.6 Debilidades de WPA2

Se dice que las redes inalámbricas que están basadas en WPA2 son considerablemente más seguras pero teóricamente la multidifusión de claves representa otra vulnerabilidad, debido a que todos los puntos de red necesitan conocerlas, por tanto si un atacante descubre una de ellas podría observar el intercambio de claves entre el punto de acceso y la estación de red. (Torres, 2010)

2.10 IEE 802.1x

802.1x es el estándar basado en IEEE para gestionar el control de acceso a la red mediante un proceso conocido como autentificación; el cual permite o impide el acceso de cualquier dispositivo que se intente conectar a la red LAN o WLAN. La letra “x”

representa el uso obligatorio de protocolo EAP (autentificación extensible) entre cualquier suplicante que pueden ser usuarios de red inalámbrica como cableada, el autenticador como los switches o access point y los servidores de autentificación como el Radius. (Chamorro, 2010). El protocolo 802.1x funciona de manera conjunta entre EAP y RADIUS, la relación existente entre ellos se describe brevemente a continuación.

- EAP: Soporta protocolos de autentificación segura, en donde los mensajes que envían los solicitantes deben ser reenviados hacia algún servidor de autentificación remoto.
- RADIUS: Es usado típicamente en la relación Autentificador – Servidor. Debido a que el sistema de autentificación es remoto, los mensajes EAP requieren de un mecanismo que les permita alcanzar su destino y es ahí donde RADIUS hace que estos mensajes puedan llegar a ese destino. (Torres, 2010)

La ilustración 10 nos muestra el flujo de autentificación que sigue un suplicante para poder tener acceso a la red.

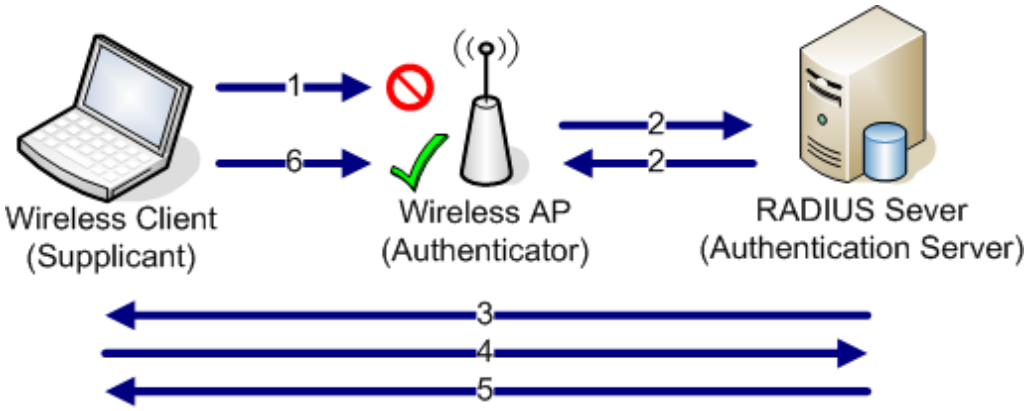


Ilustración 10. Autentificación 802.1x
Fuente: (Domínguez, 2011)

802.1x cuenta con tres componentes denominados suplicante (Cliente), autenticador (dispositivo de acceso) y el servidor de autenticación (RADIUS). Cuando EAP se ejecuta a través de una WLAN, los paquetes EAP son encapsulados por EAP (EAPOL). El proceso de autenticación comienza cuando el usuario final intenta conectarse a la WLAN,

el autenticador recibe la solicitud y crea un puerto virtual con el solicitante, obligando al autenticador actuar como un proxy para el usuario final el cual garantizara el traspaso de información entre el cliente y el servidor, por tanto:

- El cliente puede enviar un mensaje EAP-inicio.
- El punto de acceso envía un mensaje de identidad de solicitud EAP.
- El servidor de autenticación pide al cliente sus credenciales para demostrar su confiabilidad.
- El servidor de autenticación acepta o rechaza la solicitud del cliente para la conexión.
- Si el usuario final fue aceptado, el autenticador cambia el puerto virtual con el usuario final a un estado autorizado, que permite el acceso de red.
- Al iniciar la sesión inicial, el puerto virtual del cliente se cambia de nuevo al estado no autorizado.

Existen múltiples variantes de EAP, entre las cuales destacan:

- EAP-LEAP: Es el tipo de autentificación propietaria de equipos pertenecientes a la marca Cisco Systems, el cual permite la autentificación de usuarios y servidor sin la utilización de certificados digitales, simplemente se hace la autorización a la red mediante un usuario y contraseña el cual se encuentre debidamente validado dentro de algún servidor de datos como por ejemplos Windows NT, Windows Active Directory, ODBC.
- EAP- TLS: Este estándar utiliza certificados digitales en ambos extremos, tanto para el servidor como para el suplicante, el cual utiliza túneles TLS encriptados para el intercambio de las llaves públicas. Es un protocolo independiente de RADIUS.

- EAP-TTLS: Es una simplificación de protocolo anterior EAP-TTLS, el cual evita la utilización de certificados en los clientes. Es un método EAP (Extensible Authentication Protocol) que encapsula una sesión TLS (Transport Layer Security), que consiste en una fase de apretón de manos y una fase de datos.
    - ✓ Durante la fase de apretón de manos el servidor está autenticado en el cliente (o el cliente y el mutuamente autenticados) utilizando procedimientos TLS estándar, generando una conexión de túnel para el intercambio de información
    - ✓ En la siguiente fase de datos, el cliente se autentica al servidor (o cliente y el servidor están mutuamente autenticados) utilizando un archivo arbitrario como mecanismo de autenticación encapsulado dentro del túnel seguro. Los Mecanismo de autenticación encapsulado puede ser EAP, o puede ser otro protocolo de autenticación como PAP, CHAP, MS-CHAP o MS-CHAP-V2.

- EAP-PEAP: Propuesta por Cisco y Microsoft que al igual de EAP-TTLS lo que se pretende es eliminar los requisitos que necesita TLS. Es ideal para aquellos fabricantes que aún no disponen una certificación digital para cada dispositivo de su red, el cual autentifica a los usuarios en una base de datos realizando la autenticación de usuarios contra un servidor Windows (Active Directory, Windows NT), RADIUS o incluso contra los puntos de acceso de Cisco, la única falencia es que se limita a 50 usuarios.

En la tabla siguiente se muestra una comparativa de las distintas opciones anteriormente presentadas:

Tabla 5. *Comparativa EAP*

	EAP-LEAP	EAP-TLS	EAP-TTLS	EAP-PEAP
Soporte de RADIUS	Cisco FreeRadius Linux Funk Interlink MeetingHouse, Radiator	Cisco FreeRadius Linux Funk Interlink MeetingHouse, Radiator Microsoft	Funk Interlink MeetingHouse Radiator Freeradius	Cisco Funk Interlink MeetingHouse Microsoft Radiator
Soporte en cliente	Cisco Funk MeetingHouse	Cisco Funk MeetingHouse Microsoft Open 1X	Alfa-Ariss Funk MeetingHouse Open1X Microsoft	Funk MeetingHouse Microsoft
Sistemas operativos embebidos		Windows XP/2000/2003		Windows XP/2000/2003
Plataformas soportadas con software de terceros	Win 32	MacOS X, BSD, Linux, Win32	MacOS X, BSD, Linux, Win32	Win 32
Autenticación de servidor	Password hash	Clave pública (certificada)	Clave pública (certificada)	Clave pública (certificada)
Autenticación de cliente	Password hash	Clave pública (certificado o tarjeta inteligente)	CHAP, PAP, MS-CHAP (v2), EAP	Cualquier EAP, como EAP-MS-CHAP (v2) o clave pública
Claves dinámicas	Si	Si	Si	Si

Fuente: (Domínguez, 2011)

2.11 Sistema de control de acceso AAA

Es una arquitectura de sistema que se utiliza para configurar el trío de funciones de seguridad Authentication, Authorization and Accountig de una forma coherente. (Guiza, 2010). AAA brinda una forma modular de proveer los servicios siguientes:

- **Autenticación:** Proporciona el método de identificación de usuarios, incluyendo nombre de usuario y contraseña, desafío y respuesta, soporte de mensajería, y, dependiendo del protocolo de seguridad que se elija, puede ofrecer cifrado. La

autenticación es la manera en la que el usuario se identifica antes de que se le permita acceder a la red y sus servicios. Para configurar la autenticación AAA es necesaria la definición de una lista denominada “métodos de autenticación”, y posteriormente aplicar esta lista a varias interfaces. En esta lista están definidos los tipos de autenticación a realizarse y el orden en el que se llevará a cabo, además debe ser aplicado a una interfaz específica antes de que los métodos de autenticación definidos se utilicen. La excepción es la lista método por defecto, denominada “default”, que se aplica automáticamente a todas las interfaces si ninguna lista de otro método está definida. Los métodos de autenticación deben ser definidas a través de AAA, excepto local, line de contraseña y habilitación de autenticación. (Guiza, 2010)

- **Autorización:** Otorga el método de control de acceso remoto, incluyendo la autorización total o para cada servicio, lista de cuentas y perfil por usuario, soporte para grupos de usuarios, y soporte para IP, IPX, ARA y Telnet. La autorización de AAA trabaja formando el grupo de atributos que describen lo que el usuario tiene permitido usar o a lo que puede acceder. Estos atributos se comparan con la información existente en una base de datos de un usuario determinado, y el resultado es devuelto a AAA con el fin de determinar las capacidades reales de los usuarios y sus restricciones. Es posible localizar de forma local la base de datos en el servidor de acceso o router, también puede ser alojado de forma remota en un servidor de seguridad RADIUS o TACACS+. Estos servidores remotos de seguridad autorizan a los usuarios de los derechos específicos mediante la asociación de atributos de valor (AV) pares, que definen los derechos con el usuario apropiado. AAA debe definir todos los métodos de autorización. (Guiza, 2010). Tal como en la autenticación, la configuración de

AAA autorización es definida por la lista de métodos de autorización y la posterior aplicación de esta lista a varias interfaces.

- **Contabilización:** AAA cuenta con un método de recolección y envío de información al servidor de seguridad, mismo que es utilizado para facturar, auditar y reportar los nombres de usuario, el tiempo de inicio y final, los comandos que se ejecutaron, la cantidad de paquetes enviados y el número de bytes. Contabilidad permite ejecutar el seguimiento de los usuarios con acceso a los servicios, también la cantidad de recursos que están utilizando. Al activarse AAA contabilidad y según el método de seguridad que se haya implementado, el acceso a la red del servidor informa la actividad del usuario a el servidor de seguridad de RADIUS o TACACS+ a manera de registros contables. Cada registro contable está formado por la contabilidad de pares AV, y es almacenado en el servidor de control de acceso. Estos datos se analizan para la gestión de la red, facturación del cliente o auditoría. (Guiza, 2010). De la misma forma que con la autenticación y autorización, la contabilidad AAA se configura mediante una lista denominada métodos de contabilidad con la posterior aplicación de esta lista a varios interfaces.

2.11.1 Beneficios AAA

AAA proporciona los siguientes beneficios:

- Incrementa la flexibilidad y control de la configuración de acceso.
- Escalabilidad.
- Cuenta con métodos de autorización estandarizados, como RADIUS, TACACS+ o Kerberos.
- Posee múltiples sistemas de backup.

AAA se ha diseñado para permitirle al administrador de la red la configuración dinámica del tipo de autenticación y autorización que se requiera, ya sea por línea o por servicio base. La definición del tipo de autenticación y autorización que se busca es realizada mediante la creación de listas de método y su posterior aplicación para determinados servicios o interfaces. La lista de método es el conjunto secuencial de datos que definen los métodos de autenticación utilizados para autenticar a los usuarios. (Guiza, 2010). Estas listas de método permiten designar uno o algunos de los protocolos de seguridad que se utilizarán para la autenticación, garantizando un sistema de copia de seguridad en caso de que el método inicial fallara.

El primer método de la lista es utilizado por el software, en caso de que ese método no responda, el software escoge el siguiente método de autenticación en la lista de métodos. Este proceso continúa hasta que se establezca una comunicación exitosa con un método de autenticación, o hasta que la lista se haya terminado, determinando la autenticación como un caso de falla.

2.11.2 Protocolo AAA: Diameter

El protocoloDiameter proporciona autenticación, autorización y contabilidad (AAA) en las redes 3G, IMS y 4G para aplicaciones como acceso a la red y la movilidad de datos. Los protocolos AAA conforman la base de la administración de servicios en la industria de las telecomunicaciones, por ejemplo, deciden los servicios a los que tiene permitido acceder un usuario, la calidad de servicio (QoS) y el costo. La denominación de “diámetro” es, en realidad” un juego de palabras de su predecesor, el protocolo RADIUS (autenticación remota telefónica de usuario de servicios). (F5 Networks, 2016).Diameter ha sido incluido en diversos organismos de normalización, como 3GPP y ETSTI, como base para las funcionalidades AAA en redes de próxima generación (NGN).

Diameter se desarrolló a manera de apoyo de las necesidades adicionales, como el control de políticas, reglas dinámicas, calidad de servicio, la asignación de ancho de banda, y los nuevos sistemas de tarificación. Ciertas mejoras en 4G, como la funcionalidad en tiempo real para transacciones, únicamente pueden ser manejadas con el protocolo Diameter. (F5 Networks, 2016)

Las ventajas del protocolo Diameter son:

- Escalabilidad ilimitada, misma que permite el crecimiento.
- Tolerancia a fallos, garantizando la entrega de mensajes.
- Transmisión segura de paquetes de mensajes Diameter.
- Transmisión confiable a través de TCP o SCTP.

2.11.3 Protocolo AAA: TACACS+

El Sistema de Control de Acceso de Control de Acceso a Terminal (TACACS) es un protocolo de seguridad que brinda validación centralizada de los usuarios que tratan de acceder a un enrutador o NAS. TACACS+ es la versión más reciente del protocolo original, proporcionando los servicios de autenticación, autorización y contabilidad (AAA). El protocolo TACACS+ proporciona información precisa de contabilidad y control administrativo sobre los procesos de autenticación, autorización y contabilidad. Este protocolo permite que el usuario TACACS+ solicite un control de acceso detallado, y que el proceso TACACS+ responda a cada componente de esa solicitud. TACACS+ usa el Protocolo de Control de Transmisión, TCP, para su transporte, proporcionando seguridad, cifrando el tráfico entre NAS y el proceso. El cifrado tiene como base una clave secreta que es conocida por el usuario y por el sistema (Juniper Networks, 2014).

2.11.3.1 Arquitectura TACACS+

De manera fundamental, TACACS+ proporciona los mismos servicios que RADIUS. En cada inicio de sesión, la autenticación en un NAS es verificada mediante un proceso TACACS+ remoto (ilustración 11). La autenticación TACACS+ utiliza tres tipos de paquetes, los de “inicio” y los “continuar” suelen ser enviados por el usuario, mientras que los paquetes de respuesta son enviados por el proceso TACACS (Juniper Networks, 2014)

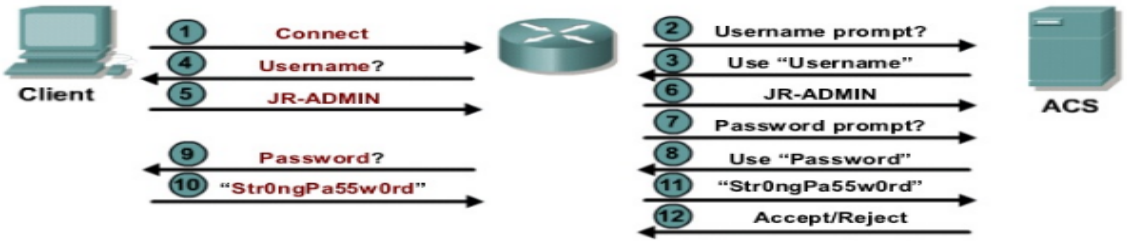


Ilustración 11. Autentificación Tacacs+.
Fuente: http://image.slidesharecdn.com/chapter3overview-121008145637-phpapp02/95/ccna-security-chapter-3-37-728.jpg?cb=1349708426

Cuando TACACS + establece una conexión TCP con el host TACACS +, es enviado un paquete Start; entonces el host de TACACS + responde con un paquete de Respuesta, mismo que otorga o rechaza el acceso, informa de un error o desafía al usuario.

2.11.4 Protocolo AAA: RADIUS

Remote Authentication Dial-In User Server, RADIUS, se desarrolló inicialmente por Livingston Enterprises en 1991 y posteriormente publicado en las RFC 2138 y 2139. En la actualidad está definido por la RFC 2865 para autenticación y autorización; y en la 2866 para contabilización. Este protocolo se utiliza para el control de acceso a la red y se ha implementado en dispositivos tales como routers, switch y servidores (Escalona, 2011). Proporciona autenticación centralizada, autorización y manejo o contabilización de cuentas (AAA). Este sistema de seguridad garantiza el acceso remoto a las redes y sus servicios contra el acceso no autorizado.

2.11.4.1 Arquitectura RADIUS

Como se puede observar en la ilustración 12, al realizarse la conexión con el punto de acceso WIFI se envía un nombre de usuario y una contraseña en lugar de una clave de red típica. Esta información es transferida a un servidor RADIUS sobre el protocolo RADIUS. El servidor se encarga de comprobar que la información del usuario sea correcta, dando uso a los esquemas de autenticación como PAP, CHAP o EAP. Si el usuario es aceptado, el servidor autoriza el acceso al sistema del dispositivo, ya sea un ordenador, Smartphone, Tablet, entre otros; además se le asigna los recursos de red que necesita para establecer la conexión, como la dirección IP y puerta de enlace (Ramírez, 2012).

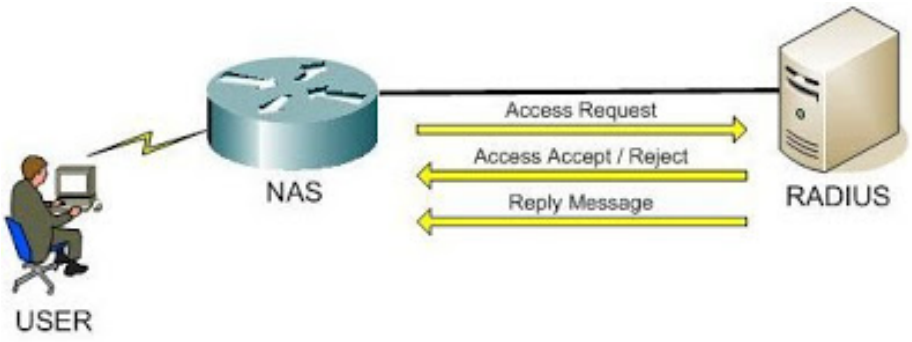


Ilustración 12. Componentes RADIUS
Fuente: (Novoa, 2013)

RADIUS está formado por tres componentes:

- Un protocolo con formato de trama, mismo que utiliza el protocolo de datagramas de usuario (NAS).
- Servidor (RADIUS)
- Cliente (SUPLICANTE

2.11.4.2 Principales características

- Su funcionamiento se realiza bajo el modelo cliente – servidor, dado que precisan un cliente RADIUS que puede ser un NAS, mismo que interactúe con los

servidores RADIUS. La información del usuario, nombre y contraseña, es transmitida por los clientes a los servidores, mismos que reciben las solicitudes de conexión de usuarios y se encargan de autenticar y otorgarle la información de configuración necesaria al cliente RADIUS, con el fin de ofrecerle al usuario el servicio deseado.

- Ofrece un nivel limitado de seguridad en la red ya que, aunque las comunicaciones entre el cliente y el servidor son validadas mediante un secreto compartido que no se envía por la red, solo se encripta la clave del usuario en los paquetes de solicitudes de acceso desde el cliente al servidor, utilizando el método de encriptación MD5. El resto del paquete no está encriptado pudiendo ser objeto de captura el nombre de usuario, servicios autorizados y la contabilización de estos.
- Los servidores RADIUS soportan varios esquemas de autenticación de usuario como EAP (Extensible Authentication Protocol), PAP (Password Authentication Protocol) y CHAP (Challenge Handshake Authentication Protocol) además de varios orígenes de información como una base de datos del sistema (/etc/passwd), o una base de datos interna (del propio servidor RADIUS), mecanismos PAM y otros como Active Directory, LDAP y Kerberos.
- Es un protocolo de la capa de aplicación que utiliza UDP como transporte. Los puertos oficialmente definidos por la IANA (Internet Assigned Numbers Authority) son el 1812 para la autenticación y el 1813 para la contabilización, pero están los puertos 1645 y 1646 no oficiales, pero ampliamente usados en implementaciones de servidores y clientes RADIUS.
- Capacidad para el manejo de sesiones, notificando el inicio y cierre de conexión, permitiéndole al usuario determinar su consumo y facturar en consecuencia; esta

constituye una de las características fundamentales de este protocolo. (Portilla, 2011).

2.12 Método de autentificación

Al enviarse una solicitud por un usuario o un equipo al servidor de acceso a la red (NAS) para obtener el acceso a una red en particular, generalmente se envía un nombre de usuario y una contraseña. Esta información es transmitida al dispositivo NAS mediante los protocolos de la capa de enlace como PPP, que redirige la solicitud a un servidor RADIUS sobre el protocolo RADIUS solicitando el acceso a la red (ilustración 13). El servidor RADIUS comprueba que la información es correcta haciendo uso de algunos de los esquemas de autenticación mencionados anteriormente, dependiendo del mismo servidor RADIUS. (Escalona, 2011)

El servidor entonces devuelve una de las tres respuestas siguientes:

- Acceso aceptado: Una vez que el usuario se ha autenticado, el servidor RADIUS le asigna los recursos de red como dirección IP y otros parámetros y a menudo comprobará que el usuario está autorizado a utilizar el servicio de red solicitado.
- Reto de acceso: En esta respuesta se le solicita al usuario cierta información adicional, tal como PIN, una contraseña secundaria; o pueden emplearse diálogos de autenticación entre el usuario y el Server RADIUS por medio del uso de túneles seguros entre ellos, ocultando las credenciales de acceso para el servidor.
- Acceso rechazado: El rechazo puede darse por distintas razones, ya sea porque la cuenta del usuario esté desactivada o sea desconocida, o por proporcionar una prueba no válida de identificación. (Escalona, 2011)

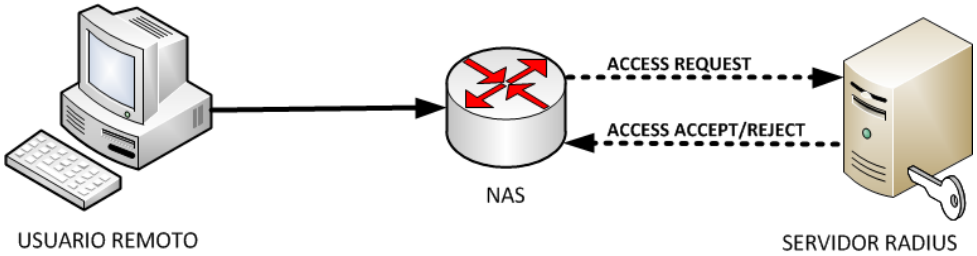


Ilustración 13. Funcionamiento RADIUS.
Fuente: (Simal, 2012)

Cuando ya se ha garantizado el acceso a la red y los recursos que esta ofrece, se puede transmitir información e inicia el proceso de contabilización de uso de los servicios asignados al usuario. En este proceso se registran los datos del usuario, tales como identificación, dirección IP, punto de conexión y un identificador de sesión único. Estos datos se actualizan de manera continua mientras la sesión está activa, del mismo modo se procede al terminar la misma. (Escalona, 2011). Este proceso se enfoca a la facturación del usuario por el uso del servicio, aunque los datos recopilados pueden ser empleados para fines estadísticos.

2.13 Tipos de servidores de autentificación

En la actualidad existe una variedad de servidores de tipo Radius, tanto comerciales como de código abierto, en los cuales varían las prestaciones desde el modo de configuración hasta el entorno gráfico. De todas maneras, cualquier variedad cumple con los objetivos de gestionar a los usuarios basados en archivos de texto, bases de datos, librerías. La tabla 6 muestra algunos servidores de autentificación:

Tabla 6. *Comparación entre servidores de autenticación*

	S.O	802.1x	Libre
AS Windows	Windows	TLS, PEAP Y LEAP	No
Tekradius	Windows	MD5, PEAP y TLS	No
EmeraldV5	Windows	PEAP, TTLS y LEAP	No
Odyssey	Windows	MD5, TLS, PEAP, TTLS y LEAP	No
RAD-Series	Windows	MD5, TLS, PEAP, TTLS y LEAP	No
Steef – Belted	Windows	MD5, TLS, PEAP, TTLS y LEAP	No
Freeradius	Linux	MD5, TLS, PEAP, TTLS y LEAP	Si

Fuente: (Didac, 2013)

2.13.1 TEKRADIUS (Radius server para Windows)

TekRADIUS es el servidor RADIUS para Windows que cuenta con el servidor DHCP incorporado. TekRADIUS se prueba en Microsoft Windows XP, Vista, Windows 7/8 Y Windows 2003/2008/2012 server. TekRADIUS cumple con RFC 2865 y RFC 2866. Además, posee dos ediciones: la primera, apoya a Microsoft SQL Server, y la segunda, TekRADIUS LT, que soporta SQLite. Se ejecuta como un servicio de Windows e incorpora una interfaz de administración de Win32. (TekRadius, 2016).

Sus características más relevantes son:

- Es compatible con las características descritas en el RFC 2865 y RFC 2866 del protocolo RADIUS.
- Limita el número de sesiones simultáneas para los usuarios.
- Como elemento de comprobación RADIUS se utiliza el método de autenticación.
- Las bases de datos y tablas SQL pueden ser creadas a través de TRManager, interfaz gráfica de usuario.
- Los métodos de autenticación compatibles son: PAP, CHAP, MS-CHAP v1 y v2, EAP-MD5, EAP-TLS, LEAP, EAP-SIM, EAP-MS-CHAP v2, PAEP (PEAPv0-EAP-MS-CHAP v2), EAP-TTLS.
- Se encuentra incorporada en el servidor DHCP.
- Es posible especificar una fecha y hora de caducidad para los usuarios, además de los días y horas en los que el inicio de sesión será permitido. (TekRadius, 2016).

Para la instalación de este programa se necesita unos requerimientos mínimos que **se** muestran a continuación:

- Sistema Windows que cuente con 2 GBytes de RAM.

- Microsoft.NET Framework 4.0 Perfil del cliente
- (Min.)
- Espacio en disco de 10 Mbyte.
- Privilegios administrativos.

2.13.2 FREERADIUS (Radius server para Software Libre)

FreeRADIUS es un paquete de distribución en software libre Linux de código abierto, que implementa diversos elementos concernientes con RADIUS, por ejemplo, una biblioteca BSD para clientes, módulos para soporte en apache, y lo más importante, un servidor Radius. (Duran, 2012)

El servicio de FreeRADIUS es modular, para facilitar su extensión, y es muy escalable, además de contar con otras buenas características como:

- Realización de trabajos AAA, al cual se podrá almacenar y acceder a la información por medio de múltiples bases de datos: LDAP (AD, OpenLdap,), SQL (Mysql, PostgreSQL, Oracle,) y ficheros de texto (fichero local de usuarios, mediante acceso a otros Reales, fichero de sistema /etc/passwd,).
- Soporta prácticamente toda clase de clientes Radius (por ejemplo, ChilliSpot, JRadius, mod_auth_radius, pam_auth_radius, Pyrad, extensiones php de RADIUS, etc).
- Se puede ejecutar en múltiples sistemas operativos: Linux (Debian, Ubuntu, Suse, Mandriva, Fedora Core, etc.), FreeBSD, MacOS, OpenBSD, Solaris, e incluso MS Windows por medio de cygwin.
- Soporta el uso de proxys y la replicación de servidores.

2.13.2.1 Ficheros FreeRADIUS

Radius utiliza el fichero "radiusd.conf" (ilustración 14) en el cual se puede encontrar y relacionar todos los aspectos del servidor (ficheros de log, parámetros de uso máximo, usuarios, grupos, etc), las bases de datos a utilizar para autenticar y autorizar (ficheros, SQL, LDAP, Samba) y sobre todo los métodos AAA. Para evitar una excesiva longitud este fichero, se subdivide en varios ficheros mediante la directiva "$INCLUDE" (Duran, 2012).

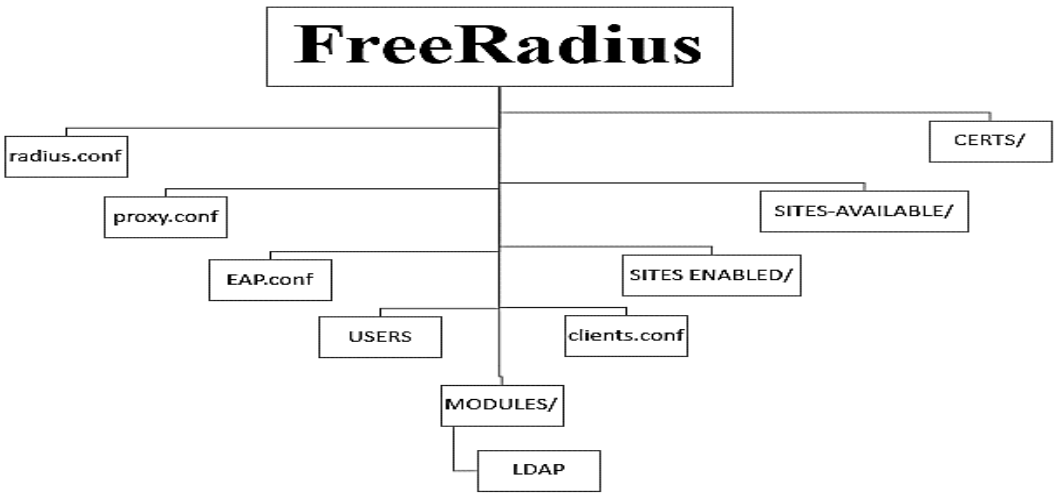


Ilustración 14. Ficheros FreeRADIUS.
Fuente: elaborado por el autor

Las características de cada una de los ficheros se describen en la tabla 7.

Tabla 7. Descripción de Ficheros FreeRADIUS

Fichero	Descripción
radius.conf:	Fichero principal, donde se encuentran especificaciones y directivas del servidor.
eap.conf:	Utilizado para configurar el tipo de EAP (extensible authentication Protocol) a emplear.
users	Fichero donde se podra indicar usuarios a permitir acceso. Todas las entradas se procesan en el orden en que aparecen en el archivo de usuarios.
clients.conf	Tiene la lista de clientes que están autorizados para usar los servicios de AAA proporcionados.
proxy.conf	Este fichero configura directivas relacionadas con el funcionamiento en modo proxy y la lista de realms.
ldap.attrmap	Fichero donde es la asignación de atributos de diccionario de RADIUS a los atributos de directorio LDAP. Para ser utilizado por el módulo de autenticación y autorización LDAP (rlm_ldap).
certs:	Es el directorio donde se guardarán los certificados que se vayan a usar o enlaces simbólicos de estos.

modules:	Directorio donde se encuentran los diferentes módulos que puede usar este servidor.
Otros ficheros como sql.conf (para configurar el acceso a bases de datos SQL), policy.conf, hints.conf, etc.	

Fuente: (Duran, 2012)

2.14 Servicio de directorios

"Directorio" es el término que se utiliza para referirse a la información contenida, el conjunto de hardware y software que gestiona esta información, las aplicaciones que usan esta información, entre otros. Entonces, se concluye que el Servicio de Directorio es el complejo conjunto de componentes que trabajan de forma organizada para prestar un determinado servicio. Estos directorios determinan la información que se almacena y la manera en la que se organiza, permitiendo localizar la información (Pradas, 2013).

2.14.1 BASE DE DATOS LDAP

Lightweight Directory Access Protocol, o Protocolo Ligero en Acceso a Directorios, es un protocolo de tipo aplicación que permite el acceso a un servicio de directorio ordenado y distribuido, que se utiliza para buscar información diversa en un entorno de red. Entre las ventajas que tiene sus aplicaciones es: la autenticación de usuarios basado en Radius controlando el acceso a una red, garantiza además una lectura rápida de los registros asegurando que cada uno de ellos sea único, permite crear múltiples directorios independientes y de forma jerárquica para asignación de privilegios, sencillo de instalar y mantener. (Acosta, 2013).

Ilustración 15. Funcionamiento LDAP.
Fuente: http://somebooks.es/wp-content/uploads/2015/01/cap11v2-001.png

Según (Pradas, 2013) el esquema de interacción entre el cliente y el servidor LDAP (ilustración 15) sigue el siguiente orden:

1. El cliente establece la sesión con el servidor LDAP, indicándole el puerto en el que el servidor LDAP está escuchando. También puede proporcionar información de autenticación o establecer una sesión anónima.
2. El cliente realiza las operaciones sobre los datos, mientras LDAP le otorga capacidades de búsqueda, lectura y actualización.
3. Al terminar las operaciones, el cliente cierra sesión.

2.15 Software libre

Se define como aquel software el cual respeta la libertad de los usuarios y la comunidad para ejecutar, copiar, distribuir, estudiar, modificar y mejorar el código fuente del mismo. (ilustración 16). Es quiere decir que los usuarios tanto individualmente como en forma colectiva, controlan el programa fuente, las características funcionales del SO, y todo lo que hace el mismo (Mejía, 2016).

Ilustración 16. Versiones Software Libre
Fuente: https://sites.google.com/site/isp60seminario3lemosleandro/software/soft-x-licencia

2.15.1 Sistema Operativo Debian GNU/Linux

Se trata de una distribución del sistema operativo LINUX, la cual es muy utilizada debido a su estabilidad. En los sistemas Debian se usa el núcleo de Linux o de FreeBSD, el cual lo hace un sistema operativo completamente libre. Por otra parte, Debian se encuentra disponible para la mayor parte de arquitecturas como son PowerPc, x86 (32 y 64 bits), 68k. System Z, entre otras, la cual puede ser ejecutada en la mayoría de equipos que actualmente existen en el mercado. Ideal para servidores por su robustez y facilidad de instalación (Debian, s.f.).

Debian incluye 4 tipos de escritorio: KDE, GNOME XFCE y LXDE, y cuenta con más de 43000 paquetes (software precompilado y empaquetado en un formato amigable para una instalación sencilla en su máquina), un gestor de paquetes (APT), y otras utilidades que hacen posible gestionar miles de paquetes en miles de ordenadores de manera tan fácil como instalar una sola aplicación (Debian, s.f.).

2.15.2 Sistema operativo servidor (Ubuntu Server)

Ubuntu forma parte de una distribución de software libre basada en Debian GNU/Linux, que ofrece un sistema operativo preferentemente enfocado a ordenadores de escritorio, aunque también proporciona soporte para servidores. Ubuntu está focalizado

en la facilidad de uso, la libertad en la restricción para el uso del mismo, sus lanzamientos regulares (cada 6 meses) y sobre todo su facilidad de instalación (Sánchez, LinuxZone, 2012).

Entre las principales características de Ubuntu Server destacan:

- Disponible en arquitecturas: x86, AMD64 o ARM.
- Las versiones estables se liberan cada 6 meses y se mantienen actualizadas en materia de seguridad hasta 18 meses después de su lanzamiento.
- El entorno de escritorio oficial es GNOME.
- Para labores/tareas administrativas en terminal incluye una herramienta llamada sudo (similar al Mac OS X), con la que se evita el uso del usuario root (administrador).

2.15.3 Sistema operativo CentOs

El Community ENTerprise Operating System (CentOs), forma parte del sistema operativo de Linux en software libre. Este un sistema operativo de fuente abierta, basado en la distribución Red Hat Enterprise Linux, el cual estuvo predestinado a ser un sistema de programación con empresarial completamente libre. CentOs es robusto, estable y fácil de instalar y utilizar con su escritorio por defecto GNOME, el cual se opera de forma similar al RHEL (CentOs, s/f)

CentOs soporta la mayoría arquitecturas disponibles en el marcado como Intel x86-compatible (32 bit), (Intel Pentium I/II/III/IV/Celeron/Xeon, AMD K6/II/III, AMD Duron, Athlon/XP/MP),Intel Itanium (64 bit),Advanced Micro Devices AMD64(Athlon 64, etc) e Intel EM64T (64 bit),PowerPC/32 (Apple Macintosh PowerMac corriendo sobre procesadores G3 o G4 PowerPC),IBM Mainframe (eServer zSeries y S/390) (CentOs, s/f).

2.15.4 Sistema operativo Zeroshell

Zeroshell es una distribución Linux para servidores y dispositivos integrados destinados a proporcionar los servicios de red principal de una LAN requiere. Está disponible en forma de Live CD o de imagen de Compact Flash y se puede configurar y administrar utilizando el navegador web. Las principales características de esta distribución de Linux para aplicaciones de red se enumeran a continuación (Zeroshell, s/f):

- Zeroshell implementa la funcionalidad de Portal Cautivo en forma nativa, sin necesidad de utilizar otro software específico NoCat o Chillispot.
- Servidor proxy de HTTP que es capaz de bloquear las páginas web que contienen virus.
- Enrutador con rutas estáticas y dinámicas (RIPv2).
- Servidor RADIUS para proporcionar una autenticación segura y la gestión automática de las claves de cifrado para el Wireless 802.11b, 802.11g y 802.11a redes que soportan el protocolo 802.1x en el EAP-TLS, EAP-TTLS y PEAP forma o la autenticación menos segura del cliente de dirección MAC, WPA con TKIP y WPA2.
- Servidor Syslog para la recepción y catalogación de los registros del sistema producido por los hosts remotos, incluidos los sistemas Unix, routers, switches, puntos de acceso Wi-Fi, impresoras de red y otros compatibles con el protocolo syslog.
- LDAP, NIS y RADIUS autorización.
- X509 entidad emisora de certificados para la emisión y gestión de certificados electrónicos.

2.15.5 Sistema operativo Pfsence

Se trata de un software de código abierto y distribución gratuita personalizada de FreeBSD bajo la licencia Apache 2.0, el cual fue adaptado específicamente para su uso como un Firewall y Router el cual es gestionado en su totalidad a través de la interfaz web. Además de ser un cortafuego potente, flexible y plataforma de enrutamiento, incluye otras funcionalidades importantes como (PfSence, s/f):

- Network Address Translation (NAT)
- Multi-WAN
- VPN que puede ser desarrollado en IPsec, OpenVPN y en PPTP
- Servidor PPPoE
- Servidor DNS
- Portal Cautivo
- Servidor DHCP

Capítulo III: Situación Actual de la Red Inalámbrica de la FICA

Para este capítulo se identificará el estado actual y el desempeño de la red inalámbrica existente dentro de la facultad, mediante la recolección de información.

3.1 Ubicación

La Universidad Técnica del Norte (ilustración 17) se encuentra situada en la ciudad de Ibarra, provincia de Imbabura, perteneciente a la República del Ecuador. Pertenece a la Región 1, zona norte del País, Imbabura, Carchi, Norte de Pichincha, Esmeraldas y Sucumbíos (Departamento de Informática UTN, 2010).

Ilustración 17. Campus UTN "El Olivo".
Fuente: http://www.utn.edu.ec/web/uniportal/?page_id=2015

3.2 Facultad de Ingeniería en Ciencias Aplicadas (FICA)

"La Facultad de Ingeniería en Ciencias Aplicadas, educa, investiga, promueve el conocimiento, la cultura y el desarrollo; forma profesional de alta calidad académica, humanística y competitiva, con valores y principios." (FICA, 2016). En el presente periodo la facultad cuenta con un número de estudiantes, personal docente y administrativo definido en la tabla siguiente.

Tabla 8. *Usuarios FICA en el periodo marzo 2017 – agosto 2017*

Estudiantes por Carreras	Total
Ingeniería en Electrónica y Redes de Comunicación	372
Ingeniería en Mecatrónica	350
Ingeniería en Sistemas Computacionales	331
Ingeniería Industrial	235
Ingeniería Textil	210
Ingeniería en Mantenimiento Eléctrico	248
Ingeniería en Mantenimiento Electromotriz	364
Total de estudiantes matriculados	**2110**
Personal Docente por Carreras	
Ingeniería en Electrónica y Redes de Comunicación	25
Ingeniería en Mecatrónica	22
Ingeniería en Sistemas Computacionales	22
Ingeniería Industrial	20
Ingeniería Textil	16
Ingeniería en Mantenimiento Eléctrico	16
Ingeniería en Mantenimiento Electromotriz	16
Total de docentes	**137**
Personal Administrativo por Carreras	
Ingeniería en Electrónica y Redes de Comunicación	1
Ingeniería en Mecatrónica	1
Ingeniería en Sistemas Computacionales	2
Ingeniería Industrial	1
Ingeniería Textil	1
Ingeniería en Mantenimiento Eléctrico Ingeniería en Mantenimiento Electromotriz	1
Otros (Decanato, Secretario abogado, laboratorios)	10
Total de Personal Administrativo	**17**

Fuente: Información recolectada por el personal administrativo de cada carrera en el periodo marzo 2017 – agosto 2017

3.3 Metodología de la investigación

3.3.1 Tipo de investigación

Para poder determinar el nivel de disponibilidad de la red ficawifi se realizó un estudio descriptivo y propositivo.

3.3.2. Área de estudio

El estudio se realizó en la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte en el PERIODO MARZO 2017 - AGOSTO 2017.

3.3.3 Universo

El universo lo constituyen los 2110 estudiantes matriculados legalmente, 137 docentes y 17 de personal administrativo pertenecientes a las carreras de Ingeniería en Electrónica y Redes de Comunicación (CIERCOM), Ingeniería Mecatrónica (CIME), Ingeniería en Sistemas Computacionales (CISIC), Ingeniería en Mantenimiento Eléctrico (CIMANELE), Ingeniería en Mantenimiento Automotriz (CIMANAU), Ingeniería Industrial e Ingeniería Textil, dando un total de 2264 usuarios.

3.3.4 Cálculo de la muestra

La muestra determina un subconjunto del universo. Suárez (2012) afirma que "para calcular el tamaño de la muestra suele utilizarse la fórmula propuesta por Fisher y Navarro (1994) la cual establece lo siguiente:" (ecuación 1)

$$n = \frac{Z^2 \sigma^2 N}{e^2(N-1) + Z^2 \sigma^2}$$

Ecuación 1. Determinación de la muestra
Fuente: (Suárez, 2012)

Donde:

n = tamaño muestra.

N = Universo.

Ơ=Desviación estándar (0,5)

Z = confianza que varía en 90% (1.64), 95% (1.96) y el 99% (2.75), valores que quedan a criterio del encuestador.

e = Límite aceptable de error que varía entre el 1% (0,01) y 10% (0,1), el cual dependerá del investigador.

Se aplica la formula correspondiente de la muestra, para poder determinar el número de encuestas a realizarse dentro de la facultad, donde se tomó los valores de:

N = 2264 → Estudiantes, Docentes y Personal Administrativo de la Facultad.

Z= 1.64 → Confianza del 90% debido a que "cuanto más pequeño sea el intervalo de confianza, más precisa será la estimación." (Rodriguez, 2015)

e= 0.1 → Error muestral del 10%, debido a que mayor margen de error requiere menor muestra.

0,5 → Desviación estándar de valor constante.

$$\boldsymbol{n = \frac{(1.64)^2 * (0.5)^2 * 2264}{(0.1)^2(2264 - 1) + (1.64)^2(0.5)^2}}$$

$$\boldsymbol{n = 66}$$

3.3.5 Criterio de inclusión

Se incluirá a los estudiantes, docentes y personal administrativo de sexo masculino y femenino de la facultad en el periodo MARZO 2017 - AGOSTO 2017.

3.3.6 Criterios de encuesta y entrevista

En la tabla 9 se muestra los objetivos planteados para poder formular las preguntas de la encuesta y la entrevista.

Tabla 9. Objetivos de encuesta y entrevista

Encuesta	Entrevista
Determinar el grado de aceptación de la red inalámbrica para los usuarios de la red inalámbrica de la facultad.	Determinar el desempeño y el funcionamiento de la red inalámbrica por parte del administrador de la misma.
Determinar los tipos de inconvenientes que se presentan con mayor frecuencia.	Determinar los inconvenientes que se presentan en la red en base a datos obtenidos mediante pruebas de conectividad, pruebas de consumo de ancho de banda, test de velocidad, ping por parte del administrador de red

Determinar horas pico para fallas de conexión a la red.	Conocer la distribución del ancho de banda para la red inalámbrica y el número aproximado de usuarios que pueden conectarse a la misma.
Determinar el tipo de información que manejan los usuarios al hacer uso de la red inalámbrica.	Conocer el tipo seguridades inalámbricas que posee la red.
Determinar el número de dispositivos con los que acceden a la red.	Conocer las posibles mejoras que puedan implementarse dentro de la red para su mejor funcionamiento.

Fuente: Elaborado por el Autor.

3.3.7 Técnicas e instrumentos a utilizar

Para este trabajo investigativo se realizó una encuesta con 5 preguntas cerradas (Anexo A) y una entrevista con 6 preguntas abiertas y cerradas (Anexo B), al administrador actual de la red, con el fin de identificar la situación actual de la misma; cuyos resultados nos permitirán resolver posibles fallas existentes y de esta manera poder alcanzar los objetivos planteados.

3.4 Interpretación y análisis de resultados

Se realiza la interpretación de resultados con sus respectivos análisis en el Anexo C de este trabajo investigativo.

3.5 Descripción de la red inalámbrica

El aumento de dispositivos electrónicos ha provocado falencias en la red, tanto en el desempeño como en disponibilidad, debido a las configuraciones deficientes de los equipos y a su baja administración; algunos AP no son capaces de soportar los numerosos usuarios que se encuentran dentro de la Facultad de Ingeniería en Ciencias Aplicadas (FICA).

La facultad cuenta con un ancho de banda de 90 Mbps (50/40 bajada-subida) de salida a internet en su puerto LAN, la cual es distribuida a través de 15 APs mediante la red

denominada ***ficawifi***, como se muestra en la ilustración 18, la cual es administrada desde el cuarto de equipos de la misma. Para poder acceder a esta red, se ha implementado un Hotspot para todos los usuarios (ilustración 19), mismo que no cuenta con mecanismos de autentificación, ni cifrado.

Ilustración 18. SSID "ficawifi"
Fuente: Hotspot Mikrotik

Ilustración 19. Hotspot "ficawifi".
Fuente: Hotspot Mikrotik

El Hotspot implementado maneja 2 perfiles, una para estudiantes con un AB = 5Mbps para subida/bajada, la cual al ser compartida con varios usuarios a la vez (40 – 100) aproximadamente provoca inconvenientes en la navegación (ilustración 20). El otro perfil que se maneja es para docentes y cuenta con un AB=10 Mbps subida/bajada para un total de 137 docentes.

Ilustración 20: Test de velocidad
Fuente: www.speedtest.net

3.6 Equipamiento

La Facultad de Ingeniería en Ciencias Aplicadas posee una infraestructura de red inalámbrica robusta para controlar y dar accedo a la misma sin embargo los equipos y dispositivos de la misma no son aprovechadas al máximo por lo que aún se tiene falencias en rendimiento y disponibilidad.

Los equipos que conforman la infraestructura de red inalámbrica se describen en la tabla 10 que se muestra a continuación:

Tabla 10. *Equipos para Wlan FICA*

Cant	Equipo/Marca	Modelo	Estado	Os	Frec
15	Access Point Mikrotik	Router BOARD cAP-2n	Funcional	Mikrotik RouterOS WISP AP (Level 4) license	2.4 GHz
1	Switch de Core Cisco	Catalyst 4506E	Funcional	cat4000−I5S−M	
1	Router Mikrotik	RB1100AHx2	Funcional	MikroTik RouterOS, Level 6 license	
1	Switch de distribución QPCOM	1240-R	Funcional	No administrable	

Fuente: Centro de datos de la Facultad de Ingeniería en Ciencias Aplicadas

3.6.1 Infraestructura de la red inalámbrica en Data Center FICA

Todos los servicios de red los provee el Departamento de Desarrollo de Informático y Tecnológico de la Universidad Técnica del Norte (DDTI) a través de un cable de fibra

óptica 62.5/125 µm de 6 hilos, el cual está conectado a un switch marca Cisco Catalyst 4506- E. Desde el puerto 30 del switch CORE se conecta un cable de par trenzado STP categoría 6, enganchando al puerto 13 de un router marca Mikrotik serie RB1100AH para proveer conectividad a internet en sus 12 puertos restantes (ilustración 21)

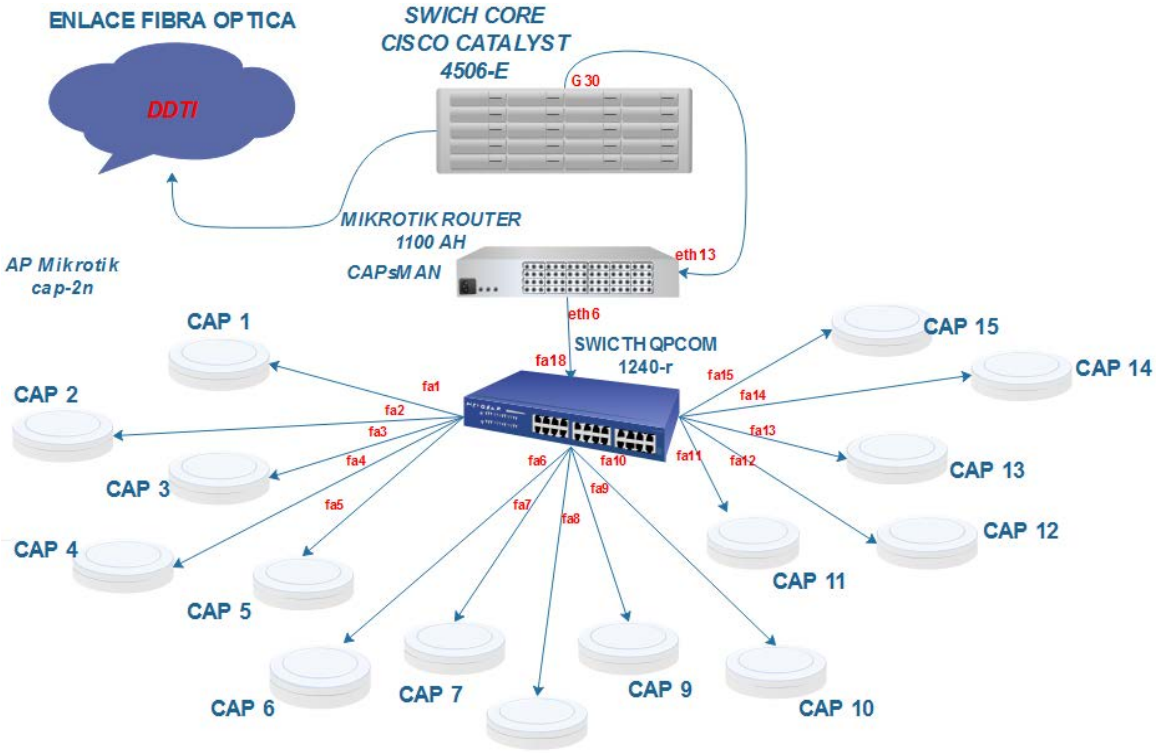


Ilustración 21. Infraestructura red inalámbrica "ficawifi".
Fuente: Elaborado por el Autor

3.6.2 Configuración inicial de equipos CAP y CAPsMAN

La red inalámbrica de la facultad lo constituyen 15 Access Point marca Mikrotik configurados en modo CAP (Controlled Access Point) y conectados a un switch de capa 2 no administrable marca QPCOM desde los puertos 1 al 15. Estos AP se encargan de proveer conectividad a los equipos finales. La gestión de dichos CAP se la realiza a través del servidor Mikrotik el cual se encuentra configurado en modo CAPsMAN (Controlled Access Point system MANager). El CAPsMAN soporta un total de 32 interfaces y permite autentificación MAC vía Radius.

