UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

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

TEMA

“IMPLEMENTACIÓN DE LA RED LAN INALÁMBRICA QUE GARANTICE LA PERFORMANCE DE ADMINISTRACIÓN MEDIANTE EL ACCESO A LOS RECURSOS DE LA RED EN LA UNIVERSIDAD TÉCNICA DEL NORTE (UTN)”

AUTOR: EDWIN VINICIO GUERRA MORALES

DIRECTOR: ING. CARLOS VÁSQUEZ

IBARRA- ECUADOR

2014

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.
Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1002934998		
APELLIDOS Y NOMBRES:	GUERRA MORALES EDWIN VINICIO		
DIRECCIÓN:	LA VICTORIA CALLE CARLOS BARAHONA CASA 10-56		
EMAIL:	vinicio.guerra@utn.edu.ec		
TELÉFONO FIJO:	062615903	**TELÉFONO MÓVIL:**	0981210702 0979285267
DATOS DE LA OBRA			
TÍTULO:	IMPLEMENTACIÓN DE LA RED LAN INALÁMBRICA QUE GARANTICE LA PERFORMANCE DE ADMINISTRACIÓN MEDIANTE EL ACCESO A LOS RECURSOS DE LA RED EN LA UNIVERSIDAD TÉCNICA DEL NORTE (UTN)		
AUTOR (ES):	GUERRA MORALES EDWIN VINICIO		
FECHA:	2014-12-01		
PROGRAMA:	PREGRADO		
TITULO POR EL QUE OPTA:	INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN		
ASESOR /DIRECTOR:	ING. CARLOS VÁSQUEZ		

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Edwin Vinicio Guerra Morales, con cédula de identidad Nro. 1002934998, en calidad de autor (es) y titular (es) de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, Diciembre del 2014

EL AUTOR:

Firma
Nombre: Edwin Vinicio Guerra Morales
Cédula: 1002934998

V

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

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

Yo, Edwin Vinicio Guerra Morales, con cédula de identidad Nro. 1002934998, 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 (es) de la obra o trabajo de grado denominado: **IMPLEMENTACIÓN DE LA RED LAN INALÁMBRICA QUE GARANTICE LA PERFORMANCE DE ADMINISTRACIÓN MEDIANTE EL ACCESO A LOS RECURSOS DE LA RED EN LA UNIVERSIDAD TÉCNICA DEL NORTE (UTN)**, que ha sido desarrollado para optar por el título de: **Ingeniero en Electrónica y Redes de Comunicación** en 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 este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Ibarra, Diciembre del 2014

Firma
Nombre: Edwin Vinicio Guerra Morales
Cédula: 1002934998

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DECLARACIÓN

Yo, Edwin Vinicio Guerra Morales, declaro bajo juramento que el trabajo aquí descrito es de mí autoría; y que éste no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes 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.

Firma
Nombre: Edwin Vinicio Guerra Morales
Cédula: 1002934998

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado en su totalidad por Edwin Vinicio Guerra Morales, bajo mi supervisión.

ING. CARLOS VÁSQUEZ
DIRECTOR DEL PROYECTO

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

AGRADECIMIENTOS

Agradezco en primer lugar a Dios por permitirme disfrutar de las maravillas de la vida.

Expreso mi más sincero agradecimiento a las autoridades de la Universidad Técnica del Norte, en especial al Administrador de Redes y Comunicaciones, Ing. Cosme Ortega por la amistad y confianza depositada, además de su invaluable y apreciable colaboración para la realización del siguiente proyecto.

A mi director del proyecto de titulación Ing. Carlos Vásquez a quien considero un gran amigo, por dedicarme su valioso tiempo, apoyo incondicional y conocimientos importantes que aportaron a la culminación del presente trabajo de grado, de igual manera a mis maestros que formaron parte de mi crecimiento personal y profesional en especial al Ing. Jaime Michilena por su amistad y consejos brindados.

Edwin Vinicio Guerra Morales

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DEDICATORIA

A mi hijo David Vinicio que es el motor de superación que impulsa mi vida día a día. A mis padres Vinicio Guerra y María de Lourdes Morales por haberme dado la vida, por su amor, comprensión y el ejemplo de bien que me han inculcado enseñándome los buenos valores.

A mis hermanos Alexis, Juan Luis y María Paula por el apoyo incondicional brindado para seguir adelante, superando las barreras que se presentaron en el camino.

A mis familiares y demás seres queridos que me ayudaron con alguna palabra de aliento y motivación para desarrollar mi proyecto de tesis.

Edwin Vinicio Guerra Morales

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo de titulación tiene como objetivo, implementar una Red LAN Inalámbrica que permita el acceso por autenticación a los recursos de red mediante un servidor AAA encargado de validar el ingreso de cada usuario y adicionalmente controlar el acceso a Internet por medio de un Portal Cautivo en la Universidad Técnica del Norte (UTN).

Se realizó un estudio de los fundamentos básicos de redes inalámbricas para comprender conceptos importantes como el protocolo IEEE 802.11, tipos de antenas, handoff / roaming, seguridad en las redes inalámbricas, entre otros. Luego se analizó como se encontraba actualmente funcionando la red inalámbrica que tenía deficiencias enormes de cobertura. Posterior a ello en el diseño e implementación se procedió a analizar los requerimientos del diseño, tecnología de la red inalámbrica, diseño de modelo jerárquico, direccionamiento de la red, análisis de escalabilidad, determinación de equipos, cobertura de los Access Points (APs), distribución de canales, gestión y configuración del Wireless LAN Controller (WLC), análisis comparativo de portales cautivos, políticas de seguridad, instalación y configuración del Portal Cautivo, del servidor de Autenticación y del Firewall – Proxy.

Finalmente, el análisis costo beneficio ayudó a determinar la rentabilidad del proyecto como un indicador de mucha relevancia para la acreditación institucional como por cada carrera.