En la ilustración 22 se puede constatar el estado inicial de un CAP en la red ***ficawifi,*** el ingreso se lo hace vía MAC, esto debido a una mala asignación de IP, donde se verifica que se está trabajando con otra mascara de red en eth1, por tal motivo el AP no gestiona y el CAPsMAN no lo reconoce.

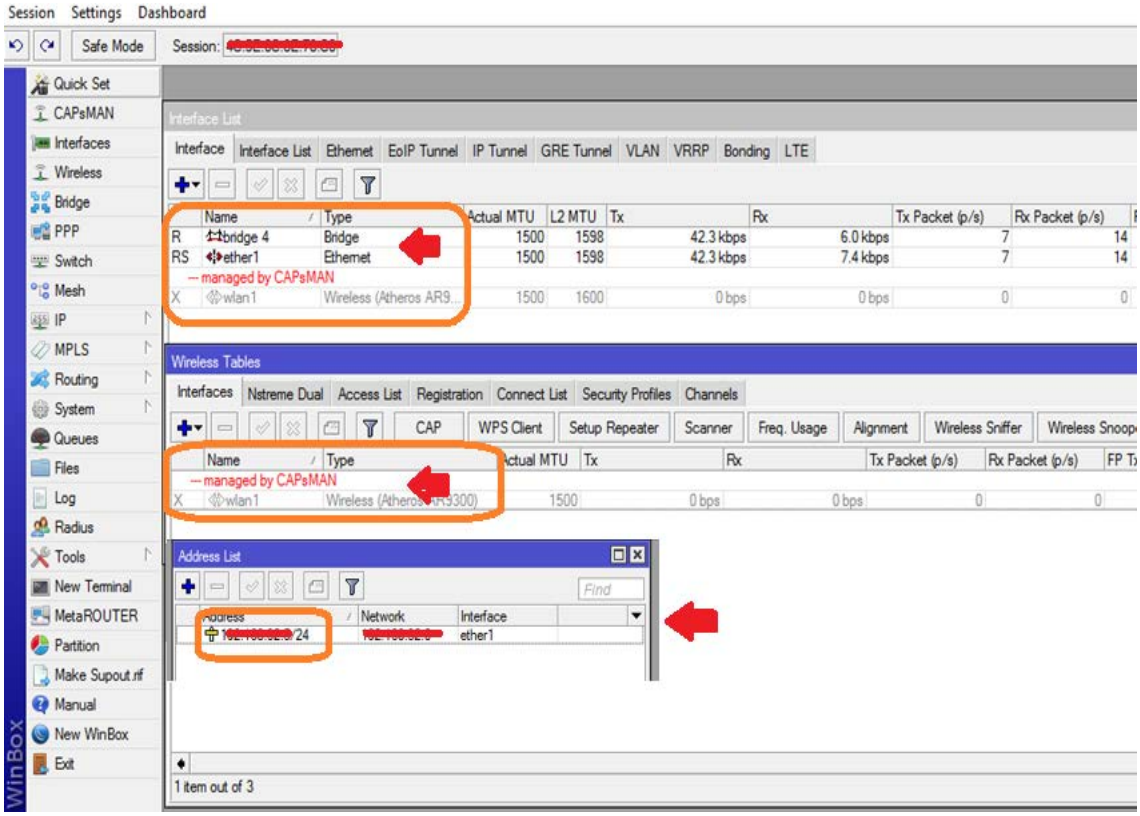


Ilustración 22. Configuración inicial CAP
Fuente: Mikrotik

En la ilustración 23 se observa la interfaz del CAPsMAN, el cual contiene el estado de todos sus CAP, los cuales se describen como:

- **RSMB:** Running Slave Master Bound, el cual nos indica que el CAP está operativo, gestionando usuarios o trasmitiendo paquetes de datos.
- **SMB:** Slave Master Bound, el cual indica que dicho CAP esta funcional, pero sin trasmitir ningún tipo de dato.
- **MI:** Master Inactive, el cual indica que no existe una propagación de información desde el CAP, esto debido a una mala configuración del CAP o por que se encuentra apagado.

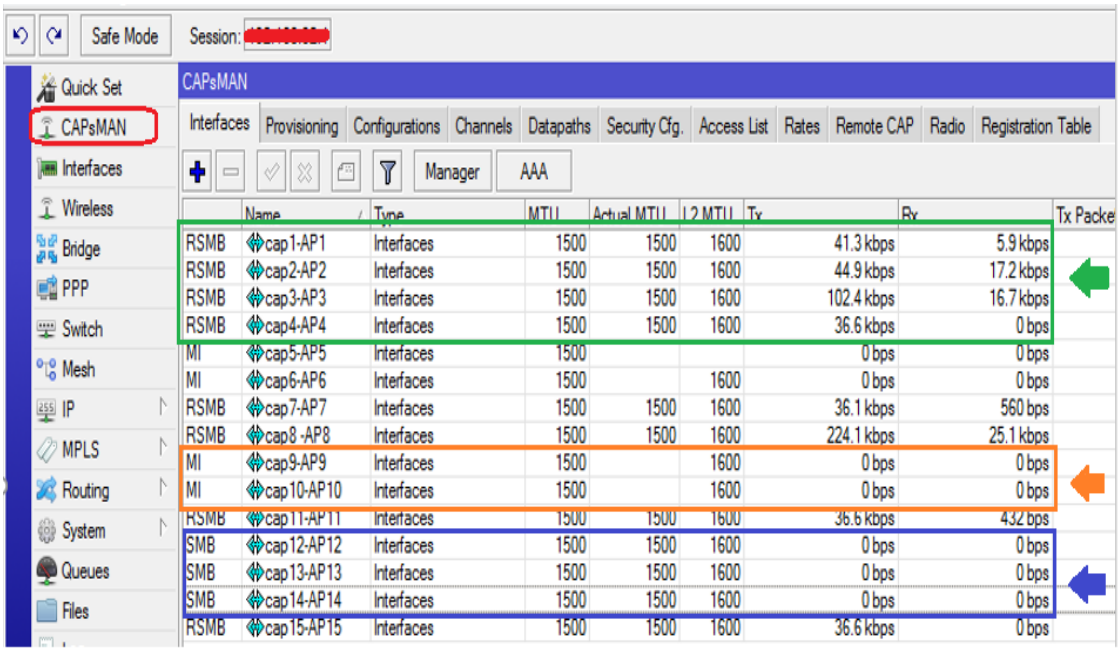


Ilustración 23. Configuración inicial CAPsMAN
Fuente: Mikrotik

3.7 Descripción técnica de equipos

3.7.1 Access point MikroTik cAP – 2n

El access point cAP – 2n fue el primer AP de techo que trabaja a 2.4 GHz. Su diseño es exclusivo para empresas de hospitalidad como hoteles, aeropuertos, centros comerciales debido a que se mezcla debidamente con el ambiente (ilustración 24).

***Ilustración* 24.** cAP - 2n.
Fuente: Extraído de https://routerboard.com/RBcAP2nD

El cAP 2n tiene compatibilidad con 802.11b / g / n y puede ser alimentado por PoE (alimentación a través de Ethernet). En la tabla 11 se puede observar sus especificaciones (Anexo F).

Tabla 11. *Especificaciones técnicas cAP - 2n*

Código Producto	RBcAP2nD
RAM	64 MB
10/100 puertos Ethernet	1
Estándares Wireless	802.11b/g/n
Dimensiones	185mm diameter, 31mm heigh
OS	RouterOS
Licencia nivel	4
Ganancia de la antena DBI	2
Almacenamiento	16 MB

Fuente: https://routerboard.com/RBcAP2nD

3.7.2 QP-COM switch 24 puertos – 1240R

Se trata de un switch capa 2 no administrable de 24 puertos 10/100/1000 Mbps (ilustración 25), compatible con funciones de auto-negociación es decir los equipos ya sean PC's, servidores, switches, routers, etc, cooperan entre sí y acuerdan emplear una velocidad y un dúplex (half o full) concreto y la función MDI-X, el cual elimina la necesidad de cables específicos, ya sean estos cruzados o pin-a-pin, conectando el receptor y el transmisor a ambos hilos del par. Gracias al estándar Gigabit Ethernet el receptor sabe qué es lo que está enviando el transmisor. Además de cumplir con el estándar IEEE802.3x para el control de flujo de datos en modo Full Dúplex (Anexo G).

Ilustración 25. QPCOM SWITCH 24 PUERTOS
Fuente: Extraído de http://qpcom.com.co/Portals/116/QP-1240R_espanol.pdf.

3.7.2.1 Características

- Cumple con las especificaciones de los estándares IEEE 802.3 10Base-T Ethernet, 802.3u 100 Base-TX Fast Ethernet, 802.3ab 1000Base-T.

- Switch Ethernet con auto negociación de velocidad 10/100/100 Mbps de 24 puertos.
- Ofrece la velocidad de 1000 Mbps solo en modo Full Dúplex.
- Genera automáticamente direcciones MAC.
- Control de flujo para Full Dúplex (IEEE 802.3x)
- Función contrapresión para el modo de operación Half Dúplex 10/100 Mbps.
- Green Ethernet.

En la tabla 12 se puede observar las especificaciones técnicas requeridas.

Tabla 12. Especificaciones técnicas switch QPCOM

Estándares	IEEE 802.3 10Base-T, 802.3u, 100Baste-TX, 802.3ab 1000Base- T, 802.3x Flow Control
Tasa de transmisión	10/100 Mbps en modo Half Dúplex 10/100/1000 Mbps en modo Full Dúplex
Método de transmisión	Almacenar y enviar (Store and forward)
Control de flujo	IEEE 802.3x (Full Dúplex)
Puertos	24 puertos RJ-45 con auto negociación de velocidad 10/100/1000 Mbps (Auto- MDI/MDIX)
Medio de red	10BASE-T: UTP Categoría 3 o superior. 100BASE-TX: UTP Categoría 5 o superior. 1000BASE-T: UTP Categoría 5 o superior.
Método de acceso	CSMA/CD
Dimensiones	445mm x 120 mm x 45 mm

Fuente: Extraído de http://qpcom.com.co/Portals/116/QP-1240R_espanol.pdf.

3.7.3 Router MIKROTIK RB1100AHx2

Se trata de un enrutador Gigabit Ethernet de rack 1U, cuenta con una CPU de doble núcleo, el cual es capaz de alcanzar hasta un millón de paquetes por segundo, soportando cifrado de hardware (Anexo H). Cuenta con trece puertos Gigabit Ethernet individuales, dos grupos de conmutadores de 5 puertos e incluye capacidad de bypass Ethernet. Tiene 2 GB de RAM y una ranura para tarjeta microSD, un beeper y un puerto serial (ilustración 26).

Ilustración 26. RouterBoard Mikrotik 1100AH.
Fuente: Extraído de https://routerboard.com/rb1100ahx2

En la tabla 13 se puede observar sus especificaciones:

Tabla 13. *Especificaciones técnicas RouterBoard Mikrotik 1100AH*

Características	RB1100AHx2
Frecuencia nominal CPU	1 GHz
Tamaño RAM	2 GB
10/100/1000 Ethernet puertos	13
PoE	Si
Dimensiones	1U case: 44 x 176 x 442 mm, 1200g. Board only: 365g
OS	RouterOS
Licencia level	6
Puerto serial	RS232
Tamaño almacenamiento	128 MB

Fuente: Extraído de https://routerboard.com/rb1100ahx2

3.8 Distribución de AP's para la red inalámbrica

Todos los APs que conforman la red inalámbrica de la facultad se encuentran distribuidos de acuerdo al diseño de la ilustración 27, sin embargo, debido a los procesos de mejora continua que posee la universidad, uno de ellos fue reubicado de su sitio y en su lugar se colocó un AP marca Cisco el cual es gestionado por el Departamento de Desarrollo de Informático y Tecnológico de la Universidad Técnica del Norte.

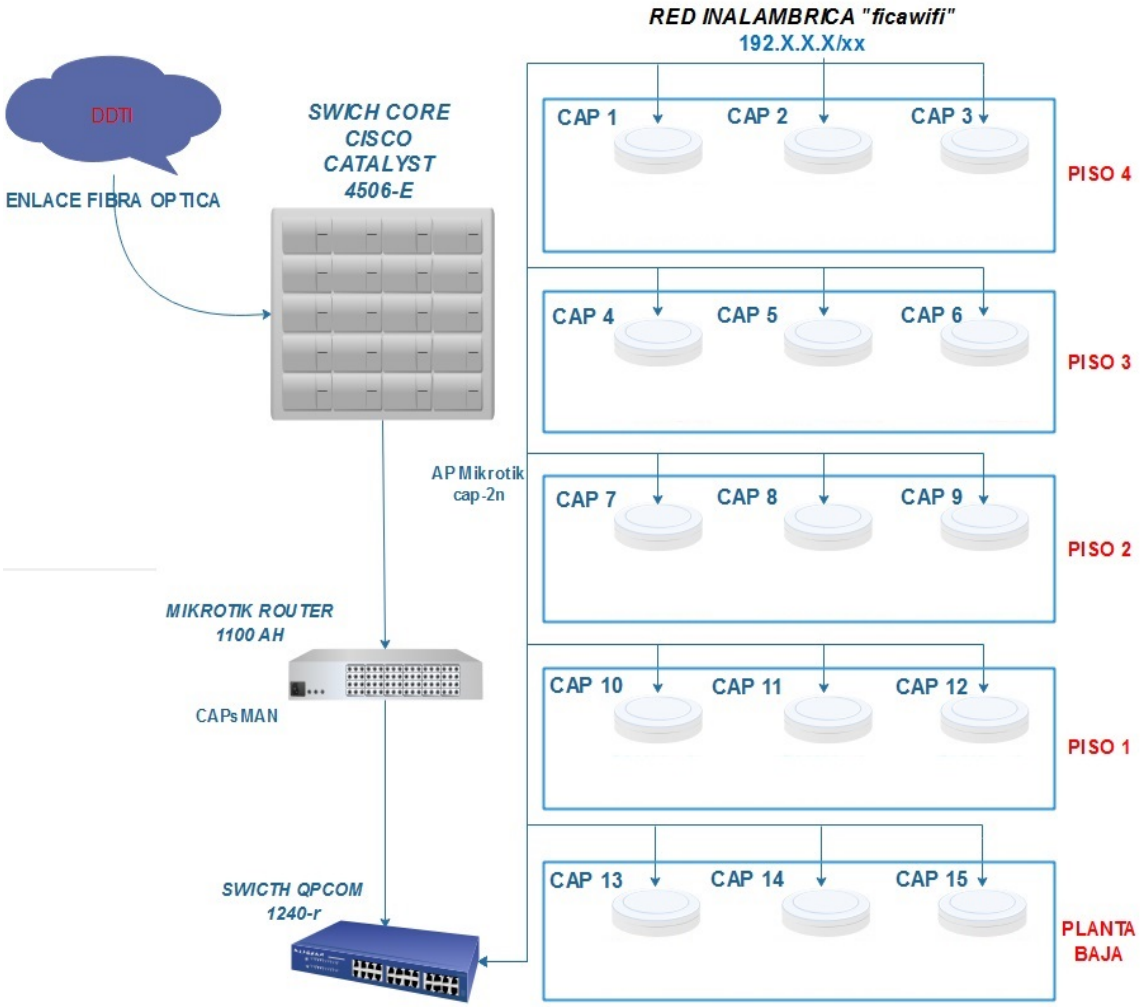


Ilustración 27. Distribución cAP-2n
Fuente: Elaborado por el Autor

Como se puede observar en el diseño de red tipo estrella, se han colocado 3 APs en cada uno de los pisos de la facultad para ofrecer una mayor cobertura de red. El Ap-3 fue reubicado dentro del cuarto de equipos (DataCenter FICA).

3.9 Distribución de canales en la red inalámbrica

Con la enorme propagación de dispositivos WiFi, tales como tablets, access point, routers, portátiles y Smartphones, el espectro radioeléctrico comienza a saturarse, lo que perjudica seriamente al rendimiento en las conexiones inalámbricas. La coexistencia de varias tecnologías inalámbricas (b, g y n) en las mismas frecuencias obliga a los dispositivos a adaptar su velocidad para asegurar la comunicación. En la actualidad existe un total de once canales en la banda de los 2.4 GHz donde sus frecuencias centrales se encuentran

separadas por 5Mhz, de los cuales solo tres no presentan solapamientos en el espectro radioeléctrico, permitiendo tener comunicaciones inalámbricas simultaneas sin sufrir interferencias significativas (Mengual, Garcia Villegas, & Vidal, 2013). Al poseer un gran número de APs mayores son las probabilidades de sufrir interferencias, siendo la solución más apropiada el cambio de canal como indica la ilustración 28.

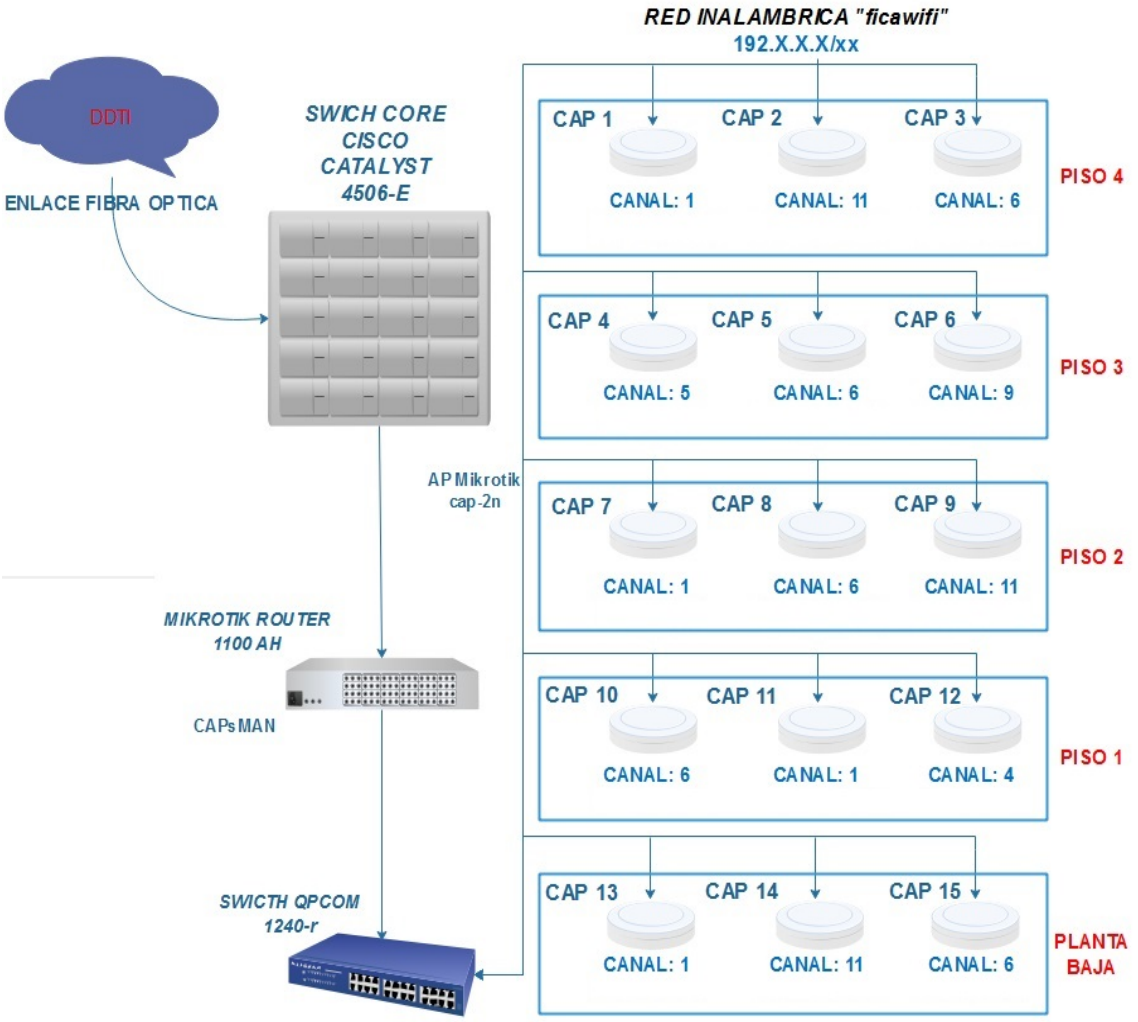


Ilustración 28. Distribución de canales.
Fuente: Elaborado por el Autor

Nota: Los canales más apropiados a utilizar fueron: canal 1 (2412MHz), canal 6 (2437MHz) y el canal 11 (2462MHz) sin embargo, al ser los más utilizados se encuentran saturados por otras redes, por lo tanto se utiliza también el canal 2 (2417MHz), canal 4 (2427MHz), canal 5 (2432MHz) y el canal 9 (2452MHz).

3.10 Direccionamiento IP de la red inalámbrica.

Para el direccionamiento Ip de los equipos, se cuenta con una ip fija del pool de direcciones privadas Clase B 172.17.42.0/24, la cual se conecta al puerto 13 del router Mikrotik (WAN), mientras que para la red LAN se cuenta con un pool de direcciones privadas Clase C 192.168.32.0/22 en cual será distribuido en la red inalámbrica de la facultad (ilustración 29).

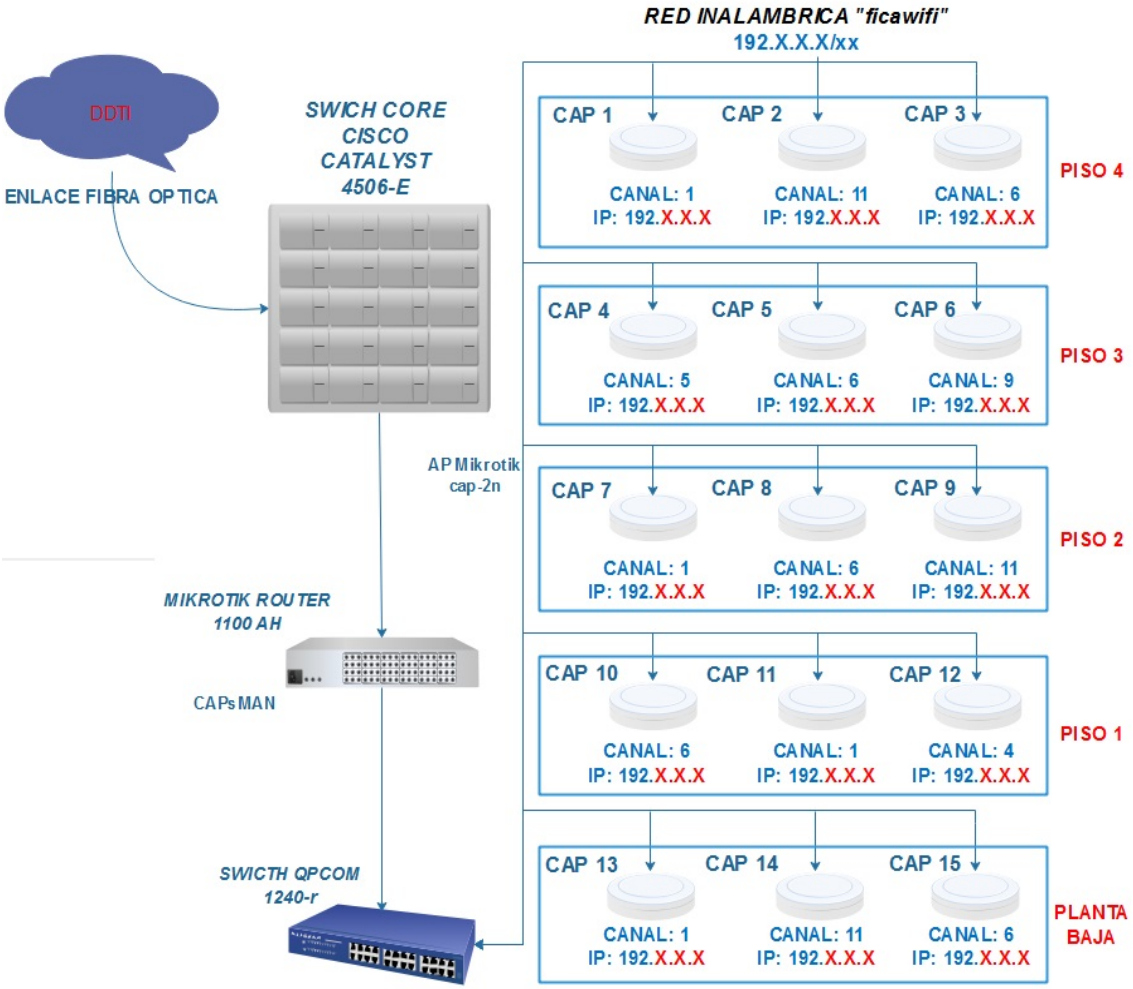


Ilustración 29. Direccionamiento IP – "ficawifi"
Fuente: Elaborado por el Autor

Capítulo IV: Diseño de la infraestructura con soporte AAA

En este capítulo se procederá a establecer requerimientos tanto en software como en hardware para la posterior implementación de un servidor de autentificación con soporte AAA.

4.1 Descripción de la problemática existente

La problemática que se identificó en el levantamiento de la situación actual, es tratar de disponer un sistema centralizado que permita de manera más eficiente, realizar un acceso controlado y de forma segura hacia los recursos que posee la facultad conjuntamente con la universidad. Un punto importante a considerar es que se deberá contar con equipos modulares, que permitan realizar los cambios necesarios sin que esto afecte a los demás equipos o a su vez represente una reestructuración de todo el sistema.

Con la presente propuesta se tratará de suplir requerimientos necesarios para el buen uso de la red inalámbrica de la facultad, por tanto, se creará un servicio de autentificación con soporte AAA mediante software libre, el cual se encargará de realizar un control de acceso seguro a la red, y a su vez logre llevar un registro del desempeño de la misma. El software y hardware a elegirse deben contar con la capacidad y almacenamiento necesario para garantizar el correcto funcionamiento del sistema inalámbrico, y posteriormente deberán ser compatibles con los equipos que posee la facultad dando como resultado la optimización de los recursos.

4.2 Requerimientos del sistema

Para poder elegir los requerimientos necesarios para este proyecto, se tomará como referencia el estándar ISO/IEC/IEEE 29148:2011, el cual contiene lineamientos con relación a la ingeniería de requisitos, enfocados a los sistemas y productos de software y

servicios a lo largo de su ciclo de vida útil. (International Organization for Standardization, 2011)

Dicho estándar define la construcción de un buen requisito, el cual proporcione atributos y características teniendo en cuenta la aplicación iterativa del ciclo de vida del sistema. El estándar ISO / IEC / IEEE 29148: 2011 se relaciona con procesos de requisitos de ingeniería y gestión de actividades descritas en las normas ISO / IEC 12207: 2008 e ISO / IEC 15288: 2008 (International Organization for Standardization, 2011). Las tablas mostradas a continuación se basan en las consideraciones propuestas por el estándar antes mencionado, los cuales contienen los requerimientos iniciales del sistema, requerimientos de arquitectura, así como también requerimientos para Stakeholder, con el fin de presentar de una manera más sencilla dicha información, permitiendo realizar la selección de software, hardware y algunos aspectos específicos para el diseño del servidor de autentificación AAA.

Cada tabla está diseñada con diferentes columnas en las cuales se identifica: el número del requerimiento, la descripción detallada del requerimiento, la prioridad de la misma, subdividida en Alta, Media y Baja; por último, se crea dos adicionales llamadas relación y verificación, que serán utilizadas solamente cuando algún requerimiento sea totalmente dependiente de otra.

La tabla 14 contiene los requerimientos iniciales del sistema y emplea la abreviatura SySR, en ella se define los límites funcionales, requerimientos de uso, interfaces, estados así como también los requerimientos físicos del sistema.

Tabla 14. *Requerimientos iniciales del sistema*

SySR				
#	REQUERIMIENTO	PRIORIDAD		
		Alta	Media	Baja
Requerimiento de Funciones				
SySR_1	El sistema no debe estar expuesto a altas temperaturas ni a humedad.	X		
Requerimiento de Uso				
SySR_2	El sistema debe poseer una conexión estable a internet para el buen funcionamiento del servicio.	X		
Requerimiento de Interfaces				
SySR_3	Se deberá ingresar a la plataforma vía web para poder configurar y gestionar el servicio.	X		
SySR_4	La visualización debe ser clara, con gráficas fáciles de comprender por el administrador del sistema.	X		
Requerimiento de Estados				
SySR_5	EL sistema depurara de su base de datos a todos los usuarios que ya no se encuentren matriculados legalmente, conjuntamente con aquellos que inicien el nuevo periodo académico.	X		
Requerimiento Físicos				
SySR_6	El sistema debe estar ubicado en un lugar exclusivo para servidores, el cual no interfiera con las actividades académicas de los estudiantes	X		

Fuente: Elaborado por el Autor

La tabla 15 que se muestra a continuación describen todos los requerimientos de hardware, software y eléctricos del sistema los cuales conforman la arquitectura del mismo y se denotará con la abreviatura SrSH. Esta tabla es de suma importancia debido a que estos requerimientos serán empleados al momento de seleccionar el software y hardware acorde para este trabajo investigativo.

Tabla 15. *Requerimientos de Arquitectura*

SrSH				
#	REQUERIMIENTO	PRIORIDAD		
		Alta	Media	Baja
Requerimientos de Software				
SrSH_1	Se requiere de sistema operativo de distribución libre, estable, actualizado y con entorno grafico agradable al usuario.	X		
SrSH_2	Se requiere de un software con soporte AAA (Radius server , Cliente Server) incorporado.	X		
SrSH_3	Se requiere de una base de datos (LDAP) incorporado.	X		
Requerimientos de Hardware				
SrSH_5	Se requiere una velocidad de procesamiento mínimo de 3.5 GHz, para una buena gestión del S.O a utilizar.	X		
SrSH_6	Se requiere de una capacidad de memoria RAM mínimo 2 GB para el procesamiento de los datos así como también 100 GB de espacio en disco duro.	X		
SrSH_7	Se requiere de 1 puerto GigabitEthernet para la transmisión de datos, uno para la entrada y otro para la salida de los mismos.	X		
SrSH_8	Se requiere compatibilidad para sistemas operativos en software libre o a su vez capacidad de virtualización.	X		
Requerimientos Eléctricos				
SrSH_9	Se requiere que el sistema funcione las 24 horas del día, por tanto debe poseer un banco de baterías.	X		

Fuente: Elaborado por el Autor

Por último, para finalizar la descripción de requerimientos se presenta la tabla 16, en ella se detalla los requerimientos de Stakeholders, es decir los requerimientos de todo grupo o individuo que tiene una estrecha relación para el resultado que se obtendrá con el desarrollo del proyecto, se especifican además los requerimientos operacionales y de usuarios. La abreviatura que se utilizará para esta tabla será StSR.

Tabla 16. *Requerimientos de Stakeholders*

StSR				
#	REQUERIMIENTO	PRIORIDAD		
		Alta	Media	Baja
Requerimientos de Stakeholders				
StSR_1	Todos los usuarios deberán estar legalmente matriculados para poder constar en la base de datos LDAP.		X	
StSR_2	El usuario dispondrá de un ancho de banda mínimo de 10M para subida y descarga de datos.	X		
Requerimientos Operacionales				
StSR_3	Se requiere de conexión física entre el servidor de autentificación, los AP's y el router para dar acceso al recurso.	X		
StSR_4	La información será almacenada en una base de datos por tanto se requiere que el software y hardware elegidos sean compatibles.	X		
StSR_5	Solo el administrador del servicio podrá modificar, leer, quitar o eliminar los datos de la base de datos LDAP.		X	
Requerimientos de Usuarios				
StSR_6	Solo se permitirá utilizar un máximo de 2 dispositivos electrónicos por estudiante (el cual podría variar según el administrador de red).	X		
StSR_7	Cada usuario dispondrá de un usuario y una contraseña única.	X		
StSR_8	El tiempo de conexión al recurso estará asignado por el administrador de toda la red según sea necesario.		X	

Fuente: Elaborado por el Autor

4.3 Selección del software y hardware para el servicio de autentificación.

Luego de tener claros los requisitos de todo el sistema, se procede a seleccionar el hardware y el software necesario para el buen funcionamiento del sistema. Para lo cual se procede a realizar una valoración de cada una de las posibles opciones en software libre que actualmente existe en el mercado, las opciones con mayor valoración serán utilizadas en la posterior implementación del sistema.

4.3.1 Selección de Software

Primero se dará lugar a seleccionar el software, esto debido a las características y requerimientos planteados anteriormente, en donde hay que tomar en cuenta que solamente se analizará software libre.

En la tabla 17 que se presenta a continuación se indica las opciones en software libre que actualmente están disponibles en el mercado, los requerimientos que fueron propuestos en la sección 4.2 del mismo, el cual se indicara con la abreviatura correspondiente a la tabla que hace referencia, y para finalizar se dispondrá de una valoración total donde se indica un cierto puntaje obtenido para cada uno de los distintos sistemas operativos propuesto. Para poder comprender los datos descritos en la tabla, se le ha asignado un valor: 1 en caso de que dicho software cumpla con el requerimiento y 0 si no cumple con el mismo, por último, se justificara el software elegido.

Para el caso del Sistema Operativo en software libre donde se montará un servidor Radius, se dispone de 5 distintos tipos de sistemas que se adaptan a los requerimientos antes señalados y se analizarán a continuación.

Tabla 17. *Selección de Software*

Tipo de Sistema Operativo	REQUERIMIENTOS (TABLA 15)			
	SrSH_1	SrSH_2	SrSH_3	Total
Ubuntu 12.04 server	0	1	1	2
CentOs 7.0	0	1	1	2
Debian 8.6	1	1	1	3
Zero Shell	0	1	0	1
Pfsence	0	1	1	2

1-Cumple
0-No cumple

Nota: Para la implementación del sistema AAA, se escoge el Sistema Operativo Debian 8.6**.**

Fuente: Elaborado por el autor

Según la tabla descrita anteriormente, el software que se escoge para este proyecto será una distribución de Linux denominada Debian. A diferencia de los demás tipos de sistemas operativos, Debian se encuentra en su versión más nueva y estable "8", lanzada el 25 de abril del 2015, y completamente funcional con soporte "8.6" denominada Jessie.

Entre sus características principales se puede decir que posee soporte para la mayoría de arquitecturas entre las cuales se tiene arm64, adaptación de 64 bits para sistemas ARM, PC de 32 bits («i386») y PC de 64 bits («amd64»), ARM de 64 bits («arm64»), PowerPC («powerpc»), IBM System z («s390x») entre las más destacadas, además de contar con muchas aplicaciones de escritorio y entornos. Entre otros ahora incluye el entorno de escritorio GNOME 3.14, KDE 4.11, Xfce 4.10, y LXDE.

La tabla 18 muestra los requerimientos mínimos necesarios para la instalación del sistema.

Tabla 18. *Requerimientos para la instalación del sistema operativo Debian Jessie*

Tipo de instalación	RAM (mínimo)	RAM (recomendado)	Disco duro
Sin escritorio	128 Megabytes	512 Megabytes	2 Gigabytes
Con escritorio	256 Megabytes	1 Gigabyte	10 Gigabytes

Fuente: Elaborado por el autor

Debian incluye alrededor de 43512 paquetes, entre los cuales uno denominado FreeRADIUS el cual nos brindara soporte AAA. La mayoría de estos paquetes no vienen instalados por defecto, cada paquete extra ser debe ser descargado y configurado manualmente vía consola mientras que a diferencia de Zero Shell y Pfsence todas las configuraciones se lo hacen a través de su propia interfaz web.

La tabla 19 muestra el requerimiento mínimo para la instalación de este paquete.

Tabla 19. *Requerimientos para la instalación de FreeRADIUS*

RAM (mínimo)	Procesador mínimo	Disco duro	Sistema Operativo
256 Megabytes	Pentium 2.1 GHz	80 Megabytes	Software libre

Fuente: Elaborado por el autor

Zero Shell posee una extensión LDAP, el cual no es incorporado dentro del sistema, por tanto, se ve la necesidad de poseer un servidor externo, provocando un desperdicio de recursos. A diferencia de Debian, entre sus miles de paquetes, posee uno denominado OpenLdap, la cual se encuentra en su última versión 2.4.40. Al igual que FreeRADIUS, el OpenLdap 2.4.40 debe ser descargado e instalado manualmente vía consola. Su administración se la llevara a cabo por medio de exploradores Ldap como por ejemplo “Apache Directory Studio”, “PhpLDAPadmin” y “JXplorer” (bastante potente y desarrollado en Java).

Todos estos diferentes sistemas operativos poseen diversos tipos de portales cautivos en los que se puede escoger para su uso tales como: PepperSpot (Linux), GRASE Hotspot (Linux), NoCatAuth (Linux), Chillispot (Linux), CoovaChilli (Linux), WifiDog (Linux), sin embargo, para este proyecto se utilizará el propio portal cautivo que nos ofrecen los dispositivos MikroTik 1100 y cAP2n, los cuales son compatibles con cualquier tipo de servidor Radius que se disponga.

4.3.2 Selección de Hardware

Para conocer cuál es la mejor opción de hardware se toma en cuenta dos aspectos fundamentales que son:

- La elección del software establecida en el punto anterior
- Los requerimientos ya analizados en la tabla 16

En la actualidad la Facultad de Ingeniería en Ciencias Aplicadas (FICA) cuenta con un DataCenter tipo TIER I, el cual alberga equipos de alta gama con marcar muy conocidas como son IBM, HP, CISCO, entre otras.

La tabla 20 muestra los equipos con almacenamiento disponible dentro del rack 2 del DataCenter FICA.

Tabla 20. *Servidores Disponibles DataCenter Fica*

MARCA MODELO		**HP Proliant DL360 G9**	**HP Proliant DL360 G9**	**HP Proliant DL360 G9**	**IBM System x3200 M2**	**IBM System x3250 M3**
CARACTERÍSTICAS	RAM	32 GB	32 GB	32 GB	2 GB	8 GB
	Procesador	Intel Xeon E5-2630v3 2.4GHz / 8-core	Intel Xeon E5-2630v3 2.4GHz / 8-core	Intel Xeon E5-2630v3 2.4GHz / 8-core	Intel Xeon (doble núcleo) 2,4 GHz	Intel Xeon E3-1200 series (quad-core) 3.5 GHz
	Disco duro	3x 450 GB	3x 450 GB	3x 450 GB	1 TB	500 GB
	Tarjeta de red	4x1 Gigabit Ethernet	4x1 Gigabit Ethernet	4x 1 Gigabit Ethernet	1 Gigabit Ethernet	2 x 1Gigabit Ethernet
	Sistema operativo compatible	Ubuntu Server 14.04 LTS	Ubuntu Server 14.04 LTS	CentOS 6.5	Ubuntu Server 14.04 LTS	Ubuntu Server 14.04 LTS
DIRECCIÓN IP		10.24.8.74/24 172.16.3.74	10.24.8.75/24 172.16.3.75	10.24.8.76/24 172.16.3.76	Sin asignar	Sin asignar
FUNCIÓN		Proyecto Cloud OpenNebula	Proyecto Cloud Eucalyptus	Proyecto Cloud OpenStack	DHCP Fica (inactivo)	Sin servicio

Fuente: Elaborado por el Autor

Como se puede observar en la tabla anterior, la facultad cuenta con equipos en marcas HP e IBM con disco duro disponible, tres de ellos de la marca HP son utilizados en

procesos de virtualización con plataformas Open Source dentro del Cloud, por tanto, para la selección de hardware se analizarán los dos equipos IBM restantes y se detallarán en la tabla 21; se realizará la valoración de cada uno tomando en cuenta que cumplan los requerimientos de hardware indicados con anterioridad. El formato de esta será igual al detallado en la selección de software.

Tabla 21. *Selección del Hardware*

Equipos	**Requerimientos (tabla 15)**				
	SrSH_5	SrSH_6	SrSH_7	SrSH_8	Total
IBM System x3250 M3	0	1	0	1	2
IBM System x3200 M2	1	1	1	1	4

1 – Cumple
0 – No Cumple
Nota: Para la implementación del sistema AAA, se escoge el equipo IBM System x3200 M2

Fuente: Elaborado por el autor

Para la implementación del presente proyecto se utilizará el equipo IBM System x3200, debido a que presenta una valoración mayor en los requerimientos SrSH_5, SrSH_6, SrSH_7, SrSH_8, el cual presenta las siguientes características:

- Procesador: Intel Xeon E3110 / 3 GHz Dual-Core.
- Memoria Cache: Hasta 6 MB.
- Capacidad máxima de memoria: Hasta 8 GB de memoria double data rate (DDR) II a 667 MHz.
- Almacenamiento interno máximo: Hasta 1,2 TB en unidades de disco duro SAS o hasta 2,0 TB en unidades de disco duro SATA.
- Puertos externos Parte frontal: Dos puertos USB, Parte trasera: Cuatro puertos USB, uno Ethernet; dos series; uno paralelo, puertos de ratón y teclado.
- Características de seguridad: Contraseña de encendido, contraseña de administrador.

- Los sistemas operativos soportados : Microsoft® Windows® Server 2003 Standard Edition/Enterprise, Edition, Windows Small Business Server 2003, Red Hat Enterprise Linux®, SUSE Linux Enterprise Server, Novell NetWare, IBM operating system 4690.

4.3.3 Diseño del Sistema

Mediante el análisis de la información recolectada en los dos puntos anteriores se logró definir algunas directrices enfocadas al correcto diseño y funcionamiento del sistema. A continuación, se presentan los criterios que se tomaran en cuenta para el desarrollo e implementación del sistema de autentificación.

- El objetivo principal del sistema es tratar de brindar al administrador una gestión centralizada de usuarios para la red inalámbrica, por medio de un servidor de autentificación Radius con soporte AAA.
- Mediante la utilización de software libre, se instalarán los paquetes necesarios para poder gestionar la información en una base de datos (Ldap) y el ingreso será exclusivo de todos los estudiantes, docentes y personal que trabaje dentro de las instalaciones, el cual exigirá al usuario autentificarse para poder ingresar a la red.
- Debido a que el Router 1100 MikroTik registra los denominados “cookies”, el administrador de red podrá verificar la cantidad de usuarios que se conectan a la misma, el estado de la red, el tráfico que genera entre otras funciones, mediante herramientas propias del mismo.

Como parte del diseño del sistema se presenta a continuación la estructura jerárquica de la base de datos LDAP y el diagrama de bloques que guiara el funcionamiento y procesos para autentificar a un usuario y que este a su vez pueda utilizar el recurso.

4.4 Estructura jerárquica base de datos LDAP FICA

La estructura de la base de datos que se implementará en la facultad y albergará a los usuarios de la red fica-wifi, se encuentra en un orden jerárquico como se muestra en la ilustración 30.

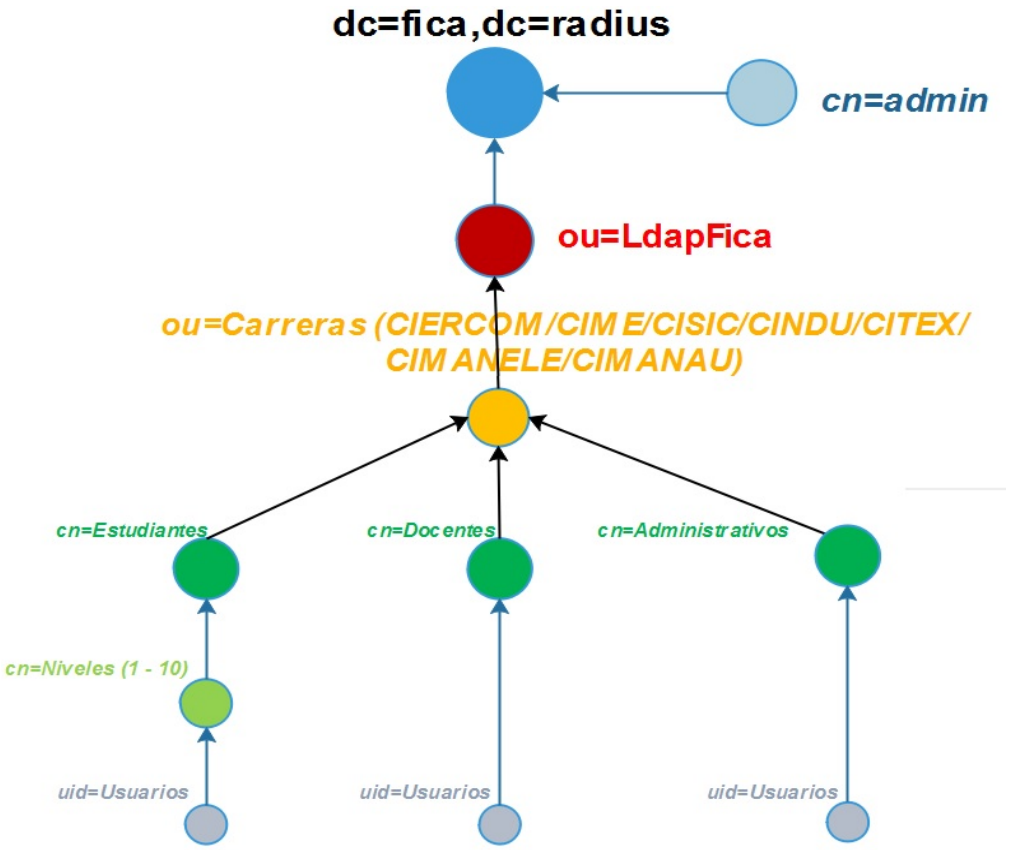


Ilustración 30. Estructura jerárquica de la Base de Datos LDAP FICA
Fuente: Elaborado por el autor

De acuerdo a la anterior, los componentes que conforman la base de datos LDAP son los siguientes:

- **dc: Componente de Dominio,** es decir el dominio a la que pertenece nuestra LDAP, que en este caso es dc=fica,dc=radius.
- **ou: Unidad Organizativa**, los cuales son todos los subdominios de estructura LDAP, los cuales constituyen las diferentes carreras que son: ou=CIERCOM, ou=CIME,ou=CISIC,ou=CITEC,ou=CINDU,ou=CIMANELE,ou=CIMANAU), las cuales a su vez poseen sus propios subdominios denominados: Estudiantes, Docentes y Administrativos

- **cn: Nombre Común,** grupos de Dependencias, es decir los diferentes niveles que posee cada carrera, es decir de primero a decimo.
- **uid: ID de usuario**, correspondiente a sus nombres completos para su identificación.

4.5 Diagrama de funcionamiento del sistema

El diagrama de bloques que se muestra en la ilustración 31, presenta las fases de funcionamiento del sistema, el cual estará formado por 4 bloques que serán detallados a continuación. Se deberá tomar en cuenta que dichos bloques serán referentes solo a los usuarios que dispongan de una cuenta almacenada en la base de datos, por lo que el proceso que deben seguir para utilizar el recurso se basa solamente en establecer conexión a la red.