ABSTRACT

The present work titling was aimed, implement a wireless network that allows access for authentication to network resources through a AAA server in charge of validating the entry of each user and additionally control access to Internet through a Captive Portal at the “Universidad Técnica del Norte” (UTN).

A study was made of the basics fundamentals of wireless networks to understand some important concepts such as the IEEE 802.11 protocol, types of antennas, handoff / roaming, security in wireless networks, among others. Then analized as it was currently operating the wireless nework that had great coverage deficiencies. Following this in the design and implementation proceeded to analyze the design requeriments, the wireless network technology, design hierarchical model, network addressing, scalability analysis, determination of equipment, coverage of Access Points (APs), distribution of channels, management and configuration of Wireless LAN Controller (WLC), comparative analysis of captive portals, security policies, install and configure the captive portal, authentication server and Firewall - Proxy.

Finally, the cost benefit analysis helped to determine the project profitability as an indicator of much relevance for the institutional accreditation as each career.

PRESENTACIÓN

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS

CARRERA DE INGENIERIA EN ELECTRONICA Y REDES DE COMUNICACIÓN

ANTEPROYECTO DE TRABAJO DE GRADO

DATOS GENERALES

1. TEMA: "Implementación de la Red LAN Inalámbrica que garantice la performance de administración mediante el acceso a los recursos de red en la Universidad Técnica del Norte (UTN)."
2. ÁREA / LÍNEA DE INVESTIGACIÓN: Networking, Seguridad en Redes, Cableado Estructurado, WLAN, Comunicación Inalámbrica, Base de Datos.
3. ENTIDAD QUE AUSPICIA: Universidad Técnica del Norte
4. DIRECTOR: Ing. Carlos Vásquez
5. AUTOR: Guerra Morales Edwin Vinicio **DIRECCIÓN:** Ciudadela "La Victoria" calle Carlos Barahona Mz 19 Cs 10-56 **TELÉFONO:** 081210702 **CORREO ELECTRÓNICO:** vinicio.guerra@utn.edu.ec
6. DURACIÓN (Estimado): 6 meses
7. INVESTIGACIÓN: Nueva (*) Continuación ( )
8. PRESUPUESTO (estimado): 41,231.52 USD

PARA USO DEL CONSEJO ACADÉMICO	
FECHA DE ENTREGA:	FECHA DE REVISIÓN:
APROBADO: SI ( ) NO ( )	FECHA DE APROBACIÓN:
OBSERVACIONES:	

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS

CARRERA DE INGENIERIA EN ELECTRONICA Y REDES DE COMUNICACIÓN

PLAN DEL PROYECTO DE TITULACIÓN

Propuesto por:	**Áreas Técnicas del Tema:**
Guerra Morales Edwin Vinicio	Networking, Seguridad en Redes, Cableado Estructurado, WLAN, Comunicación Inalámbrica, Base de Datos
Director sugerido:	**Fecha:**
Ing. Carlos Vásquez	Julio 2012

1. Tema

Implementación de la Red LAN Inalámbrica que garantice la performance de administración mediante el acceso a los recursos de red en la Universidad Técnica del Norte (UTN).

2. Problema

El aumento significativo de aplicaciones en la red ha provocado en la Universidad Técnica del Norte (UTN) muchas falencias en el rendimiento y la capacidad de sus servicios y recursos.

Los estudiantes requieren tener acceso a una red LAN Inalámbrica en el interior de cada una de las facultades de la UTN, pero dadas las circunstancias no se ha logrado establecer buenas políticas sobre el uso, consumo y capacidad donde los procesos realizados garanticen su funcionalidad. En puntos estratégicos de los alrededores de la institución se implementaron Access Points (APs), los mismos que no abastecen a cubrir un área de cobertura eficiente y mucho menos movilidad.

Toda fuente de información confiable es un complemento para la educación académica de los alumnos de la UTN, por ello la conexión a la Internet es una herramienta metodológica para los partícipes del aprendizaje y la enseñanza identificando los criterios y procedimientos de estudio.

3. Objetivos

Objetivo General

Implementar una Red LAN Inalámbrica que permita el acceso por autenticación a los recursos de red mediante un dispositivo AAA controlando el acceso a Internet por un Portal Cautivo en la Universidad Técnica del Norte (UTN).

Objetivos Específicos

- Analizar los fundamentos de las redes LAN Inalámbricas y los principales métodos de autenticación soportados por el estándar IEEE 802.1x para brindar el servicio de acceso a la red de la UTN.
- Determinar la situación actual de la distribución de la red inalámbrica realizando un análisis que permita establecer los requerimientos actuales y futuros de la UTN.
- Diseñar la Red LAN Inalámbrica previo al análisis situacional realizado que servirá como base para su futura implementación.
- Analizar los requerimientos de seguridad para controlar el acceso a los recursos de la red, de acuerdo al perfil de usuario perteneciente a la red de datos de la UTN.
- Instalar el equipamiento hardware y software una vez determinado el posicionamiento de los equipos.
- Configurar los Equipos y el Portal Cautivo, corroborar su funcionalidad partiendo de las pruebas realizadas garantizando la factibilidad y fiabilidad como una solución idónea en la UTN.
- Realizar el análisis Costo- Beneficio considerando las herramientas de hardware y software utilizadas en la implementación de la red inalámbrica en la UTN.

4. Alcance

Inicialmente se estudiará los fundamentos de las Redes LAN Inalámbricas y Servicios. Se determinará una comparación sobre los principales métodos de autenticación del protocolo 802.1x y un análisis de los diferentes portales cautivos.

El Proyecto planteado consiste en el diseño e implementación de una red inalámbrica utilizando un dispositivo Wireless LAN Controller que permita la autenticación de usuarios para el control de acceso a los recursos de la red aplicando los protocolos del estándar 802.1x.

Para el desarrollo de este proyecto se iniciará por determinar la situación actual de la distribución de la red inalámbrica realizando un análisis de frecuencias, canales, puntos de red de datos disponibles lo cual permita establecer los requerimientos actuales y futuros a utilizar en la red inalámbrica y el software a emplear en la autenticación y control de usuarios.

A continuación se diseñará la red LAN inalámbrica de acuerdo al análisis estudiado de frecuencias, canales de operación, ubicación de los Access Points (AP), área de cobertura de los APs en todo el campus de la UTN y en cada una de las facultades. Se realizará un levantamiento de información para determinar los puntos críticos donde se puede representar mayor requerimiento de usuarios, de esta manera se describirán políticas de acceso mediante grupos que se definirán en el proceso para la parte interna de las facultades como para los exteriores de cada una de ellas tomando en cuenta la movilidad aplicando el proceso de Handoff que permitirá que el usuario al alejarse del rango de cobertura de una estación base automáticamente se conecte a la estación base siguiente sin necesidad de reconexión. Cabe resaltar que la distribución de los recursos de la red LAN inalámbrica será gestionable dependiendo de los puntos críticos que se crearen en su funcionamiento.

Luego se procederá con la instalación, configuración de equipos y pruebas de funcionalidad. En el equipo Wireless LAN Controller se habilitará la seguridad del protocolo estándar 802.1x por el cual se receptará las peticiones del suplicante al AP. Se implementará un Equipo AAA y un Portal Cautivo que funcionará como gateway a la Internet para controlar el acceso a red LAN Inalámbrica.

Finalmente realizar un Análisis Costo-Beneficio considerando las herramientas de hardware y software utilizadas en la implementación de la red LAN Inalámbrica en la UTN. Para ello se tendrá en cuenta algunos parámetros importantes en el análisis como: Retorno de inversión (ROI), optimizar el tiempo de vida útil, prestaciones de la red, mejoramiento del servicio, garantizar el acceso, escalabilidad, condiciones ambientales y mantenimiento.

5. Contexto

Cabrera Proaño, Claudio Armando (2011). Análisis a la Seguridad de Redes Inalámbricas como extensión de una Red LAN. (Tesis de Ingeniería en Sistemas Computacionales). Universidad Técnica del Norte, Facultad de Ingeniería en Ciencias Aplicadas, Ibarra, Ecuador.

El siguiente proyecto de tesis realizado es un análisis de Seguridad de las Redes Inalámbricas, en el cual se señala las diferencias que existen entre una red cableada y una red inalámbrica, defensas y ataques que con sistemas de autenticación de usuarios y algoritmos encriptación se puede proteger de mejor manera una red LAN Inalámbrica.

6. Contenidos

CAPÍTULO I: Fundamentos de Redes LAN Inalámbricas

Se estudiará los conceptos básicos e importantes, características y seguridades en las redes inalámbricas. Se analizará para el control de acceso los principales métodos de autenticación y una comparación de portales cautivos.

CAPÍTULO II: Situación actual de la Red LAN Inalámbrica y Recursos

En este capítulo se identificará como se encuentra formada actualmente la red inalámbrica de la Universidad Técnica del Norte, que permita establecer los requerimientos actuales y futuros a ser considerados en el diseño de la Red LAN Inalámbrica.

CAPÍTULO III: Diseño de la Infraestructura de Movilidad de la Red LAN Inalámbrica para la Universidad Técnica del Norte.

Se diseñará la red LAN Inalámbrica de acuerdo al análisis estudiado de frecuencias, canales de operación, ubicación de los Access Points (AP), área de cobertura de los APs en todo el campus de la UTN y en cada una de las facultades como también el dimensionamiento del AAA y el portal cautivo.

CAPÍTULO IV: Implementación de la Red LAN Inalámbrica y Pruebas de Funcionalidad en la Universidad Técnica del Norte.

En el siguiente capítulo se procederá con la configuración de los equipos a utilizar y las pruebas de funcionalidad que demuestren el mejoramiento de la performance de acceso de los usuarios y la confiabilidad de la solución planteada en la implementación de la red LAN Inalámbrica en la UTN.

CAPÍTULO V: Análisis Costo-Beneficio.

Se realizará el análisis costo-beneficio considerando las herramientas de hardware y software utilizadas en la implementación de la red LAN Inalámbrica en la UTN.

Conclusiones y Recomendaciones

BIBLIOGRAFÍA

ANEXOS

CAPÍTULO I

1. FUNDAMENTOS DE REDES LAN INALÁMBRICAS

Se estudió los conceptos básicos, características y seguridades en las redes inalámbricas. Para el control de acceso se analizará los principales métodos de autenticación y una comparación de portales cautivos.

1.1. INTRODUCCIÓN

En la actualidad, el crecimiento de las redes LAN[1] Inalámbricas se ha extendido en el mundo de las telecomunicaciones por las ventajas que ofrecen de flexibilidad y movilidad en relación a una red LAN Cableada. Los sistemas de comunicación que se basan en el cableado son notablemente más rápidos, confiables y seguros que los sistemas inalámbricos, pero se debe tomar en cuenta que la instalación de una infraestructura cableada puede ser muy costosa.
El conocimiento de la historia y evolución de la tecnología LAN inalámbrica es una parte esencial de los principios fundamentales de las redes LAN inalámbricas. Una investigación profunda indica que las WLAN[2] llegaron a formar parte de una solución a las necesidades de comunicación, donde las entidades y aplicaciones que han ayudado a madurar la tecnología permitirán aplicar de mejor manera las redes LAN Inalámbricas para su organización o los requerimientos de sus clientes.