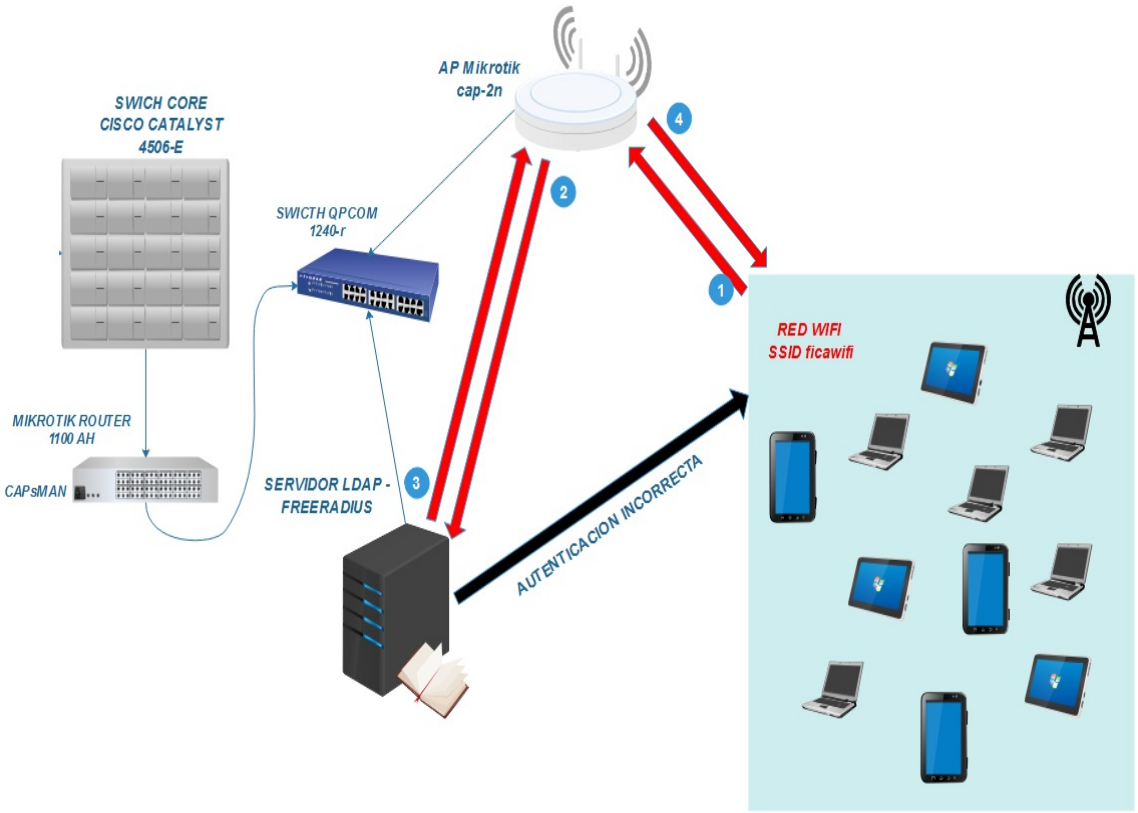


Ilustración 31. Diagrama de funcionamiento del sistema.
Fuente: Elaborado por el autor

4.5.1 Bloque 1 (Petición)

En primer lugar, se da inicio al bloque 1, en este bloque un estudiante desea acceder al recurso de la facultad mediante la red inalámbrica, para lo cual utilizará un dispositivo electrónico personal, buscará la red denominada ficawifi y establecerá conexión con dicha red introduciendo su usuario y contraseña previamente registrado en LDAP.

4.5.2 Bloque 2 (Autentificación)

Una vez que el usuario estableció una conexión con la red, se procede a efectuar el bloque 2, el punto de acceso redireccionará las credenciales (user/Password) directamente al servidor RADIUS para que sean autenticadas. En caso de que no estén registradas en la base de datos LDAP no se concederá la autorización para acceder a la red y no efectuara el establecimiento de una dirección ip.

4.5.3 Bloque 3 (Autorización)

En caso que las credenciales del usuario sean correctas, el servidor Radius autorizará al cliente al acceso a la red, comunicando al punto de acceso que el usuario se encuentra dentro de su base de datos y tiene permisos.

4.5.4 Bloque 4 (Registro)

El punto de acceso, a través del protocolo DHCP, enviará la dirección IP, mascara, puerta de enlace y DNS al cliente para que este pueda acceder a la red ficawifi.

4.6 Topología Física y lógica del sistema

Una vez que se logró determinar los requerimientos de software / hardware, conjuntamente con el modo de funcionamiento del sistema, se procede a diseñar la topología física y lógica de la misma, presentada en la ilustración 32.

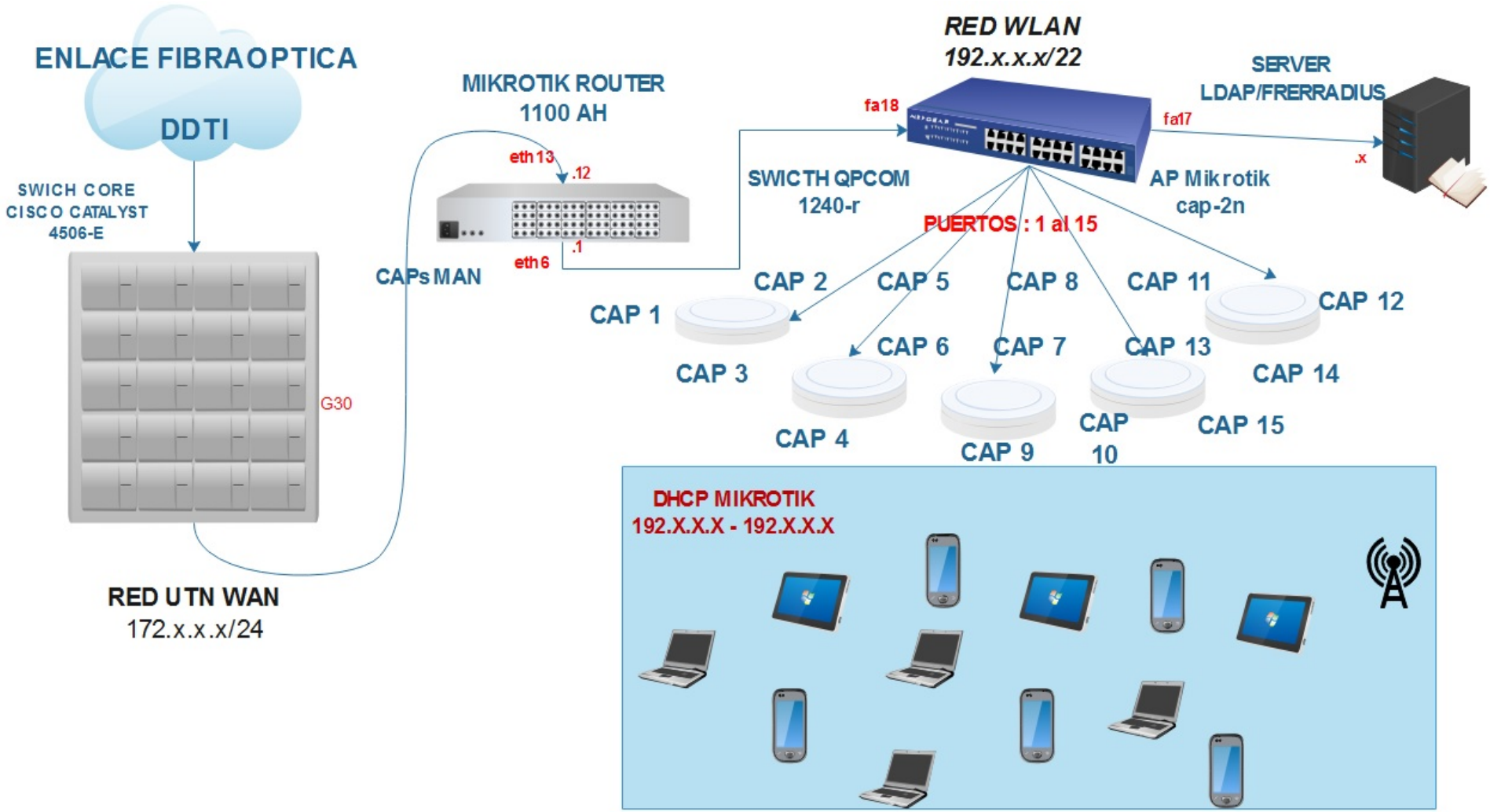


***Ilustración* 32** Topología final del sistema.
Fuente: Elaborado por el autor

Capítulo V: Implementación Servidor Radius

En este capítulo se procederá a la instalación y configuración del servicio de autentificación con soporte AAA.

5.1 Instalación del Sistema Operativo Debian 8.6

A continuación, se muestra los pasos para la instalación del sistema operativo en distribución libre denominada Debian Jessie 8.6.

- Como primer paso se debe bootear el equipo que se escogió en el apartado 4.3.2 del mismo, que cumplirá con la función de servidor.
- Desde la unidad óptica DVD-ROM, se insertará el CD que contiene los paquetes de instalación del mismo, se escogerá el tipo de entorno que se va a utilizar para instalar dicho sistema, como muestra la ilustración 33.

***Ilustración* 33.** Entornos de Instalación Debian 8.6.
Fuente: Debian 8.6 - Jessie

- Se establece una contraseña de superusuario ROOT (ilustración 34). Dicho superusuario posee el permiso para poder configurar todos los servicios necesarios del sistema, debe contener un gran nivel de seguridad por lo que se empleara letras, signos y números para asegurar que el sistema no sea invadido por terceros.

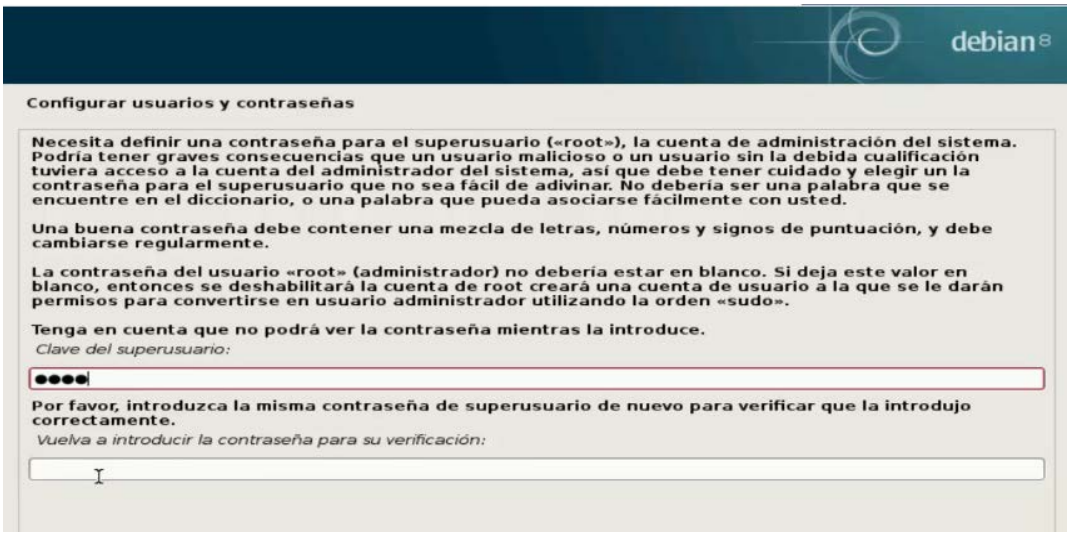


***Ilustración* 34.** Contraseña ROOT.
Fuente: Debian 8.6 - Jessie

Una vez que se ha instalado y probado el sistema operativo, se procede a descargar e instalar todos los paquetes necesarios para levantar el servicio FreeRADIUS y la base de datos LDAP, en el ANEXO D se muestra con mayor detalle el proceso de instalación y configuración.

Un paso previo que se debe realizar, será actualizar la lista de paquetes disponibles mediante las instrucciones que se muestran a continuación, para lograr obtener la versión más actual de los programas a ejecutar.

#apt-get update (*Actualiza los paquetes)*
#apt-get upgrade (*instala los paquetes actualizados)*

5.2 Configuración de red

Se procede a configurar la red ingresando al fichero interfaces, para ello ejecutar el comando ***nano /etc/network/interfaces*** y agregar los siguientes campos:

- Address: “Direccion ip del servidor”
- Netmask: “Mascara de red”
- Network: “Red”
- Broadcast:
- Gateway:

5.3 Instalación LDAP

Adicionalmente se instala un paquete extra (ilustración 35), con el comando ***#apt-get install slapd ldap-utils,*** para la configuración de nuestro servidor.

Ilustración 35. Instalación Ldap-Server
Fuente: Servidor OpenLdap

Nos pedirá una contraseña del administrador LDAP con su correspondiente verificación (ilustración 36).

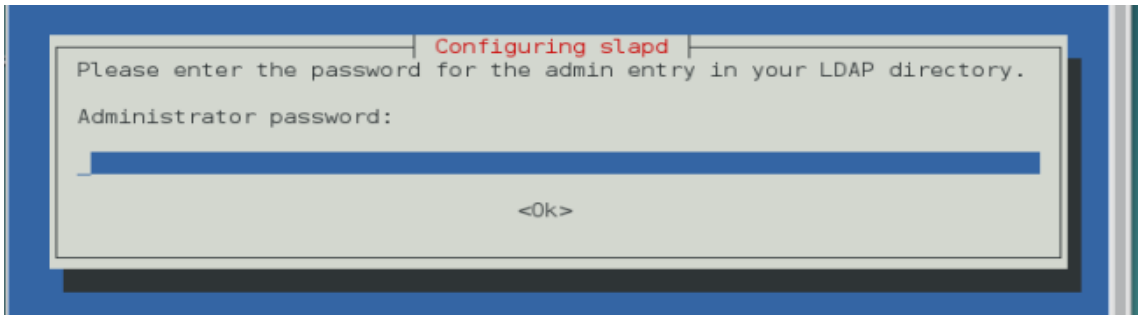


Ilustración 36. Contraseña Administrador LDAP.
Fuente: Servidor OpenLdap

Una vez terminado la instalación de los dos paquetes, se procede a activar los certificados como se muestra en el anexo D. El método de autenticación EAP-TTLS no nos obliga a crear una autoridad de certificación, aunque sí se necesitaría tener un certificado de servidor. Para disponer de dicho certificado se tendrá varias opciones:

1. Usar el certificado que se crea automáticamente al instalar FreeRADIUS.
2. Crear un certificado autofirmado.
3. Crear nuestra propia autoridad de certificación, con la que genera dicho certificado.

Una vez activado los certificados de autentificación EAP-TTLS, se procede a configurar nuestra base de datos LDAP.

5.3.1 Reconfiguración LDAP

El primer paso que se hará es verificar si se ha creado nuestro árbol LDAP dentro del sistema, para lo cual se digita el comando ***#slapcat*** como muestra la ilustración 37. Se puede observar que se encuentran dos objetos ya creados, uno conformado por el nodo raíz del árbol LDAP (dn=debian-server, dc=com) y el otro el nodo de administrador con su propio dominio (cn=admin, dn=debian-server, dc=com).

```
root@debian:/etc/freeradius# slapcat
dn: dc=debian-server,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: debian-server.com
dc: debian-server
structuralObjectClass: organization
entryUUID: 5c38c070-7200-1036-8940-5dbd8fa54a0e
creatorsName: cn=admin,dc=debian-server,dc=com
createTimestamp: 20170118193049Z
entryCSN: 20170118193049.016432Z#000000#000#000000
modifiersName: cn=admin,dc=debian-server,dc=com
modifyTimestamp: 20170118193049Z

dn: cn=admin,dc=debian-server,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9bnBDZHZ5eGNKeUR3UGtvR0hFeGdWRmlsUFJJNUU5NEQ=
structuralObjectClass: organizationalRole
entryUUID: 5c392bd2-7200-1036-8941-5dbd8fa54a0e
creatorsName: cn=admin,dc=debian-server,dc=com
createTimestamp: 20170118193049Z
entryCSN: 20170118193049.019073Z#000000#000#000000
modifiersName: cn=admin,dc=debian-server,dc=com
modifyTimestamp: 20170118193049Z
```

Ilustración 37. Objetos LDAP.
Fuente: Servidor OpenLdap

Se debe cambiar el domino por defecto dc=example, dc=com, para lo cual se ingresa al directorio ***/etc/phpldapadmin/config.php***, donde se comenta la línea que se muestra en la ilustración 39, para que el sistema busque automáticamente el dominio.

```
$servers->setValue('login','bind_id','cn=admin,dc=radius,dc=fica');
```

Ilustración 38. Fichero phpldapadmin/config.php.
Fuente: PhpLdapAdmin

Una vez que se modificó el fichero ***config.php,*** se procede a borrar los ficheros de configuración inicial de LDAP, los cuales se encuentran en el directorio ***/var/lib/ldap***, para esto se utilizará la línea de comando siguiente:

#rm /var/lib/ldap/*.mdb

Con esto se asegura que la reconfiguración que se realizó con el comando ***dpkg-reconfigure slapd*** surja efecto; en donde se siguen los siguientes pasos:

1. Desea omitir la configuración del servidor OpenLdap: **<NO>**
2. Introducir el nombre del dominio: **utn**
3. Introducir nombre de la organización: **fica.radius**
4. Introducir una contraseña para Ldap y con su confirmación: ******
5. Motor de base de datos a utilizar: **MDB**
6. Borrar la base de datos cuando se purgue el paquete slapd: **<SI>**
7. Permitir protocolo LDAPv2: **<NO>}**

Al finalizar nos mostrara un mensaje exitoso sobre la creación del árbol LDAP, la cual se confirma con el comando ***#slapcat*** nuevamente. (ilustración 39).

```
root@debian:/var/lib/ldap# slapcat
dn: dc=radius,dc=fica
objectClass: top
objectClass: dcObject
objectClass: organization
o: radius.fica
dc: radius
structuralObjectClass: organization
entryUUID: f0d5277a-7929-1036-800e-8fd47a20625d
creatorsName: cn=admin,dc=radius,dc=fica
createTimestamp: 20170127221605Z
entryCSN: 20170127221605.849599Z#000000#000#000000
modifiersName: cn=admin,dc=radius,dc=fica
modifyTimestamp: 20170127221605Z

dn: cn=admin,dc=radius,dc=fica
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9dDl4eDFIN3o1NlpTU0ErVTBoWUF6QytmTXJRZ3ViVUk=
structuralObjectClass: organizationalRole
entryUUID: f0d5ab64-7929-1036-800f-8fd47a20625d
creatorsName: cn=admin,dc=radius,dc=fica
createTimestamp: 20170127221605Z
entryCSN: 20170127221605.853030Z#000000#000#000000
modifiersName: cn=admin,dc=radius,dc=fica
modifyTimestamp: 20170127221605Z
```

Ilustración 39. Verificación árbol LDAP.
Fuente: Servidor OpenLdap

5.3.2 Schema para usuarios FICA

El servidor freeradius incluye por defecto schema en la instalación, entonces se procede a copiar el archivo de su directorio original al directorio del servidor OpenLDAP con el comando ***cp /usr/share/doc/freeradius/examples/openldap.schema /etc/ldap/schema/UsuariosLdapUTN.schema*** como indica la ilustración 40.

Ilustración 40. Fichero schema.
Fuente: Servidor OpenLdap

El siguiente paso es crear un archivo temporal dentro de ***/tmp/*** como muestra la ilustración 41, dentro de la cual se insertarán las siguientes líneas de código:

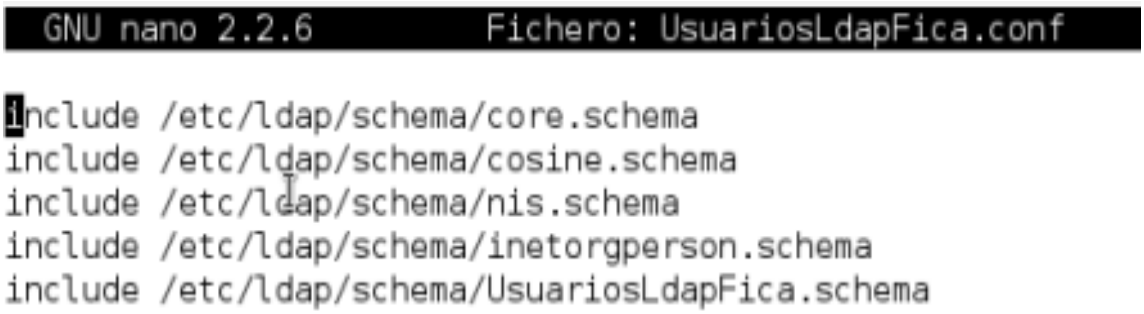


Ilustración 41. Fichero UsuariosLdapFica.conf.
Fuente: Servidor OpenLdap

Ahora se crea un directorio temporal que almacenará la estructura LDIF, que generará el esquema Radius ejecutando el comando ***mkdir /tmp/UsuariosLdap.d,*** seguido de la conversión de la misma con el comando ***slaptest –f /tmp/UsuariosLdapFica.conf –F /tmp/ UsuariosLdap.d/***, de esta forma se crea la estructura necesaria de los ficheros ***ldif***.

El esquema LDIF que se ha creado requiere algunas modificaciones que prevendrán posibles errores, el fichero que se debe modificar es el siguiente #***nano /tmp/UsuariosLdap.d/cn\=config/cn\=schema/cn\=\{4\}usuariosldapfica.ldif,*** en la cual se colocara lo que se indica en la ilustración 42.

```
  GNU nano 2.2.6 Fichero: ...a/cn={4}usuariosldapfica.ldif Modificado

# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 cf7a169e

##########################################
##########################################
dn: cn=usuariosldapfica,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: usuariosldapfica
##########################################
##########################################
```

Ilustración 42. Esquema ldif.
Fuente: Servidor OpenLdap

Nota: las líneas finales del fichero deberán ser eliminadas, esto con el fin de que no interfieran con la configuración realizada.

5.3.3 Añadir esquema al Directorio LDAP

Agregar la jerarquía al directorio principal LDAP añadiendo schema con el comando ldapadd como se muestra en la ilustración 43.

```
root@debian:/# ldapadd -Q -Y EXTERNAL -H ldapi:/// -f /tmp/UsuariosLdap
.d/cn\=config/cn\=schema/cn\=\{4\}usuariosldapfica.ldif
adding new entry "cn=usuariosldapfica,cn=schema,cn=config"

root@debian:/#
```

Ilustración 43. Adición de esquema para el directorio Ldap.
Fuente: Servidor OpenLdap

Y se procede a verificar con el comando ***ldapsearch –x –b "dc=Radius,dc=fica"*** o con el comando ***ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config*** como se muestras en la ilustración 44 y 45.

```
root@debian:/# ldapsearch -x -b "dc=radius,dc=fica"
# extended LDIF
#
# LDAPv3
# base <dc=radius,dc=fica> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# radius.fica
dn: dc=radius,dc=fica
objectClass: top
objectClass: dcObject
objectClass: organization
o: radius.fica
dc: radius

# admin, radius.fica
dn: cn=admin,dc=radius,dc=fica
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
root@debian:/#
```

Ilustración 44. Verificación 1.
Fuente: Servidor OpenLdap

```
root@debian:/# ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema
,cn=config
dn: cn={4}usuariosldapfica,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: {4}usuariosldapfica
```

Ilustración 45. Verificación 2.
Fuente: Servidor OpenLdap

Por último se reinician los servicios con los comandos:

#/etc/init.d/slapd restart
#/etc/init.d/freeradius restart

5.3.4 Ingreso de datos para LDAP

Una vez añadido los esquemas, y reconfigurado nuestro servidor se procede a generar nuestro archivo desde la dirección web http://appweb.utn.edu.ec:7001/apex/f?p=189:LOGIN_DESKTOP:5799040347115::::: , para posteriormente subirlos a nuestro servidor. El primer paso será crear una carpeta

(ilustración 46), con el comando ***mkdir*** dentro del directoio ***/etc/ldap/,*** en él se ubicará el fichero con extensión .ldif

```
root@debian:/# cd /etc/ldap
root@debian:/etc/ldap# ls
ldap.conf  sasl2  schema  slapd.d
root@debian:/etc/ldap# mkdir ldif
```

Ilustración 46. Directorio de ficheros ldif.
Fuente: Servidor OpenLdap

5.3.4.1 Formato de unidades organizativas

Para poder organizar de manera lógica dentro de la jerarquía LDAP, se crea varias unidades organizativas de acuerdo al número de carreras que posee la facultad actualmente, tomando en cuenta que cada una de estas carreras debe poseer 3 subdominios dentro de cada uno y deben seguir el formato que se presenta en la ilustración 47 y 48.

```
#####################################################################
####CARRERA DE INGENIERIA EN ELECTRÓNICA Y REDES DE C.##########
#####################################################################

dn: ou=CIERCOM,ou=LdapFica,dc=fica,dc=radius
ou: CIERCOM
objectclass: top
objectClass: organizationalUnit

dn: ou=Estudiantes,ou=CIERCOM,ou=LdapFica,dc=fica,dc=radius
ou: Estudiantes
objectclass: top
objectClass: organizationalUnit

dn: ou=Docentes,ou=CIERCOM,ou=LdapFica,dc=fica,dc=radius
ou: Docentes
objectclass: top
objectClass: organizationalUnit

dn: ou=Administrativos,ou=CIERCOM,ou=LdapFica,dc=fica,dc=radius
ou: Administrativos
objectclass: top
objectClass: organizationalUnit

#####################################################################3
```

Ilustración 47. Formato de OU para CIERCOM
Fuente: Servidor OpenLdap

```
############################################################
######CARRERA DE INGENIERIA EN MECATRÓNICA#################
############################################################

dn: ou=CIME,ou=LdapFica,dc=fica,dc=radius
ou: CIME
objectclass: top
objectClass: organizationalUnit

dn: ou=Estudiantes,ou=CIME,ou=LdapFica,dc=fica,dc=radius
ou: Estudiantes
objectclass: top
objectClass: organizationalUnit

dn: ou=Docentes,ou=CIME,ou=LdapFica,dc=fica,dc=radius
ou: Docentes
objectclass: top
objectClass: organizationalUnit

dn: ou=Administrativos,ou=CIME,ou=LdapFica,dc=fica,dc=radius
ou: Administrativos
objectclass: top
objectClass: organizationalUnit

############################################################
```

***Ilustración* 48**. Formato de OU para CIERCOM
Fuente: Servidor OpenLdap

5.3.4.2 Formato de grupos o dependencias

Ahora se procede a escribir otro tipo de jerarquía denominada “cn”, esta es la encargada de distribuirlas diferentes dependencias que posee cada unidad organizativa. Para a este caso se procede a crear los diferentes niveles (primero a décimo), la cual seguirá el formato que se muestra en la ilustración 49. Se debe tomar en cuenta que cada nivel se lo incluirá a la unidad organizativa ou=Estudiantes, en cada carrera de la facultad.

```
#########################################################################
#########################CARRERAS-NIVELES################################
#########################################################################

dn: cn=01-Primero,ou=Estudiantes,ou=CIERCOM,ou=LdapFica,dc=fica,dc=radius
cn: Primero
objectClass: top
objectClass: posixGroup
gidNumber: 101

dn: cn=02-Segundo,ou=Estudiantes,ou=CITEX,ou=LdapFica,dc=fica,dc=radius
cn: Segundo
objectClass: top
objectClass: posixGroup
gidNumber: 102

dn: cn=07-Septimo,ou=Estudiantes,ou=CISIC,ou=LdapFica,dc=fica,dc=radius
cn: Septimo
objectclass: top
objectClass: posixGroup
gidNumber: 307

dn: cn=10-Decimo,ou=Estudiantes,ou=CIMANAU,ou=LdapFica,dc=fica,dc=radius
cn: Decimo
objectclass: top
objectClass: posixGroup
gidNumber: 710
```

***Ilustración* 49.** Formato de dependencias dentro de cada unidad organizativa.
Fuente: Servidor OpenLdap

5.3.4.3 Usuarios

Por último se crean los “uid” o ID de usuarios, el cual contara con información necesaria del registro de cada usuario. La estructura de este archivo se muestra en la ilustración 50 a continuación

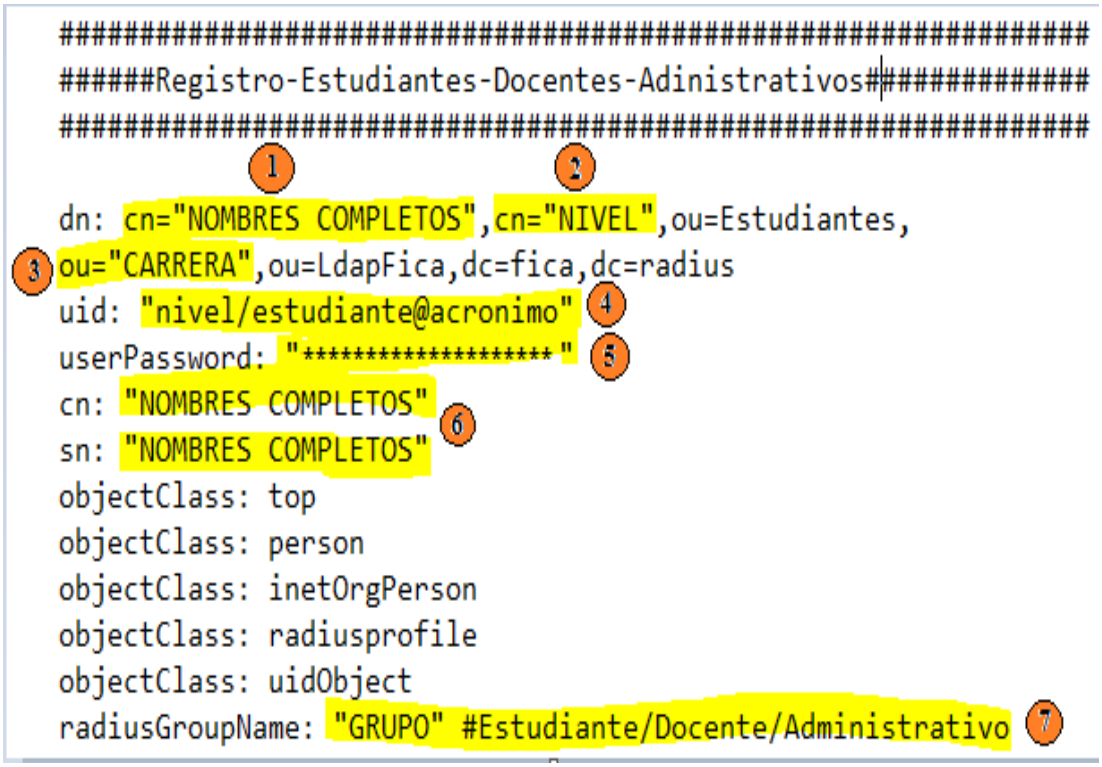


***Ilustración* 50**. Formato de ID Usuario
Fuente: servidor LDAP

De la ilustración anterior se puede describir lo siguiente:

1. Nombres Completos de los estudiantes legalmente matriculados, docentes o personal administrativo
2. Nivel al que pertenece dicho estudiante; en caso de ser docente u administrativo no es tomado en cuenta este ítem, ya que se ubicaran en la unidad organizativa Docentes o Administrativos respectivamente.
3. Carrera a la que pertenece dicho estudiante, docente o personal administrativo.
4. Uid o usuario, el cual se describe como:
    - Nivel al que pertenece seguido de la letra que identifica el grupo (e=estudiante); para docente y personal administrativo solo es necesario el grupo (d=docente, a=administrativo) sin necesidad del nivel.
    - El signo “@”
    - El acrónimo personal, que serán las dos primeras letras de sus nombres, seguido de su apellido y la primera letra de su segundo apellido. Ejemplo:

CAMPO TIXICURO CRISTIAN DAVID = 4e@cdcampot

5. El Password personal que el administrador asignará y difundirá a cada usuario
6. El cn y sn lo constituyen de igual manera los nombres y apellidos completos del usuario. Ambos componentes forman parte del ObjectClass person.
7. Grupo perteneciente al servidor Radius: Estudiantes, Docentes, Administrativos respectivamente.

5.4 Instalación FreeRADIUS

Una vez que se ha actualizado e instalado los paquetes con los dos comandos anteriores, se procede a descargar el paquete FreeRADIUS con soporte LDAP mediante el comando #***apt-get install freeradius-ldap***, la cual en la ilustración 51.

Ilustración 51. Instalación FreeRADIUS
Fuente: Servidor FreeRADIUS Fica

5.4.1 Configuración FreeRADIUS

5.4.1.1 Fichero radius.conf

La configuración del servidor se comenzará por el fichero radiusd.conf del directorio /etc/freeradius/.

- Si se necesita los logs de las solicitudes de autenticación, se procede a la activación del mismo en la siguiente sección del fichero (ilustración 52)

  Se modifican las líneas siguientes:

  auth = no ---------> yes
  auth_badpass = no --------> yes
  auth_goodpass = no --------> yes

  Esto permitirá que todo los logs del FreeRADIUS tenga más detalles.

```
auth = no

#  Log passwords with the authentication requests.
#  auth_badpass  - logs password if it's rejected
#  auth_goodpass - logs password if it's correct
#
#  allowed values: {no, yes}
#
auth_badpass = no
auth_goodpass = no
```

***Ilustración* 52.** Fichero radiusd. conf
Fuente: Servidor FreeRADIUS Fica

- Se desactiva el proxy que viene activado por defecto (ilustración 53).

```
proxy_requests  = yes
$INCLUDE proxy.conf
```

Ilustración 53. Fichero radius.conf: Proxy.
Fuente: Servidor FreeRADIUS Fica

Modificar las líneas siguientes:

Proxy_request = yes ---------> no
$INCLUDE proxy.conf --------> anteponer #

- Al usar LDAP para los usuarios y no MYSQL se dejan comentadas las siguientes líneas en este fichero:

#$INCLUDE sql.conf
#$INCLUDE sql/mysql/counter.conf
#$INCLUDE sqlippool.conf

5.4.1.2 Ficheros sites enabled / /inner-tunnel

Luego de haber terminado el fichero anterior se procede a la configuración del fichero sites-enabled del directorio /etc/freeradius/. En este directorio se encuentra los archivos de configuración de cada uno de los servidores que se va a crear. El servidor preconfigurado se denomina fichero default (ilustración 54), y el virtual denominado inner-tunnel a los cuales se los edita con ***nano*** (ilustración 55).

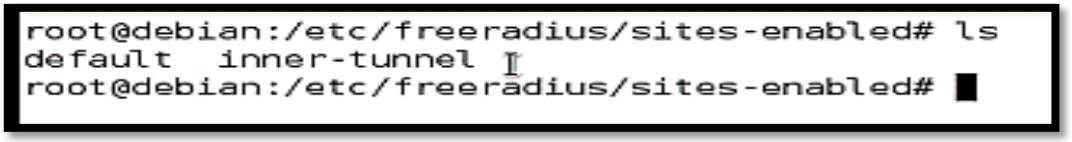


***Ilustración* 54.** Fichero sites-enabled.
Fuente: Servidor FreeRADIUS Fica

módulo para la autorización
authorize {
preprocess
auth_log
chap
mschap
digest
suffix
eap
{ ok = return
} files
ldap
expiration
logintime
pap
}
	#módulo para la autenticación
	authenticate {
	Auth-Type LDAP {
	ldap
	}
	# Allow EAP authentication
	eap
	}
	
	#módulo de filtros de Contabilidad Solicitud de paquetes
	preacct {
	preprocess
	acct_unique
	suffix
	files
	}

#módulo de contabilidad
accounting {
detail
unix
radutmp
 	
attr_filter.accounting_response
}
#módulo para la despues de autenticar
post-auth {
exec
Post-Auth-Type REJECT {
attr_filter.access_reject
}
}
	#módulo de contabilidad
	accounting {
	detail
	unix
	radutmp
	attr_filter.accounting_response
	}
	#módulos para el proxy que no vamos a usar, por lo tanto no tiene directivas
	pre-proxy {
	}
	post-proxy {
	}
	#módulo para la sesiones
	session {
	radutmp
	}

***Ilustración* 55.** Fichero sites-enable / inner-tunnel.
Fuente: Servidor FreeRADIUS Fica

5.4.1.3 Fichero eap.conf

Este es uno de los ficheros más importantes, donde se va a definir el tipo de autenticación EAP-TTLS. Adicionalmente se indicará los certificados de servidor que se usarán para establecer la comunicación Radius. La configuración del fichero será dentro del directorio /etc/freeradius/eap.conf y constará con lo que muestra la ilustración 56 y 57.

```
eap{
#protocolo de autenticación por defecto
    default_eap_type = ttls
#tiempo de expiración de la entrada
    timer_expire = 60
#ignorar tipos desconocidos de eap
    ignore_unknown_eap_types = no
#máximas sesiones
    max_sessions = 2500
}
```

```
tls{
#entidad certificadora, certificados de entidad y servidor
    certdir = ${confdir}/certs
    cadir = ${confdir}/certs
    private_key_password = whatever
    private_key_file = ${certdir}/server.key
    certificate_file = ${certdir}/server.pem
    CA_file = ${cadir}/ca.pem
    dh_file = ${confdir}/certs/dh
    random_file = /dev/urandom
# permitir los sitios de cifrado tls
    cipher_list = "DEFAULT"
```

***Ilustración* 56.** Fichero eap.conf: eap-tls.
Fuente: Servidor FreeRADIUS Fica

```
cache
 {
 # activar la caché
   enable = no
   lifetime = 24 # hours
    max_entries = 255
 }
```

```
ttls
{
#protocolo de autenticación por defecto
    default_eap_type = tls
#cualquier atributo se copia en la solicitud de túnel
    copy_request_to_tunnel = no
#uso replicado del tunel
    use_tunneled_reply = no
#incluir longitud del mensaje
    include_length = yes
 }
```

***Ilustración* 57.** Fichero eap.conf: cache – ttls.
Fuente: Servidor FreeRADIUS Fica

5.4.1.4 Fichero LDAP

El fichero ldap permite configurar el acceso de freeradius con el servidor ldap y se lo puede encontrar dentro del directorio /etc/freeradius/modules/. Se tiene que configurar nuestro servidor Radius para que se conecte a al ldap usando conexiones TTL por el puerto 389 tcp (ilustración 58). El fichero a modificar seria:

- ***Server = debe ir la dirección IP o el nombre de dominio del servidor.***
- ***Identity = Usuario con privilegios en el LDAP y dominio de búsqueda.***
- ***Password = Password de este usuario (de conexión al LDAP).***
- ***Base dn= Define la rama base de búsquedas, es decir le donde buscar en el LDAP.***
- ***Filter= aquí se define la búsqueda LDAP.***

```
ldap {
        port = "389"
        server = "192.x.x.x"
        identity = "cn=admin,dc=fica,dc=radius"
        password = ****************
        basedn = "dc=fica,dc=radius"
        filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
        base_filter = "(objectclass=radiusprofile)"
        ldap_connections_number = 5
        max_uses = 1
        timeout = 4
        timelimit = 3
```

***Ilustración* 58.** Configuración módulo Ldap.
Fuente: Servidor FreeRADIUS Fica

5.4.1.5 Fichero clients.conf

Por último se modicanuestro fichero clients, en el cual se define los clientes o puntos de acceso que van a tener acceso a nuestro servidor (ilustración 59). Se debe tomar muy en cuenta el papel de estos APs, los mismos no realizaran ningún tipo de autentificación, su única función es encapsular paquetes de tipo EAP en paquetes Radius.

```
client localhost {
        ipaddr = 127.0.0.1
        secret          = testing123
        require_message_authenticator = no
        nastype     = other     # localhost isn't usually a NAS...
}

client 192.x.x.x {
        secret          = *************
        shortname     = ficawifi
        nastype     = MikroTik
}
```

***Ilustración* 59.** Fichero clients.conf.
Fuente: Servidor FreeRADIUS Fica

5.5 Reconfiguración de los puntos de acceso (CAP y CAPsMAN)

La configuración depende de la marca del punto de acceso, en nuestro caso será los AP's marca Mikrotik, modelo cAP2n y su router modelo RB1100 AX2, al cual se accede mediante ***WinBox*** (ilustración 60).

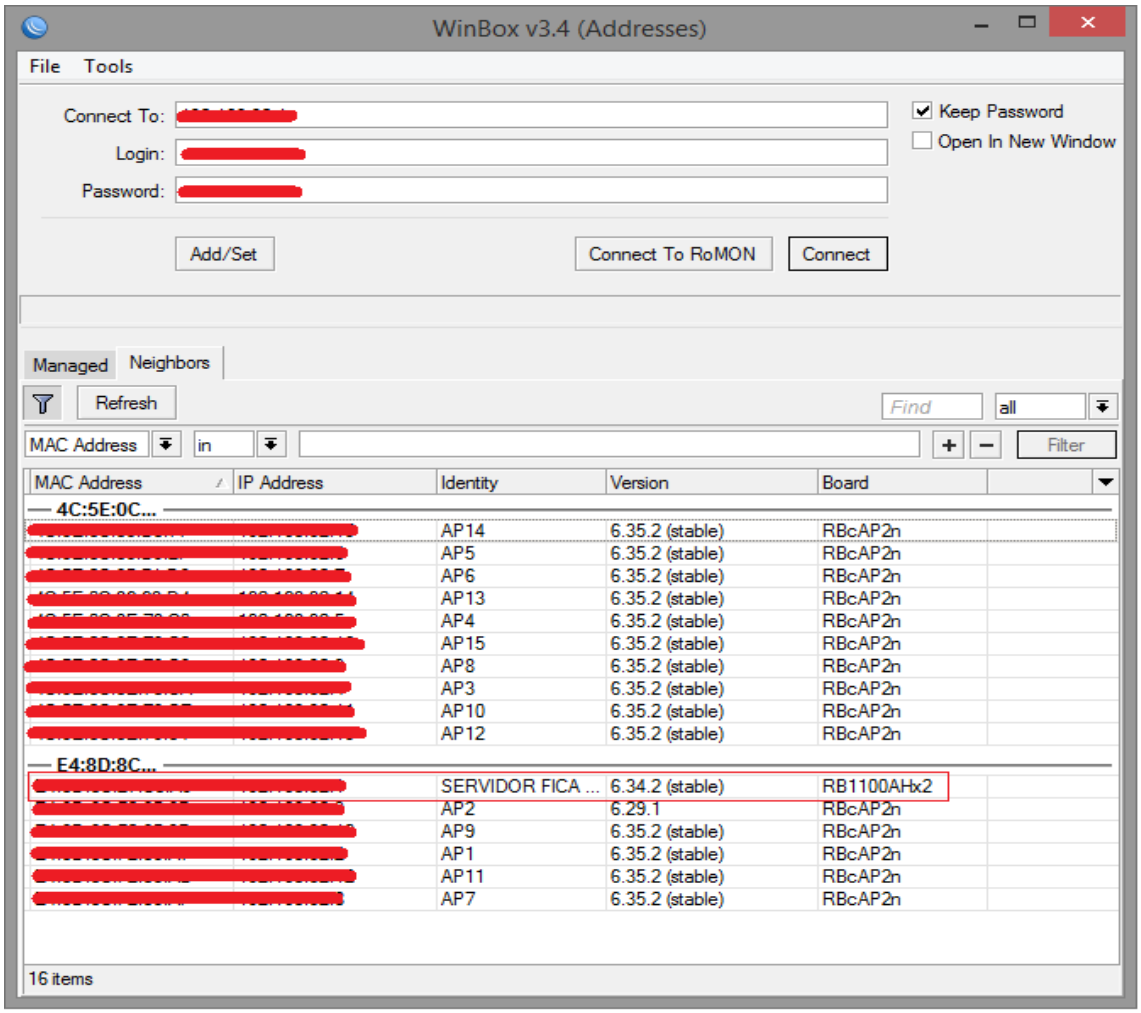


Ilustración 60. Ventana principal Winbox.
Fuente: Winbox.exe

5.5.1 Configuración CAP

En primer lugar, se procede a reconfigurar uno de nuestros CAP, el cual servirá de base para poder configurar el resto de equipos, nos vamos a la pestaña ***IP/ADDRESSES/ADDRESS LIST/NEW ADDRESS*** y en ella se coloca la dirección IP correspondiente a dicho CAP (ilustración 61).

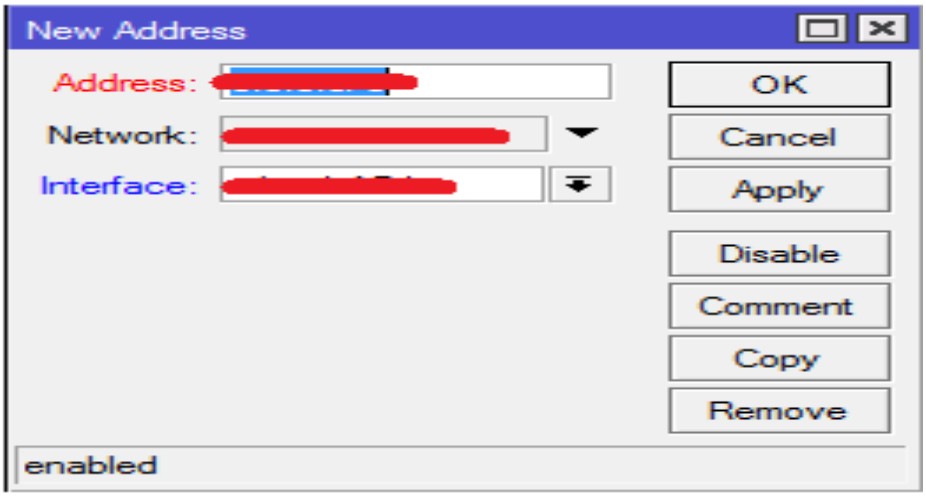


Ilustración 61. Configuración IP estática
Fuente: Mikrotik

Luego se procede a cambiar el nombre de cada interfaz, el cual permita al administrador de red identificar el equipo de una manera más sencilla (ilustración 62) para ello se busca la pestaña INTERFACES/INTERFACE LIST. Esto debido a que la configuración anterior no se tenía claro el identificativo de dicho AP.

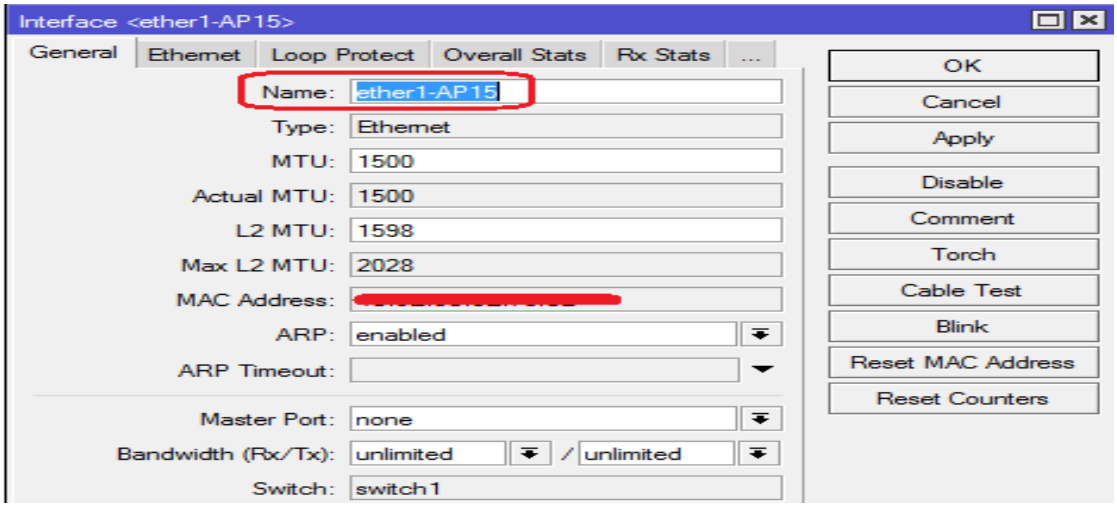


Ilustración 62. Identificación de interfaces
Fuente: Mikrotik

Se crea a continuación un puente en la pestaña ***BRIDGE/AGREGAR NUEVO***, el cual permitirá la interconexión de la LAN y WLAN que opera en la capa 2 para formar una sola subred (ilustración 63).

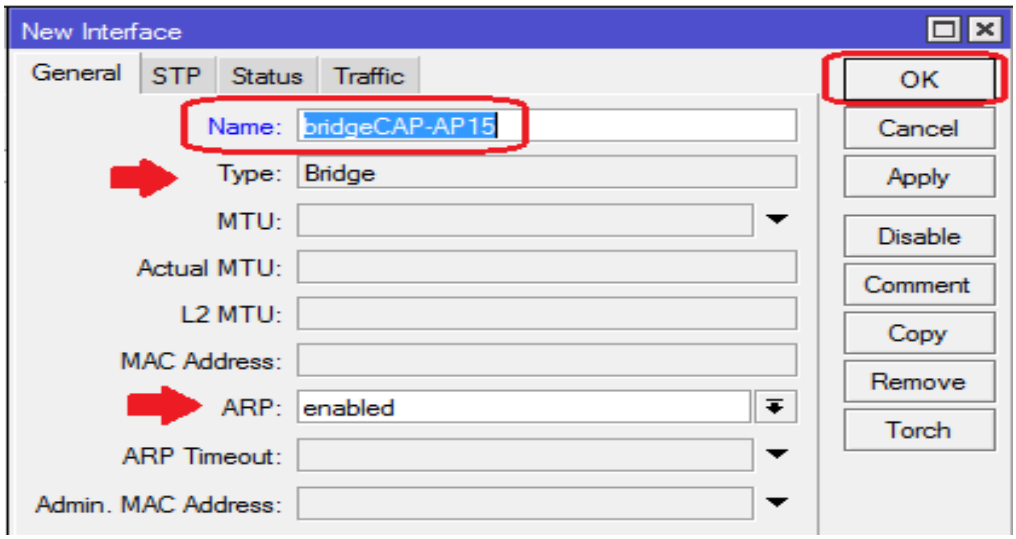


Ilustración 63. Configuración Bridge
Fuente: Mikrotik

Una vez que se hace el bridge y se colocan los puertos (LAN y WLAN), luego se activa el CAP en la pestaña ***WIRELESS,*** donde se procede a configurar tal y como se muestra en la ilustración 64.

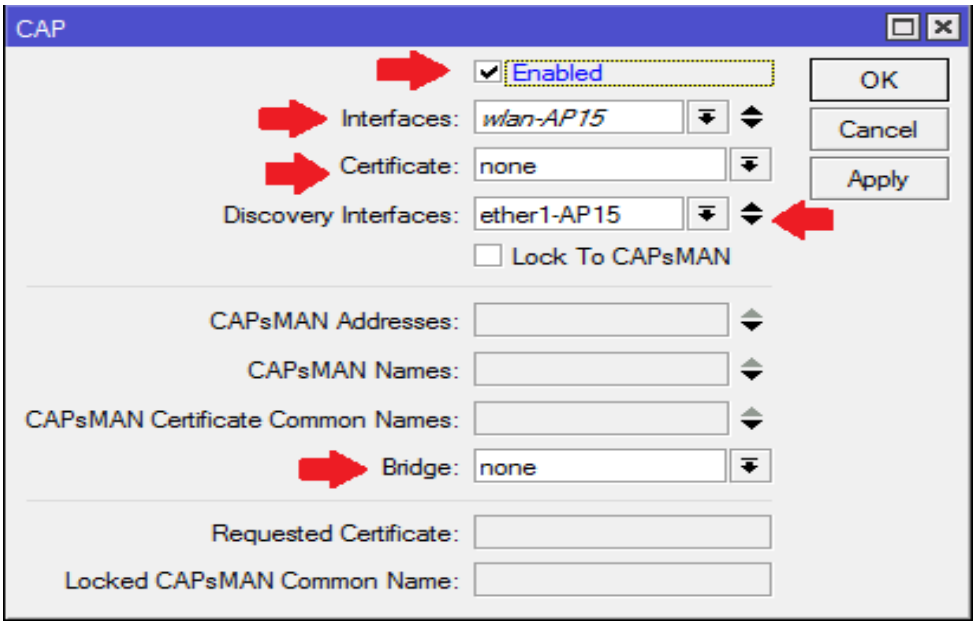


Ilustración 64. Configuración CAP
Fuente: Mikrotik

Nota: Por último se verifica que el CAP propague la información al CAPsMAN.