1.2. HISTORIA

Las redes de propagación del espectro inalámbrico, como muchas otras tecnologías, alcanzó su auge en el área militar. El ejército necesitaba que sea simple, fácil de implementar, y sobre todo un método seguro de intercambio de datos en un entorno de combate donde no se puede acceder con tecnología cableada.
La tecnología inalámbrica ofrece una forma relativamente barata de campus corporativos para que los edificios se conecten entre sí, sin implementar el cableado de cobre o fibra. Hoy en día, el costo de la tecnología inalámbrica es tal que la mayoría de las empresas pueden poner en práctica segmentos inalámbricos de su red sin problemas, convirtiendo por completo su red en una LAN inalámbrica, ahorrando tiempo y dinero; lo que permite flexibilidad y escalabilidad de los sistemas inalámbricos. Los hogares también se benefician de los bajos costos y la disponibilidad del hardware de la tecnología inalámbrica.

Muchas personas están creando redes LAN inalámbricas de bajo costo que se benefician de la movilidad lo que hace que se dé un gran número de instalaciones de redes inalámbricas

[1] **LAN** Local Area Network
[2] **WLAN** Wireless Local Area Network, Sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas

permitiendo que siga aumentando su uso. Como el número de usuarios crece se pueden presentar ciertos inconvenientes como la interoperabilidad, lo que puede causar que una red quede inútil o interfiera con el buen funcionamiento de la misma.

1.3. GENERALIDADES DE LAS REDES LAN INALÁMBRICAS

1.3.1. ANTECEDENTES

Debido a que las redes LAN inalámbricas en la transmisión utilizan frecuencias de radio, las redes inalámbricas están reguladas por los mismos organismos que gobiernan radio AM[3] / FM[4] que es el caso de la Comisión Federal de Comunicaciones (FCC[5]) cuya misión es regular el uso de dispositivos de una LAN inalámbrica. En el actual mercado de las WLAN hay varias normas aceptadas de funcionamiento como Wi-Fi[6]; y proyectos que son creados y mantenidos por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE[7]) en los Estados Unidos.

Estas normas son creadas por grupos de personas que representan diversas organizaciones, incluyendo académicos, empresarios, militares, y el gobierno. Debido a que normas establecidas por la IEEE pueden tener tal impacto en el desarrollo de la tecnología, estas tardan muchos años en ser publicadas, por lo que son sometidas a varios estudios y pruebas de factibilidad.

Las nuevas tecnologías requieren normas que describan y definan su correcto funcionamiento. El desafío de los fabricantes y responsables de las normas es agotar sus recursos para influir en los diversos problemas de interoperabilidad y compatibilidad.

1.3.2. DEFINICIÓN

Una red de área local inalámbrica (WLAN) proporciona un sistema flexible de comunicaciones en distancias cortas utilizando señales de radio o infrarrojas en lugar del cableado de red tradicional.

Una WLAN se construye conectando un dispositivo llamado Access Point (AP[8]) al borde de la red cableada (ver FIGURA 1), a través del cual los usuarios finales se asocian por medio

---

[3] **AM** Amplitude Modulation
[4] **FM** Frequency Modulation
[5] **FCC** Organismo estatal del Gobierno de los Estados Unidos encargado de la regulación de las telecomunicaciones
[6] **Wi-Fi (Wireless-Fidelity)** Conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11.
[7] **IEEE** Asociación técnico-profesional mundial dedicada a la estandarización
[8] **AP** Punto de conexión entre redes inalámbricas y alámbricas

de un adaptador de red inalámbrico que tiene mucha similitud a un adaptador Ethernet[9] tradicional.

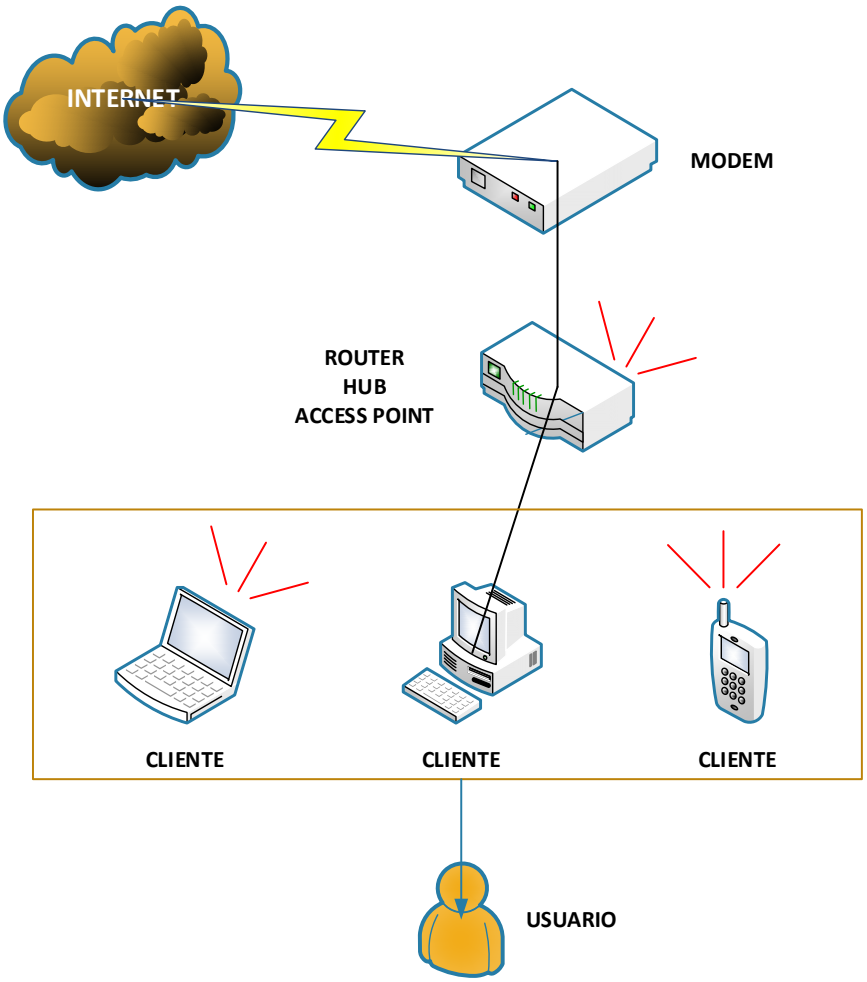


FIGURA 1 Conectividad WLAN
http://lima-lima.olx.com.pe/instalacion-de-redes-wifi-empresariales-domiciliarias-entorno-indoor-iid-479256848