5.5.2 Configuración CAPsMAN

Antes de configurar nuestro Router-Mikrotik en modo CAPsMAN, se activa la función RADIUS, para lo cual se ingresa a nuestro servidor Mikrotik, en la pestaña de Radius, se crea una nueva entrada y se configura con los siguientes parámetros (ilustración 65).

Address -> dirección ip del servidor Radius
Secret -> contraseña configurada en Fichero clients.conf
Authentication port -> 1812
Accouting port -> 1813

Se activa la pestaña "Wireless", la cual nos permitirá vincular el servidor LDAP con la tarjeta inalámbrica del router MikroTik.

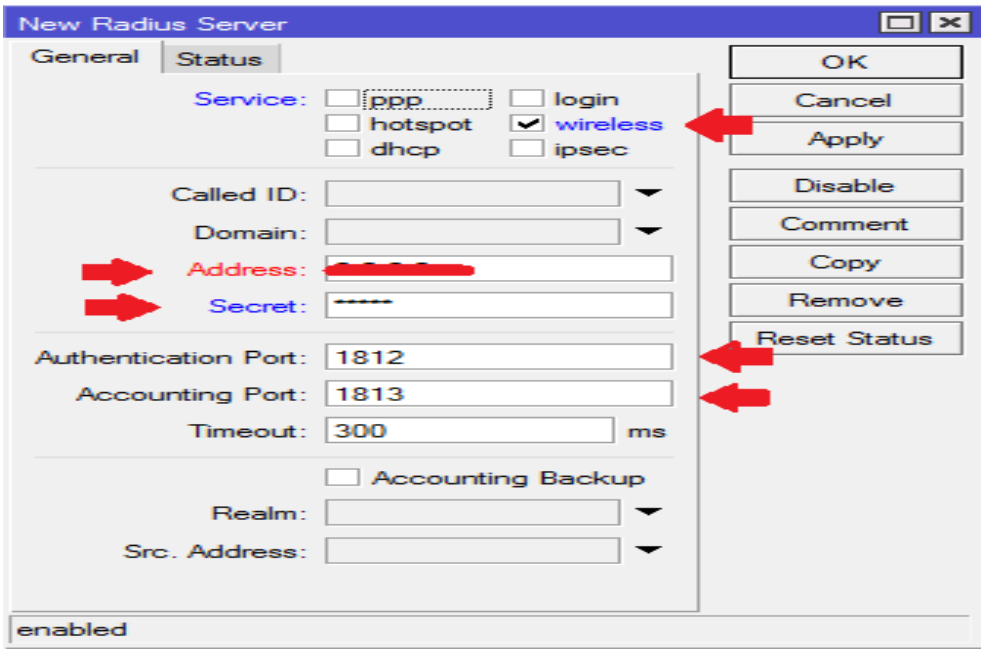


Ilustración 65. Radius- Mikrotik.
Fuente: Router - Mikrotik

Una vez activado RADIUS, se habilita el Manager en nuestro CAPsMAN en el cual constara con todos los perfiles o configuraciones de redes inalámbricas que serán luego configuradas de forma automática en cada CAP (ilustración 66). En la pestaña ***CAPsMAN/INTERFACES/MANAGER/ENABLE,*** se pulsa aceptar y todos los CAP se añadirán automáticamente.

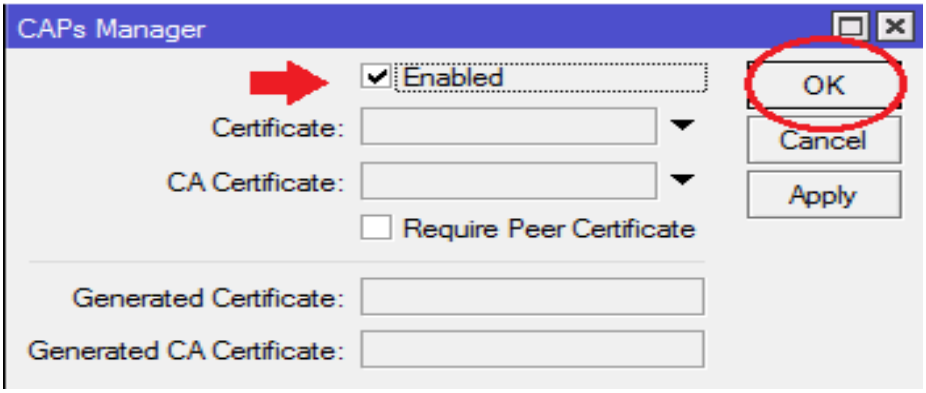


Ilustración 66. Activación Manager CAPsMAN
Fuente: Router – Mikrotik

El CAPsMAN puede entregar parámetros de configuración para cada CAP, dichas configuraciones se encuentran en las pestañas:

- **Channels:** configuraciones relativas a los canales, como por ejemplo banda, frecuencia y ancho de canal.
- **Datapaths:** configuración relacionada con el bridge donde se integrará la interfaz de los CAPs. De esta forma se configura el reenvió de tráfico hacia el CAPsMAN
- **Security Cfg:** configuraciones de autenticación y cifrado. Soporta métodos estáticos (como llaves pre compartidas), EAP y TLS
- **Configurations:** se encuentran los perfiles principales para cada red inalámbrica. En esta pestaña se configura SSID, se asigna algún canal especifico, el datapath y la correspondiente seguridad. Estas configuraciones se pueden cargar para todos los CAP del controlador, para un grupo o para un solo CAP.

Una vez creada la configuración (al menos una), se la puede cargar en los diversos CAP los cuales se encuentran en la tabla de interfaces del CAPsMAN (ilustración 67).

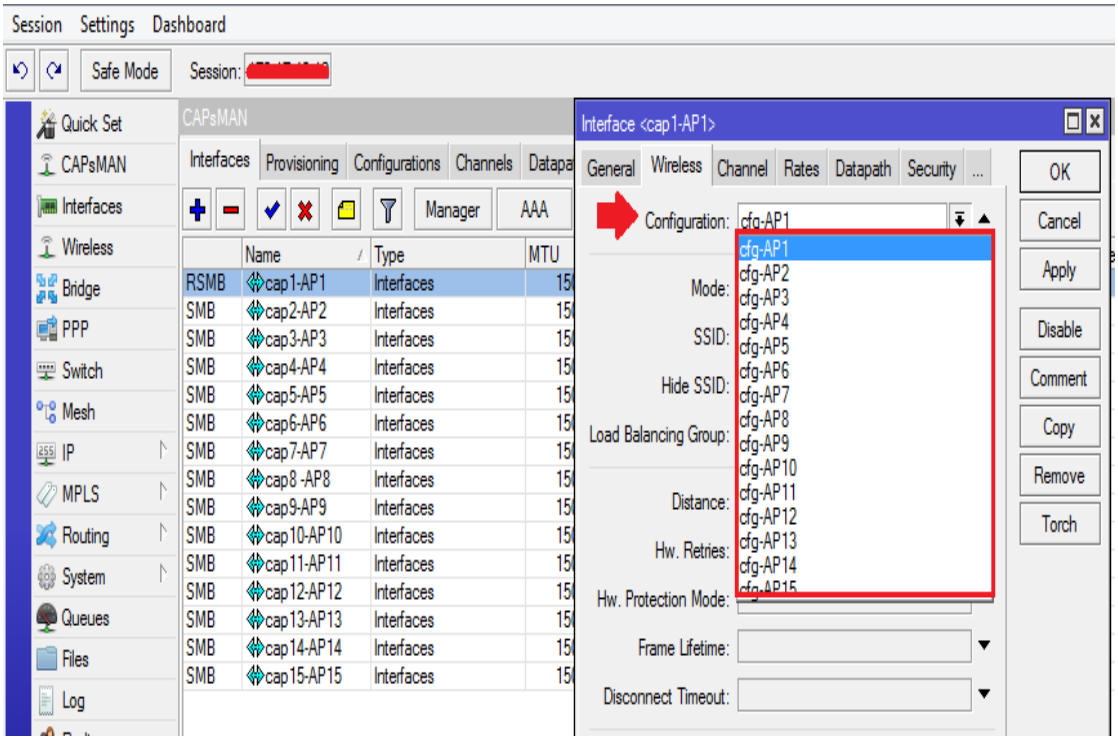


Ilustración 67. Configuración de Interfaces en CAPsMAN
Fuente: Router – Mikrotik

5.5.3 Control de ancho de banda (QUEUE - PCQ)

La forma más sencilla de limitar la velocidad de datos de direcciones y / o subredes específicas, es el uso de colas simples con algoritmo PCQ. Para lo cual se crean dos nuevas entradas en la pestaña de ***QUEUES,*** una para estudiantes y otra para docentes (ilustración 68).

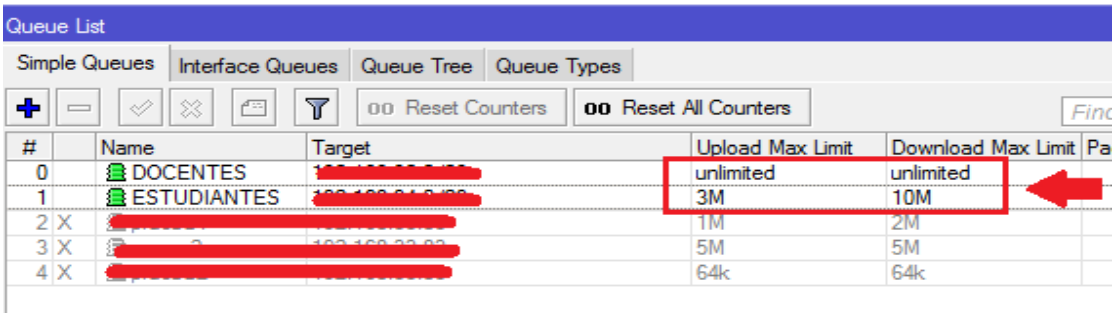


Ilustración 68. Control AB
Fuente: Router – Mikrotik

5.6 Wlan SSID

Una vez realizadas todas las configuraciones respectivas, el SSID de la facultad seguirá siendo “ficawifi” (ilustración 69), las credenciales de acceso de esta red están

descritas en el apartado 5.3.4.3 del mismo, las cuales serán difundas a cada usuario a través de del portafolio institucional personal.

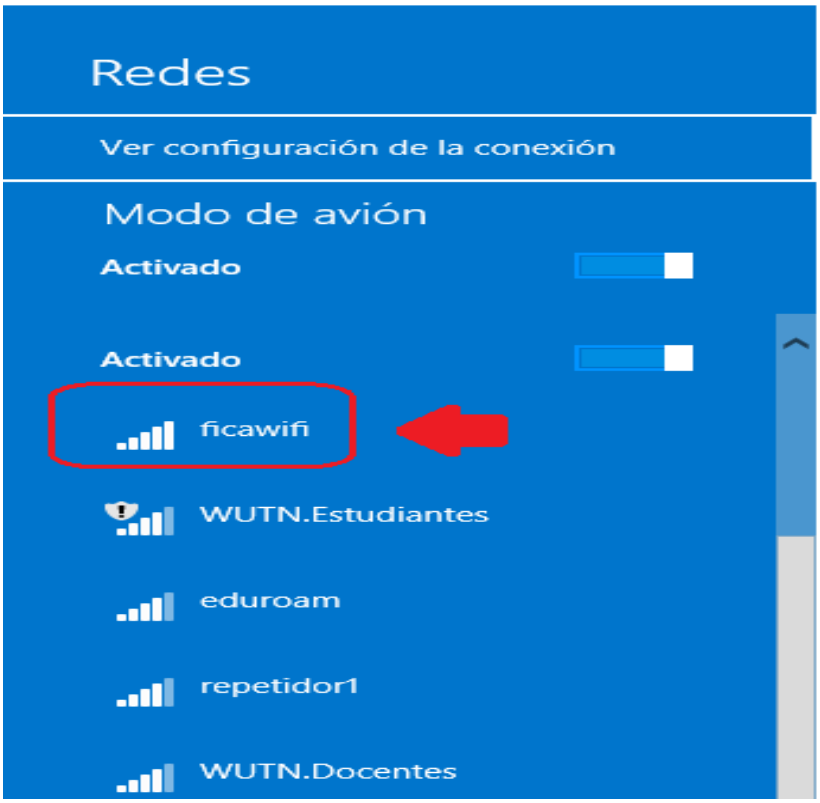


Ilustración 69. SSID Facultad.
Fuente: MikroTik

5.7. Pruebas de funcionamiento

Para poder comprobar el buen funcionamiento del servidor RADIUS, se presenta una serie de ítems en la tabla 22, la cual nos permitirá mejorar el estado actual de la red inalámbrica.

Tabla 22. *Tabla de pruebas*

N° Ítem	Criterio de evaluación
1	Difusión de SSID con seguridad 802.1x y verificación de canales dentro de las instalaciones FICA.
2	Conexión entre cliente y servidor utilizando radtest (local) y NTRadPing (remota).
3	Pruebas de conexión de estudiantes, docentes y personal administrativo (FICA) desde dispositivos portátiles (laptop) y móviles (Smartphone).
4	Asignación de IP dinámicas, control de ancho de banda, test de velocidad.

5.7.1 Difusión de SSID con seguridad 802.1x y verificación de canales dentro de las instalaciones FICA.

Para poder determinar si nuestros APs están propagando la el SSID se hace uso de un monitor de redes inalámbricas denominado Acrylic WiFi (ilustración 70) en la planta baja de la facultad; además de comprobar la seguridad que posee la misma.

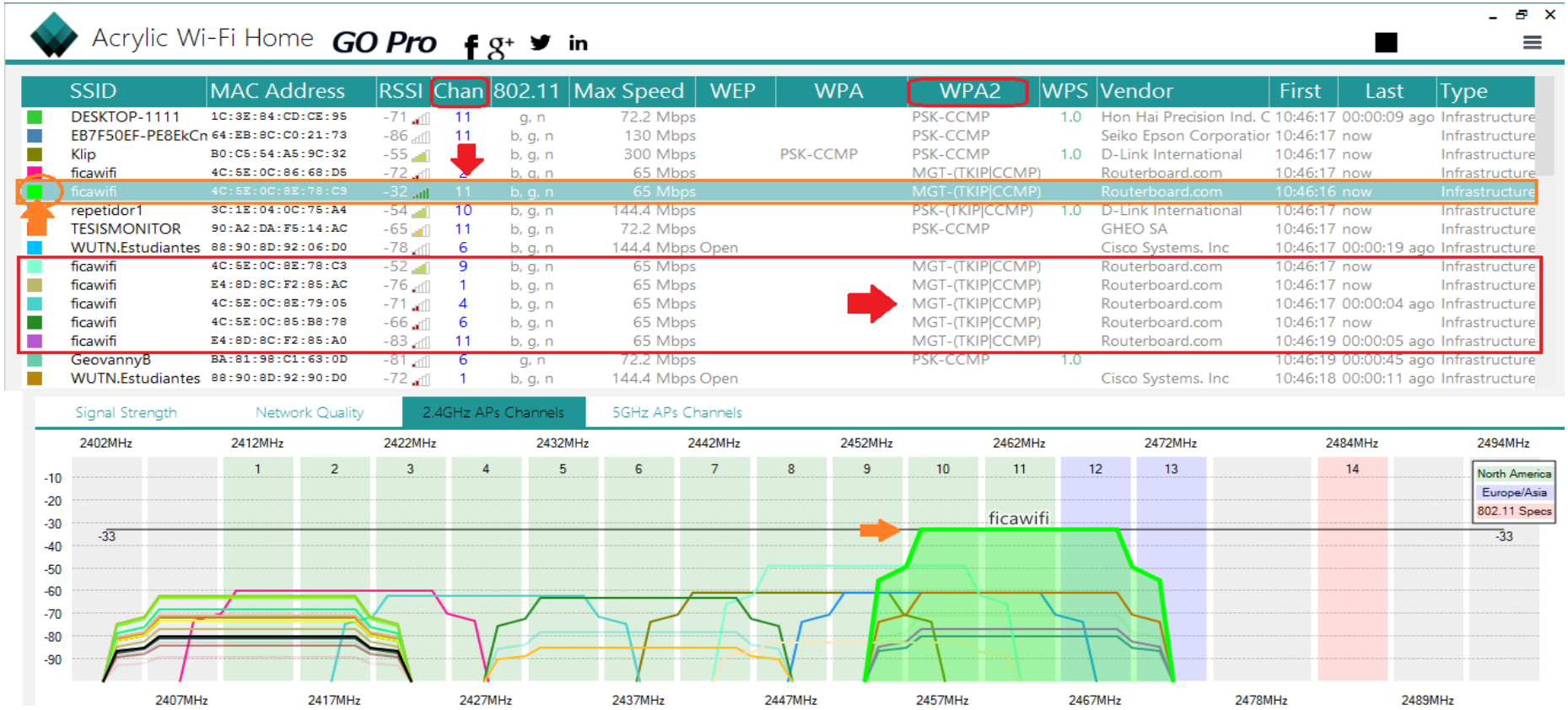


Ilustración 70. Prueba 1: Difusión SSID

Fuente: Acrylic Wifi

Análisis: Como se puede observar en la ilustración anterior existen varias redes inalámbricas en la banda de los 2.4GHz dentro de la facultad, cada red está ocupando un canal especifico sin embargo se nota la saturación de redes en los canales 1 y 11. La red ficawifi hace uso de los estándares 802.11 b/h/n con una velocidad de trasmisión igual a 65Mbps y las siglas ***MGT-(TKIP/CCMP)*** indican que la contraseña no es una clave pre compartida y en su lugar la red está conectada a un sistema o servicio de autenticación (RADIUS.

5.7.2 Pruebas de conexión entre cliente y servidor utilizando radtest (local) y NTRadPing (remota).

Para poder asegurar el buen funcionamiento de nuestro sistema se verifica que todos los usuarios se encuentren en la base de datos LDAP, haciendo uso del programa de gestión ***phpLdapAdmin*** (ilustración 71). Para comprobar la conexión entre el servidor FreeRADIUS y la base de datos LDAP, utilizando los 2 métodos siguientes:

- El comando radtest (Debian 8 – Prueba local)
- Software NTRadPing (Ejecutable Windows – Prueba remota)

Ilustración 71. Verificación de usuarios LDAP.
Fuente: PhpLdapAdmin

Caso 1: Se procede a ejecutar el comando ***radtest*** el cual envía requerimientos a un servidor RADIUS. Para ello se debe digitar el siguiente comando (ilustración 72):

```
# radtest "Usuario" "Contraseña" "localhost" "1812" "contraseña2"
```

Ilustración 72. Formato radtest.
Fuente: Server FreeRADIUS

Donde:

Usuario → 10e@username
Contraseña→ User-Password
localhost → Ip del servidor
1812 → Nas-Port
Contraseña → password compartido entre radius y punto de acceso.

La línea ***radtest*** debería recibir alguno de los mensajes definidos por los RFC 2865 y 2866 en unos pocos segundos, entre las cuales podrían constar aceptación o rechazo, como muestra la ilustración 73.

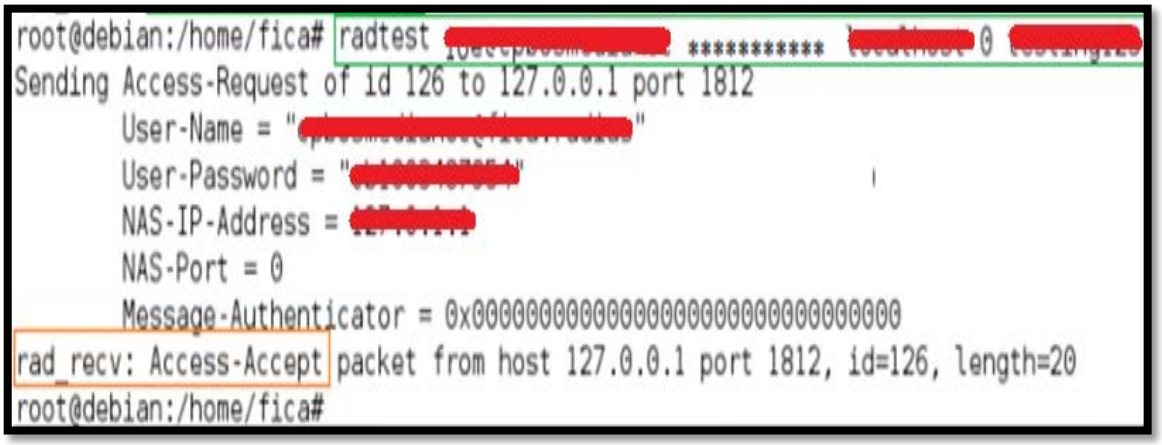


Ilustración 73. Prueba 2: local con el comando radtest
Fuente: Servidor FreeRADIUS

Análisis: Según los datos obtenidos en la ilustración anterior se puede describir lo siguiente:

- ***Access-Request:*** Es la petición enviada por el cliente RADIUS para solicitar autenticación y autorización para conectarse a la red.

- ***Access-Accept:*** Respuesta emitida por un servidor RADIUS. Informa que la conexión está autenticada y autorizada y le envía la información de configuración para comenzar a usar el servicio.
- ***Access-Reject:*** Emitido por servidor RADIUS en respuesta a un mensaje de Access-Request. Este mensaje informa al cliente RADIUS que el intento de conexión ha sido rechazado. (Credenciales erróneas o por prohibición de acceso).

Caso 2: Una vez que se comprobó que el servidor Radius es completamente funcional a nivel local aceptando o rechazando usuarios, se ejecta el programa ***NTRadping*** (ilustración 45), desde el sistema operativo Windows 8, para poder verificar que nuestro sistema acepta peticiones fuera del propio servidor LDAP.

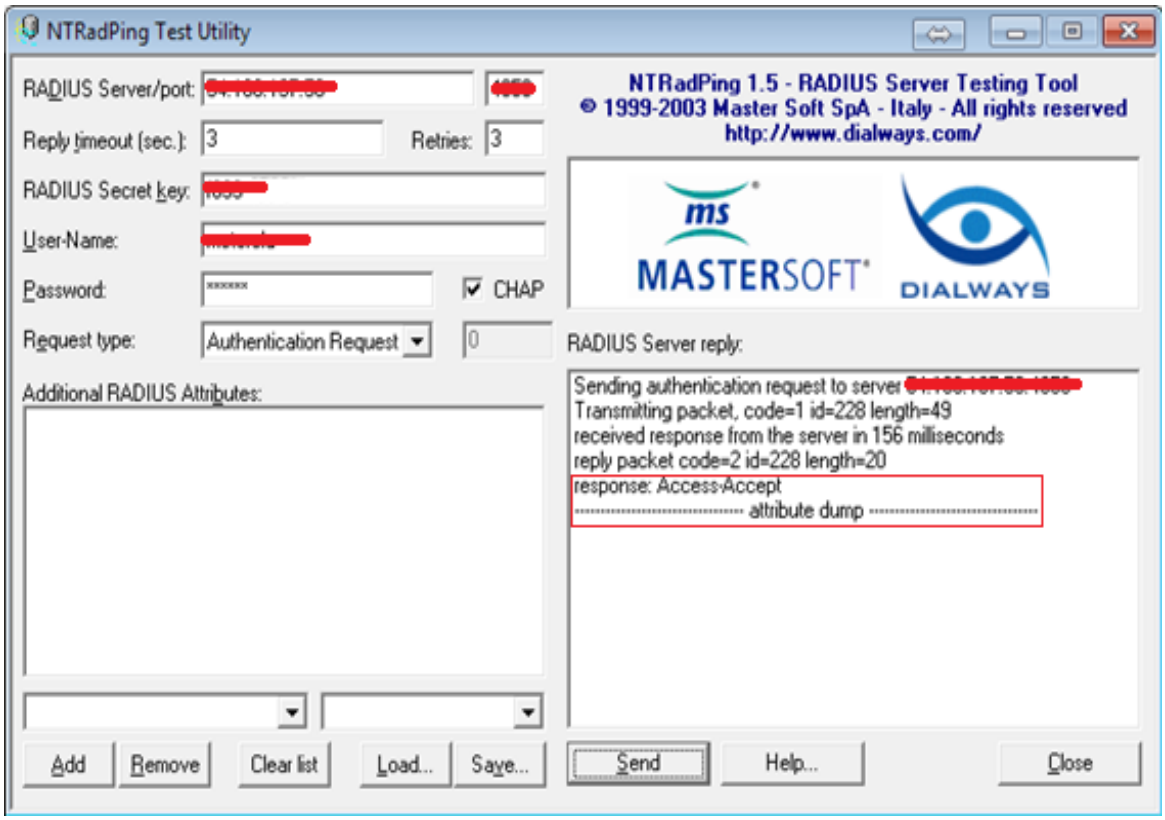


Ilustración 74. Prueba remota de usuarios
Fuente: NTRadping

Análisis: Para poder hacer uso del programa NTRadping se debe proveer información específica de nuestro servidor, como por ejemplo la dirección IP y el puerto por defecto

de comunicación, el KEY o password de comunicación del LDAP, seguido sus credenciales (user + pass). Una vez que se envían los datos, el servidor responde el mensaje de confirmación Aceptando o Rechazando a dicho usuario.

5.7.3 Pruebas de conexión de estudiantes, docentes (FICA) en diferentes dispositivos (laptops – Celulares – Tablets).

Para poder probar el funcionamiento correcto de la red inalámbrica y poder engancharnos a la misma en dispositivos portátiles con sistema operativo Windows 7, 8 y 8.1, se procede a instalar el programa denominado SecureW2 (Anexo E), ya que Windows 10, Linux y MacOS-Appl poseen incorporados autentificación EAP-TTLS/PAP de forma nativa. En primer lugar, se procede a configurar la red ubicándonos en ***Centro de redes y recursos compartidos, configurar una nueva conexión de red, conectarse manualmente a una red inalámbrica,*** en ella se coloca los siguientes datos:

- Nombre de la Red: **ficawifi**
- Tipo de Seguridad: **wpa2 – enterprise**

Se preciona continuar y se nos desplegara la ventana de cambio de configuración, se procede a cambiar las configuraciones dentro de la pestaña seguridad como muestra la ilustración 76.

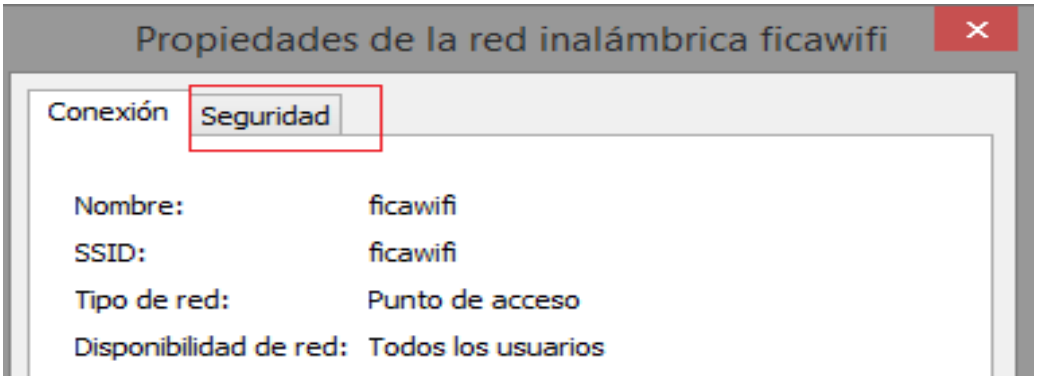


Ilustración 75. Pestaña de seguridad red inalámbrica.
Fuente: Windows 8.1

Dentro de la pestaña se haran las siguientes modificaciones:

Método de autentificación: *Microsoft EAP-TTLS*

Configuración: *deshabilitar la casilla (Privacidad de identidad)*
Autentificación de cliente (PAP).

Configuración Avanzada: *Marcar la casilla (Especificar modo de*
(autentificación), autentificación de usuarios

Luego de configurar se procede a verificar que nuestro ordenador reconozco la nueva red creada, donde se tendrá que especificar nuestro usuario y contraseña. Una vez que valide el servidor Radius se tendra acceso a la red (ilustración 76).

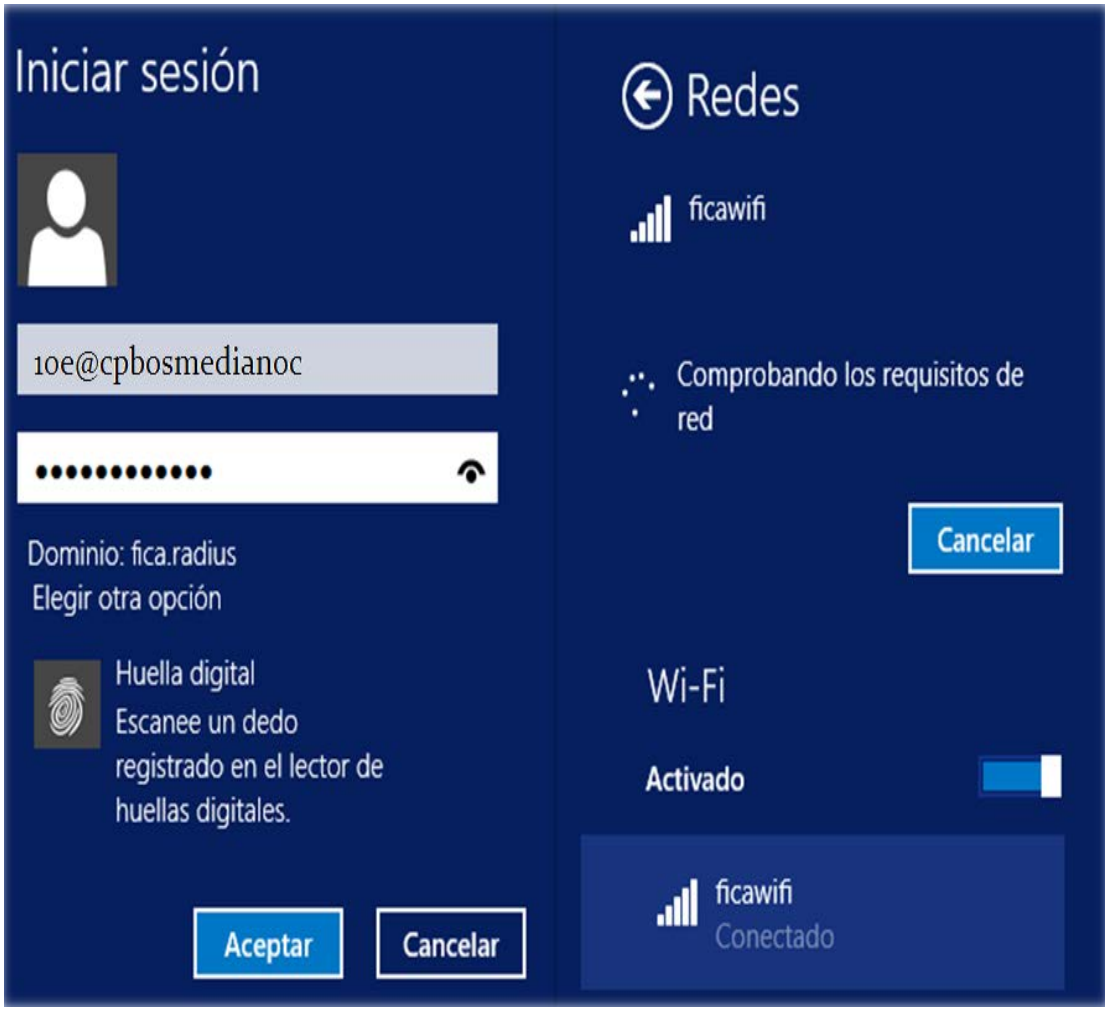


Ilustración 76. Prueba 3: Conexión EAP-TTLS.
Fuente: Windows 8.1

Además, se realiza las pruebas en los dispositivos electrónicos con sistema operativo Android e IOS (iPhone OS) como muestra la ilustración 77, debido a que ambos poseen

autenticación EAP-TTLS/PAP de forma nativa. Para conectarnos a nuestra red, sólo se necesita especificar los siguientes parámetros.

Método EAP: ***TTLS (Android)***
Autentificación de fase 2: ***PAP (Android)***
Certificado de CA: ***(Sin especificar) (Android)***
Identidad: ***usuario (Android – IOS)***
Contraseña: ***password (Android – IOS)***

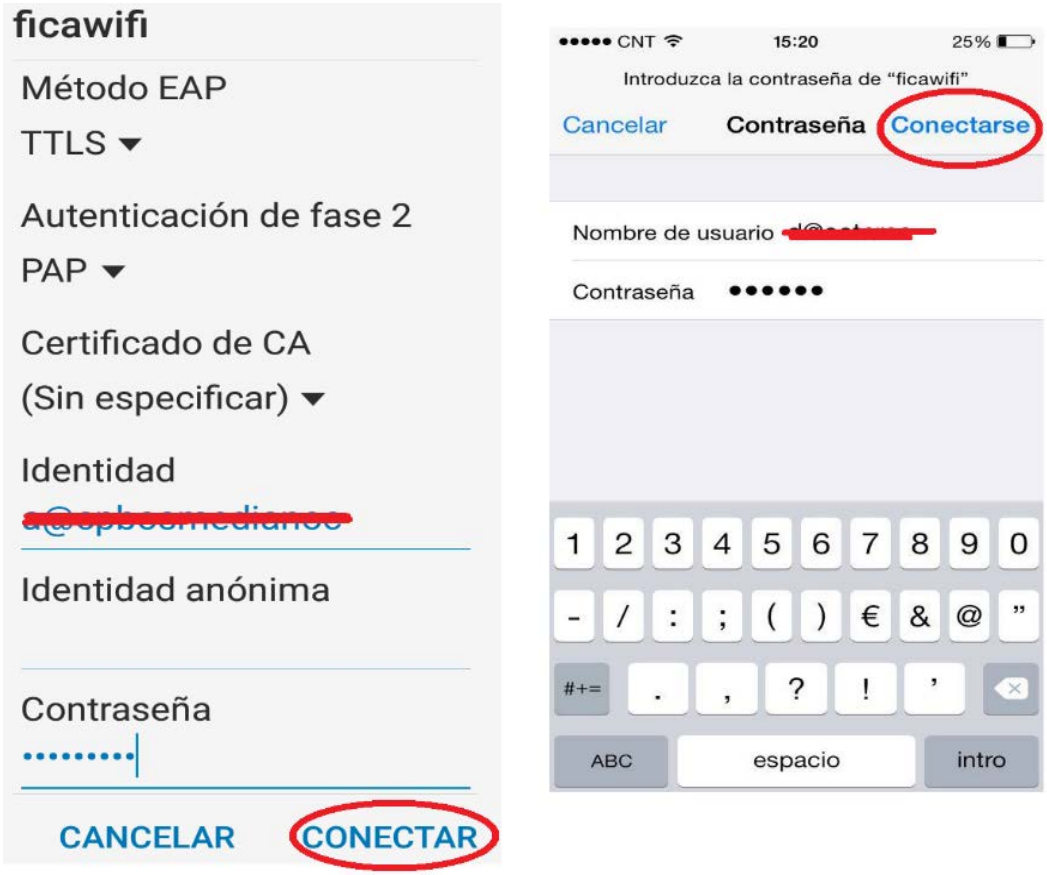


***Ilustración* 77.** Prueba 4: Conexión Smartphone.
Fuente: Android – IPhone

Con el fin de verificar cuantos accesos se tiene en nuestra red, se hará uso de los registros LDAP (ilustración 78), ubicándonos en el directorio siguiente: ***cat /var/log/freeradius/radius.log,*** el cual nos permitirá observar la cantidad de intentos exitosos y fallidos se han logrado en la red.

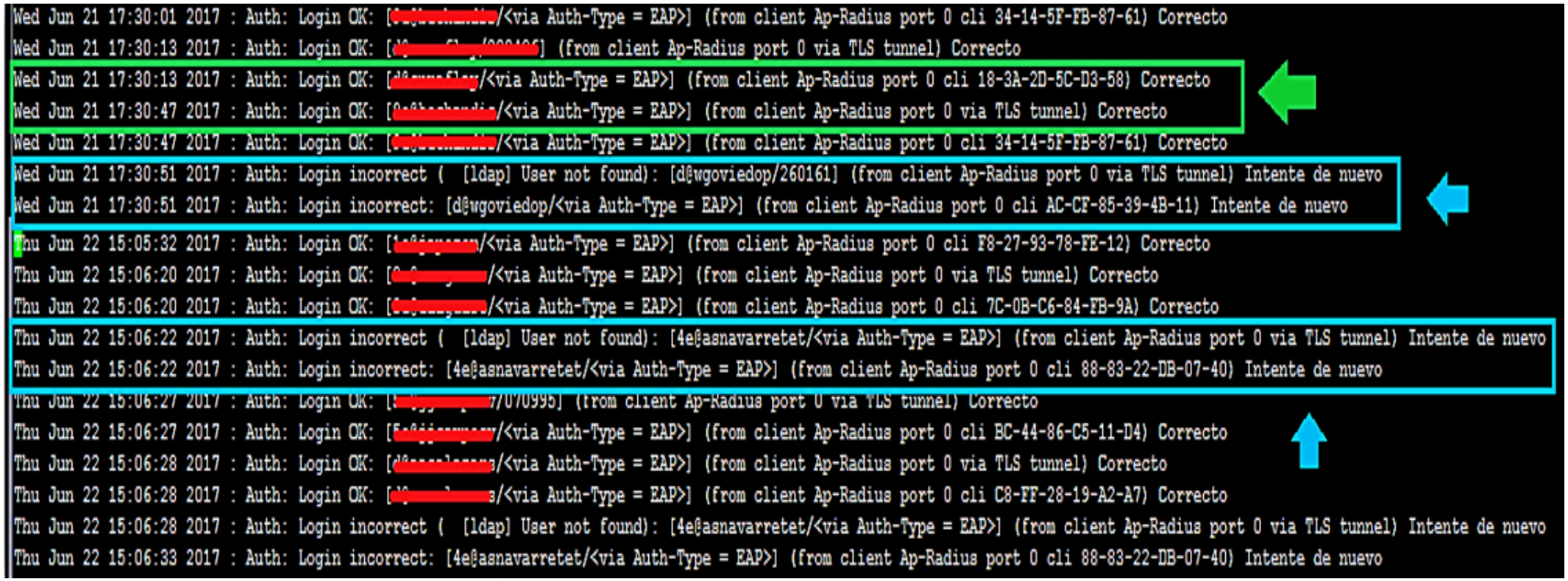


Ilustración 78. Log Ldap
Fuente: Server Ldap

Análisis: En la ilustración se puede comprobar el proceso de validación de credenciales por parte de nuestro servidor LDAP; todo usuario que se encuentre dentro de la base de datos es autorizado con un ***Auth: Login OK – Correcto***, (docentes, estudiantes, administrativos), su dirección MAC queda guardada para futuras conexiones a nivel local dentro del servidor; por otra parte se le asigna un dirección IP vía DHCP desde el router Mikrotik y podrá acceder al recurso; mientras que los usuarios que han colocado mal sus credenciales o simplemente no se encuentran en la base de datos son rechazados, dejando el siguiente mensaje ***Auth: Login Incorrect – Intente de nuevo,*** al administrador de la red. De esta forma se evita que usuarios no autorizados se enganchen a la red.

5.7.4 Asignación de IP dinámicas, control de ancho de banda - test de velocidad

Caso 1: Para la asignación de Ip dinámicas se utilizó un DHCP-SERVER, para todos los usuarios de la red (ilustración 79). Para poder verificar el estado de mismo se busca la pestaña ***IP/IP POOL***

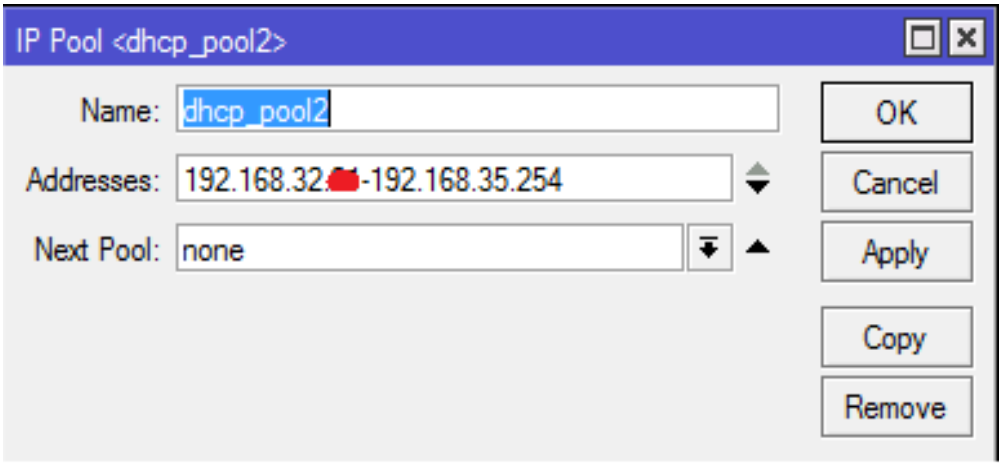


Ilustración 79. Configuración DHCP-SERVER
Fuente: Server- Mikrotik

De acuerdo a la ilustración anterior se puede notar que se cuenta con un total de 1022 direcciones IP utilizables, de las cuales las 20 direcciones ya se encuentran ocupadas por los diferentes APs, el servidor LDAP y un algunas IPs de reserva para futuros equipos.

Caso 2: Para poder limitar la velocidad de navegación se estableció dos nuevas entradas por el método de colas simples como se muestra en la ilustración 69 del apartado 5.5.3, dichas entradas manejan un perfil para el grupo de docentes y personal administrativo en la subred ***192.16X.XX/xx,*** asignando el máximo ancho de banda existente tanto para subida/bajada de datos; el cual deberá ser compartida entre todos los usuarios del área docente/administrativos que se encuentren enganchados a la red (ilustración 80).

Ilustración 80. Ancho de banda grupo Docentes-Administrativos
Fuente: http://beta.speedtest.net/es

De igual manera se asignó un perfil para todos los estudiantes en la subred ***192.Y.Y.Y/yy,*** dando un ancho de banda máximo de 3M/10M subida/bajada que de la misma forma debe ser compartida entre todos los usuarios que estén haciendo uso de la red (ilustración 82).

Ilustración 81. Ancho de banda grupo Estudiantes
Fuente: http://beta.speedtest.net/es

Para poder determinar el correcto funcionamiento del sistema se procede a realizar pruebas de velocidad en horas determinadas donde exista el mayor y menor número de usuarios conectados en la red “ficawifi”. La ilustración 82 y 83 muestra un total de 92 y 26 usuarios activos a las 10:20 am y las 14:00 pm respectivamente.

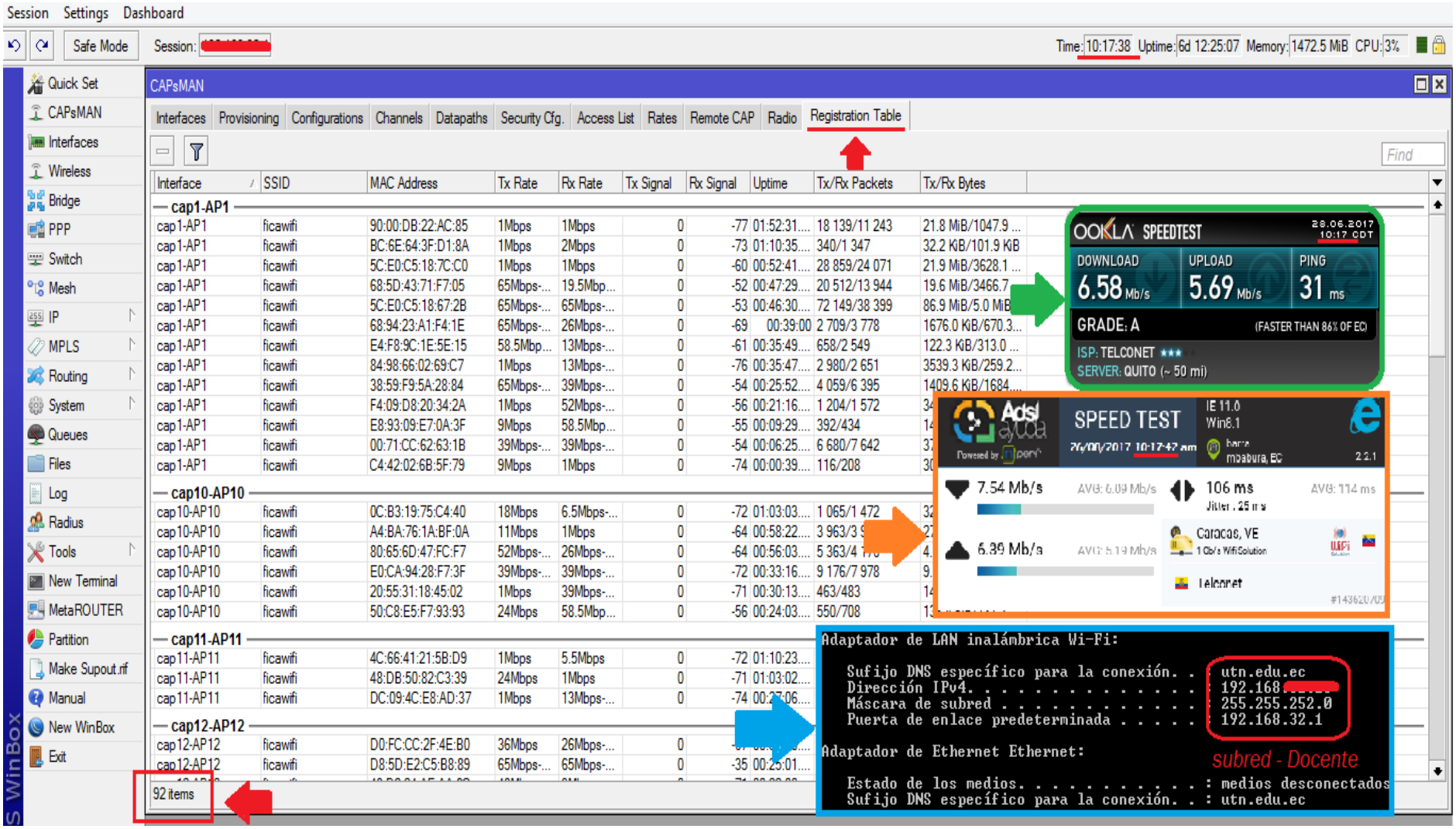


Ilustración 82. Prueba 5 - Subred Docentes/Administrativos

Fuente: Servidor MikroTik

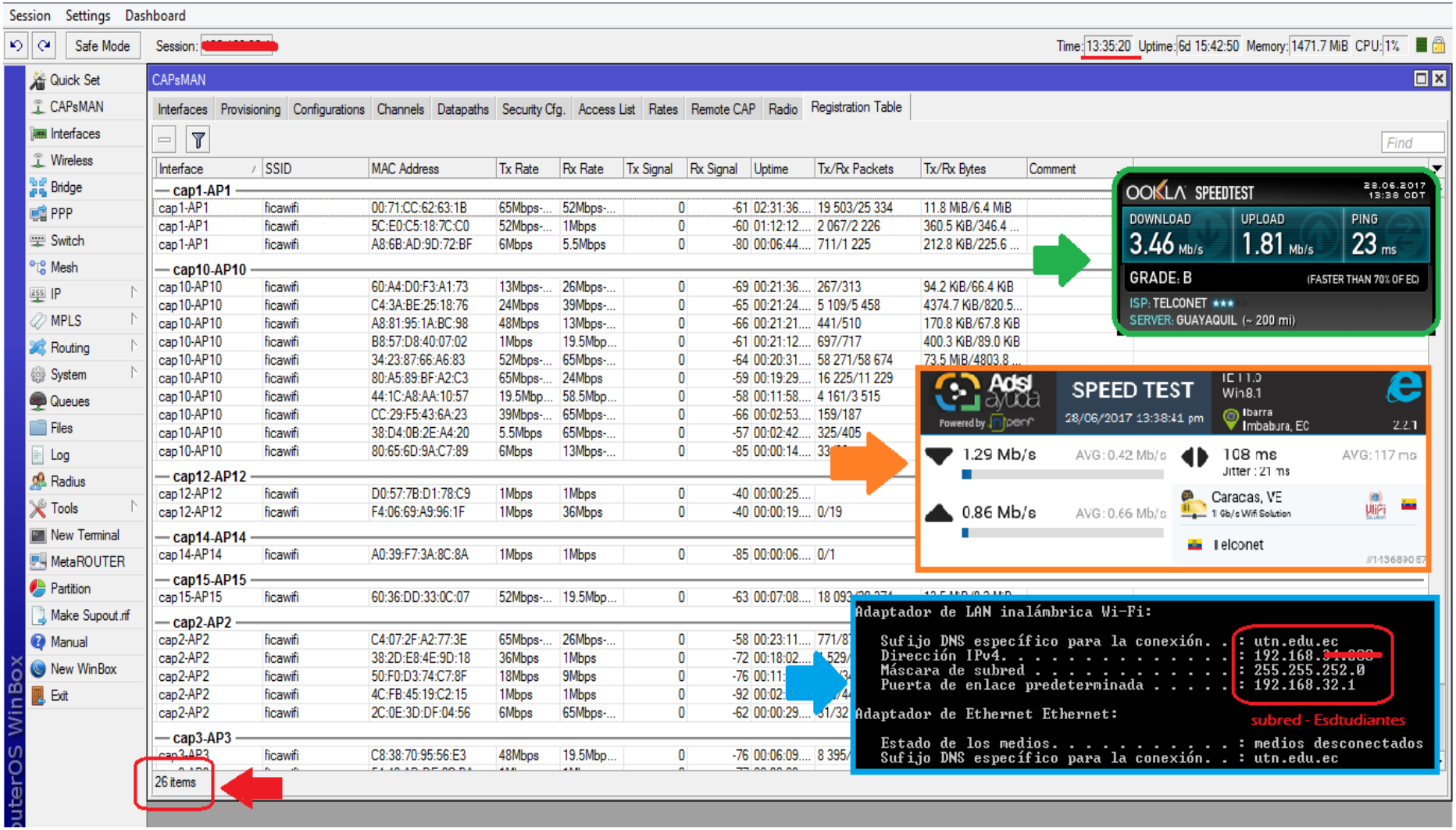


Ilustración 83. Prueba 6: Subred Estudiantes

Fuente: Servidor MikroTik

Análisis: De acuerdo a las ilustraciones anteriores se verifica que para el control de ancho de banda se hace uso de colas simples distribuidas en dos sub redes, una para estudiantes y otra para el personal docente-administrativo con sus debidas limitaciones de velocidad. Al contar con un total de 92 usuarios activos se puede notar como la velocidad inicial ha bajado de 15/21 Mbps a 6/5 Mbps, esto quizá se podría decir debido al gran número de usuario conectados, sin embargo, con la ilustración siguiente se nota que la velocidad 3/10 Mbps ha descendido mucho más en la subred Estudiantes dando solamente 3/1 Mbps, lo cual indica que el ancho de banda pese a estar distribuida en dos grandes subredes, no trabaja de la forma adecuada. El Server DHCP, asignará una dirección indistintamente si es un estudiante, un docente o un empleado, lo que da como consecuencia que el ancho de banda no se asigne correctamente al usuario que acabe de engancharse a la red, por consiguiente, es necesario realizar más cambios en las configuraciones de los equipos para solventar esta falencia, tomando en consideración un amarrado de MAC/IP.

Para poder determinar el grado de satisfacción y aceptación del servicio AAA implementado en la red inalámbrica de la facultad se aplica por segunda ocasión la metodología de investigación descrita en el apartado 3.3.4. (ANEXO A)

La interpretación de resultados obtenidos con sus respectivos análisis se encuentra detallados en el Anexo C de este trabajo investigativo, de los cuales se puede concluir que:

- El desempeño de la red inalámbrica en el último mes de julio se califica como Muy Bueno y Excelente en comparación al anterior mecanismo de autentificación (Hotspot) permitiendo a los usuarios una velocidad de navegación aceptable, sin presentar problemas en la conexión y disponibilidad de la misma para la mayoría de los usuarios.

- Se logró mitigar las fallas de conexión en el horario de 7am – 10am, el cual presentaba problemas de conexión por el ex eso de dispositivos enganchados a un solo Access Point, de esta manera se ratifica el buen funcionamiento de los puntos de acceso, al permitir conectar un máximo de 2 dispositivos por usuario para hacer uso de la red inalámbrica.
- De acuerdo a la tabulación de datos se establece que los de usuarios utilizan la red para acceder a páginas de consultas, YouTube y redes sociales, los cuales pueden ocasionar problemas de disponibilidad en la red, por tanto se debe optar por mecanismos de control extras como la marcación de paquetes, filtros para disminuir la calidad de los videos, entre otras; para evitar que se consuma más AB de lo establecido a cada usuario.
- Los sistemas operativos más utilizados para acceder a la red en ordenadores portátiles son Windows 8 y Windows 10, indicando de esta forma que el hacer uso de software de terceros (SECURE W2) no representa un requisito fundamental para poder conectarse a la red, por otra parte en dispositivos móviles se pudo determinar que no existe problema alguno para lograr una conexión exitosa a la red ya que el sistema operativo Android y iOS-IPhone poseen mecanismo EAP-TTLS de forma nativa

5.8 Optimización de la red “ficawifi”

Debido a la gran cantidad de usuarios enganchados a la red inalámbrica de la facultad, se logra descubrir algunas falencias en las configuraciones de los equipos, los cuales provocan una deficiencia en la red. La tabla 23 muestra las fallas encontradas en la fase de implementación.

Tabla 23. Fallas en la red

N° Ítem	Criterio
1	Amarre IP/MAC para Docentes y personal administrativo
2	Reasignación direcciones IP mediante DHCP-SERVER
3	Reconfiguración DNS para servicios internos (Portal UTN, portafolios, biblioteca, repositorio)

Fuente: Elaborado por el autor

5.8.1 Amarre IP/MAC para Docentes y personal administrativo

Según la ilustración 69, se observa que existe una subred para docentes/personal administrativo y una subred para estudiantes, cada una con su respectivo ancho de banda. Sin embargo, existe una pequeña dificultad al momento de configurar la dirección IP que el servidor DHCP asignará a cada usuario, debido a que nuestro Router-Mikrotik no distingue entre un dispositivo del docente, el estudiante o un administrativo, asignando la IP disponible en el pool de direcciones sin considerar el grupo al que pertenece, produciendo de tal manera una asignación errónea del ancho de banda. Por tanto, se ve la necesidad de implementar un amarrado IP/MAC el cual consiste en dar una única dirección IP a cada docente y personal administrativo evitando que esta dirección sea copiada, o utilizada por alguien más.

Para ello se va a la pestaña IP/ARP/AÑADIR NUEVO (ilustración 84), en el cual se colocara los siguientes datos:

Ip Address: Dirección IP de la subred Docentes/Personal Administrativo
Mac Address: Dirección MAC del equipo
Interface: Interface de salida a internet (bridge 1)
Comment: Nombre de usuario para dicha configuración

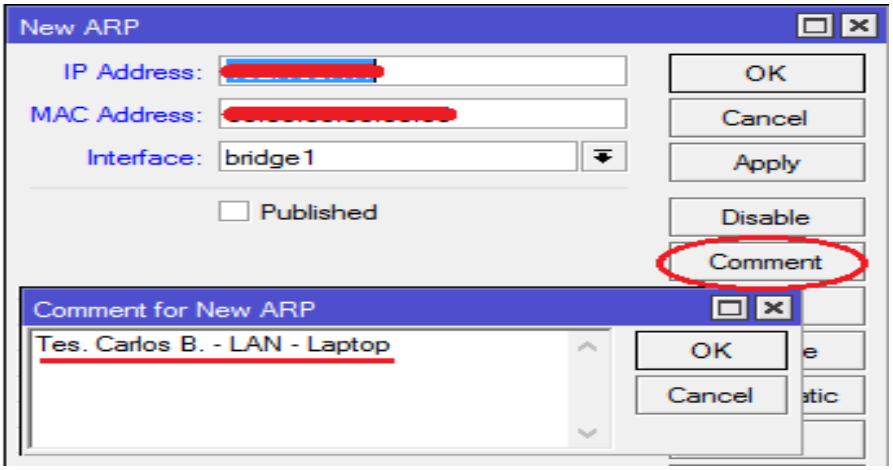


***Ilustración* 84**. Configuración ARP
Fuente: Router-Mikrotik

Una vez creada una nueva entrada se procede a realizar tantas copias como sea necesario de la misma configuración como indica la ilustración 85.

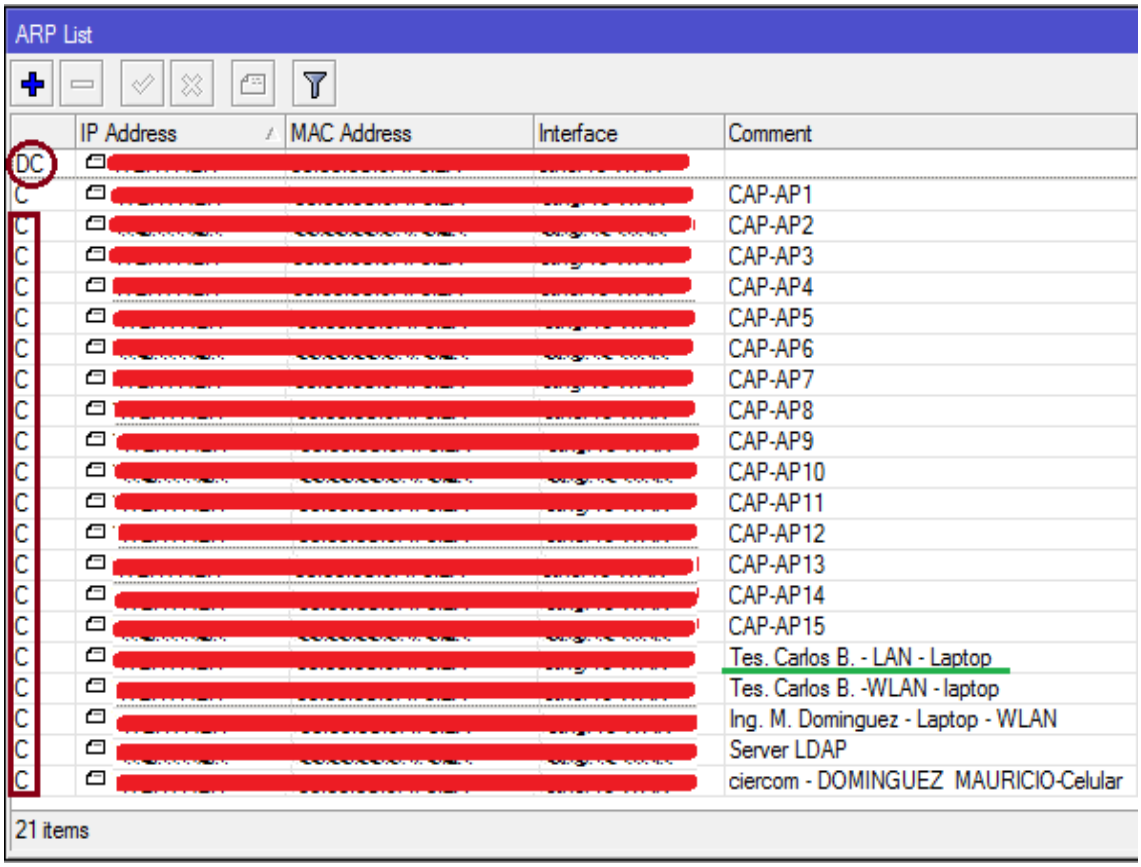


***Ilustración* 85.** Tabla ARP
Fuente: Router-Mikrotik

Como se puede observar en la ilustración anterior, se asigna una dirección IP a cada CAP que conforma a red inalámbrica de la facultad, así como también a todos los dispositivos de Docentes y personal Administrativo, se verifica con la letra “C” al lado

izquierdo de la misma que la configuración ha sido completada y exitosa. Una vez que la tabla ARP esté llena se continua con nuestro servidor DHCP, en la pestaña **IP/DHCP-SERVER/LEASES/** en el cual se puede notar a todos los usuarios que se encuentran enganchados a la red. Para poder agregar una nueva dirección IP , se pulsa el botón NEW (ilustración 86), y se colocan los mismos datos que en nuestra TABLA ARP, tales como:

Address: Dirección IP de la subred Docente/Administrativos
MAC Address: Dirección MAC del equipo
Server: Nombre del servidor DHCP
Insert Queue before: Nombre de la lista QUEUE
Comment: Nombre de usuario para dicha configuración

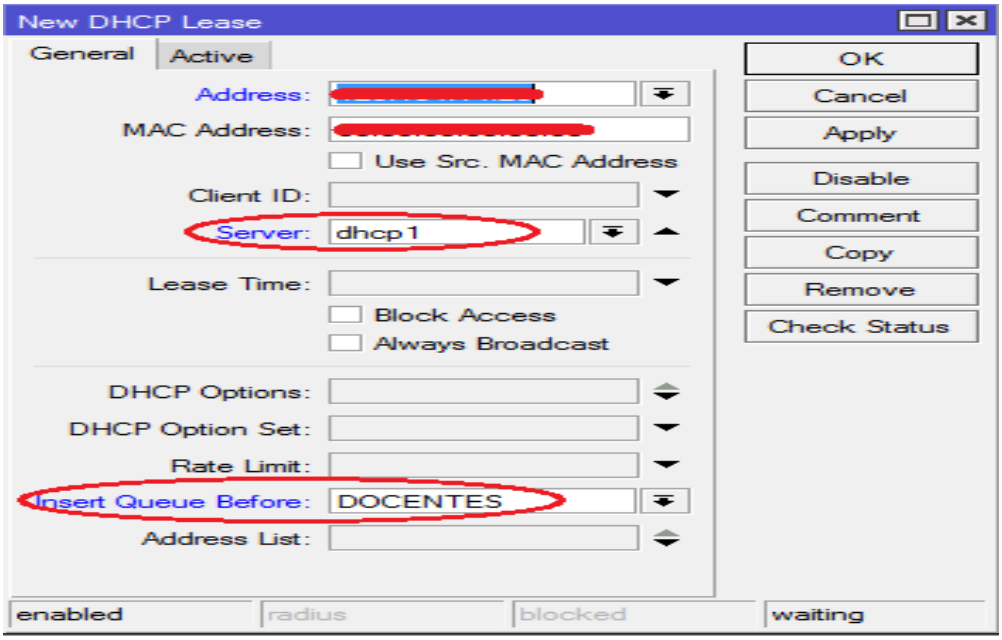


***Ilustración* 86.** Asignación IP por DHCP
Fuente: Router-Mikrotik

De la misma forma que en la tabla ARP, se verifica que todas las direcciones estén registradas en el DHCP, para lograr de esta forma la configuración automática de las mismas en los equipos finales de los docentes y el personal administrativo (ilustración 87). Cabe recalcar que al realizar esta configuración se asegura la distribución correcta del ancho de banda para todo el grupo de Docentes/Personal Administrativo evitando que los estudiantes cambien su IP manualmente para suplantar las direcciones de sus profesores.

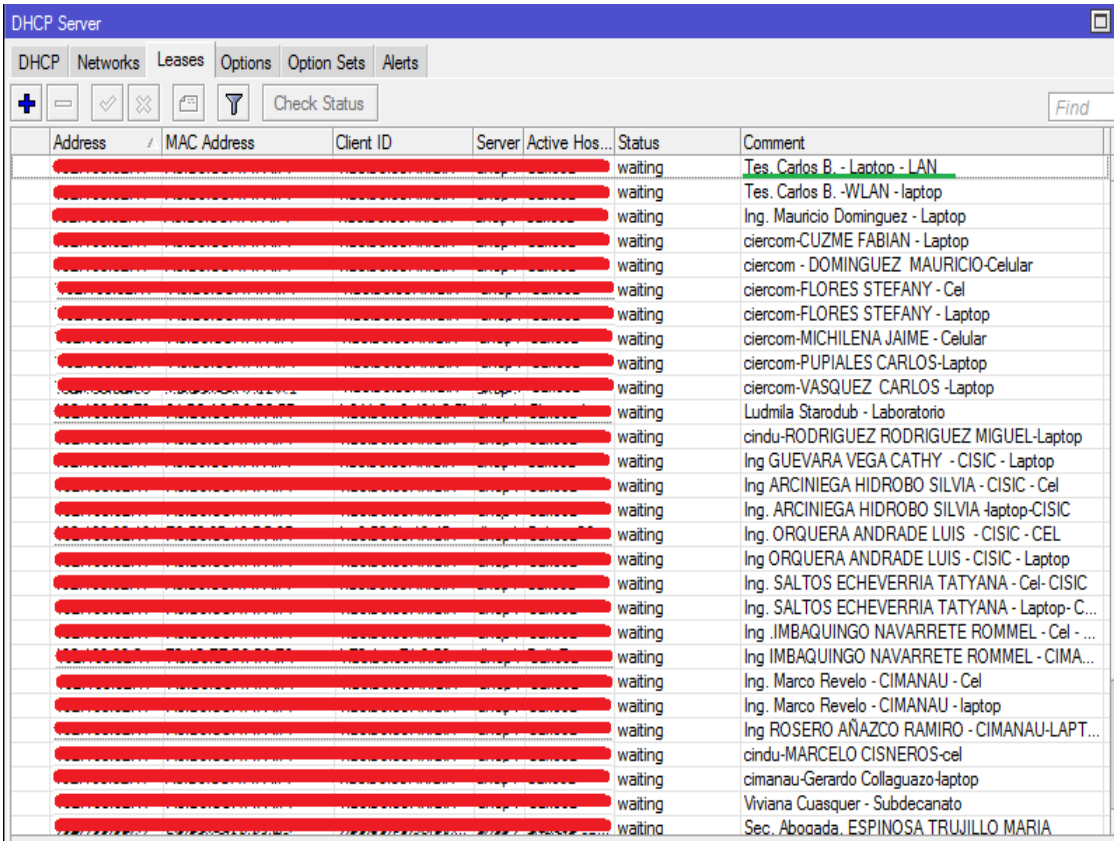


***Ilustración* 87.** Verificación DHCP-SERVER
Fuente: Router-Mikrotik

5.8.2 Reasignación de rango IP en DHCP-SERVER

De acuerdo a la ilustración 79, se tiene la red 192.X.X.X/xx dando un total de 1022 direcciones ip validas utilizables, de las cuales aproximadamente 328 direcciones son asignados a todo el personal docentes y administrativo según la tabla 7, por lo tanto, se ve la necesidad de mover el rango de IP en el servidor DHCP para que asigne dichas configuraciones solo a los estudiantes, ya que anteriormente se asignó una ip específica a cada docente de la institución con el amarrado IP/MAC. Para esto se situa en IP/POOL/Edit y se coloca nuestro nuevo rango de direcciones IP (ilustración 88) que en este caso vendría a ser:

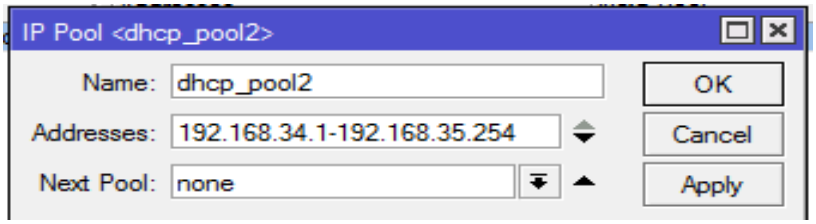


***Ilustración* 88.** Rango IP

Fuente: Router-Mikrotik

5.8.3 Reconfiguración DNS para servicios internos (Portal UTN, portafolios, biblioteca, repositorio)

Debido a que la red “ficawifi” es una red inalámbrica privada dentro de la facultad esta debe constar con los permisos respectivos para poder acceder a los recursos q brinda la universidad tales como el portal UTN, los portafolios para el control de asistencia de los alumnos, aula virtual, entre otros, por lo cual es de suma importancia que estos servicios estén disponibles todo momento. Para asegurar los servicios se busca la pestaña **IP/DNS,** se verifica la pestaña **STATIC** donde se muestra las direcciones IP correspondientes a dichos servicios. (ilustración 89).

#	Name	Regexp	Address	TTL (s)
0	utn.edu.ec		172.16.44.2	1d 00:00:00
1	biblioteca.utn....		172.16.1.248	1d 00:00:00
2	repositorio.utn....		172.16.3.31	1d 00:00:00
3	svrapp3.utn.e...		172.16.3.14	1d 00:00:00

***Ilustración* 89.** Redireccionamiento DNS

Fuente: Router-Mikrotik

De acuerdo a la ilustración anterior se tiene:

- **Utn.edu.ec** = Dominio del portal UTN (172.16.44.2)
- **Bilioteca.utn.edu.ec** = Dominio del recurso Biblioteca Universitaria (172.16.1.248)
- **Repositorio.utn.edu.ec** = Dominio del recurso Repositorio Digital UTN (172.16.3.31)
- **Svrapp3.utn.edu.ec** = Dominio de portales (Estudiantes, Docentes, Administrativos) (172.16.3.14)

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- La Facultad de Ingeniería en Ciencias Aplicadas (FICA) cuenta con un sistema de seguridad y autentificación AAA de usuarios, que permite al administrador de la red una gestión y administración centralizada de todos los recursos.
- Para poder manejar las cuentas de usuarios almacenados en la base de datos LDAP se hace uso de la herramienta de gestión PhpLdapAdmin, la cual facilita la creación, modificación o eliminación de datos, de esta manera permiten al administrador de la red manejar la enorme cantidad de usuarios de un amanera más sencilla y fácil.
- Las pruebas de funcionamiento de los equipos, permitieron conocer las condiciones iniciales en las que se encontraban tanto a nivel lógico como físico, se verificó la capacidad de información que podían almacenar, el tipo de sistema operativo compatible, memoria RAM, ROM, entre otras para poder levantar el servidor de autentificación.
- Mediante la implementación del sistema AAA y las pruebas realizadas en el capítulo 5 se logró determinar que se está brindando un servicio de calidad a todos los usuarios de la red, se asegura una conexión confiable y segura, mejorando la calidad en la navegación de internet por medio de mecanismos de control para el ancho de banda.

6.2 Recomendaciones

- Antes de utilizar los equipos se debe proceder a sacar respaldos de todas las configuraciones existentes, de esta manera se evita borrar algún tipo de información relevante almacenado en los mismos.
- Antes momento de implementar algún tipo de servicio, se debe incluir todo tipo de seguridades a nivel lógico (firewall) en los servidores, así como también una buena segmentación de la red (vlans).
- Realizar mantenimientos periódicos por lo menos cada 6 meses de las infraestructuras tecnológicas para garantizar el buen funcionamiento de las mismas (revisión de logs, almacenamiento, actualizaciones, entre otras).
- Para el buen funcionamiento del sistema implementado será necesario indicar a los usuarios las formas adecuadas de utilización, como puede ser la manera correcta de conectarse a la red, el número de dispositivos permitidos, el ancho de banda otorgado, entre otras. Esto con el fin de evitar que se intente colapsar el sistema con ataques informáticos, siendo el más común DoS (Denegación de servicio)
- El sistema implementado se encuentra enfocado para todos aquellos dispositivos con soporte del estándar 802.1x, esto debido a que en la actualidad la mayoría de marcas comerciales dan este tipo de soporte en forma nativa, sin embargo se debe implementar más mecanismos de acceso para usuarios invitados que no cuenten con una cuenta dentro de la base de datos.
- Cada vez que un usuario acaba su carrera estudiantil u opta por dejar la carrera, tanto su cuenta como su password se quedará grabado en la base de datos LDAP, por tanto, el administrador de red deberá dar de alta a este tipo de usuarios al inicio

de cada nuevo ciclo estudiantil generando un nuevo archivo (sección 5.3.4) y eliminando el anterior, para no desperdiciar la memoria del servidor.

- Para brindar una mayor eficiencia del servicio se debe implementar otro servidor Radius que actué como soporte en caso de que el actual falle, brindando alta disponibilidad en la red.
- El uso de sistemas operativos en distribución libre se convierte en un pilar fundamental para el desarrollo de seguridades tecnológicas, sin embargo, es necesario tener un cierto nivel de conocimientos teóricos y prácticos para lograr poner en funcionamiento el sistema.

Glosario de Términos

AAA: Corresponde a un tipo de protocolo que ejecuta tres funciones: Autentificación, Autorización y Contabilización.

AES: Advanced Encryption Standard, protocolo de cifrado más seguro introducida con WPA2, sustituto de TKIP el cual ofrece un mayor nivel de seguridad, pero requiere un hardware específico que no es compatible con los dispositivos que sólo funcionaban con WEP y con WPA.

DataCenter: centro de procesamiento de datos, mantiene servidores y equipamiento electrónico para el funcionamiento de una red robusta de datos.

EAP/TTLS: EAP de túnel-Transport Layer Security, elimina la necesidad de un certificado para cada cliente de la red, estableciendo un túnel de conexión segura.

EAP: (Extensible Authentication Protocol): Protocolo de autenticación de usuarios en Radius.

IEEE 802.1X: solución de seguridad que puede autenticar (identificar) a un usuario que quiere acceder a la red (ya sea por cable o inalámbrica). Esto se hace a través del uso de un servidor de autenticación.

ISO/IEC/IEEE 29148: contiene disposiciones para los procesos relacionados con ingeniería, determina requisitos para los sistemas y productos de software y servicios a lo largo del ciclo de vida.

LAN: Local Area Network, interconecta los ordenadores en un área relativamente pequeña (Oficina, aulas, hogar).

LDAP: (Lightweight Directory Access Protocol): Protocolo Ligero/Simplificado de Acceso a Directorios, hace referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

MAN: Metropolitan Area Network, caracterizada por realizar conexiones de muy alta velocidad, resistentes a interferencias radioeléctricas.

NAS: Network Access Server, Es un sistema que proporciona acceso a la red. En algunos casos también se conoce como RAS (Remote Access Server) o Terminal Server. En general, NAS es un elemento que controla el acceso a un recurso protegido.

PAP: Password Authentication Protocol, protocolo de autentificación simple (ASCII sin cifrar) entre usuario y cliente remoto.

PEAP: Protected Extensible Authentication Protocol, es un método para transmitir de manera segura información de autenticación, incluyendo contraseñas, sobre redes cableadas e inalámbricas.

PHPLDAPADMIN: Conocido como PLA, es una herramienta para la administración de servidores LDAP escrito en PHP, basado en interfaz Web y da acceso a la base de datos LDAP desde cualquier lugar de la red.

PoE: Tecnología que incorpora la alimentación eléctrica en infraestructura de redes locales por medio de un cable Ethernet con RJ45.

RADIUS: Remote Authentication Dial-In User Service, protocolo de autentificación y autorización en redes cableadas o inalámbricas, utiliza el puerto 1812 UDP para establecer conexiones.

RFC: Request For Comments, consiste en un documento que posee una propuesta sobre nuevas tecnologías, información de uso, proyectos experimentales y demás, escrito por algunas personas.

SMP: Symmetric Multi-Processing, arquitectura de computadores en las que se comparte dos o más unidades de procesamiento en una solo memoria central.

SPX/IPX: Internetwork Packet Exchange/Sequenced Packet Exchange, protocolo orientado a paquetes y no a conexión, interconecta redes locales, actualmente reemplazado por TCP/IP.

TACACS: Terminal Access Controller Access Control System, se trata de un protocolo exclusivo de cisco para la autentificación segura de forma remota.

TCP/IP: Modelo utilizado para comunicaciones en redes jerarquizado en 7 capas, provee conectividad de extremo a extremo.

TKIP: Protocolo de integridad de clave temporal, similar a la encriptación WEP, es bastante débil y fácilmente vulnerado.

WAN: Wide Area Network, interconecta varias redes LAN, abarca más territorio al ser una red de área amplia.

WEP: Wired Equivalent Privacy, sistema de cifrado nivel 2 basado en CR4, utiliza claves de 64 o 128 bits para brindar confidencialidad a las redes inalámbricas.

WLAN: Wireless Local Network, sistema de transferencia de datos sin una conexión cableada existente.

WPA: Wi-Fi Protected Access, sistema de protección para redes inalámbricas debido a las falencias que posee su antecesor el cifrado WEP.

WPA2 ENTERPRISE: Wi-Fi Protected Access 2, en la versio de autentificación basado en 802.1x/EAP para redes empresariales, la cual establece una contraseña y un Password único de acceso a la red.

Referencias Bibliográficas

CCM. (06 de 2016). Obtenido de http://es.ccm.net/contents/785-802-1x-eap

Acosta, J. A. (2013). Servicio de Directorio LDAP. Obtenido de https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=60&ved=0ahUKEwjUg_bIyZzQAhUD5WMKHY10Do44MhAWCFQwCQ&url=http%3A%2F%2Fwww.iesjacaranda-brenes.org%2Fredmine%2Fattachments%2Fdownload%2F66%2FDocumentacion.pdf&usg=AFQjCNHbqqJ2J-KADf_nB_Fh3hHGMy

Alvarez, B. R. (s/f). *Avances en criptología y seguridad de la información.* Díaz de Santos.

apser. (19 de 08 de 2015). Obtenido de http://www.apser.es/blog/2015/08/19/que-es-la-disponibilidad-informatica-y-cual-es-su-importancia/

Bertolín, J. A. (2010). *Seguridad de la información. Redes, informática y sistemas de información.* Paraninfo.

buffalo-technology. (2015). Tecnología estándar - Tecnologías 802.11 inalámbricas. Obtenido de http://www.buffalo-technology.com/es/tecnologia/software-asociado/wireless-80211-technologies/

Caicedo, A. (10 de 08 de 2013). ADMINISTRACIÓN DE REDES DE COMPUTADORES. Obtenido de https://www.academia.edu/11531163/ADMINISTRACI%C3%93N_DE_REDES_DE_COMPUTADORES_Conceptos_Generales

Castro, A. (s/f). *Google Sites*. Obtenido de https://sites.google.com/site/jachsistemascomputacionales/about-me

CCM. (15 de 10 de 2016). Introducción a Wi-Fi (802.11 o WiFi). Obtenido de http://es.ccm.net/contents/789-introduccion-a-wi-fi-802-11-o-wifi

CCM. (2016). WiMAX - 802.16 - Interoperabilidad mundial para acceso por micro. Obtenido de http://es.ccm.net/contents/795-wimax-802-16-interoperabilidad-mundial-para-acceso-por-micro

CentOs. (s/f). Obtenido de https://www.centos.org/

Chamorro, J. M. (02 de 2010). *SANS Institute InfoSec Reading Room.* Obtenido de https://www.sans.org/reading-room/whitepapers/wireless/consideraciones-para-la-implementacion-de-8021x-en-wlans-1607

Chillispot. (s/f). Obtenido de http://www.chillispot.org/

CISCO. (2012). Lo que usted necesita saber sobre redes inalambricas. Obtenido de http://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/wireless/pdfs/brochure_wireless.pdf

Debian. (s.f.). Obtenido de https://www.debian.org/intro/about.es.html

Delgado, A. R. (18 de 11 de 2015). *Wiki Centos*. Obtenido de https://wiki.centos.org/es

Departamento de Informática UTN. (09 de 2010). CENTRO DE ENTRENAMIENTO Y CERTIFICACIÓN INTERNACIONAL EN TICs.

Domínguez, M. V. (2011). Soluciones de seguridad en redes inalámbricas.

Duran, J. M. (2012). Servidor Radius - FreeRadius.

ECURED. (10 de 2012). Redes Informaticas. Obtenido de https://www.ecured.cu/Administrador_de_red

Escalona, S. B. (2011). Protocolos de control de acceso RADIUS. *Revista Digital de las Telecomunicaciones*. Obtenido de http://revistatelematica.cujae.edu.cu/index.php/tele/article/download/51/50.

F5 Networks. (2016). Obtenido de https://f5.com/glossary/diameter-protocol

FICA. (2016). Vision. Obtenido de http://www.utn.edu.ec/fica/

García, A. A. (12 de 2007). Desarrollo de herramientas web de gestión docente. Cartagena. Obtenido de http://repositorio.upct.es/bitstream/handle/10317/179/pfc2475.pdf;jsessionid=A9C3A6D91A7C25E7A9C3769FEDB7CF0F?sequence=1

García, C., Quezada, C., & Bello, D. (14 de 07 de 2010). Trabajo Investigativo Portal Cautivo. Chile. Obtenido de http://es.slideshare.net/valericio1/portal-cautivo

Guiza, J. A. (2010). *PROYECTO AAA UD NET*. Obtenido de https://proyecto-teleco-2010.wikispaces.com/file/view/Marco+teorico+AAA.pdf

Hernández López, J. (2012). Implementación de un portal cautivo para la autenticacion de usuarios en redes usando software libre. Mexico. Obtenido de http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/2644/tesis.pdf?sequence=1

Herrera, D. R. (2011). Diseño e implementacion de un portal cautivo que permita la venta de tickets. Quito. Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/3953/1/CD-3714.pdf

Hi-Tech IP. (29 de 07 de 2015). Obtenido de http://www.hi-techip.com/seguridad-en-redes-informaticas/

Huerta, A. V. (julio de 2014). *RedIris.* Obtenido de Red Academica y de investigación Nacional: https://www.rediris.es/cert/doc/unixsec/unixsec.pdf

International Organization for Standardization. (12 de 2011). *ISO/IEC/IEEE 29148*. Obtenido de http://www.iso.org/iso/catalogue_detail.htm?csnumber=45171

Juniper Networks. (20 de 08 de 2014). TACACS+ Server. Obtenido de http://www.juniper.net/techpubs/en_US/junose15.1/information-products/topic-collections/broadband-access/tacacs+-server/tacacs+-server.pdf

López, I. B. (20 de 10 de 2014). *belt*. Obtenido de http://www.belt.es/expertos/experto.asp?id=2245

Lorente, V. M. (21 de 05 de 2014). Implementación de un portal cautivo con Wifidog. Obtenido de https://www.uco.es/aulasoftwarelibre/375-implementacion-de-un-portal-cautivo-con-wifidog/

Mejía, L. M. (28 de 12 de 2016). *GNU*. Obtenido de https://www.gnu.org/philosophy/free-sw.es.html

Mengual, E., Garcia Villegas, E., & Vidal, R. (2013). Uso de canales solapados en una red de área de campus inalámbrica con IEEE 802.11. España. Obtenido de http://upcommons.upc.edu/e-prints/bitstream/2117/22326/1/MengualGarciaVidal_Jitel2013.pdf.

Microsoft Official Academic Course. (08 de 01 de 2014). Fundamentos de Redes. Obtenido de http://movil.sigma.gob.bo/formulario/redes/fundamentos_de_redes.pdf

Molero, L. (2010). Planificacion y Gestion de Red. Maracaibo, Venezuela. Obtenido de http://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/planificacion-gestion-red/Unidad-I.pdf

Navarro, F. P. (07 de 2013). ANÁLISIS TEÓRICO Y EXPERIMENTAL SOBRE SEGURIDAD EN REDES WI-FI. Málaga. Obtenido de http://riuma.uma.es/xmlui/bitstream/handle/10630/8409/pfc.pdf?sequence=1

Network Radius. (2014). THE FREERADIUS TECHNICAL GUIDE. Obtenido de http://networkradius.com/doc/FreeRADIUS-Technical-Guide.pdf

networkradius. (2014). *http://networkradius.com/.* Obtenido de http://networkradius.com/doc/FreeRADIUS%20Technical%20Guide.pdf

Novoa, J. M. (01 de 10 de 2013). Seguridad en redes inalámbricas de área local (WLAN). Cataluña, España. Obtenido de

http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf

Orqueta, G. D. (2010). *Seguridad en las comunicaciones y en la información.* UNED.

Panda Software Internacional. (2011). Seguridad en redes inalambricas. Obtenido de http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf

Paz, M. M. (03 de 2010). *SEGURIDAD LÓGICA Y DE ACCESOS Y AUDITORÍA*. Madrid.

Portilla, D. C. (2011). Investigación del servidor Radius para la seguridad en redes LAN inalámbricas. Riobamba. Obtenido de http://dspace.unach.edu.ec/bitstream/51000/627/1/UNACH-EC-ISC-2011-0005.pdf

Pradas, R. C. (2013). *RedIRIS.* Obtenido de Red Academica de Investigacion Nacional: https://www.rediris.es/ldap/doc/ldap-intro.pdf

Pymes.com. (31 de 05 de 2011). Obtenido de http://www.pymesyautonomos.com/management/administrar-organizar-dirigir-gestionar-parecido-pero-no-es-lo-mismo

Ramírez, J. M. (08 de 03 de 2012). *https://www.jmramirez.pro/*. Obtenido de https://www.jmramirez.pro/tutorial/wifi-mas-seguro-con-freeradius/

Ramos, M. d. (2012). *SEGURIDAD INFORMATICA ED.11*. Paraninfo.

Rodriguez, R. E. (2015). *Grado en Estadistica y Empresa. Tecnicas de Inferencia Estadistica.*

Rohde & Schwarz. (2016). Tecnología Bluetooth. Obtenido de https://www.rohde-schwarz.com/es/tecnologias/conectividad-inalambrica/bluetooth/tecnologia-bluetooth/tecnologia-bluetooth_55694.html

Romero, O. R. (2010). *SERVICIOS EN RED.* Paraninfo.

Sánchez, M. Á. (10 de 10 de 2007). *Linux Zone*. Obtenido de http://linuxzone.es/distribuciones-principales/ubuntu/

Sánchez, M. Á. (10 de 10 de 2012). *LinuxZone*. Obtenido de https://linuxzone.es/distribuciones-principales/ubuntu/

Segu-Info. (2009). Obtenido de Seguridad de la Informacion: http://www.segu-info.com.ar/logica/seguridadlogica.htm

Seguridad Informática SMR. (10 de 2010). Obtenido de https://seguridadinformaticasmr.wikispaces.com/TEMA+3+-+SEGURIDAD+L%C3%93GICA

Significados.com. (2013). Obtenido de http://www.significados.com/administracion/

Simal, T. (12 de 02 de 2012). Redes Wifi - Seguridad en redes Wi-Fin. Obtenido de http://recursostic.educacion.es/observatorio/web/es/component/content/article/961-monografico-redes-wifi?start=7

somebooks. (13 de 08 de 2013). Obtenido de http://somebooks.es/?p=3442

Suárez, M. (2012). *INTERAPRENDIZAJE DE PROBABILIDADES Y ESTADÍSTICA INFERENCIAL* (rimera Edición ed., Vol. P). Ibarra: Imprenta Offset M &V.

Technology, M. I. (2010). Red Hat Enterprise Linux 4: Introducción a la administración de sistemas. Massachusetts. Obtenido de http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-isa-es-4/ch-acctsgrps.html

TekRadius. (2016). TekRADIUS - RADIUS Server for Windows. Obtenido de http://www.kaplansoft.com/tekradius/Docs/TekRADIUS-Datasheet.pdf

Torres, E. V. (13 de 05 de 2010). Seguridad en redes WiFi Eduroam. Sevilla. Obtenido de http://trajano.us.es/docencia/RedesYServiciosDeRadio/2010/Seguridad%20en%20redes%20Wifi%20Eduroam.pdf

Tutorial de Seguridad Informatica. (08 de 2013). Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html

UNAM. (2009). Obtenido de UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/775/A4.pdf?sequence=4

Universidad de la Republica. (2014). Tecnologías de acceso inalámbrico. Uruguay. Obtenido de https://eva.fing.edu.uy/pluginfile.php/67112/mod_folder/content/0/Material_Complementario-Tecnologias_de_acceso_inalambrico.pdf?forcedownload=1.

Universidad del Azuay. (08 de 2012). Obtenido de https://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/capa_aplicacion.htm

VozIdea.com. (26 de 04 de 2013). Obtenido de http://www.vozidea.com/phpmyadmin-administrador-bases-de-datos

ANEXOS

ANEXO A – Formatos de Encuestas

UNIVERSIDAD TÉCNICA DEL NORTE

FORMATO DE ENCUESTA APLICADA A LOS USUARIOS DE LA RED INALÁMBRICA DE LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS DE LA UNIVERSIDAD TÉCNICA DEL NORTE EN EL PERIODO MARZO 2017 - AGOSTO 2017

Objetivo. Determinar el estado actual de la red inalámbrica de la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte.

A) Datos Informativos

Sexo

a) Masculino ( )
b) Femenino ( )

Cargo

a) Estudiante ( )
b) Docente ( )
c) Administrativo ( )

Carrera

a) CIERCOM ( )
b) CIME ( )
c) CISIC ( )
d) CIMANELE ( )
e) CIMANAU ( )
f) Textil ( )
g) Industrial ( )

B) SITUACIÓN ACTUAL DE LA RED INALÁMBRICA

1. ¿Cómo calificaría el desempeño de la red inalámbrica de la facultad? (seleccione1)

a) Excelente ( )
b) Muy buena ( )
c) Buena ( )
d) Regular ( )
e) Mala ( )

2. ¿Al acceder a la red inalámbrica de la facultad que tipo de inconveniente presenta con frecuencia? (seleccione 1)

a) Problemas de conexión ( )
b) Disponibilidad ( )
c) Cobertura de red ( )

3. ¿En qué horario a experimentado falla de la conexión a la red inalámbrica? (seleccione 1)

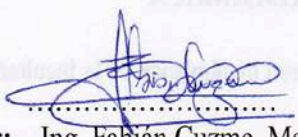
   a) De 7:00 am - 10:00 am ( )
   b) De 10:00 am – 1:00pm ( )
   c) De 1:00pm – 4:00pm ( )
   d) De 4:00pm – 7:00pm ( )

4. ¿Cuál es el tipo de información a la que accede con mayor frecuencia mediante el uso de la red inalámbrica de la facultad? (seleccione 1)

   a) Páginas de consultas académicas( )
   b) Aula virtual ( )
   c) Repositorios digitales ( )
   d) YouTube, Facebook ( )
   e) Juegos en línea ( )

5. ¿Cuantos dispositivos conecta a la red inalámbrica? (seleccione 1)

   a) 1 dispositivo ( )
   b) 2 dispositivos ( )
   c) 3 dispositivos ( )
   d) Más de 3 dispositivos ( )



Aprobado por: Ing. Fabián Cuzme, Msc
TUTOR

Ing. Mauricio Domínguez, Msc.
ADMINISTRADOR DE RED

Elaborado por: Carlos Bosmediano

UNIVERSIDAD TÉCNICA DEL NORTE

FORMATO DE ENCUESTA APLICADA A LOS USUARIOS DE LA RED "ficawifi" DE LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS DE LA UNIVERSIDAD TÉCNICA DEL NORTE EN EL PERIODO FEBRERO 2017 – AGOSTO 2017

Objetivo. Determinar el grado de satisfacción de los usuarios de la red inalámbrica "ficawifi"

A) Datos informativos

Sexo

a) Masculino ( )
b) Femenino ( )

Grupo

a) Docente ( )
b) Estudiante ( )
c) Administrativo ( )

Carrera

a) CIERCOM ( )
b) CIME ( )
c) CIMANELE ( )
d) CISIC ( )
e) CIMANAU ( )
f) CITEX ( )
g) CINDU ( )

B) Funcionamiento de red

1. ¿Cuántos dispositivos puede conectar a la red inalámbrica con su usuario y clave personal? (seleccione 1)

a) 1 dispositivo ( )
b) 2 dispositivos ( )
c) 3 dispositivos ( )
d) Más de 3 dispositivos ( )
e) Ninguno ( )

2. ¿Qué tipo de sistemas operativos utiliza en su ordenador para conectarse a la red inalámbrica "ficawifi"? (seleccione 1)

a) Windows 7 ( )
b) Windows 8 o 10 ( )
c) Linux ( )
d) Mac OS ( )

3. ¿Qué tipo de sistemas operativos utiliza en su dispositivo móvil para conectarse a la red inalámbrica ficawifi? (seleccione 1)

a) Android ( )
b) iOS-Iphone ( )
c) Windows Phone ( )
d) Otro……

4. ¿Cuál es el tipo de información a la que accede con mayor frecuencia mediante el uso de la red inalámbrica de la facultad? (seleccione 1)

a) Consultas académicas ( )
b) Aula virtual ( )
c) Repositorios digitales ( )
d) YouTube ( )
e) Redes Sociales ( )
f) Otros.....

C) Desempeño de la red

5. ¿Al acceder a la red inalámbrica de la facultad presenta algún tipo de inconveniente? (seleccione 1)

a) Problemas de conexión ( )
b) Restricción de acceso a páginas ( )
c) Cobertura de red ( )
d) Ninguna ( )
e) Otros.....

6. ¿En qué horario a experimentado fallas de la conexión a la red inalámbrica? (seleccione 1)

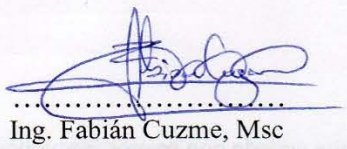
a) De 7:00 am - 10:00 am ( )
b) De 10:00 am – 1:00pm ( )
c) De 1:00pm – 4:00pm ( )
d) De 4:00pm – 7:00pm ( )
e) Ninguno ( )

7. ¿Cómo calificaría el desempeño de la red inalámbrica de la facultad en el último mes? (seleccione 1)

a) Excelente ( )
b) Muy buena ( )
c) Buena ( )
d) Regular ( )
e) Mala ( )

8. ¿Cómo calificaría la velocidad de navegación cuando se encuentra conectado a la red inalámbrica de la facultad? (seleccione 1)

a) Excelente ( )
b) Muy buena ( )
c) Buena ( )
d) Regular ( )
e) Mala ( )



Aprobado por: Ing. Fabián Cuzme, Msc
TUTOR

Ing. Mauricio Domínguez, Msc.
ADMINISTRADOR DE RED

Elaborado por: Carlos Bosmediano

ANEXO B – Formato de Entrevista

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

Entrevista – Msc. Mauricio Domínguez.

1. ¿Cuál es el desempeño de la red inalámbrica de la facultad?

   a) Excelente ( )
   b) Muy buena ( )
   c) Buena ( )
   d) Regular ( )
   e) Mala ( )

   Porque:……
   ……
   ……

2. ¿Qué problemas presenta la red inalámbrica?

   a) Problemas de conexión y acceso ( )
   b) Intermitencia en dispositovos ( )
   c) Disponibilidad ( )
   d) Cobertura de red ( )
   e) Otros ( )

   Porque:……
   ……
   ……
   ……
   …

3. ¿Cuál es la distribución de ancho de banda? ¿Es equitativa para todos los usuarios?

   ……
   ……

.....

.....

.....

4. ¿Cuántos usuarios aproximadamente pueden conectarse a la red inalámbrica?

.....

.....

.....

5. ¿Qué tipo de seguridades posee la red?

.....

.....

.....

.....

.....

6. ¿Qué tipo de mejoras se podría aplicar a la red?

.....

.....

.....

.....

.....

Carlos Bosmediano
Entrevistador

Msc. Mauricio Domínguez
Entrevistado

ANEXO C – Interpretación y Análisis de Resultados de Encuestas

ENCUESTA N°1: Determinar el estado actual de la red inalámbrica de la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte.

DATOS INFORMATIVOS

a) Sexo

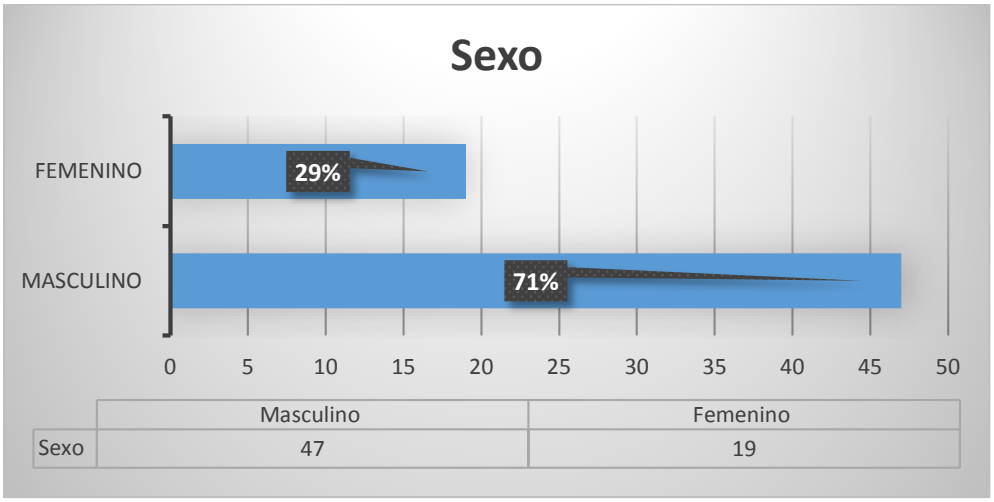


Gráfico 1 Sexo

Análisis:

En relación al sexo se determinó que 47 individuos equivalente al 71% son de sexo masculino y 19 individuos equivalentes al 29% son de sexo femenino.

b) Cargo

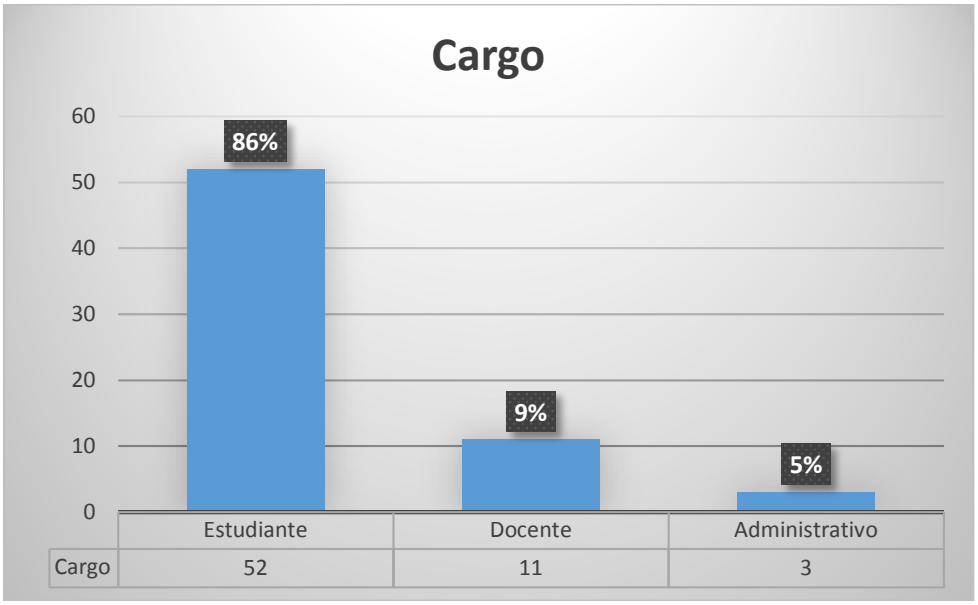


Gráfico 2 Cargo

Análisis:

El mayor número de encuestados lo constituyen los estudiantes de la facultad que representa el 86%, seguido del personal docente con el 9% y solo el 5% conformado por el personal administrativo.

c) Carrera

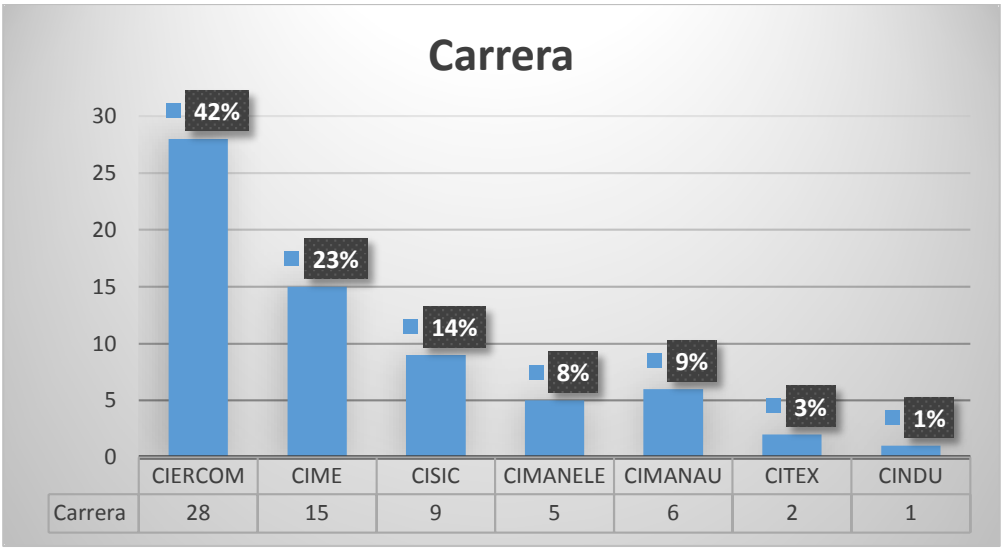


Gráfico 3 Carrera

Análisis:

Se puede evidenciar que existe un mayor número de encuestados pertenecientes a la carrera de CIERCOM equivalente al 42%, debido a que en el periodo actual se cuenta con el mayor índice de estudiantes matriculados (tabla 7), seguido de CIME con 23%, CISIC con el 14%, CIMANAU con el 9%, CIMANELE con el 8%, mientras que CITEX y CINDU con el 3 % y 1% respectivamente, presentan el más bajo porcentaje, dado que ambas carreras fueron reubicados a otros sitios de la ciudad, sin embargo pertenecen a la facultad.