Una WLAN no es más que una extensión de una LAN cableada existente, permitiendo la transmisión y recepción de información mediante ondas electromagnéticas que se propagan a través de un medio de transmisión no guiado, combinando dos factores esenciales que son: conectividad y movilidad.

1.4. PROTOCOLO IEEE 802.11

En 1990, el Comité IEEE 802 formó un nuevo grupo de trabajo, IEEE 802.11, específicamente dedicado a redes LAN inalámbricas, con la misión de desarrollar un

[9] **Ethernet** Red de área local basado en el estándar 802.3

protocolo MAC[10] y la especificación del medio físico (PHY[11]). El interés inicial estaba en el desarrollo de una WLAN funcionando en la banda ISM[12] (Industrial, Scientific, and Medical). Desde ese tiempo, la demanda de redes inalámbricas, a diferentes frecuencias y tasas de datos se incrementó. A la par con esta demanda, el Grupo de Trabajo IEEE 802.11 ha publicado una lista de estándares cada vez mayor (ver TABLA 1). (Stallings, 2005, pág. 428)

TABLA 1 Estándares IEEE 802.11

ESTÁNDARES	FECHA	DESCRIPCIÓN
802.11	1997	Estándar original Capa MAC Capa Física: Infrarrojo a 1 y 2 Mbps Capa Física: 2.4 GHz FHSS a 1 y 2 Mbps Capa Física: 2.4 GHz DSSS a 1 y 2 Mbps
802.11a	1999	Opera en la banda de 5 GHz Trabaja con OFDM Velocidades de transmisión de hasta 54 Mbps
802.11b	1999	Opera en la banda de 2.4 GHz Trabaja con DSSS Velocidades de transmisión 1,2, 5.5 y 11 Mbps
802.11c	1998	Procedimiento de operación bridge en la capa MAC de 802.11, incluido en el estándar IEEE 802.1D (2001)
802.11d	2001	Cambios en la recomendación física para extender 802.11 a países con diferentes regulaciones
802.11e	2005	Mejora la capa MAC de 802.11 para proporcionar Calidad de Servicio (QoS)

[10] **MAC** Medium Access Control
[11] **PHY** Physical Layer
[12] **ISM** Banda para uso comercial sin licencia

802.11f	2003	Protocolo Inter-access Point Protocol (IAPP), define comunicaciones del punto de acceso interno para facilitar WLAN múltiples
802.11g	2003	Opera en la banda de 2.4 GHz Trabaja con DSSS y OFDM Velocidades de transmisión de hasta 54 Mbps Compatible con el estándar IEEE 802.11b
802.11h	2003	Define la gestión de la potencia de transmisión y del espectro en la banda 5 GHz
802.11i	2004	Incorpora mejoras en los mecanismos de seguridad y autenticación
802.11.j	2004	Mejora IEEE 802.11a para ajustarse a los requerimientos Japoneses
802.11m		Mantenimiento del estándar IEEE 802.11-1999 con correcciones técnicas y editoriales
802.11	2007	Una nueva versión del estándar IEEE 802.11 que incluye modificaciones en a, b, d, e, g, h, i, j
802.11ma	2007	Mantenimiento y revisión del estándar IEEE 802.11-2007
802.11k	2008	Medidas de Recursos de Radio de las Wireless LAN Modificación 1 en IEEE Std 802.11-2012
802.11r	2008	Transición rápida entre BSS (Conjunto de Servicios Básicos) Roaming rápido Modificación 2 en IEEE Std 802.11-2012
802.11y	2008	Aplicación del estándar en la banda 3650-3700 MHz en USA Modificación 3 en IEEE Std 802.11-2012
802.11w	2009	Protección de Tramas de gestión Modificación 4 en IEEE Std 802.11-2012

802.11n	2009	Mejoras de rendimiento Throughput Redes MIMO[13] Velocidad de 300 Mbps en capa física Hace uso simultáneo de las bandas 2.4 GHz y 5 GHz Modificación 5 en IEEE Std 802.11-2012
802.11t	2009	Predicción de rendimiento Wireless (WPP[14]) Recomendaciones de métodos de prueba y métricas Estándar retirado
802.11p	2010	Comunicaciones para entornos de vehículos (WAVE[15]) Modificación 6 en IEEE Std 802.11-2012
802.11z	2010	Extensions to Direct-Link Setup (DLS) Permite el intercambio de tramas entre estaciones en un BSS Modificación 7 en IEEE Std 802.11-2012
802.11v	2011	Gestión de Redes Wireless Modificación 8 en IEEE Std 802.11-2012
802.11u	2011	Interoperabilidad con Redes Externas Modificación 9 en IEEE Std 802.11-2012
802.11s	2011	Redes Mesh Conjunto de Servicios Extendidos (ESS[16]) Modificación 10 en IEEE Std 802.11-2012
802.11mb	2011	Mantenimiento y revisión del estándar IEEE 802.11-2012
802.11	2012	Una nueva versión del estándar IEEE 802.11 que incluye modificaciones en k, n, p, r, s, u, v, w, y, z

[13] **MIMO** Multiple Input, Multiple Output
[14] **WPP** Wireless Performance Prediction
[15] **WAVE** Wireless Access in Vehicular Environments
[16] **ESS** Extended Service Set

802.11aa	2012	Transporte robusto de flujos de video y voz
802.11ae	2012	Gestión de QoS Priorización de las tramas de gestión
802.11ac	Ongoing	Very High Throughput < 6 GHz
802.11ad	Ongoing	Very High Throughput 60 GHz
802.11af	Ongoing	TV Whitespace
802.11ah	Ongoing	Extensión de capa física en bandas ISM < 1 GHz
802.11ai	Ongoing	Fast Initial Link Setup

Fuente: (Stallings, 2005, pág. 429)

1.4.1. COMPONENTES Y TOPOLOGÍAS DE UNA RED LAN INALÁMBRICA

La arquitectura IEEE 802.11 consiste de varios componentes que interactúan para proporcionar una WLAN que soporte movilidad en cada estación y entre estaciones.

1.4.1.1. CONJUNTO DE SERVICIOS BÁSICOS (BSS) – MODO DE INFRAESTRUCTURA

El BSS[17] es el bloque básico de construcción de una LAN Inalámbrica. La FIGURA 2 muestra dos BSS, cada uno de ellos con dos estaciones que son miembros del BSS.

Es útil pensar en los óvalos usados para representar un BSS como el área de cobertura dentro de la cual las estaciones que son miembros del BSS pueden permanecer en comunicación. El concepto de área, si bien no es preciso, a menudo es suficiente. Esta área es llamada Área de Servicios Básicos (BSA[18]). Si una estación se mueve fuera de su BSA no puede comunicarse directamente con otras estaciones presentes en el BSA. (IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007, 2012, pág. 45)

[17] **BSS** Basic Service Set
[18] **BSA** Basic Service Area

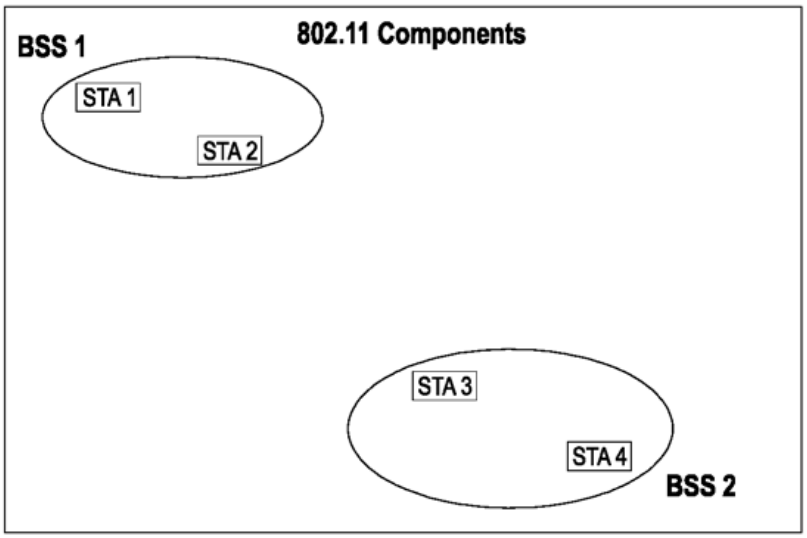


FIGURA 2 Conjunto de Servicios Básicos
Fuente: (IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007, 2012, pág. 46)

1.4.1.2. EL BSS INDEPENDIENTE (IBSS) – MODO AD-HOC

El IBSS es el tipo más básico de LAN Inalámbrico. Una mínima red WLAN puede consistir de sólo dos estaciones. Dado que los BSSs que se muestran en la FIGURA 2 son simples y carecen de otros componentes (esto contrasta con la FIGURA 3) los dos se pueden tomar para ser representativo de dos IBSSs.

Este modo de operación es posible cuando las estaciones son capaces de comunicarse directamente. Debido a que este tipo de red inalámbrica se forma a menudo sin planificación previa, sólo durante el tiempo que en la WLAN es necesario, este tipo de operación se refiere a menudo a una red ad-hoc[19].

1.4.1.3. SISTEMA DE DISTRIBUCIÓN (DS, DISTRIBUTION SYSTEM)

En lugar de existir independientemente, un BSS de infraestructura también puede formar un componente de una forma extendida de la red que está construido con múltiples BSSs. El componente arquitectónico utilizado para interconectar BSSs de infraestructura es el DS.

(IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007, 2012) Afirma:

[19] **Ad-Hoc** Red formada sin ninguna administración central que consta de nodos móviles que usan una interfaz inalámbrica para enviar paquetes de datos.

El estándar IEEE 802.11 lógicamente separa el WM[20] del medio sistema de distribución (DSM[21]). Cada medio lógico es utilizado para diferentes propósitos por un componente diferente de la arquitectura. La definición de IEEE 802.11 no impide y no demanda de que los medios múltiples para cualquiera de los dos sea el mismo o diferente. Reconociendo que los medios múltiples son lógicamente diferentes, es clave para entender la flexibilidad de la arquitectura. La arquitectura IEEE 802.11 se especifica independientemente de las características físicas de cualquier implementación específica. (pág. 47)

El DS habilita la compatibilidad con dispositivos móviles, proporcionando los servicios lógicos necesarios para gestionar la asignación de la dirección de destino y una perfecta integración de múltiples BSSs.