SITUACIÓN ACTUAL DE LA RED

1) Determinar el grado de aceptación de la red inalámbrica para los estudiantes de la facultad.

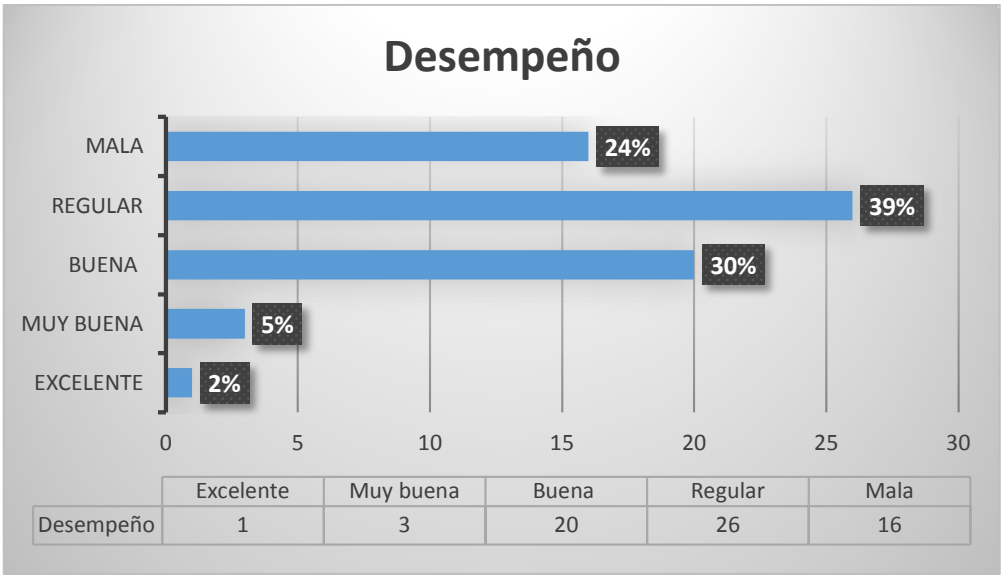


Gráfico 4 Desempeño de la red

Análisis:

Según los datos recolectados el 39% de encuestados afirman que el actual desempeño de la red es regular, el 30% de los mismos aseguran que la red es buena, a diferencia del 24% que aseguran un desempeño malo de la red debido a varios inconvenientes que se presentan a diario en la red.

2) Determinar los tipos de inconvenientes que se presentan con mayor frecuencia.

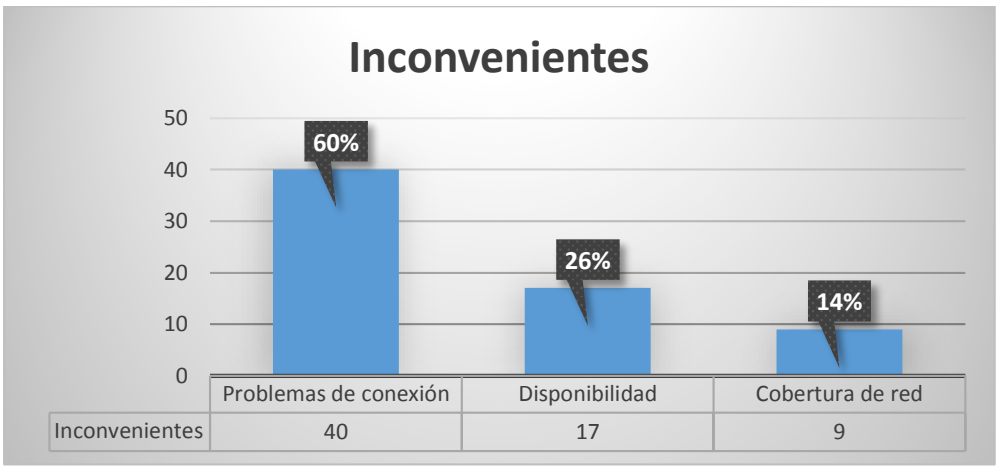


Gráfico 5 Inconvenientes presentados con el uso de la red.

Análisis:

Los datos obtenidos revelan que el mayor inconveniente que se da en la red inalámbrica se debe a problemas de conexión, registrando un total del 60% de las

personas encuestadas, esto puede deberse a varios motivos como puede ser el exceso de solicitudes que hacen los usuarios a los AP, fallas en las configuraciones de los equipos, mala distribución del ancho de banda entre otros. De igual manera otro problema que se observa es la disponibilidad registrando un 26% mientras que solamente el 14% afirma que el problema frecuente es por la cobertura de red.

3) Determinar horas pico para fallas de conexión a la red.

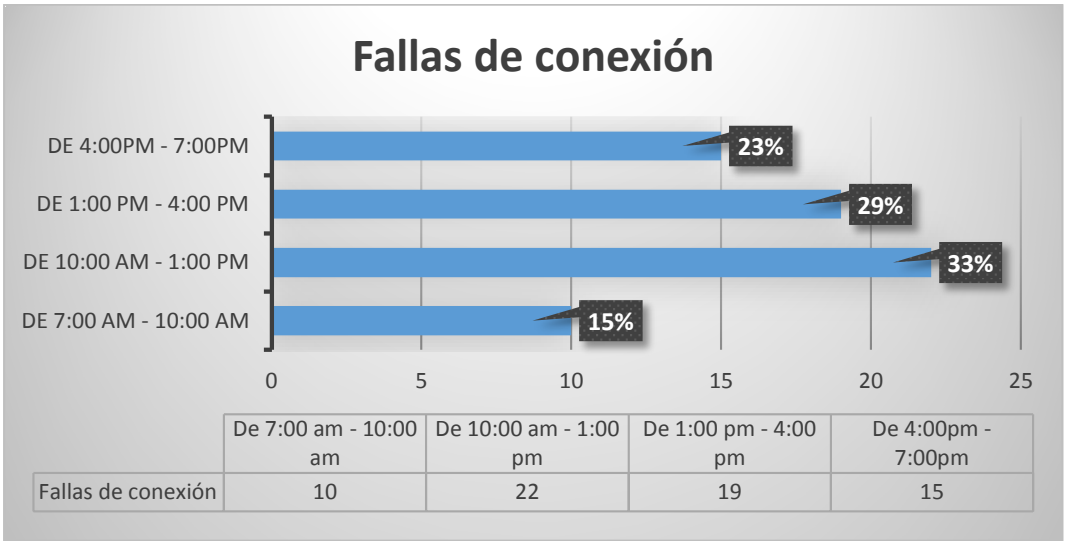


Gráfico 6 Horas pico de fallas de conexión

Análisis:

De todas las personas encuestadas, 22 individuos que representan el 33% han experimentado fallas en la conexión de red entre las 10:00 am hasta la 1:00 pm, por lo cual se puede decir que existe mayor demanda de peticiones hacia los AP en este horario, provocando una caída parcial o total del servicio, por otro lado el 29% afirman que las fallas en la conexión no solo se presentan por la mañana, ya que también se da entre la 1:00pm y las 4:00pm.

4) Determinar el tipo de información que manejan los usuarios al hacer uso de la red inalámbrica.

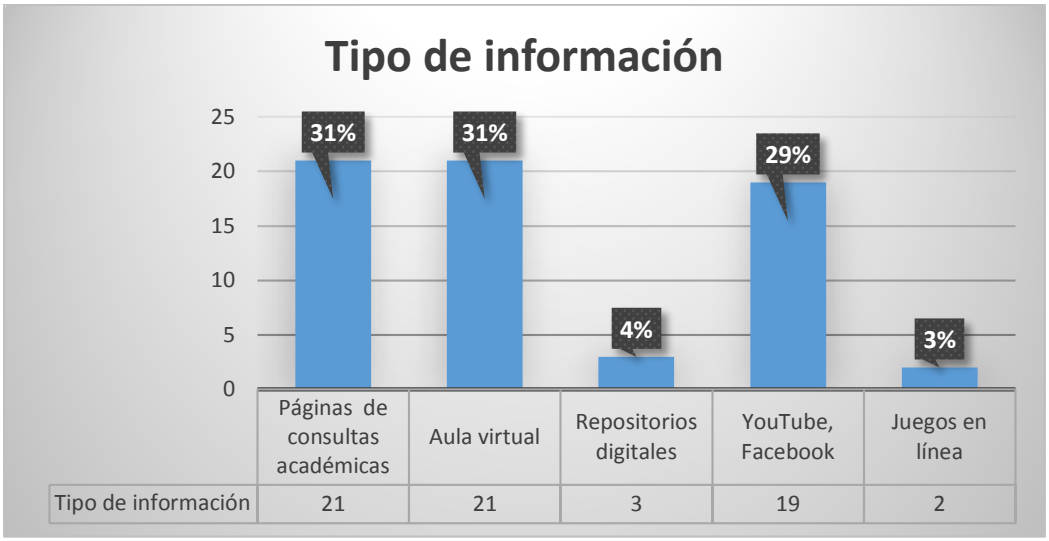


Gráfico 7 Tipo de Información que se maneja.

Análisis:

Con respecto a la información a la que se accede haciendo uso de la red como tal, se puede observar que existe un porcentaje elevado del 29%, el cual afirma que la red está siendo utilizada para redes sociales, por lo cual se ve la necesidad de colocar filtros o bloqueos en la red para que no sea desperdiciada y no cause problemas de velocidad a los demás usuarios que también están haciendo uso de la misma.

5) Determinar el número de dispositivos con los que acceden a la red inalámbrica.

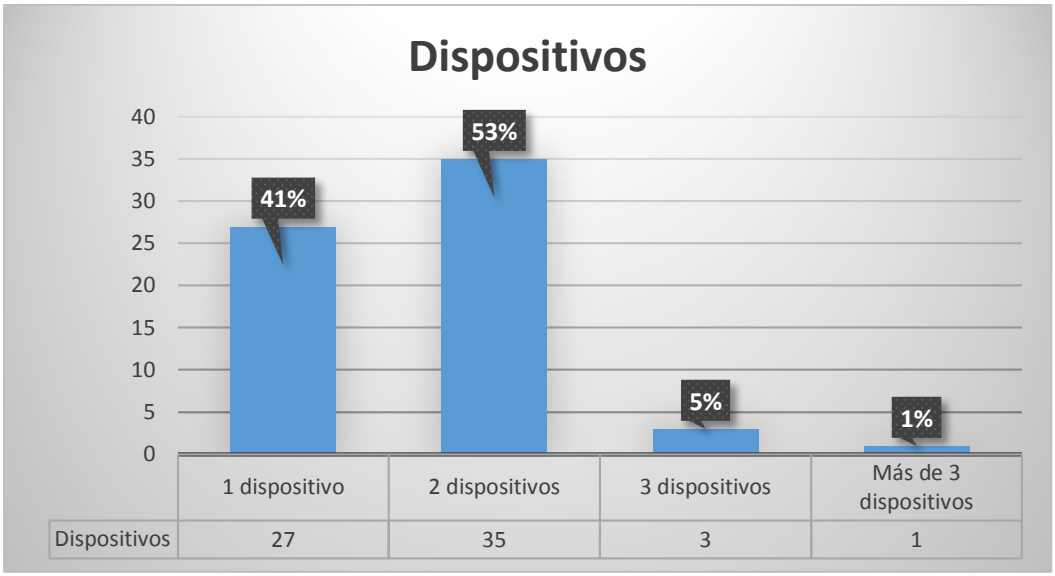


Gráfico 8 Numero de dispositivos

Análisis:

El 53% de todos los encuestados afirman que el número máximo de dispositivos con los que hacen uso de la red son 2, por tanto, se deberá implementar algún tipo de mecanismo donde se permita hacer uso solamente de este número de dispositivos.

ENCUESTA N°2: Determinar el grado de satisfacción de los usuarios de la red inalámbrica "ficawifi".

DATOS INFORMATIVOS

a) Sexo

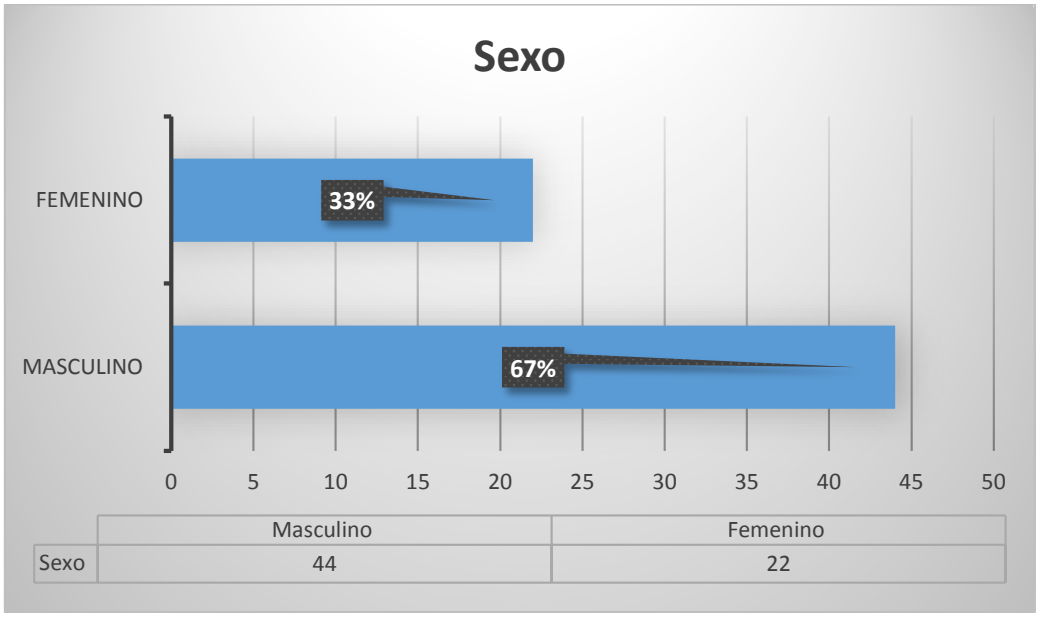


Gráfico 9 Sexo

Análisis:

En relación al sexo se determinó que 44 individuos equivalente al 67% son de sexo masculino y 22 individuos equivalentes al 33% son de sexo femenino.

b) Cargo

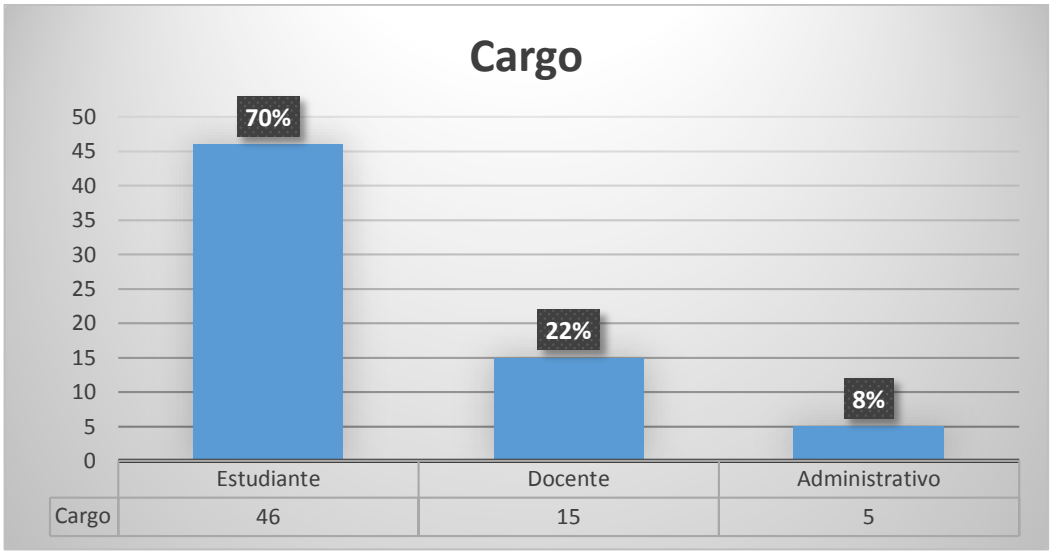


Gráfico 10 Cargo

Análisis:

El igual que en la primera encuesta realizada al inicio del semestre el mayor número de encuestados lo constituyen los estudiantes representando el 70% de todos los encuestados, seguido del personal docente con un aumento al 22% y el 8% conformado por el personal administrativo.

c) Cargo

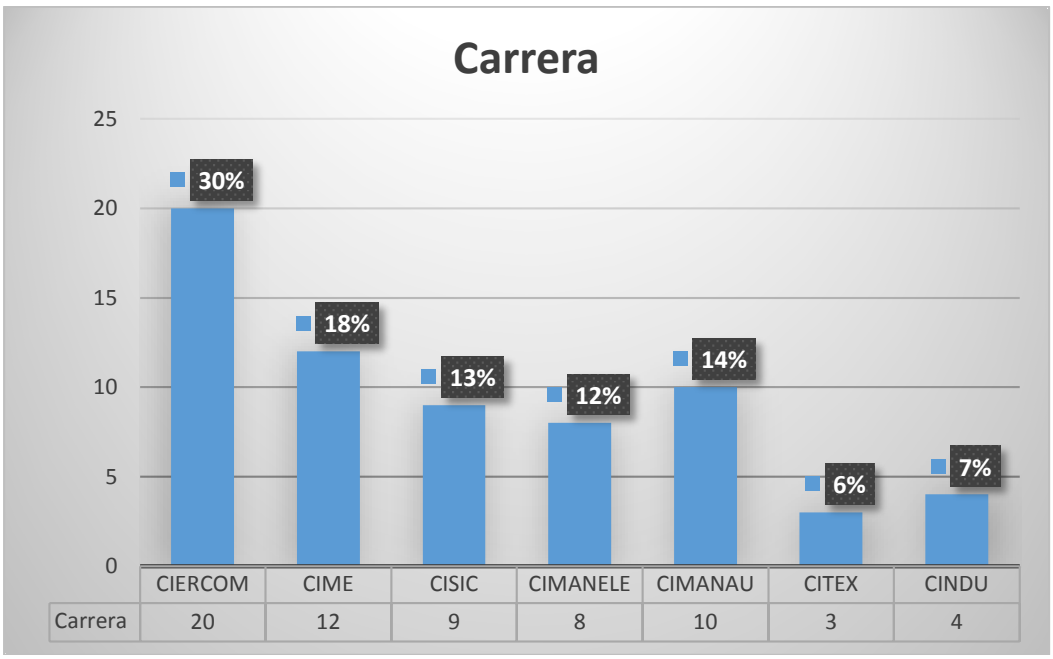


Gráfico 11 Carrera

Análisis:

Se puede observar que el mayor número de encuestados siguen siendo los estudiantes de la carrera CIERCOM como se determinó en la primera encuesta llevada a cabo a inicios del semestre con un equivalente del 30%, debido a que en el periodo académico se cuenta con el mayor índice de estudiantes matriculados como indica la tabla 7, seguido de CIME con 18%, CISIC con el 9%, CIMANAU con el 14%, CIMANELE con el 12%, mientras que CITEX y CINDU con el 6 % y 7% respectivamente, presentan el más bajo porcentaje, debido a que los estudiantes de ambas carreras no se encuentran todo el tiempo dentro de las instalaciones representando aproximadamente un 10% de margen de error para determinar el grado de satisfacción de la red inalámbrica.

FUNCIONAMIENTO DE RED

1) Determinar el número de dispositivos con los que pueden acceder a la red inalámbrica.

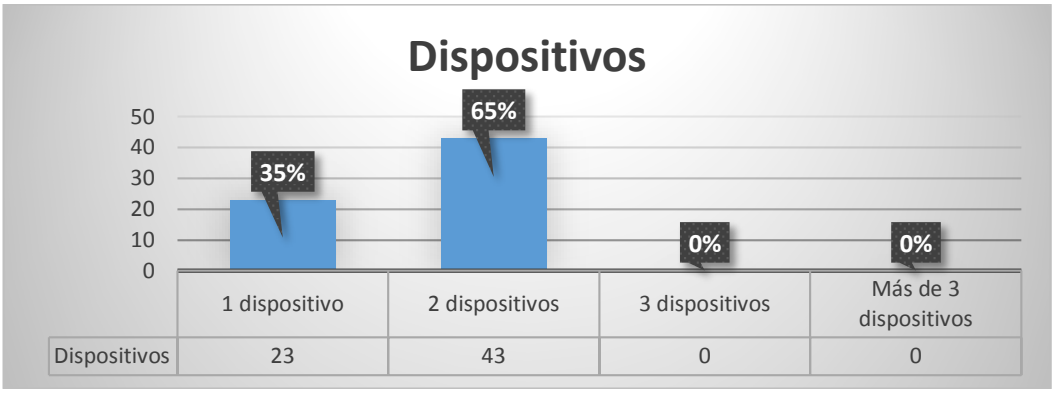


Gráfico 12. Numero de dispositivos

Análisis:

De acuerdo a los datos obtenidos sobre el funcionamiento de la red se puede observar que el 65% de los encuestados equivalentes a 43 usuarios utilizan 2 dispositivos para conectarse a la red, mientras que el 35% solo utiliza 1 dispositivo. Por tanto, se confirma que el método de autenticación implementado

en el servidor AAA Radius funciona de manera correcta, permitiendo autentificar máximo a cada usuario dos veces con su usuario y contraseña personal, brindando de esta manera una menor congestión de conexiones por AP.

2) Determinar el tipo de sistema operativo que utiliza el usuario en el ordenador portátil.

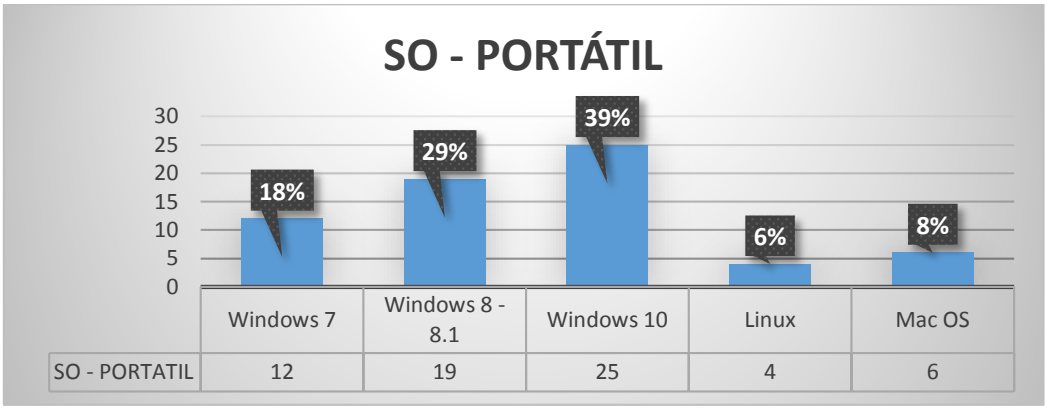


Gráfico 13. Sistema operativo en ordenadores portátiles

Análisis:

En el grafico anterior se observa que el software más utilizado es Windows 10 con un total de 25 usuarios encuestados (39%), esto se debe a la gratuidad de actualización durante el primer año de lanzamiento del software, sin embargo presenta problemas de autorización propias del sistema operativo, obligando a algunos usuarios a tener que registrarse dos o tres veces más con sus credenciales. El 18% y 29% de los encuestados equivalentes a 12 y 29 usuarios respectivamente utilizan versiones anteriores a Windows 10, los cuales afirman que no presentan este tipo de inconvenientes sobre autenticaciones extras, al igual que el 6% y 8% restante que utilizan sistemas operativos propietario y libre.

3) Determinar el tipo de sistema operativo que utiliza el usuario en su dispositivo móvil.

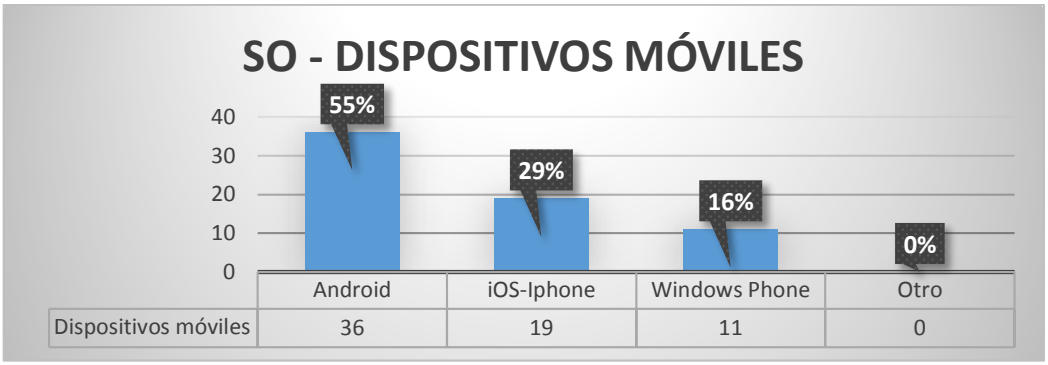


Gráfico 14. Sistema operativo en dispositivos móviles

Análisis:

De acuerdo al grafico 14 se verifica que el SO en dispositivos móviles más utilizado es Android con un total de 36 usuarios pertenecientes al 55%, el 29% utilizan el sistema operativo iOS-IPhone con 19 usuarios y el restante 16% utilizan Windows Phone, que a diferencia de su sistema operativo para ordenadores Windows 7, 8 y 10 no necesita programas de terceros para poder conectarse a la red, esto debido a que poseen autentificación EAP-TTLS de forma nativa al igual que Android y iOS-IPhone.

4) Determinar el tipo de información que manejan los usuarios al hacer uso de la red inalámbrica.

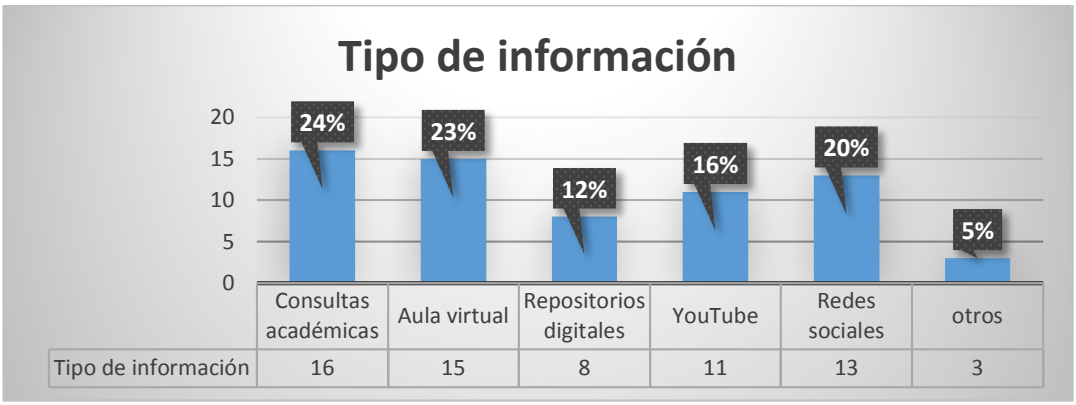


Gráfico 15. Tipo de información

Análisis

Con respecto a la información que acceden los usuarios al hacer uso de la red, se puede observar que existe un porcentaje del 20% Y 16% para redes sociales y

YouTube, por lo cual se ve la necesidad de colocar filtros o bloqueos en la red para limitar los recursos en dichas páginas y evitar problemas en la velocidad de navegación al resto de la red. Además se observa que la mayoría de usuarios utilizan los recurso de la universidad como son el aula virtual y repositorios digitales representando el 23% y 12% del total de encuestas aplicadas, mientras que el 24% y el 5% restante son utilizados para consultas académicas y otras páginas.

5) Determinar los tipos de inconvenientes que se presentan con mayor frecuencia.

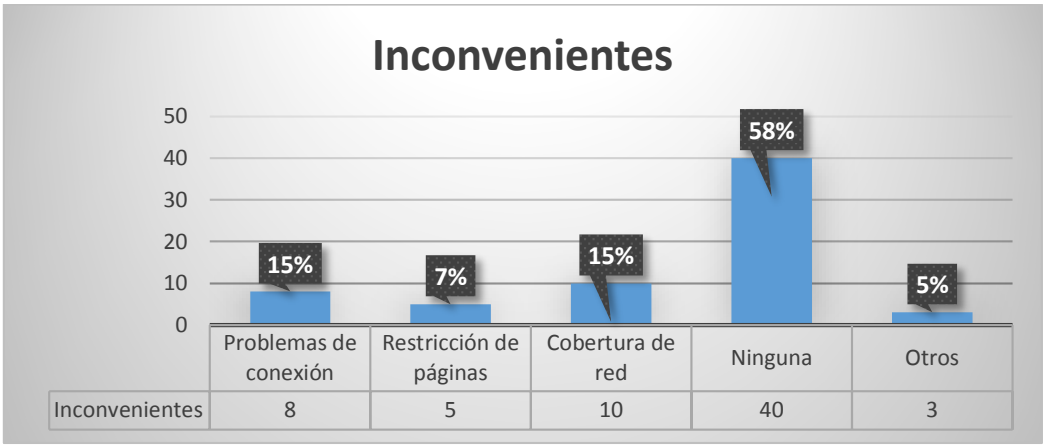


Gráfico 16 Inconvenientes con el uso de la red.

Análisis:

Los datos obtenidos revelan que se logró disminuir los problemas que existían en la red con respecto a la conexión representando el 15% equivalentes a solo 8 usuarios con dicho problema, por otra parte, en lo que a restricción de páginas y cobertura de red se refiere, existe un ligero porcentaje del 7% y 15% esto puede deberse a la indisponibilidad de la página solicitada o la una distancia fuera del rango de cobertura de los AP. Por último se observa que la mayoría de encuestados (58%) no presentan ningún tipo de inconvenientes, indicando que la red está trabajando en un nivel óptimo.

6) Determinar horas pico para fallas de conexión a la red.

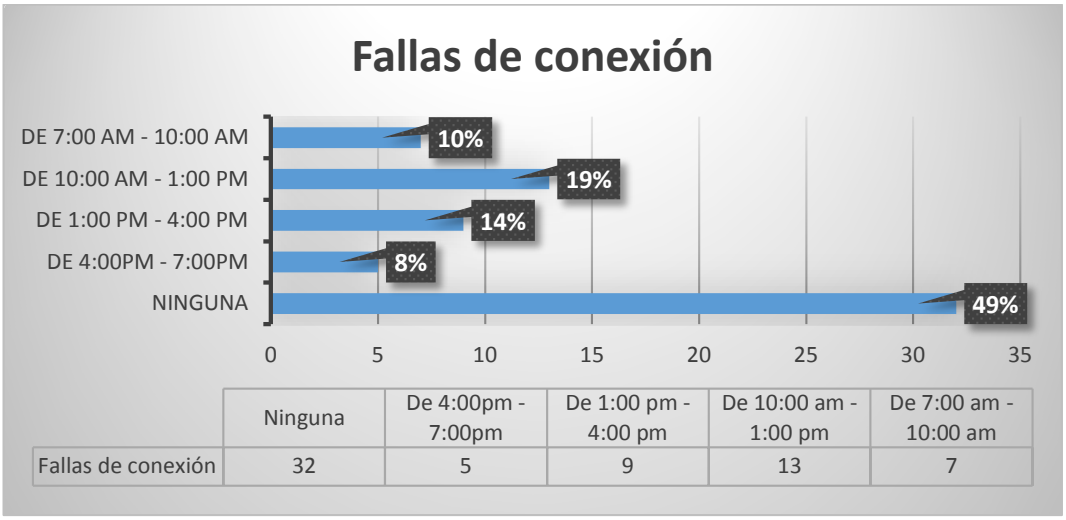


Gráfico 17. Horas de fallas en conexión

Análisis:

De todas las encuestas aplicadas se puede verificar que las fallas de conexión que se presentaban entre las 7am hasta las 5pm inicialmente, ha disminuido considerablemente en un 10%, 19%, 14% y 8% respectivamente, dando como resultado un 49% de encuestados que no presentan problema alguno con el sistema de autenticación implementado.

7) Determinar el desempeño de la red inalámbrica (último mes/Julio).

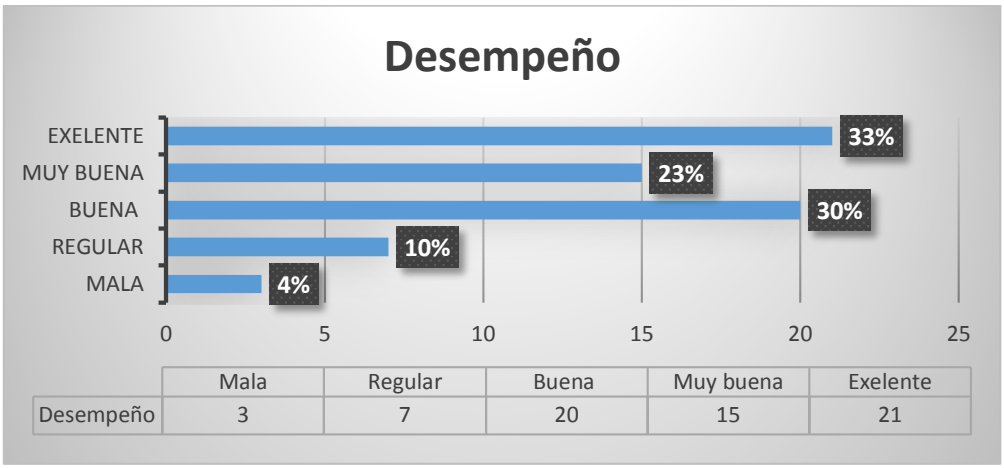


Gráfico 18. Desempeño de red inalámbrica

Análisis:

Según los datos recolectados 21 encuestados afirman que el actual desempeño de la red ha subido considerablemente de un 2% a un 33% lo cual indica que la red esta excelente en cuanto a desempeño, de igual manera 20 usuarios equivalente al 30% aseguran que es bueno el desempeño de la red, mientras que solo el 4% afirma que el desempeño de la red no es aceptable.

8) Determinar el grado de satisfacción de la navegación en internet conectado a la red inalámbrica de la facultad.

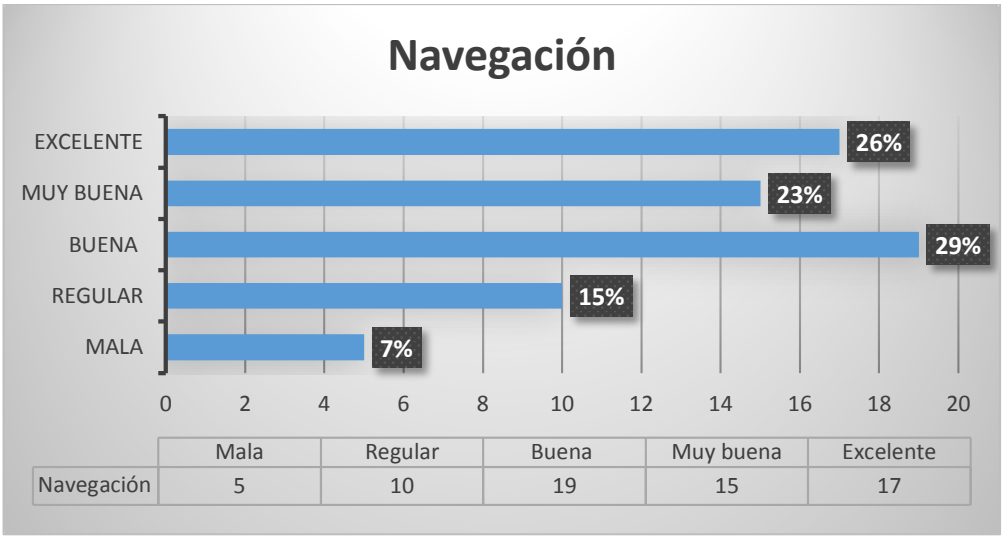


Gráfico 19. Grado de satisfacción del servicio

Análisis:

Según los datos obtenidos 19 usuarios equivalentes al 29% afirman que la velocidad de navegación en la red inalámbrica es buena en comparación a la velocidad inicial que se les asignaba por medio del hostpot, por otro lado el 26% y 23% de todos los encuestados están satisfechos con la actual distribución de red calificando a la misma como muy buena y excelente. El 15% y 7% equivalentes a 15 encuestado afirman que se debe optar por otros mecanismos para el control del ancho de banda general.

ANEXO D – Configuraciones FreeRADIUS + Ldap + Debian 8.6 + Equipos Mikrotik

El siguiente anexo muestra el proceso de instalación y configuración del servidor FreeRADIUS, la base de datos LDAP, el esquema y la unificación de la base de datos con phpLDAPadmin.

CONFIGURACIONES BÁSICAS

1. Configuración de tarjeta de red: Se aplica el comando ***nano /etc/network/interfaces*** para acceder al fichero donde se editarán los parámetros de la interfaz de red como se muestra en la ilustración 90.

```
#NETWORK
allow-hotplug eth0
iface eth0 inet static
        address 192.x.x.x
        netmask x.x.x.x
        network 192.x.x.x
        broadcast 192.x.x.x
        gateway 192.x.x.x #ip servidor mikroTik
```

***Ilustración* 90.** Fichero de configuración interfaz.
Fuente: Servidor FreeRADIUS

2. Configuración de firewall (iptables): Se crea un fichero ejecutable con el editor nano dentro del directorio ***/etc/,*** en él se coloca las líneas de comandos que se muestran en la ilustración 91, luego se procede a dar permisos de ejecución aplicando el comando ***chmod +x "fichero"***; se ejecuta el fichero con el comando ***./"fichero",*** se verifica si se aplicaron la reglas con #iptables –L, si no se tiene errores se guarda la dirección del ejecutable dentro del fichero ***/etc/rc.local*** como indica la ilustración 92, para el arranque automático de iptables al inicio del sistema .

```
#####################################################

iptables -X
iptables -F
iptables -Z

#####################################################

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

#####################################################

iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

#########################################

iptables -A INPUT -i eth0 -j ACCEPT
iptables -A OUTPUT -o eth0 -j ACCEPT

#####################################################

iptables -A INPUT -i eth0 -p icmp -j ACCEPT
iptables -A OUTPUT -o eth0 -p icmp -j ACCEPT

#####################################################

echo 1 > /proc/sys/net/ipv4/ip_forward

echo " Verificar las reglas aplicadas"

#####################################################
```

Ilustración 91. Script iptables.
Fuente: Servidor FreeRADIUS FICA

```
root@debian:/etc# nano firewall.radius
root@debian:/etc# chmod +x firewall.radius
root@debian:/etc# ./firewall.radius
Verificar REGLAS añadidas
root@debian:/etc# gedit rc.local
```

Open ▾ | *rc.local /etc | Save

```
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

/etc/firewall.radius
exit 0
```

Ilustración 92. Fichero ejecutable con iptables.
Fuente: servidor FreeRADIUS FICA

ACTUALIZACIÓN DEL SISTEMA

3. Se digitan los comandos ***#apt-get update*** para que el sistema proceda a buscar las actualizaciones más recientes de la versión Debian Jessie (ilustración 93), y se procede a instalar estas actualizaciones con el comando ***#apt-get upgrade –y*** (ilustración 94).

```
root@debian:/etc# apt-get update
Get:1 http://security.debian.org jessie/updates InRelease [63.1 kB]
Get:2 http://security.debian.org jessie/updates/main Sources [188 kB]
Get:3 http://security.debian.org jessie/updates/main amd64 Packages [345 kB]
Get:4 http://security.debian.org jessie/updates/main Translation-en [183 kB]
Ign http://ftp.es.debian.org jessie InRelease
Get:5 http://ftp.es.debian.org jessie-updates InRelease [145 kB]
Get:6 http://ftp.es.debian.org jessie Release.gpg [2,373 B]
Get:7 http://ftp.es.debian.org jessie-updates/main Sources [15.4 kB]
Get:8 http://ftp.es.debian.org jessie-updates/main amd64 Packages/DiffIndex [6,9
16 B]
Get:9 http://ftp.es.debian.org jessie-updates/main Translation-en/DiffIndex [2,7
04 B]
Get:10 http://ftp.es.debian.org jessie Release [148 kB]
Get:11 http://ftp.es.debian.org jessie/main Sources [7,056 kB]
Get:12 http://ftp.es.debian.org jessie/main amd64 Packages [6,776 kB]
Get:13 http://ftp.es.debian.org jessie/main Translation-en [4,582 kB]
Fetched 19.5 MB in 46s (416 kB/s)
Reading package lists... Done
```

Ilustración 93. Ejecución del comando update.
Fuente: Servidor FreeRADIUS FICA

```
root@debian:/etc# apt-get upgrade -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  apt apt-utils base-files bash bind9-host ca-certificates dbus dbus-x11
  dnsutils e2fslibs e2fsprogs evolution-data-server
  evolution-data-server-common exim4 exim4-base exim4-config
  exim4-daemon-light file firefox-esr host hplip hplip-data iceweasel
  libapt-inst1.5 libapt-pkg4.12 libbind9-90 libc-bin libc6 libcairo-gobject2
  libcairo2 libcamel-1.2-49 libcomerr2 libdbus-1-3 libdns-export100 libdns100
  libebackend-1.2-7 libebook-1.2-14 libebook-contacts-1.2-0 libecal-1.2-16
  libedata-book-1.2-20 libedata-cal-1.2-23 libedataserver-1.2-18 libfcgi-perl
  libgd3 libgme0 libgnutls-deb0-28 libgnutls-openssl27 libgudev-1.0-0
  libhogweed2 libhpmud0 libio-socket-ssl-perl libirs-export91 libisc-export95
  libisc95 libisccc90 libisccfg-export90 libisccfg90 libjasper1 liblcms2-2
  liblcms2-utils liblwres90 libmagic1 libmpg123-0 libnettle4 libpam-modules
  libpam-modules-bin libpam-runtime libpam-systemd libpam0g libpcsclite1
  libpng12-0 libsane-hpaio libsmbclient libss2 libssl1.0.0 libsystemd0
  libtevent0 libtiff5 libudev1 libwbclient0 libwmf-bin libwmf0.2-7 libxml2
  libxpm4 linux-image-3.16.0-4-amd64 locales minissdpd multiarch-support
  ntfs-3g openjdk-7-jre openjdk-7-jre-headless openssl printer-driver-hpcups
  printer-driver-hpijs printer-driver-postscript-hp python-libxml2 samba-libs
```

Ilustración 94. Actualización de ficheros y paquetes.
Fuente: Servidor FreeRADIUS FICA

INSTALACIÓN DE PAQUETES

4. Se procede a instalar el paquete de FreeRADIUS con soporte Ldap para lo cual se digita el comando ***#apt-get install freeradius freeradius-ldap*** tal y como se muestra en la ilustración 95.

```
root@debian:/# apt-get install freeradius freeradius-ldap
  freeradius-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
   freeradius-common libdbi-perl libfreeradius2
Suggested packages:
   freeradius-postgresql freeradius-mysql
   freeradius-krb5 libclone-perl libmldbm-perl
   libnet-daemon-perl libsql-statement-perl
The following NEW packages will be installed:
   freeradius freeradius-common freeradius-ldap
   freeradius-utils libdbi-perl libfreeradius2
0 upgraded, 6 newly installed, 0 to remove and 0 not upgr
aded.
Need to get 1,832 kB of archives.
After this operation, 5,810 kB of additional disk space w
ill be used.
Do you want to continue? [Y/n] y
```

Ilustración 95. Instalación FreeRADIUS.
Fuente: Servidor FreeRADIUS FICA

5. Se instala el paquete LDAP junto con otras dependencias del mismo con la línea de comando ***#apt-get install slapd ldap-utils phpldaladmin*** (ilustración 96).

```
root@debian:/# apt-get install slapd ldap-utils phpldapadmin
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
   libapache2-mod-php5 libodbc1 libonig2
   libqdbm14 libslp1 php5-cli php5-common
   php5-json php5-ldap php5-readline
Suggested packages:
   libsasl2-modules-gssapi-mit
   libsasl2-modules-gssapi-heimdal php-pear
   libmyodbc odbc-postgresql tdsodbc
   unixodbc-bin slpd openslp-doc
   php5-user-cache
The following NEW packages will be installed:
   ldap-utils libapache2-mod-php5 libodbc1
   libonig2 libqdbm14 libslp1 php5-cli
   php5-common php5-json php5-ldap
   php5-readline phpldapadmin slapd
0 upgraded, 13 newly installed, 0 to remove and 0 not upgrade
d.
Need to get 8,071 kB of archives.
After this operation, 31.9 MB of additional disk space will b
e used.
Do you want to continue? [Y/n] ■
```

Ilustración 96. Instalación LDAP.
Fuente: Servidor FreeRADIUS FICA

6. El proceso de instalación continuara y enseguida nos solicitara una contraseña de administrador para el directorio LDAP como indica la ilustración 97.

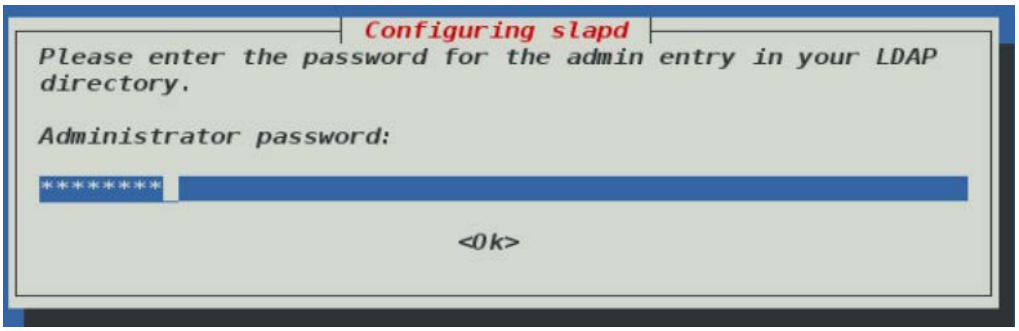


Ilustración 97. Contraseña administradora Ldap.
Fuente: Servidor OpenLdap FICA

7. Por seguridad se debe verificar la contraseña como indica la ilustración 98.

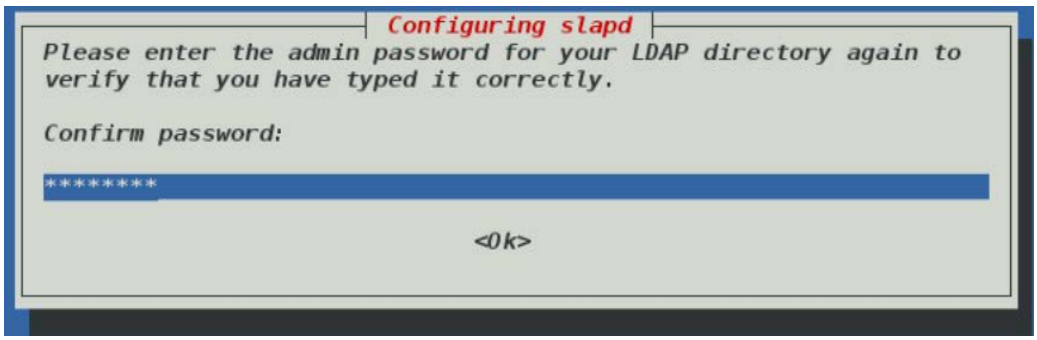


Ilustración 98. Confirmación contraseña admin LDAP.
Fuente: Servidor OpenLdap FICA

8. El proceso de instalación continuará hasta finalizar (ilustración 99).

```
Setting up slapd (2.4.40+dfsg-1+deb8u2) ...
  Creating new user openldap... done.
  Creating initial configuration... done.
  Creating LDAP directory... done.
Setting up ldap-utils (2.4.40+dfsg-1+deb8u2) ...
Setting up libqdbm14 (1.8.78-5+b1) ...
Setting up php5-common (5.6.30+dfsg-0+deb8u1) ...

Creating config file /etc/phpldapadmin/config.php with new version
apache2_invoke: Enable configuration phpldapadmin.conf
Processing triggers for libc-bin (2.19-18+deb8u7) ...
Processing triggers for systemd (215-17+deb8u6) ...
Processing triggers for libapache2-mod-php5 (5.6.30+dfsg-0+deb8u1) ...
root@debian:/#
```

Ilustración 99. Finalización del proceso LDAP.
Fuente: Servidor OpenLdap FICA

RECONFIGURACIÓN DEL LA BASE DE DATOS LDAP

9. A continuación, ejecutar el asistente de configuración slapd ingresando el comando ***#dpkg-reconfigure slapd***, que en primer lugar nos preguntara si desea omitir la configuración del servidor LDAP (ilustración 100), a lo que se debe responder NO.