Un Access Point habilita el acceso al DS, a través del WM para emisoras asociadas. También añade los componentes DS, DSM y AP a la arquitectura IEEE 802.11 tal como se muestra en la FIGURA 3

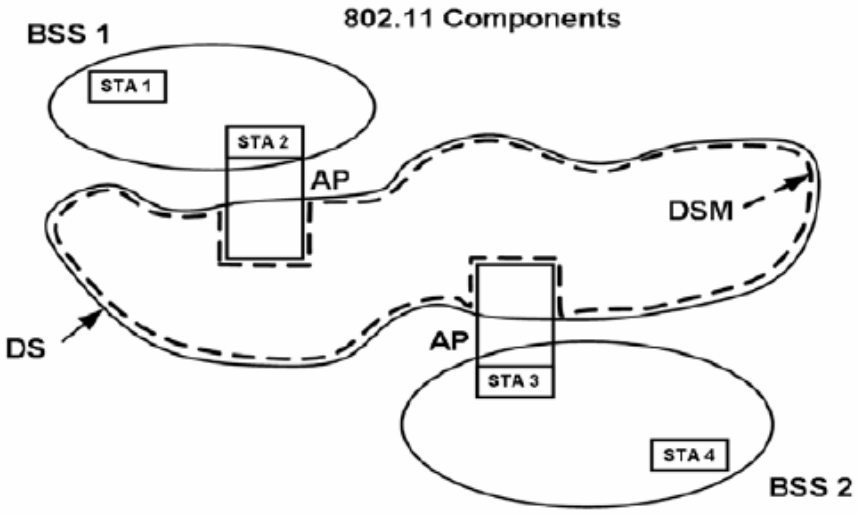


FIGURA 3 DSs y APs

Fuente: (IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007, 2012, pág. 47)

Los datos se mueven entre un BSS y el DS a través de un AP. Se debe considerar que todos los APs son también estaciones, por lo que son entidades direccionables. Las direcciones utilizadas por un AP para la comunicación en el WM y en el DSM no son necesariamente los mismos por que pueden constituirse en redes diferentes.

[20] **WM** Wireless Medium
[21] **DSM** Distribution System Medium

1.4.1.4. CONJUNTO DE SERVICIOS EXTENDIDOS (ESS, EXTENDED SERVICE SET)

El DS y los BSSs de infraestructura se basan en IEEE 802.11 para crear una red inalámbrica de tamaño arbitrario y complejo. El estándar se refiere a este tipo de redes como una arquitectura ESS. Un ESS es la unión de BSSs de infraestructura con el mismo SSID conectados mediante un DS. Cabe mencionar que el ESS no incluye el DS.

El concepto clave es que la red ESS tiene la misma apariencia a una capa LLC[22] como una red IBSS. Las Estaciones dentro de un ESS pueden comunicarse y las estaciones móviles pueden desplazarse de un BSS a otro (dentro del mismo ESS) de forma transparente a LLC. Nada es asumido por la norma sobre el área de cobertura y la ubicación física de los BSSs como se indica en la FIGURA 4.

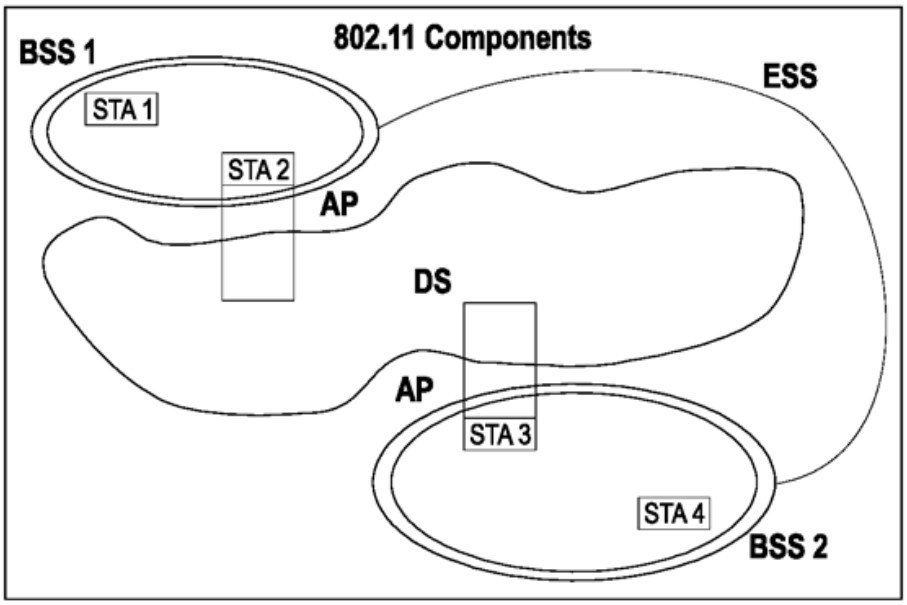


FIGURA 4 Conjunto de Servicios Extendidos (ESS)
Fuente: (IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007, 2012, pág. 48)

1.4.1.5. ACCESS POINT (AP)

El AP es una entidad que tiene la funcionalidad de una estación. Específicamente, no es más que un puente para enlazar las estaciones inalámbricas con las estaciones cableadas junto con sus recursos, o simplemente puede ser utilizado para la conexión inalámbrica de estaciones entre sí.

[22] **LLC** Logical Link Control

1.4.1.6. PORTAL

El portal se implementa en un dispositivo como puede ser un bridge o un router, que es parte de una LAN cableada y se encuentra integrado al DS como se observa en la FIGURA 5.