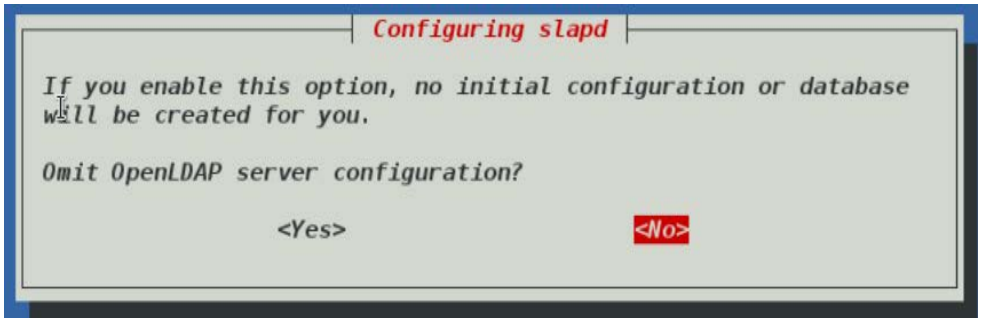


Ilustración 100. Omitir configuración inicial LDAP.
Fuente: Servidor OpenLdap FICA

10. Ahora, el asistente solicita ingresar el nombre del dominio (para la cual se tiene instalado previamente en el mismo servidor un DNS local), como muestra la ilustración 101, la cual será la base del directorio LDAP o llamado también DN.

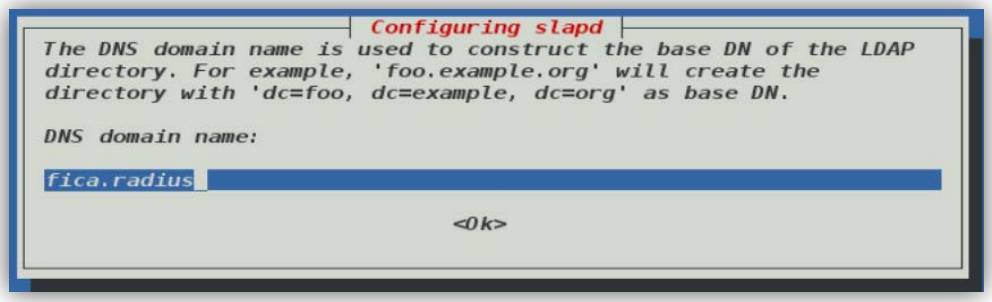


Ilustración 101. Ingreso del dominio local.
Fuente: Servidor OpenLdap FICA

11. Ingresar el nombre de la organización a utilizar en el DN base del directorio LDAP como se muestra en la ilustración 102.

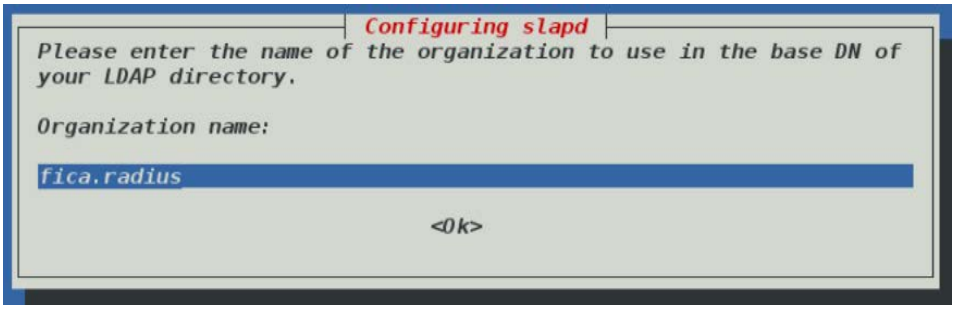


Ilustración 102. Ingreso de nombre de organización para base de datos LDAP.
Fuente: Servidor OpenLdap FICA

12. Para validar los cambios realizados se debe ingresar y confirmar una contraseña de administrador (ilustración 103), para el directorio LDAP (Puede ser la misma de la instalación).

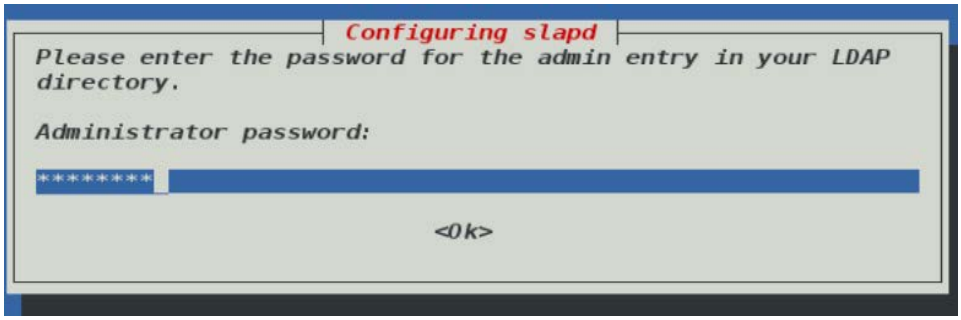


Ilustración 103. Contraseña de administrador LDAP.
Fuente: Servidor OpenLdap FICA

13. Se selecciona el motor de búsqueda de base de datos, se escoge la que viene por defecto para esta versión de Debian (ilustración 104).

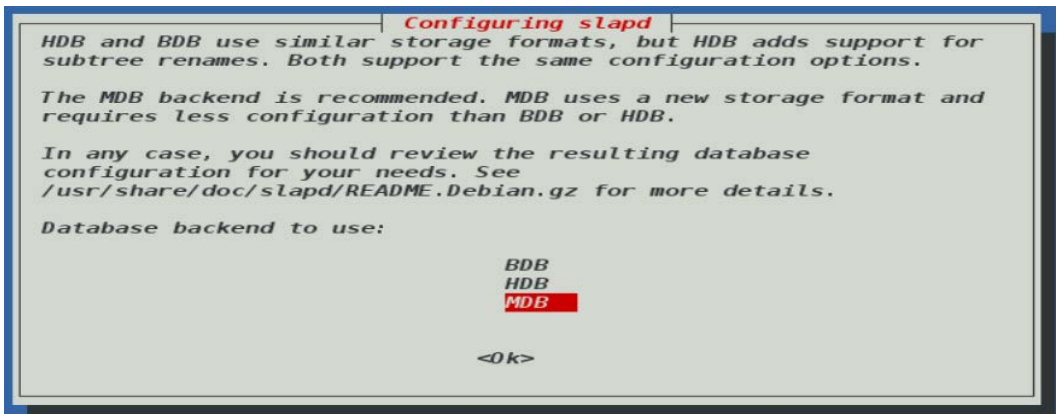


Ilustración 104. Selección de motor de búsqueda.
Fuente: Servidor OpenLdap FICA

14. Enseguida nos muestra una ventana donde pregunta si desea eliminar o remover la base de datos cada que se purgue el paquete ***slapd*** (ilustración 105), a lo que obviamente se responderá que NO, ya que la base de datos tendría que ocupar del doble de procesamiento entre borrar y crear una nueva base de datos.

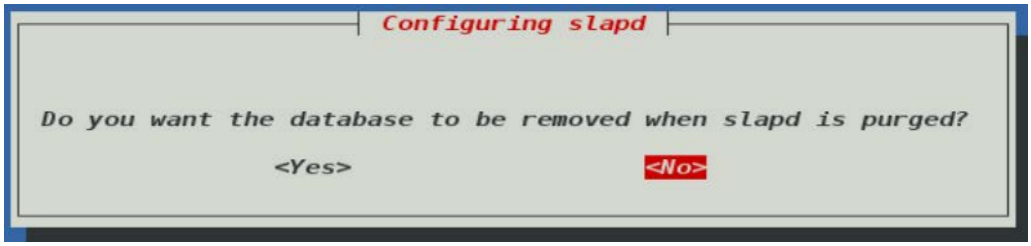


Ilustración 105. Purgar paquete slapd.
Fuente: Servidor OpenLdap FICA

15. La siguiente ventana pregunta si desea borrar las bases de datos LDAP creadas por defecto al instalar los paquetes como muestra la ilustración 106, a la cual le seleccionamos en SI para evitar posibles conflictos entre bases existentes.

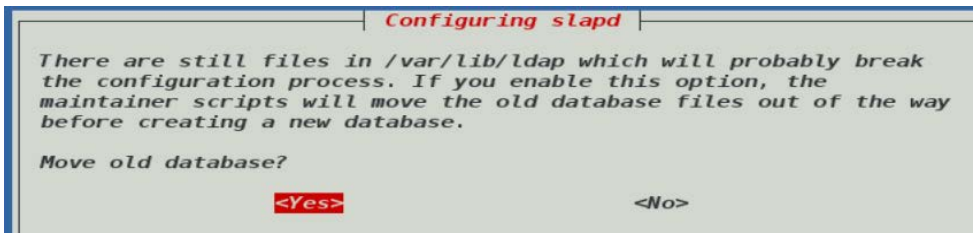


Ilustración 106. Eliminación de bases de datos antiguas.
Fuente: Servidor OpenLdap FICA

16. Por último nos preguntara si se desea trabajar con la versión antigua (v2) del protocolo LDAP (ilustración 108), la cual se responderá que NO, ya que actualmente se encuentra obsoleta.

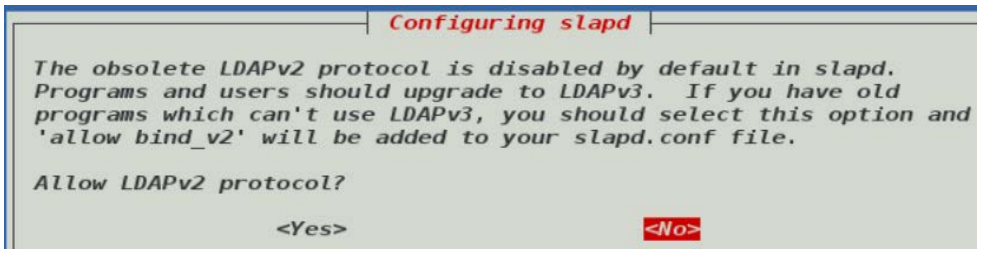


Ilustración 107. Elección de la versión para el protocolo LDAP.
Fuente: Servidor OpenLdap FICA

17. Por último, se muestra un mensaje de configuración finalizada como se puede apreciar en la ilustración 108.

```
root@debian:/# dpkg-reconfigure slapd
  Moving old database directory to /var/backups:
  - directory unknown... done.
  Creating initial configuration... done.
  Creating LDAP directory... done.
Processing triggers for libc-bin (2.19-18+deb8u7) ...
root@debian:/#
```

Ilustración 108. Finalización de configuración LDAP.
Fuente: Servidor OpenLdap FICA

ESQUEMA PARA USUARIOS FICA

18. El servidor FreeRADIUS incluye por defecto esquemas (schema) dentro de su instalación, por tanto, se procede a incorporar dichos esquemas al servidor LDAP, para que logre reconocer atributos extras con sus respectivos objectclass. Para disponer del esquema, se tiene que copiar el fichero "***openldap.schema"*** desde el directorio ***/usr/share/doc/freeradius/examples/*** al directorio del servidor OpenLDAP ***/etc/ldap/schema/,*** teniendo en cuenta que el nombre debe cambiar para no tener conflicto con otros esquemas como se muestra en la ilustración 109.

```
root@debian:/# cp usr/share/doc/freeradius/examples/openldap.schema /etc/
ldap/schema/radius.schema
root@debian:/#
```

Ilustración 109. Línea de comando que permite copiar schema a otro directorio.
Fuente: Servidor OpenLdap FICA

19. Lo siguiente es crear un fichero temporal con el comando ***#nano /tmp/schema.conf,*** al cual se le añadirá las líneas de código que se observan en la ilustración 110.

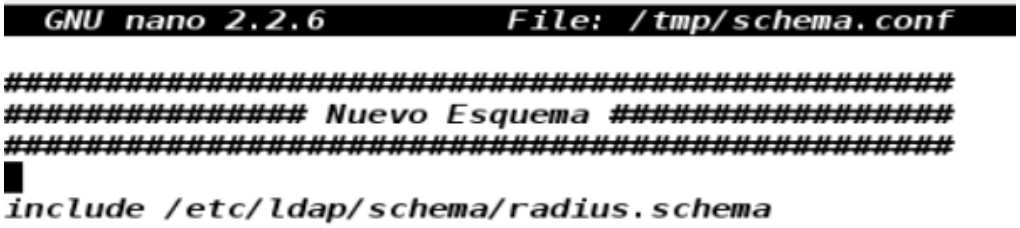


Ilustración 110. Ingreso de esquema creado previamente.
Fuente: Servidor OpenLdap FICA

20. Se hace una búsqueda de los esquemas que existen en nuestro LDAP, con el siguiente comando ***#ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \ cn=schema,cn=config dn*** y se puede verificar que claramente nuestro esquema NO existe todavía (ilustración 111).

```
root@debian:/# 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

root@debian:/#
```

Ilustración 111. Búsqueda de esquemas existentes.
Fuente: Servidor OpenLdap FICA

21. Por tanto se crea un directorio temporal con el comando ***#mkdir /tmp/users*** y ejecutar el comando ***slapcat -f schema.conf -F users -n0 –H ldap:///cn={0}radius,cn=schema,cn=config -l cn=radius.ldif*** (ilustración 112). Esto nos creará la estructura necesaria de los ficheros LDIF dentro del directorio users, y se ejecuta el comando ***#ls ./users/*** para ver dicha información (ilustración 113).

```
root@debian:/tmp# mkdir /tmp/users
root@debian:/tmp# cd /tmp
root@debian:/tmp# slapcat -f schema.conf -F users -n0 -H ldap:///
cn={0}radius,cn=schema,cn=config -l cn=radius.ldif
root@debian:/tmp#
```

Ilustración 112. Línea de comando para crear estructura LDIF.
Fuente: Servidor OpenLdap FICA

```
root@debian:/tmp# ls ./users/
cn=config   cn=config.ldif
root@debian:/tmp#
```

Ilustración 113. Archivos de configuración creados a partir de slapcat.
Fuente: Servidor OpenLdap FICA

22. El esquema LDIF que se ha creado requiere algunas modificaciones que prevendrán algunos errores, para lo cual se edita el fichero con el siguiente comando ***#nano cn\=radius.ldif y*** se cambiaran las siguientes líneas mostradas a continuación por las líneas descritas en la ilustración 114.

```
dn: cn={0}radius,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: {0}radius
```

Por:

```
  GNU nano 2.2.6        File: cn=radius.ldif

dn: cn=radius,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: radius
```

Ilustración 114. Modificación archivo radius.ldif.
Fuente: Servidor OpenLdap FICA

Y al final del fichero se eliminan las siguientes líneas:

structuralObjectClass: olcSchemaConfig
entryUUID: 85d35afa-2992-1031-8f93-0d1d8c5b6386
creatorsName: cn=config
createTimestamp: 20120503173822Z
entryCSN: 20120503173822.097163Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20120503173822Z

AÑADIR ESQUEMA

23. Luego de las respectivas configuraciones se procede a añadir el esquema al directorio principal LDAP como muestra a continuación en la ilustración 115.

```
root@debian:/tmp# ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cn\=radi
us.ldif
adding new entry "cn=radius,cn=schema,cn=config"

root@debian:/tmp#
```

Ilustración 115. Adición de schema al directorio LDAP.
Fuente: Servidor OpenLdap FICA

24. Por último se verifica si el esquema fue añadido correctamente (ilustración 116), con el mismo comando anterior ***##ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \cn=schema,cn=config dn,*** en caso de que ya existiera se procede a reiniciar ambos servicios (FreeRADIUS y OpenLdap) con los comandos mostrados en la ilustración 117.

```
root@debian:/tmp# 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

root@debian:/tmp#
```

Ilustración 116. Comprobación del schema agregado.
Fuente: Servidor OpenLdap FICA

```
root@debian:/# /etc/init.d/slapd stop
[ ok ] Stopping slapd (via systemctl): slapd.service.
root@debian:/# /etc/init.d/slapd start
[ ok ] Starting slapd (via systemctl): slapd.service.
root@debian:/# /etc/init.d/freeradius stop
[ ok ] Stopping freeradius (via systemctl): freeradius.service.
root@debian:/#
```

Ilustración 117. Reinicio de OpenLdap.
Fuente: Servidor OpenLdap FICA

25. A partir de este momento se comienzan a subir los archivos de configuración en formato LDIF a nuestra base de datos, de acuerdo a los modelos descritos en la sección 5.3.4 del documento.

INTEGRACIÓN DE LDAP CON EL SERVIDOR RADIUS

26. En el paso anterior se detiene el servicio FreeRADIUS para poder configurar los ficheros necesarios del mismo y dar soporte LDAP, se ingrasa a editar el fichero LDAP que se encuentra en el directorio ***/etc/freeradius/modules/*** y se coloca lo que se muestra en la ilustración 118.

```
ldap {
        server = "192.x.x.x" #local host
        identity = "cn=admin,dc=fica,dc=radius"
        password = *******
        basedn = "dc=fica,dc=radius"
        filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
        base_filter = "(objectclass=radiusprofile)"
```

Ilustración 118. Configuración módulo LDAP.
Fuente: Servidor FreeRADIUS FICA

CONFIGURACIÓN LDAP EN FREERADIUS

27. Ahora se procede a habilitar los parámetros de autentificación y autorización mediante el servidor LDAP (ilustración 119), dentro de los ficheros default e

inner-tunnel de FreeRADIUS en los directorios ***/etc/freeradius/sites-enabled/defaul*** y ***/etc/freeradius/sites-enabled/inner-tunne***l. (Se debe tomar en cuenta que ambos ficheros poseen los mismos datos).

```
authorize {
        #
        #  Security settings.  Take a User-Name, and do some sim$
        #  checks on it, for spaces and other invalid characters$
        #  it looks like the user is trying to play games, rejec$
        #
        #  The ldap module will set Auth-Type to LDAP if it has $
        #  already been set
        ldap
#       Autz-Type Status-Server {
#
#       }
}

#  Authentication.
#
#
#  This section lists which modules are available for authentica$
#  Note that it does NOT mean 'try each module in order'.  It me$
        # Uncomment it if you want to use ldap for authentication
        #
        # Note that this means "check plain-text password against
        # the ldap database", which means that EAP won't work,
        # as it does not supply a plain-text password.
        Auth-Type LDAP {
                ldap
        }
#               }
#       }
}
```

Ilustración 119. Ficheros default e inner-tunel.
Fuente: Servidor FreeRADIUS FICA

INTERFAZ DE ADMINISTRACIÓN PHPLDAPADMIN

28. Para poder ingresar a nuestra base de datos LDAP por medio de una interfaz web, se debe configurar el fichero config.php**,** que se encuentra en el directorito ***/etc/phpldapadmin/,*** se identifican las líneas de configuración principal y se edita las líneas que se muestran en la ilustración 120.

```
/* Array of base DNs of your LDAP server. Leave this blank to have phpLDAPadmin
   auto-detect it for you. */
$servers->setValue('server','base',array('dc=fica,dc=radius'));

   Choose wisely to protect your authentication information appropriately for
   your situation. If you choose 'cookie', your cookie contents will be
   encrypted using blowfish and the secret your specify above as
   session['blowfish']. */
$servers->setValue('login','auth_type','session');

/* The DN of the user for phpLDAPadmin to bind with. For anonymous binds or
   '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=fica,dc=radius');
#  $servers->setValue('login','bind_id','cn=Manager,dc=example,dc=com');
```

Ilustración 120. Fichero de configuración phpLDAPadmin.
Fuente: phpLDAPadmind

CONFIGURACIÓN CLIENTES RADIUS

29. Se ingresa al fichero ***clients.conf*** el cual se encuentra en el directorio ***/etc/freeradius/,*** ahí se establece la dirección del punto de acceso al cual permitirá que se comuniquen entre sí (ilustración 121).

```
  GNU nano 2.2.6        File: /etc/freeradius/clients.conf

client localhost {
        ipaddr = 127.0.0.1
        secret          = testing123
        require_message_authenticator = no
        nastype     = other     # localhost isn't usually a NAS...
}

client 192.x.x.x {
        secret          = ****** #pass autentificacion con AP
        shotname        = AP-MikroTik
        require_message_authenticator = no
        nastype     = MikroTik      # NAS
}

#############################################################################
```

Ilustración 121. Configuración de clientes RADIUS.
Fuente: Servidor FreeRADIUS FICA

CONFIGURACIÓN DE CERTIFICADOS DIGITALES

30. Para la obtención de los certificados se usa el método automatizado. Lo primero será buscar en el directorio ***/usr/share/doc/freeradius/examples/certs/,*** con el comando ***ls*** que se hayan creado los archivos por default al momento de instalar

el paquete FreeRADIUS (ilustración 122), y se procede a editar los ficheros ***ca.cnf server.cnf y client.cnf*** como muestran las ilustraciones 123,124 y 125.

```
root@debian:/# ls /usr/share/doc/freeradius/examples/certs/
bootstrap  ca.cnf  client.cnf  Makefile  README  server.cnf  xpextensions
root@debian:/#
```

Ilustración 122. Fichero de certificados.
Fuente: Servidor FreeRADIUS FICA

```
  GNU nano 2.2.6 File: .../share/doc/freeradius/examples/certs/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        = fica.radius
emailAddress            = admin@fica.radius
commonName              = Entidad Certificadora
```

Ilustración 123. Fichero ca.cnf.
Fuente: Servidor FreeRADIUS FICA

```
  GNU nano 2.2.6 File: ...re/doc/freeradius/examples/certs/server.cnf

prompt                  = no
distinguished_name      = server
default_bits            = 2048
input_password          = whatever
output_password         = whatever

[server]
countryName             = EC
stateOrProvinceName     = Imbabura
localityName            = Ibarra
organizationName        = fica.radius
emailAddress            = admin@fica.radius
commonName              = Server Certificate
```

Ilustración 124. Fichero server.cnf.
Fuente: Servidor FreeRADIUS FICA

```
  GNU nano 2.2.6 File: ...re/doc/freeradius/examples/certs/client.cnf

prompt                  = no
distinguished_name      = client
default_bits            = 2048
input_password          = whatever
output_password         = whatever

[client]
countryName             = EC
stateOrProvinceName     = Imbabura
localityName            = Ibarra
organizationName        = fica.radius
emailAddress            = user@fica.radius
commonName              = user@fica.radius
```

Ilustración 125. Fichero client.cnf.
Fuente: Servidor FreeRADIUS FICA

31. Luego se aplican estos cambios con el archivo booteable denominado "***./bootstrap",*** que será aquel que actualice y genere los certificados con los que se va a utilizar en la conexión con nuestro Ldap (ilustración 126).

```
root@debian:/usr/share/doc/freeradius/examples/certs# ./bootstrap
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.....+.....
.....+.....
..+.....+.....
.....+.....+.....
.....+.....
.....+.....+.....+.
.....
.....+.....
.....+.....+.....+.
.
Certificate is to be certified until Feb 10 20:11:08 2018 GMT (365 days)

Write out database with 1 new entries
Data Base Updated
root@debian:/usr/share/doc/freeradius/examples/certs#
```

Ilustración 126. Generación de certificados.
Fuente: Servidor FreeRADIUS FICA

32. Una vez obtenidos los ficheros necesarios producto del fichero ejecutable ***bootstrap*** se los copia en la siguiente ruta de certificados del servidor ***/etc/freeradius/certs/*** para lo cual se utilizara el comando que se describe en la ilustración 1127.

```
root@debian:/usr/share/doc/freeradius/examples/certs# ls
01.pem      ca.pem      index.txt          README      server.key
02.pem      client.cnf  index.txt.attr     serial      server.p12
bootstrap   client.crt  index.txt.attr.old serial.old  server.pem
ca.cnf      client.csr  index.txt.old      server.cnf  xpextensions
ca.der      client.key  Makefile           server.crt
ca.key      dh          random             server.csr
root@debian:/usr/share/doc/freeradius/examples/certs# ls -l /etc/freeradius
/certs/
total 4
lrwxrwxrwx 1 root freerad  34 Feb  9 22:09 ca.pem -> /etc/ssl/certs/ca-cert
ificates.crt
-rw-r--r-- 1 root freerad 245 Feb  9 22:09 dh
lrwxrwxrwx 1 root freerad  38 Feb  9 22:09 server.key -> /etc/ssl/private/s
sl-cert-snakeoil.key
lrwxrwxrwx 1 root freerad  36 Feb  9 22:09 server.pem -> /etc/ssl/certs/ssl
-cert-snakeoil.pem
root@debian:/usr/share/doc/freeradius/examples/certs#
```

Ilustración 127. Enlace simbólico de certificados.
Fuente: Servidor FreeRADIUS FICA

CONFIGURACIÓN DE PUNTO DE ACCESO (CAP Y CAPsMAN)

33. La configuración depende de la marca del punto de acceso, la facultad cuenta con 15 AP's marca Mikrotik, modelo cAP2n y un Router de la misma marca modelo RB1100 AX2, al cual se accede mediante el programa ***Winbox*** como muestra la ilustración 128.

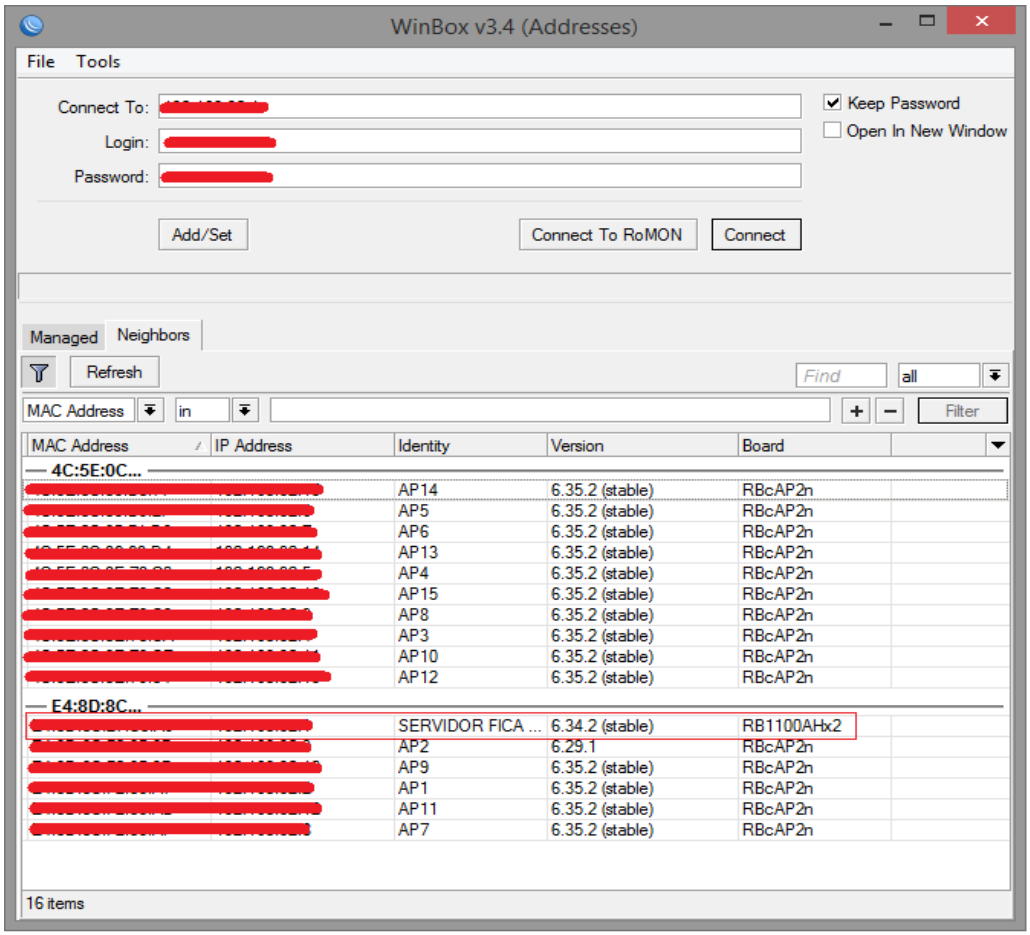


Ilustración 128. Ventana principal Winbox.exe.
Fuente: Winbox

CONFIGURACIÓN CAP

34. Para la configuración de nuestro CAP se va a realizar utilizando el protocolo de comunicación L3, el cual establece que cada AP tenga una dirección IP fija (ilustración 129). Se busca la pestaña ***IP/ADDRESSES/ADDRESS LIST/NEW***

ADDRESS donde se coloca la IP correspondiente a dicho AP (Cabe recordar que se hará el mismo procedimiento en cada AP de la red).

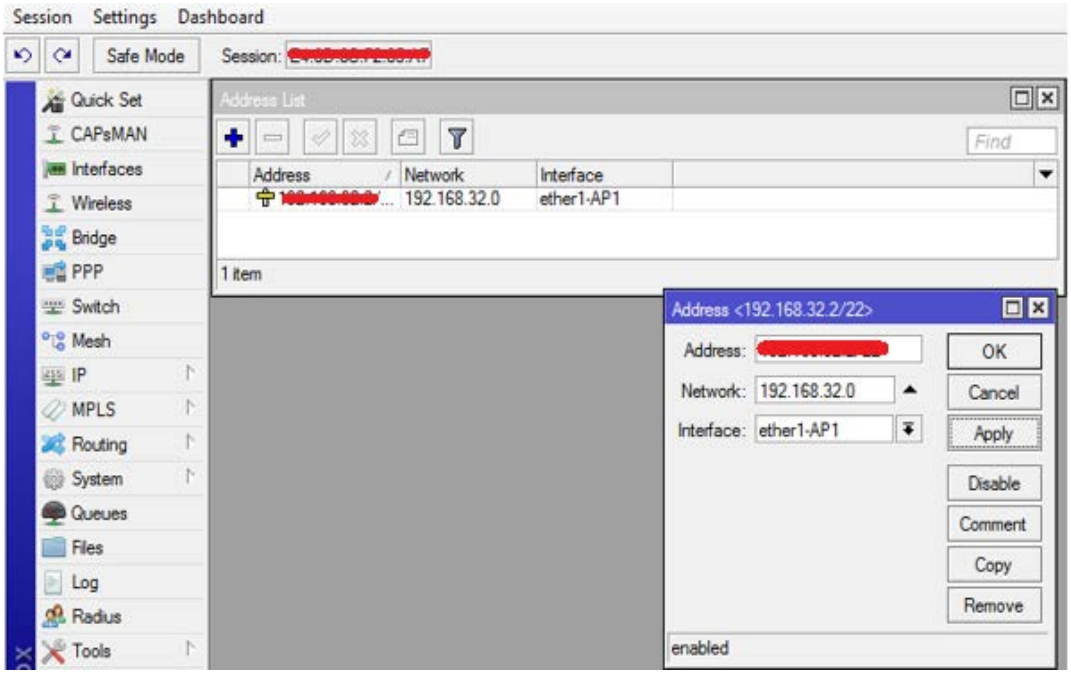


***Ilustración* 129**. Configuración IP fija CAP
Fuente: Router-Mikrotik

35. Una vez que se ha colocado la dirección IP correspondiente, se procede a cambiar el nombre de las interfaces internas en la pestaña INTERFACES para poder identificarlas de mejor manera (ilustración 130).

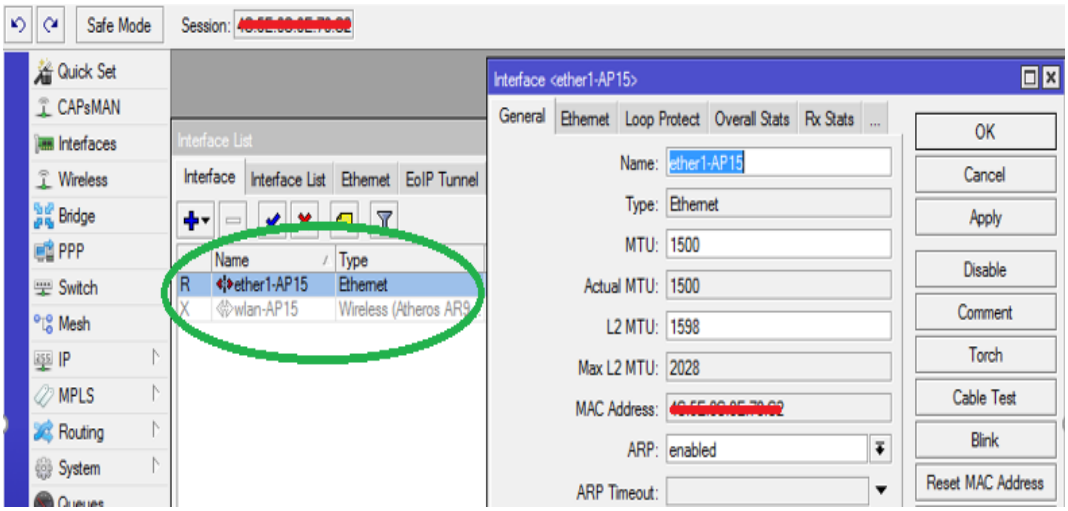


***Ilustración* 130.** Interfaces CAP
Fuente: Router-Mikrotik

36. A continuación, se crea un bridge entre la interfaz LAN y la interfaz WLAN para formar un solo segmente de red y de esta manera pueda ser reconocido

posteriormente por el CAPsMAN, se va a la pestaña BRIDGE/AGREGAR NUEVO (ilustración 131), donde se coloca el nombre correspondiente al AP en el que se esté trabajando y en la solapa PORT se seleciona las interfaces LAN y WLAN (ilustración 132).

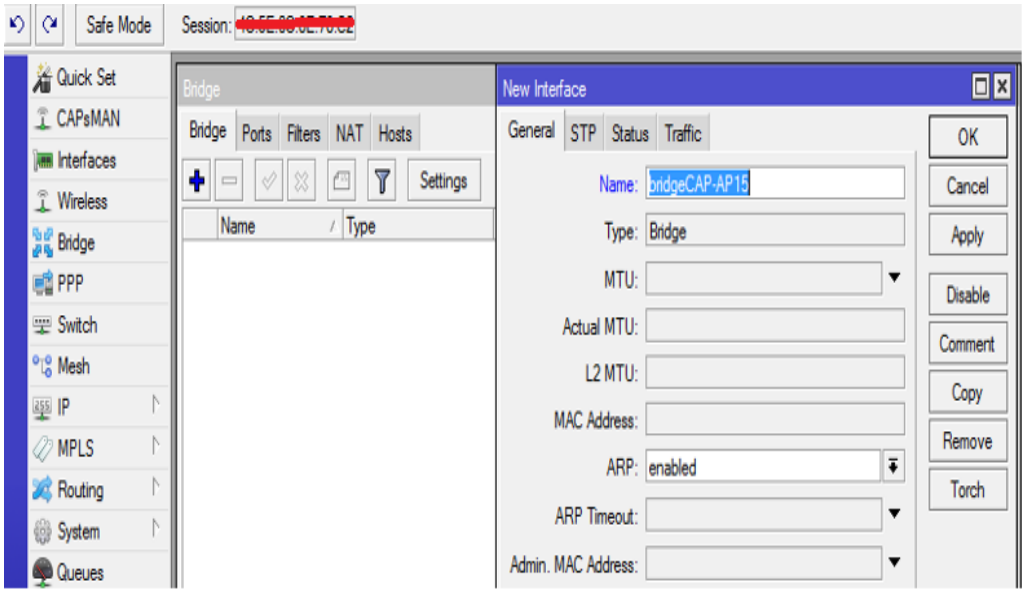


***Ilustración* 131.** Bridge CAP
Fuente: Router-Mikrotik

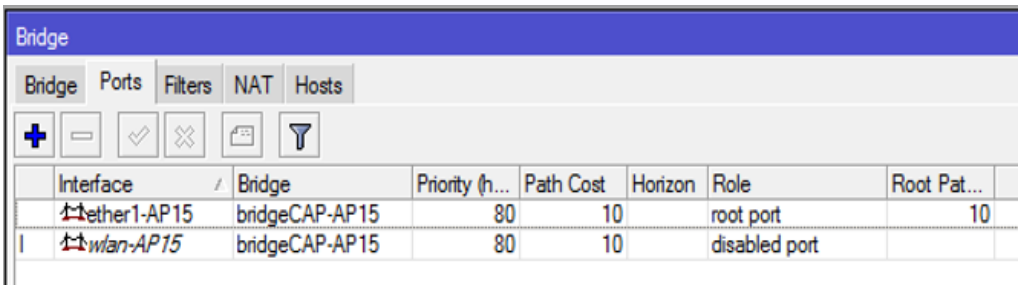


***Ilustración* 132.** Puertos Bridge
Fuente: Router-Mikrotik

37. Por último se activa el modo CAP dentro de la pestaña ***WIRELESS,*** se marca la casilla ***Enabled***, se ubica la interface inalámbrica de dicho AP, sin certificados y por último se marca un Discovery Interfaces por la interfaz LAN (ilustración 133). Una vez que se ha activado se verifica que nuestro AP sea manejado por el CAPsMAN, el cual mostrara en letras rojas un mensaje de aviso (ilustración 134).

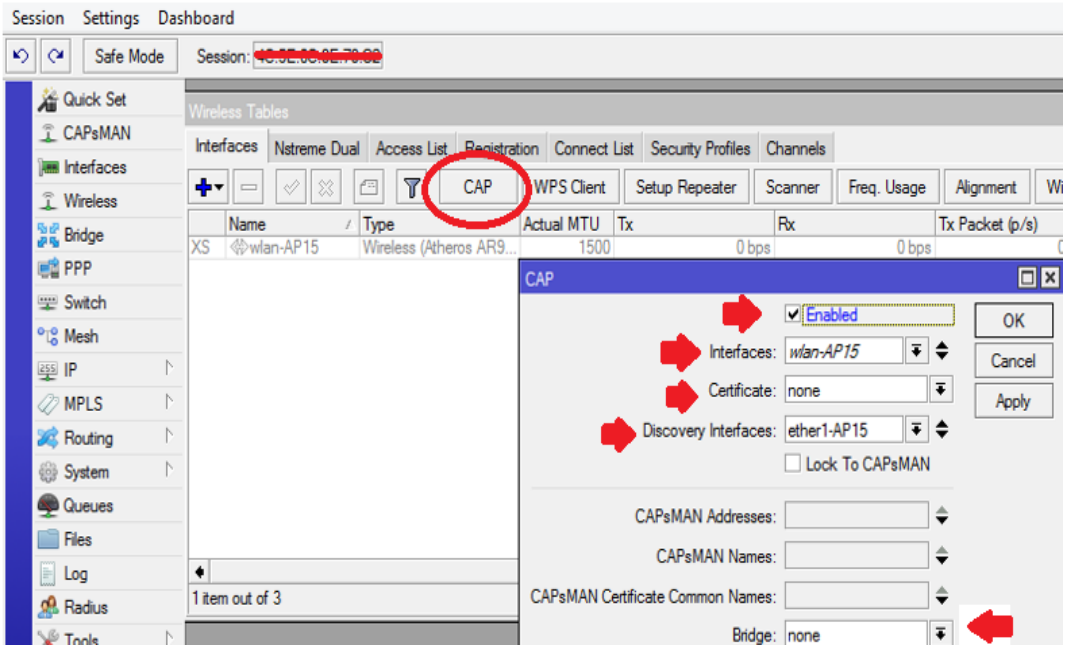


***Ilustración* 133**. Activación CAP
Fuente: Router-Mikrotik

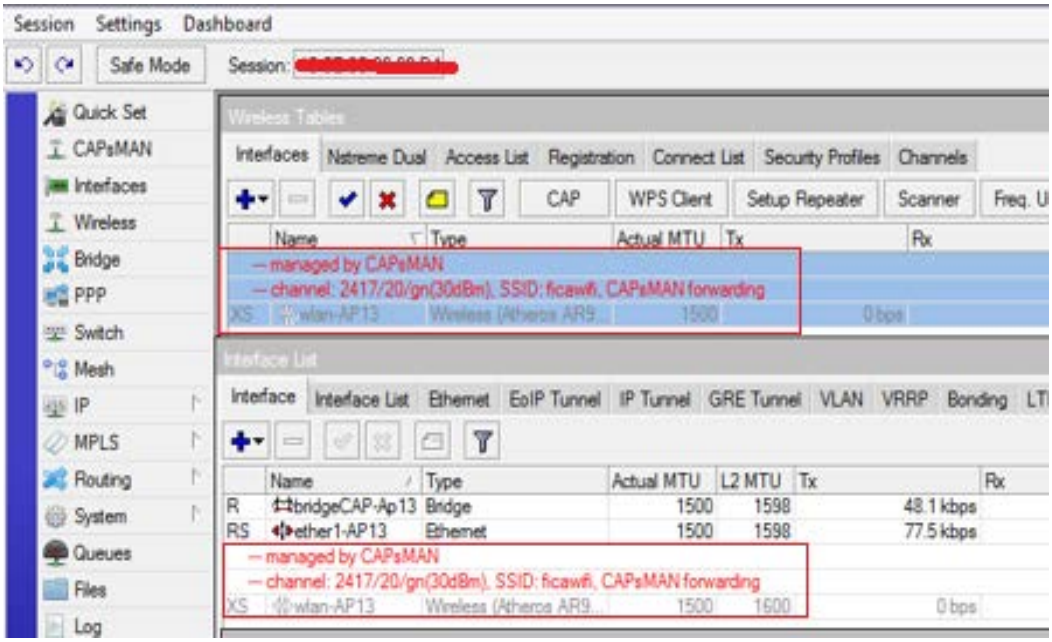


***Ilustración* 134**. Verificación CAP
Fuente: Router-Mikrotik

CONFIGURACIÓN CAPSMAN

38. Concluidas las configuraciones de todos los CAP se procede a habilitar el CAPsMAN, el cual se encargará de configurar toda la red inalámbrica desde un lugar centralizado. Se ubica la pestaña CAPsMAN/INTERFACES/MANAGER/ENABLE (ilustración 135), se pulsa

aceptar y todos los CAP se añadirán automáticamente, como muestra la ilustración 136.

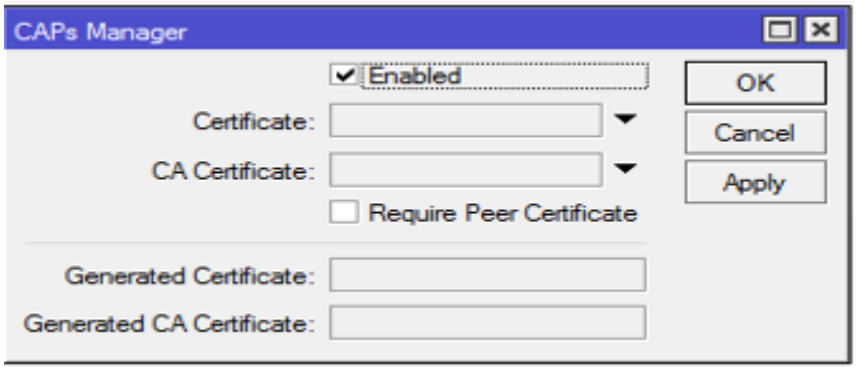


***Ilustración* 135.** CAPsMAN enable
Fuente: Router-Mikrotik

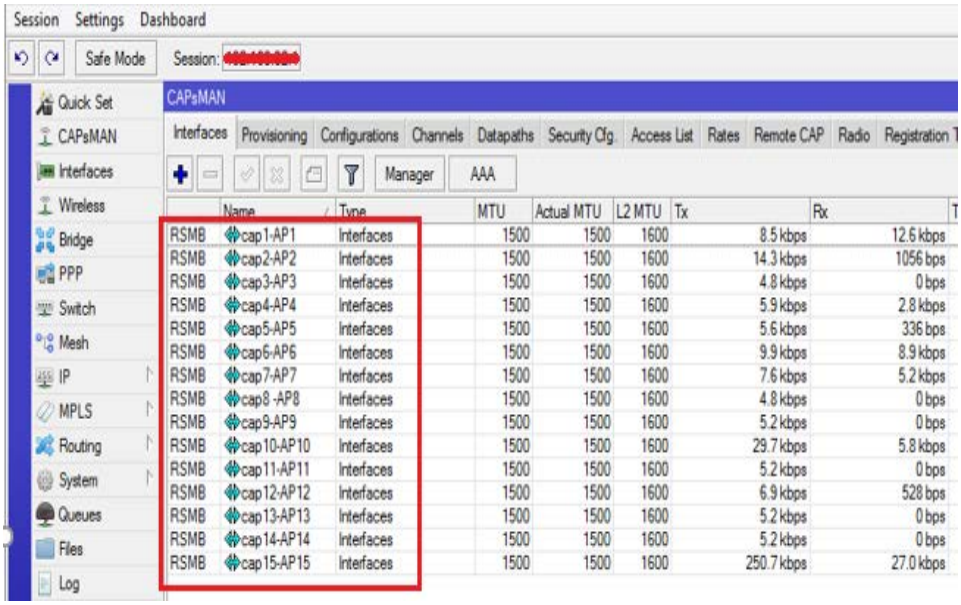


***Ilustración* 136.** Verificación CAPsMAN
Fuente: Router-Mikrotik

39. El CAPsMAN puede entregar parámetros de configuración para cada CAP, dichas configuraciones se encuentran en las solapas:

Channels: configuraciones relativas a los canales, como por ejemplo banda, frecuencia y ancho de canal (ilustración 137).

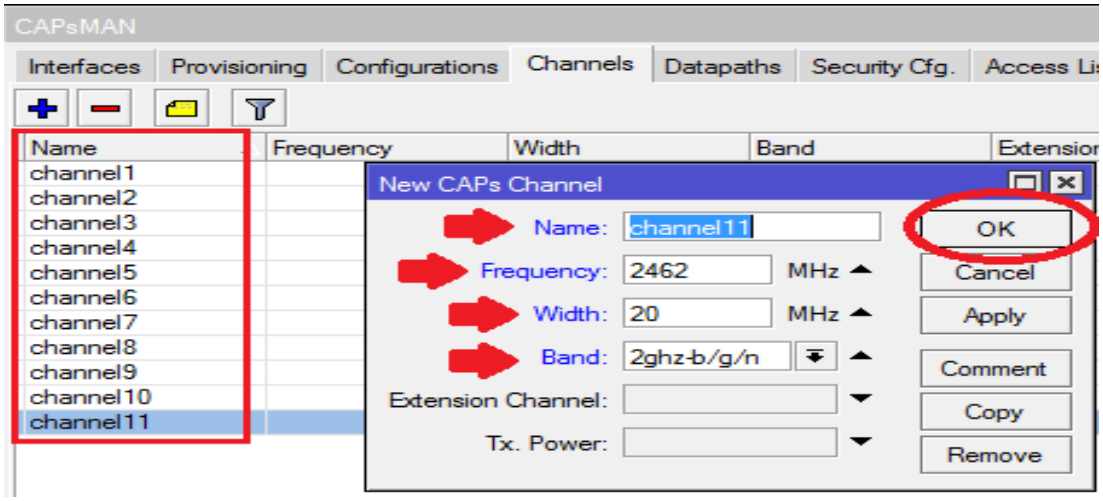


***Ilustración* 137.** Configuración Channels
Fuente: Router-Mikrotik

Datapath: configuración relacionada con el bridge donde se integrará la interfaz de los CAPs. De esta forma se configura el reenvió de tráfico hacia el CAPsMAN (ilustración 138).

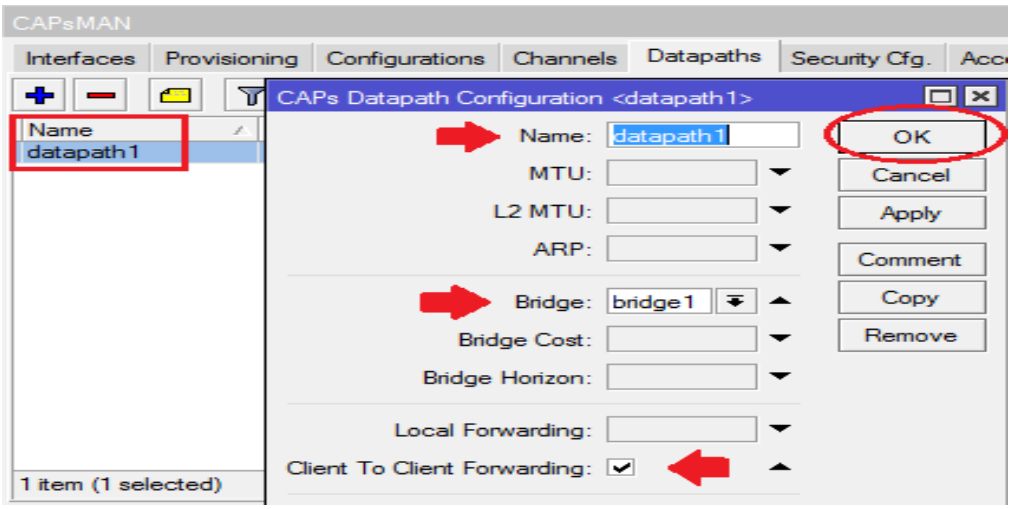


***Ilustración* 138**.Configuración Datapath
Fuente: Router-Mikrotik

Security Cfg: configuraciones de autenticación y cifrado. Soporta métodos estáticos (como llaves pre compartidas), EAP y TLS (ilustración 139).

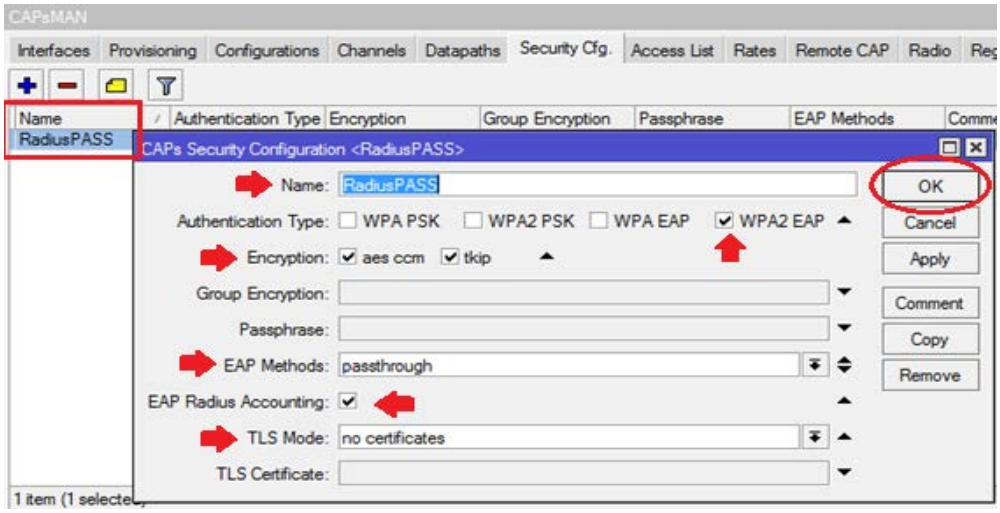


***Ilustración* 139.** Configuración Seguridades
Fuente: Router-Mikrotik

Configurations: se encuentran los perfiles principales para cada red inalámbrica. En esta pestaña se configura SSID, se asigna algún canal especifico, el datapath y la correspondiente seguridad. Estas configuraciones se pueden cargar para todos los CAP del controlador, para un grupo o para un solo CAP (ilustración 140).

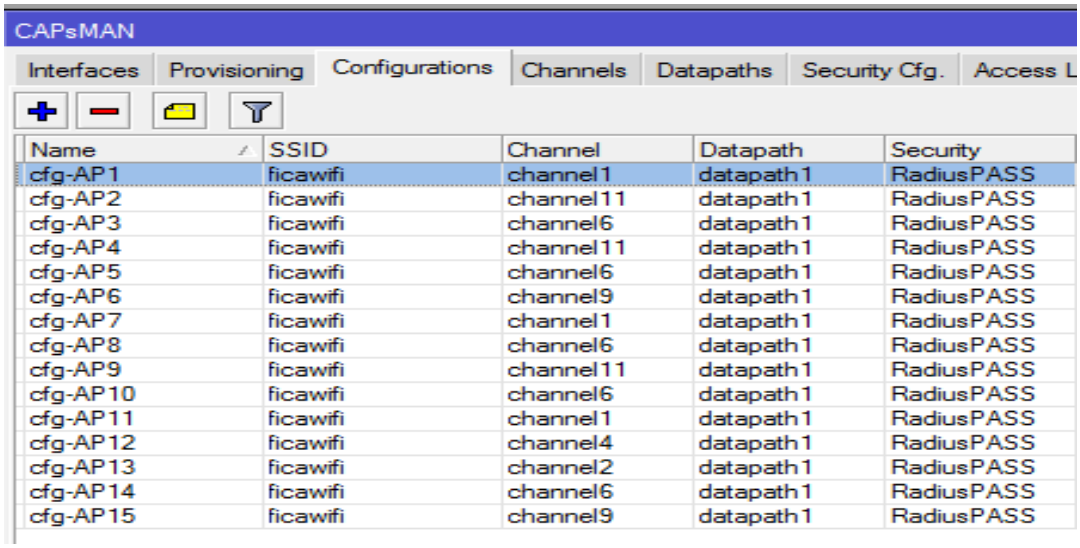


***Ilustración* 140.** Solapa Configurations
Fuente: Router-Mikrotik

Una vez creada la configuración (al menos una), se la puede cargar en los diversos CAP los cuales se encuentran en la tabla de interfaces del CAPsMAN (ilustración 141)

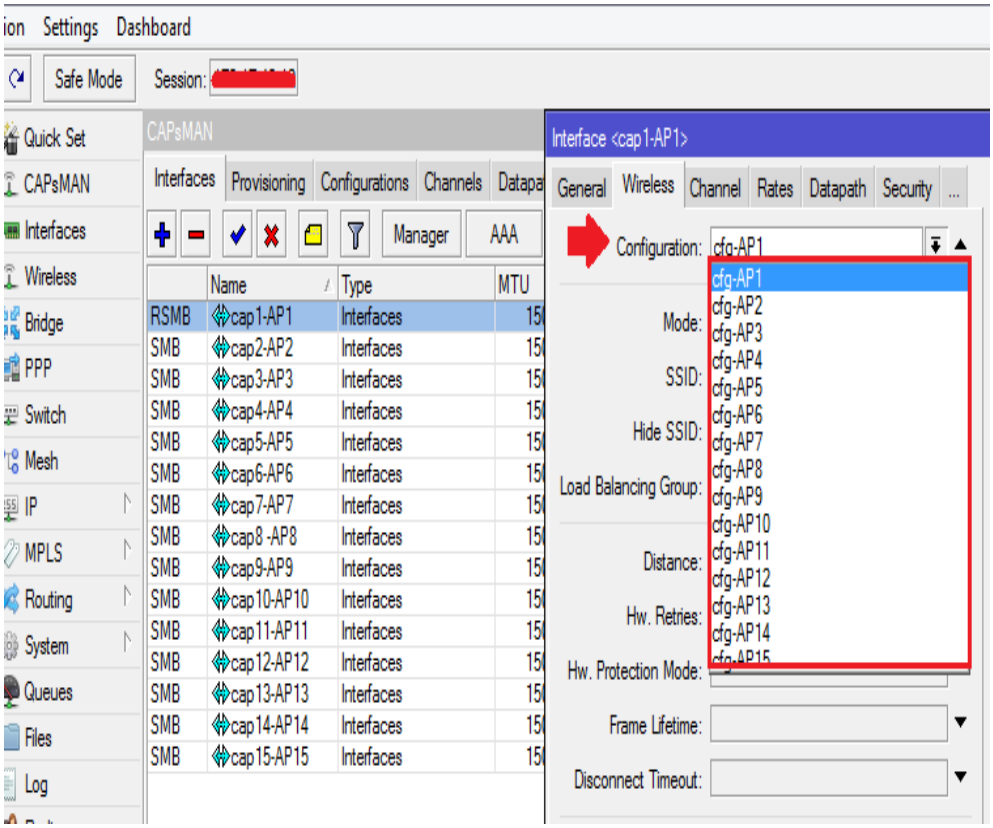


***Ilustración* 141.** Interfaces CAPsMAN
Fuente: Router-Mikrotik

SERVICIO RADIUS

40. Finalizando la configuración de nuestro CAPsMAN en el Router-Mikrotik, se activa la función RADIUS, para lo cual se única la pestaña de Radius, se crea una nueva entrada y se configura con los siguientes parámetros (ilustración 142).

Address -> dirección ip del servidor Radius
Secret -> contraseña configurada en Fichero clients.conf
Authentication port -> 1812
Accouting port -> 1813

Se activa la pestaña “Wireless”, la cual nos permitirá vincular y hacer uso del servidor LDAP con las tarjetas inalámbrica de los CAP.

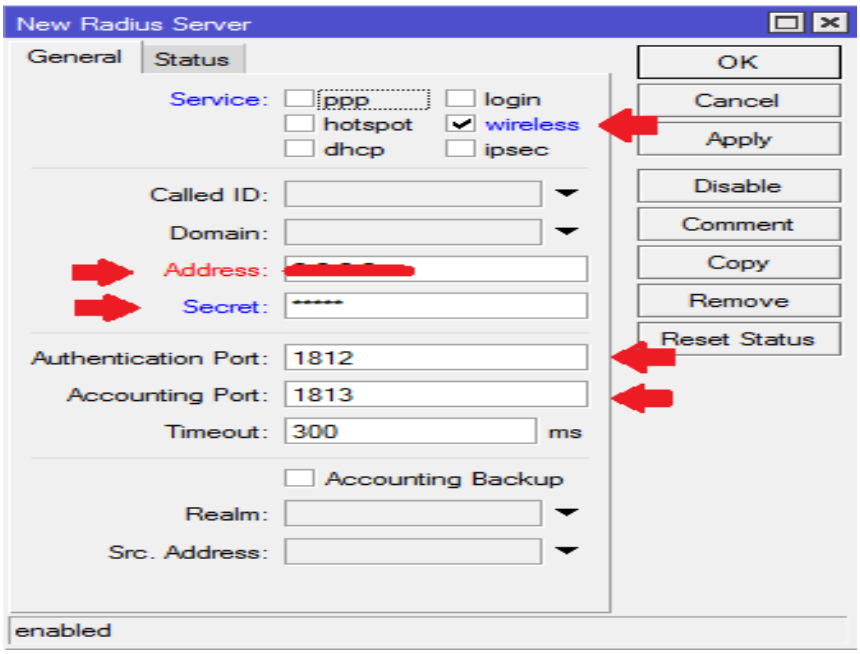


***Ilustración* 142**. Servicio RADIUS
Fuente: Router-Mikrotik

CONTROL DE ANCHO DE BANDA (QUEUE - PCQ)

41. Por último se realiza la configuración del ancho de banda, el cual se encontrará dividido en dos grandes subredes. Para ello se busca la pestaña QUEUES/QUEUE TYPES, y se crea dos ecualizadores PCQ, uno para la bajada de datos, así como también la subida de los mismos (ilustración 143). Repitiendo el proceso para ambas subredes.

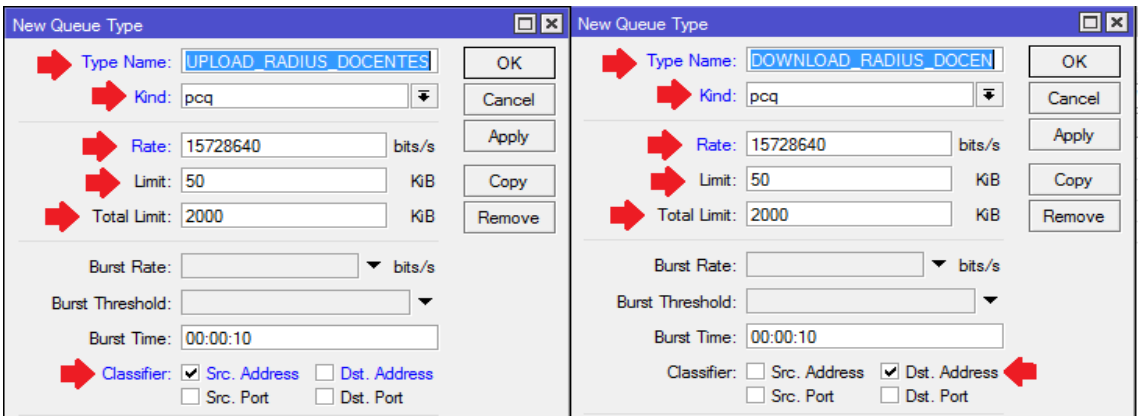


***Ilustración* 143.** Ecualizadores PCQ
Fuente: Router-Mikrotik

42. Después de crear nuestros ecualizadores se procede a crear dos nuevas reglas, una que contenga la subred de docentes y otra que contenga la subred estudiantes

(ilustración 144), en la cual se ubica dentro de la solapa ***ADVANCE*** el ecualizador que le corresponde, asignando el ancho de banda correspondiente a todos los usuarios que pertenecen a dicho grupo, conforme se muestra en la ilustración 145.

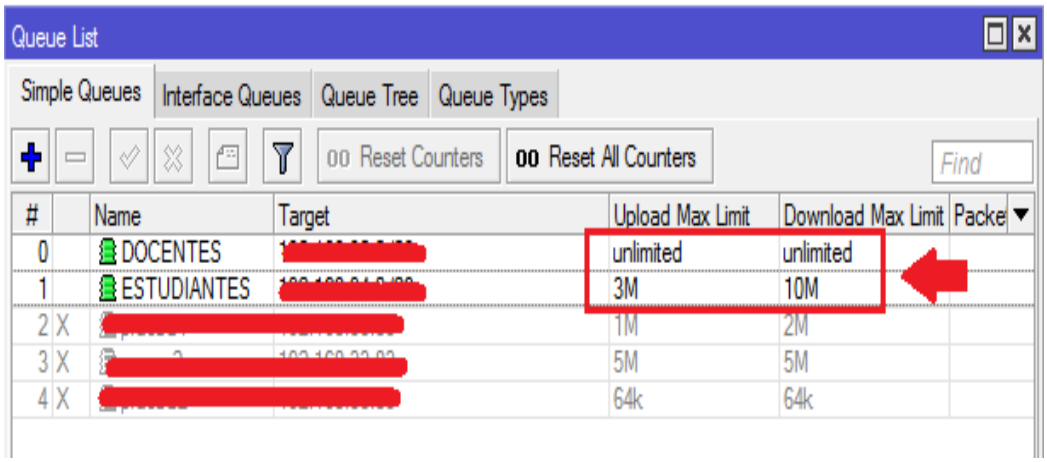


***Ilustración* 144.** Entradas QUEUE
Fuente: Router-Mikrotik

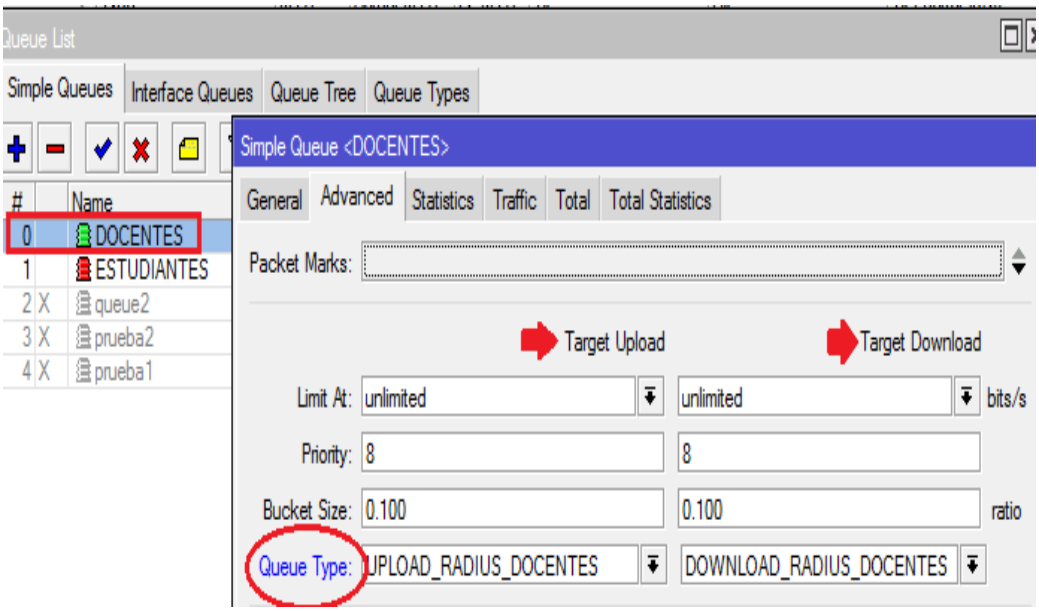


***Ilustración* 145.** Configuración avanzada QUEUE
Fuente: Router-Mikrotik

ANEXO E – Configuraciones de equipos finales (Windows – Android)

WINDOWS: Para conectase a la red inalámbrica en un sistema operativo basado en dentro de la facultad se necesitara el programa SecureW2. (Windows XP – 7 – 8.1 – 10).

1. En primer lugar se procede a descargar el programa desde el siguiente enlace https://www.redeszone.net/app/uploads/cdn/down/soft/wifi/SecureW2_Windows7.zip , se coloca en nuestro ordenador y se ejecuta el archivo (ilustración 146).

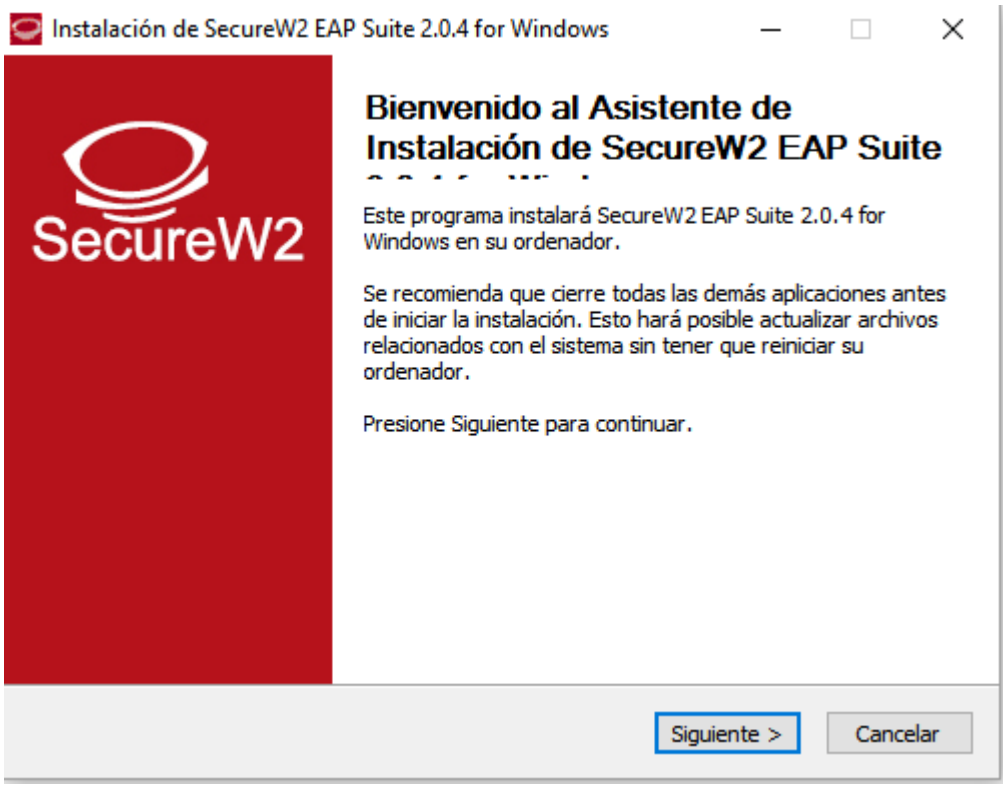


***Ilustración* 146.** Asistente de instalación SecureW2.
Fuente: SecureW2

2. Se aceptan los términos de licencia y se selecciona el componente TTLS a instalar (ilustración 147 y 148).

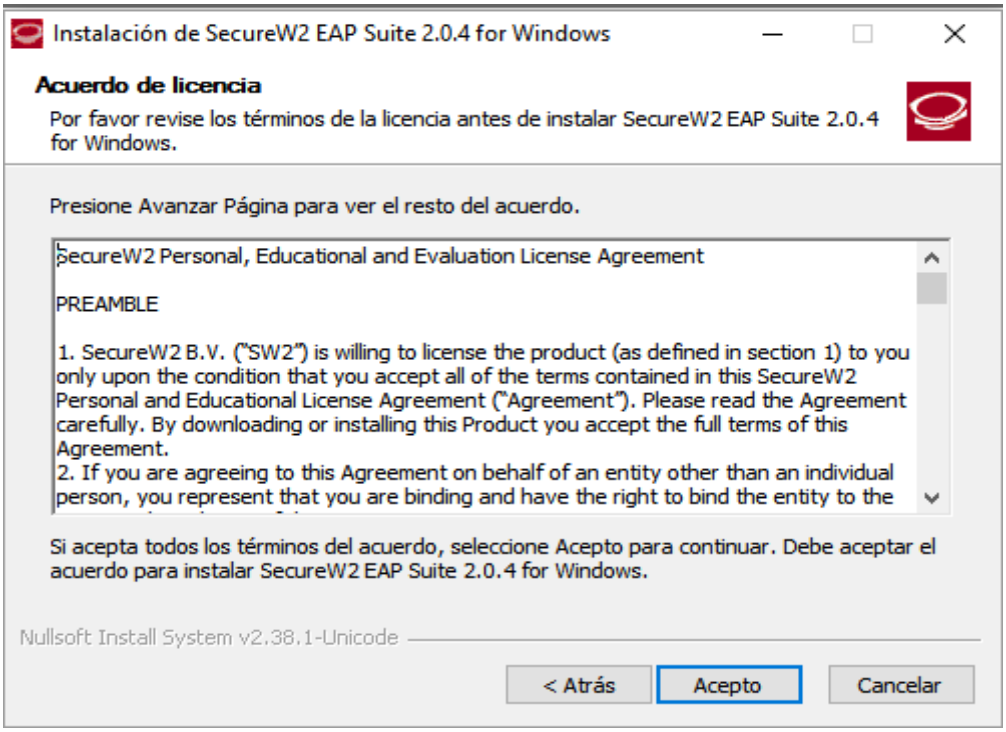


***Ilustración* 147.** Acuerdos de Licencia.
Fuente: SecureW2

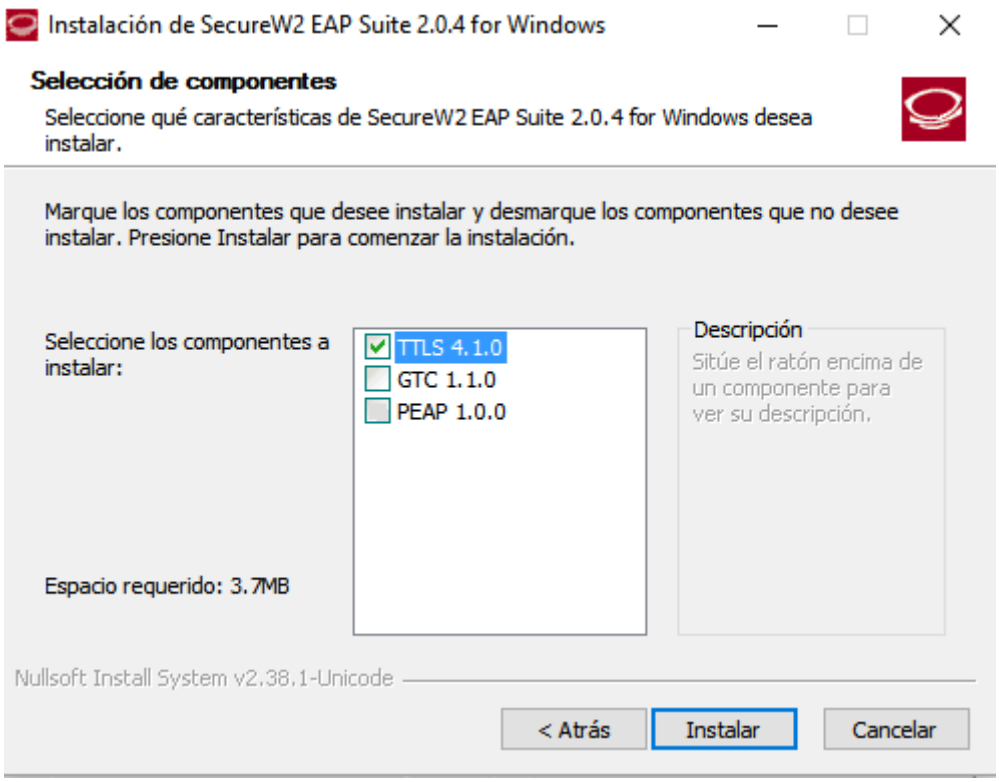


Ilustración 148. Selección de componentes a instalar.
Fuente: SecureW2

3. Se finaliza la instalación y el equipo debe ser reiniciado para guardar los cambios.

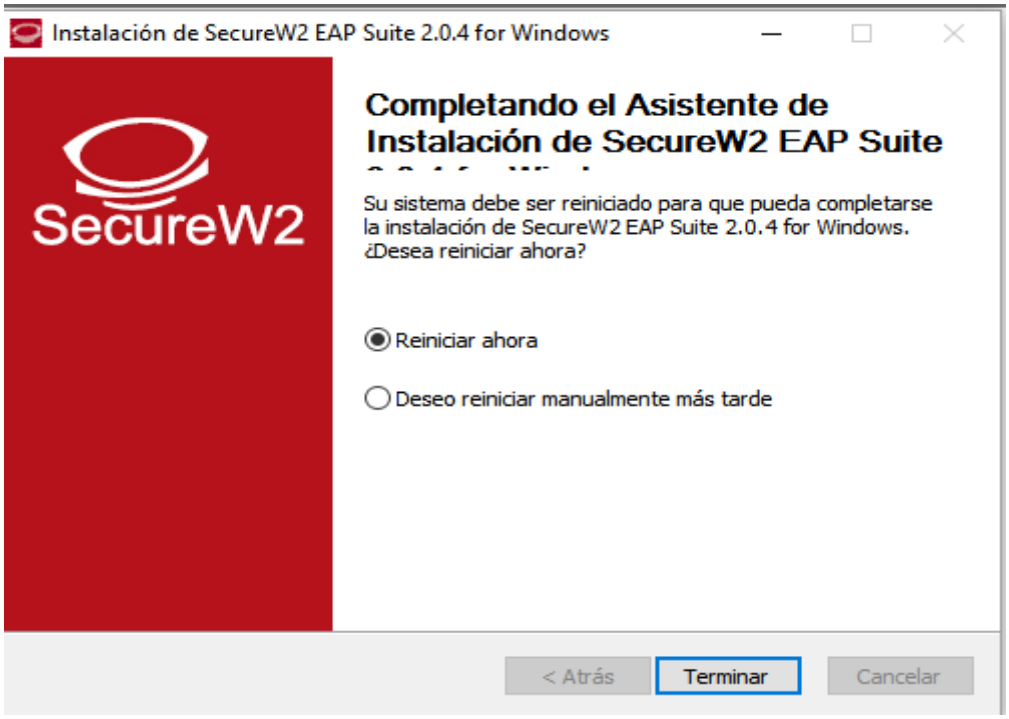


Ilustración 149. Finalización de instalación.
Fuente: SecureW2

4. Una vez que el equipo ya se haya reiniciado se procede en el directorio Inicio/Panel de Control/Redes e Internet/Centro de Redes y Recursos Compartidos/Configurar una nueva conexión o red (ilustración 150).

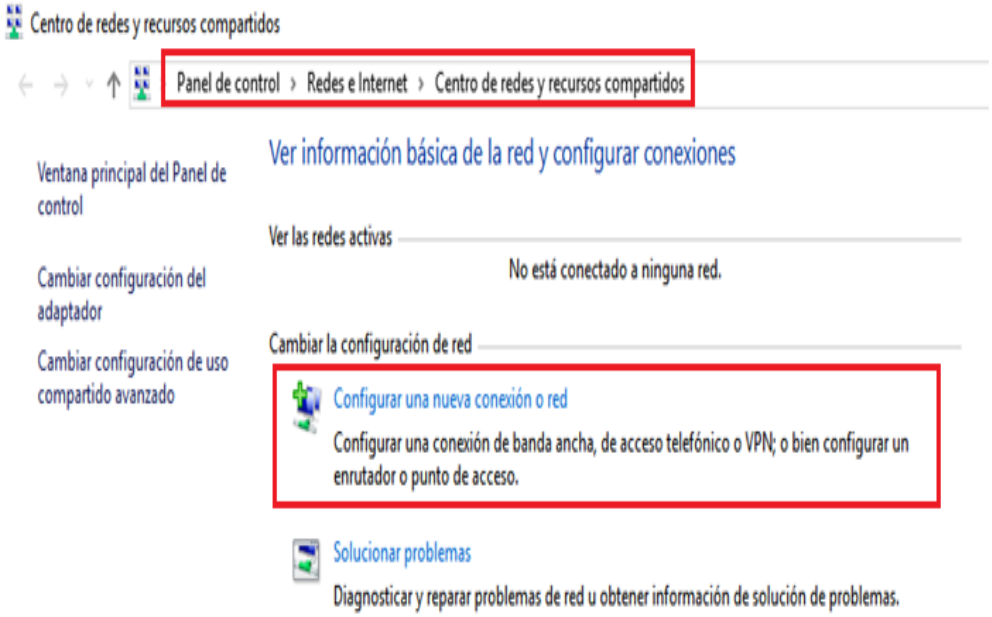


Ilustración 150. Configuración manual de red.
Fuente: Windows 10

5. Se elige el tipo de conexión que se va a configurar (ilustración 151).

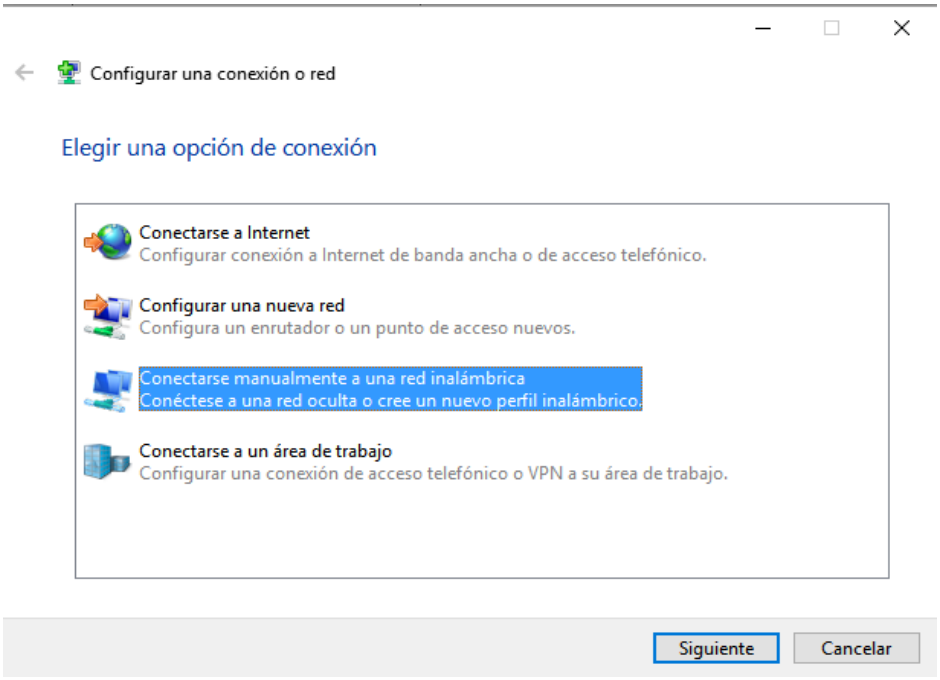


Ilustración 151. Elección del tipo de conexión.
Fuente: Windows 10

6. Se colocan los nombres del SSID de la red y el tipo de autentificación (WPA2 – Enterprise), como se indica en la ilustración 152.

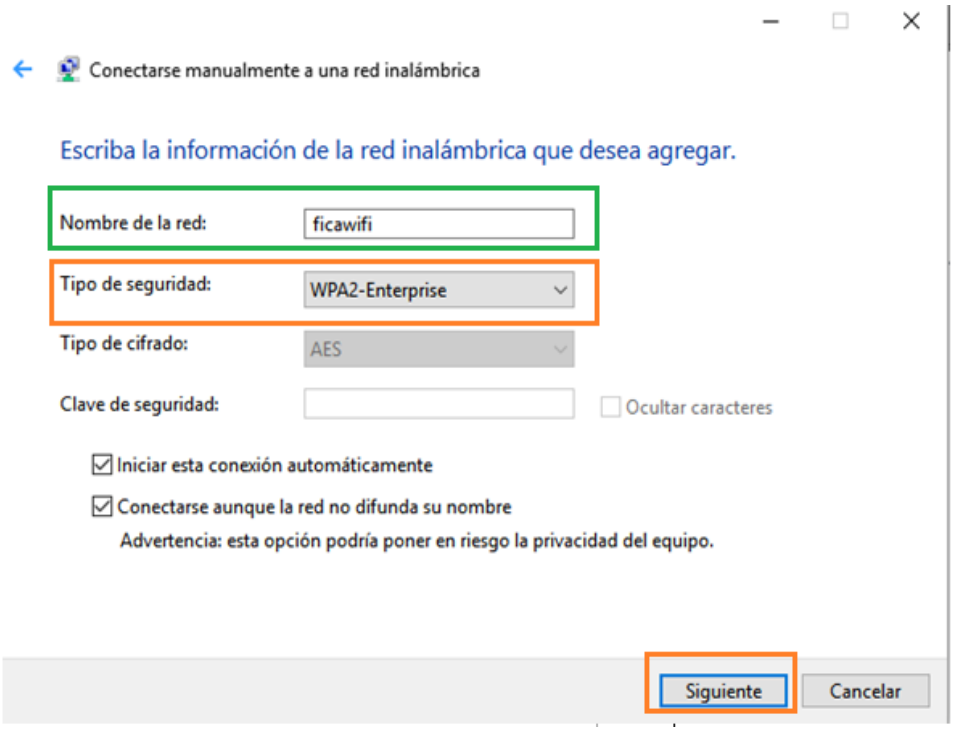


Ilustración 152. Configuración de red.
Fuente: Windows 10

7. Nos desplegara una ventana de aviso sobre la red que se agregó correctamente (ilustración 153) además indicara si se quiere modificar dicha red, para lo cual se hará click en cambiar configuración de conexión.

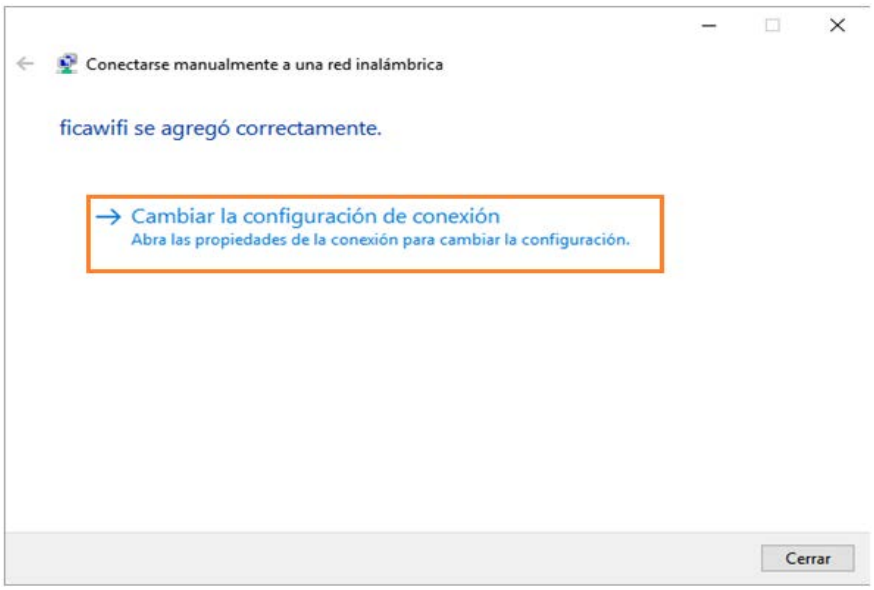


Ilustración 153. Verificación de red.
Fuente: Windows 10

8. Se busca la pestaña de seguridad y se selecciona el método de red del programa que se instaló en pasos anteriores (ilustración 154), luego se hace click en configuración.

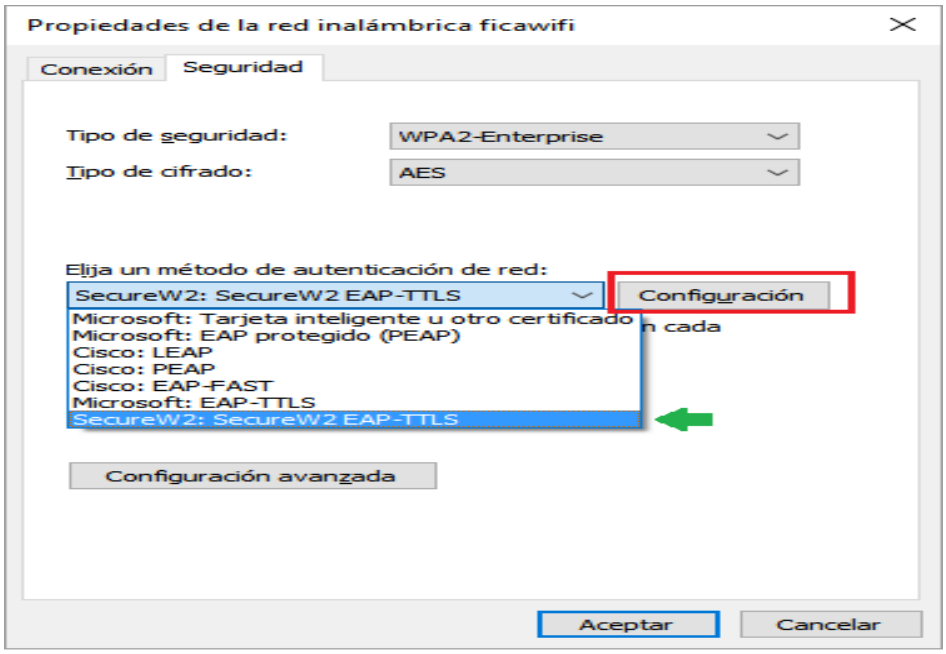


Ilustración 154. Propiedades de red inalámbrica.
Fuente: Windows 10

9. Ahora se configura un perfil por default por lo tanto se va directo a configuración (ilustración 155).

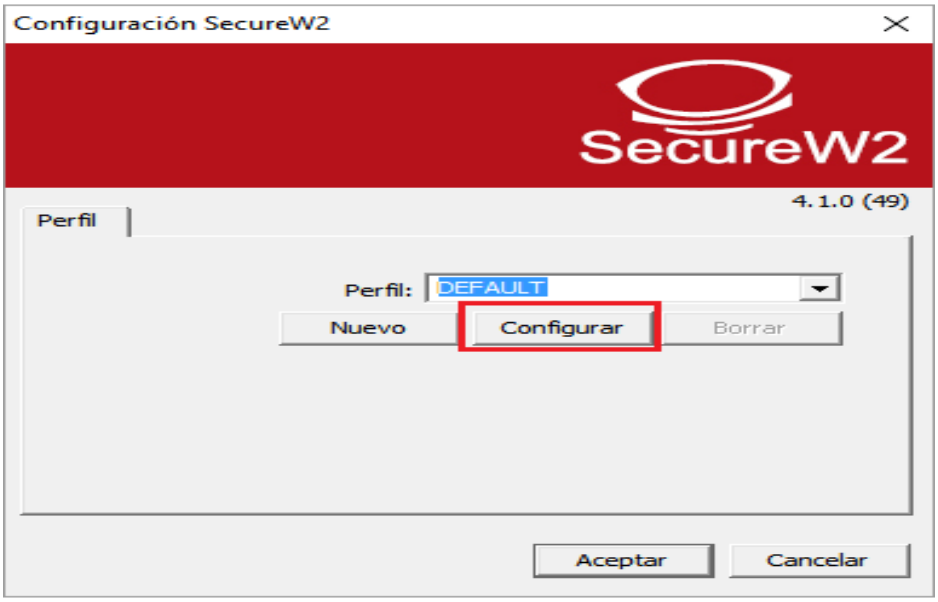


Ilustración 155. Perfil por defecto SecureW2.
Fuente: SecureW2

10. En la pestaña conexión se desmarca la casilla de identidad externa, esto debido a que las conexiones serán solo dentro de la red local con usuarios / contraseña preestablecidos en la base de datos LDAP (ilustración 156).

Ilustración 156. Configuración de conexión.
Fuente: SecureW2

11. Al utilizar la base de datos LDAP no es muy común utiliza un certificado digital, por lo tanto, en la pestaña certificados se desmarca la comprobación del servidor (ilustración 157).

Ilustración 157. Configuración de certificados.
Fuente: SecureW2

12. Se deja la autentificación PAP por defecto como indica la ilustración 158.

Ilustración 158. Configuración de Autentificación.
Fuente: SecureW2

13. Por último se escriben las credenciales correspondientes, recordando la contraseña personal y el usuario, terminado esto se cierran todas las pestañas y se guardan los cambios (ilustración 159).

Ilustración 159. Configuración de cuenta.
Fuente: SecureW2

14. Se verifica que se conecte automáticamente a la red ficawifi (en caso de algún error, volver a configurar correctamente el usuario/contraseña) o de no reportarlo al administrador de la red para generar nuevas credenciales con contraseñas (ilustración 160).

Ilustración 160. Verificación de red.
Fuente: Windows 10

ANDROID/IPHONE: Posee autenticación EAP-TTLS/PAP de forma nativa. Para conectarnos a nuestra red, sólo se tiene que seleccionar el SSID y marcar las siguientes opciones (ilustración 161 y 162).

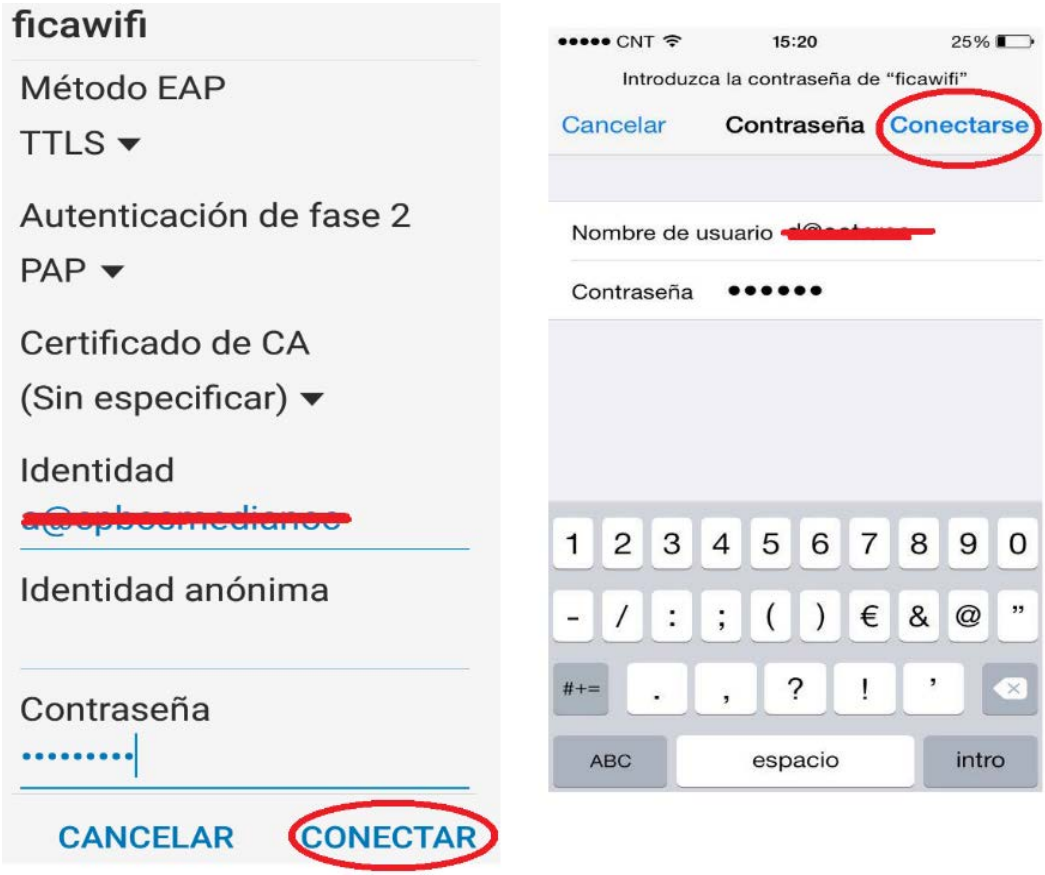


Ilustración 161. Configuración Smartphone.
Fuente: Android

Ilustración 162. Conexión Exitosa Smartphone.
Fuente: Android

ANEXO F: DATASHEET 1 - MikroTik cAP – 2n

CAP-2n

The cAP is our first 2.4GHz ceiling AP. Inconspicuously designed, it blends into the environment, perfect for hospitality businesses, such as hotels, airports, shopping malls etc.

The cAP 2n supports 802.11b/g/n and can be powered by PoE. It's a perfect companion for the MikroTik CAPsMAN (controlled AP system manager), allowing you to control all your AP devices from one central location.

Unlike traditional controller software, which requires a separate PC/Mac to run, our CAPsMAN runs on any existing RouterBOARD device in your network. No need for a separate controller machine.

Everything is included to get you started, wall/ceiling mount, PoE injector, power adapter and even the screws and screw anchors.

CPU	Atheros AR9331-AL1A 300MHz network processor
Memory	64MB DDR RAM
Ethernet	One 10/100 Mbit/s Fast Ethernet port with Auto-MDI/X
Wireless	Wireless Built-in 2.4 GHz 802.11b/g/n, one chain
Extras	Reset switch
LEDs	5x LEDs, 1x user LED
Power options	Passive PoE input 12-56V
Consumption	2W
Dimensions	⌀ 185mm, height: 31mm
Operating temperature	-30C to +70C
Operating system	WISP AP (level 4) license
Package contains	24V 0.38A power adapter, PoE injector, ceiling mount base, ceiling mount attachment
Antenna	Max gain 2dBi

802.11b/g	RX Sensitivity	TX Power
1Mbit	-96	17dBm
11Mbit	-88	17dBm
6Mbit	-92	15dBm
54Mbit	-73	11dBm
802.11n	RX Sensitivity	TX power
MCS0	-92	15dBm
MCS7	-70	10dBm

ANEXO G: DATASHEET 2 - Switch QPCOM

FICHA TÉCNICA

10/100/1000 Mbps
24 Puertos

Descripción

El switch de 24 puertos 10/100/1000 Mbps es compatible con la función de auto-negociación y auto-crossing. Cumple con el estándar IEEE802.3x para el control de flujo de datos para el modo Full Dúplex. Ideal para el uso en oficinas. Fácil instalación Plug & Play. Bajo consumo de energía.

Características

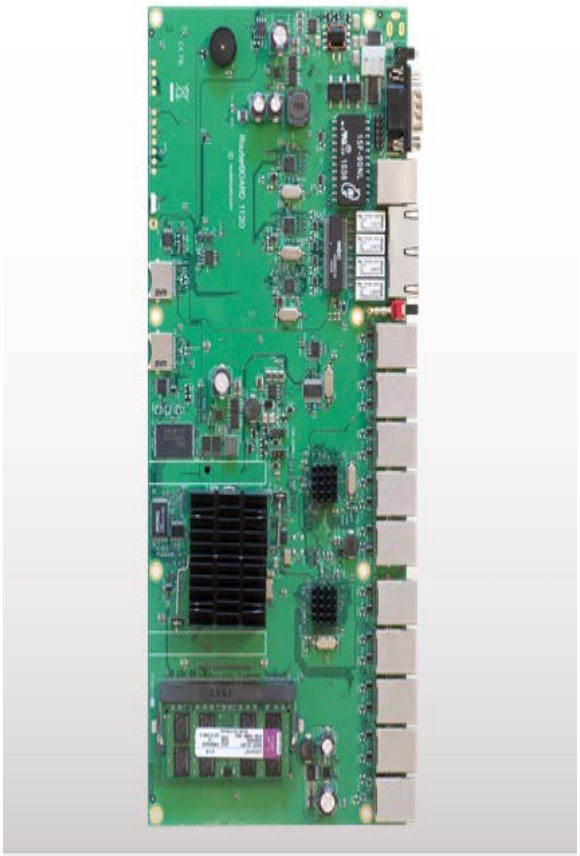
Cumple con las especificaciones de los estándares IEEE 802.3 10Base-T Ethernet, 802.3u 100 Base-TX Fast Ethernet, 802.3ab 1000Base-T.
Switch Ethernet con auto negociación de velocidad 10/100/100 Mbps de 16 puertos.
Ofrece la velocidad de 1000 Mbps solo en modo Full Dúplex.
Genera automáticamente direcciones MAC.
Control de flujo para Full Dúplex (IEEE 802.3x)
Función contrapresión para el modo de operación Half Dúplex 10/100 Mbps
Green Ethernet.

Especificaciones

Estándares:
IEEE 802.3 10Base-T, 802.3u 100Baste-TX, 802.3ab 1000Base-T, 802.3x Flow Control
Tasa de transmisión:
10/100 Mbps en modo Half Dúplex
10/100/1000 Mbps en modo Full Dúplex
Método de transmisión:
Almacenar y enviar (Store and forward)
Control de flujo:
IEEE 802.3x (Full Dúplex)
Puerto:
24 puertos RJ-45 con auto negociación de velocidad 10/100/1000 Mbps (Auto-MDI/MDIX)
Medio de red:
10BASE-T: UTP Categoría 3 o superior.
100BASE-TX: UTP Categoría 5 o superior.
1000BASE-T: UTP Categoría 5 o superior.
Método de acceso:
CSMA/CD
Indicadores LED:
Power
Link/Act.
Entorno:
Temperatura de operación: 0°C ~ 40°C (32°F ~ 104°F)
Temperatura de almacenamiento: -40°C ~ 70°C (-40°F ~ 158°F)
Humedad de operación: 10% ~ 90% no condensado
Humedad de almacenamiento: 5% ~ 90% no condensado
Alimentación eléctrica: 3.3V / 4A
Dimensiones: 445mm x 120 mm x 45 mm

Emisiones y seguridad: FCC, CE

ANEXO H: DATASHEET 3 –MikroTik RB1100 ax



RB1100AHx2

This device is our best performance 1U rackmount Gigabit Ethernet router. With a dual core CPU, it can reach up to a million packets per second.

It has thirteen individual gigabit Ethernet ports, two 5-port switch groups, and includes Ethernet bypass capability.

2GB of SODIMM RAM are included, there is one microSD card slot, a beeper and a serial port.

The RB1100AH comes preinstalled in a 1U aluminium rackmount case, assembled and ready to deploy

CPU	PowerPC P2020 dual core 1066MHz network CPU with
Memory	SODIMM DDR Slot, 2GB installed (RouterOS will use only
Boot loader	RouterBOOT, 1Mbit Flash chip
Data storage	Onboard NAND memory chip, one microSD card slot
Ethernet	Thirteen 10/100/1000 Mbit/s Gigabit Ethernet with Auto-
Ethernet	Includes switch to enable Ethernet bypass mode in two
miniPCI	none
Serial port	One DB9 RS232C asynchronous serial port
Extras	Reset switch, beeper, voltage and temperature sensors
Power options	Built-in power supply (IEC C14 standard connector 110/220V), PoE (12- 24V on port 13)
Fan	Built in fans, and Fan headers
Dimensions	1U case: 44 x 176 x 442 mm, 1275g. Board only: 365g
Operating System	MikroTik RouterOS, Level 6 license