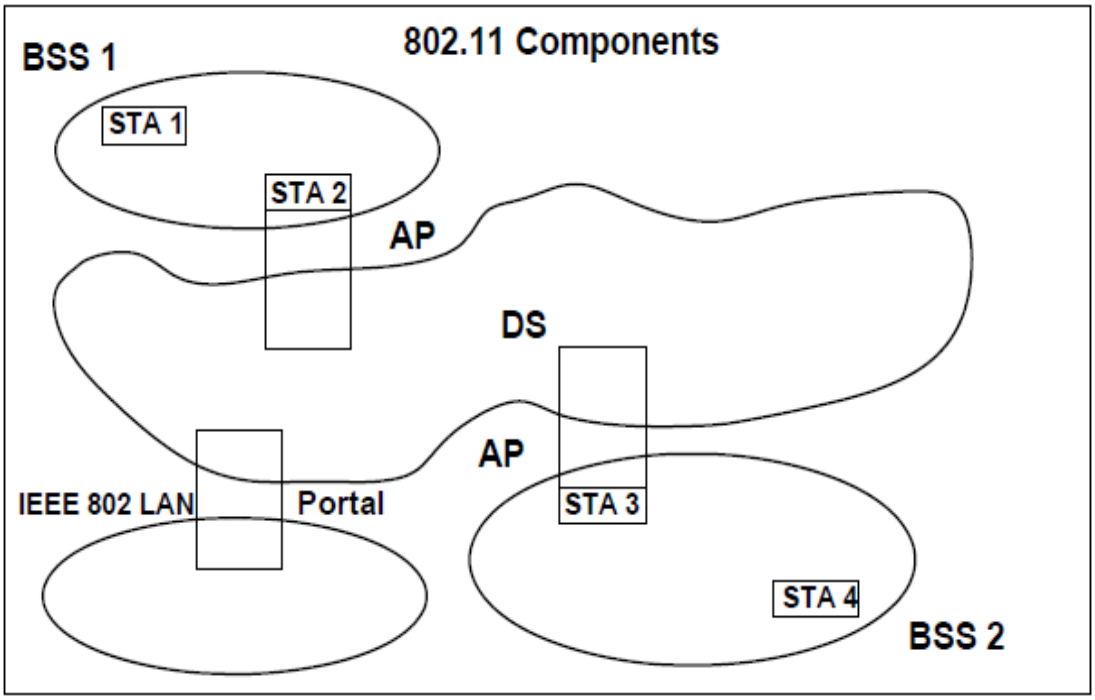


FIGURA 5 Portal

Fuente: (IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007, 2012, pág. 51)

1.4.1.7. WIRELESS MEDIUM (WM)

El medio inalámbrico (WM) es utilizado para la transferencia real de información entre las entidades de una WLAN, es decir, el aire y el espacio. Varios tipos de datos pueden ser codificados dentro de un tipo de perturbación electromagnética llamada onda de radio. Estas ondas de radio se transmiten por el aire (medio inalámbrico) a su destino, donde se decodifica de nuevo en datos útiles.

1.4.1.8. WIRELESS STATION (STA)

Cualquier dispositivo que implementa el estándar IEEE 802.11 se denomina una estación inalámbrica. Una STA es por lo tanto una simple entidad física que puede interpretar el estándar IEEE 802.11, de esta manera las estaciones inalámbricas no son muy útiles por sí mismos, necesitan de dispositivos cableados para enviar y recibir información con el fin de que sean útiles y eficientes. La FIGURA 6 muestra algunos ejemplos de estaciones inalámbricas.

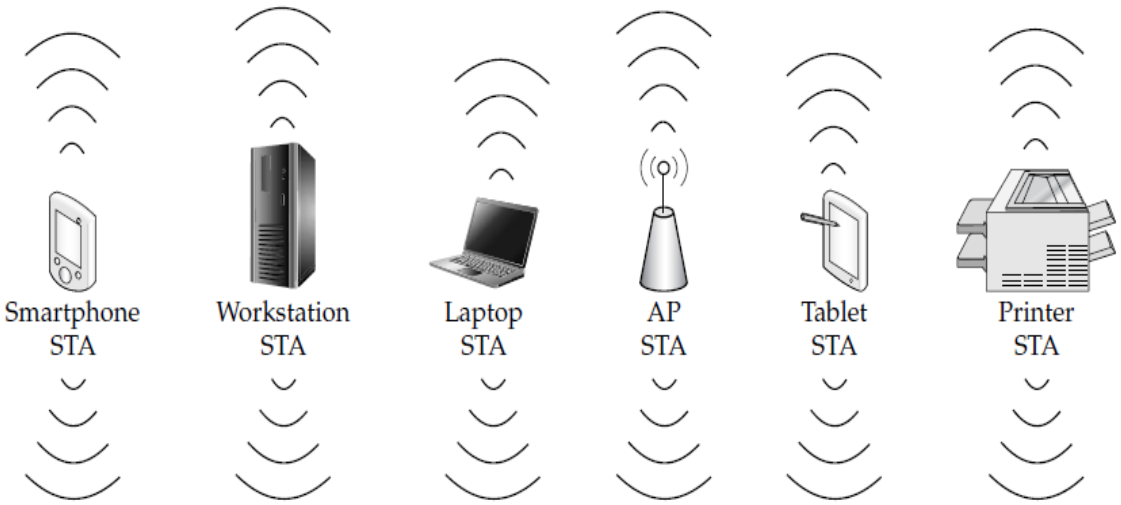


FIGURA 6 Algunos ejemplos de STAs

Fuente: (Soyinka, 2010, pág. 75)

1.4.2. SERVICIOS

Un DS puede ser creado a partir de muchas tecnologías diferentes incluyendo el actual IEEE 802 para LANs cableadas. El estándar 802.11 no limita un DS a ser centralizado o distribuido en la naturaleza.

IEEE 802.11 no especifica los detalles de las implementaciones de DS, en cambio, especifica los servicios. Los servicios se asocian con los diferentes componentes de la arquitectura mediante un controlador inalámbrico. Hay dos categorías de servicio: la estación de servicio (SS[23]) y el servicio del sistema de distribución (DSS[24]). Ambas categorías de servicio son utilizados por la subcapa MAC.

El conjunto completo de Servicios de la arquitectura IEEE 802.11 son los siguientes:

a) Authentication

b) Association

c) Deauthentication

[23] **SS** Station Service
[24] **DSS** Distribution System Service

d) Disassociation

e) Distribution

f) Integration

g) Data confidentiality

h) Reassociation

i) MSDU[25] delivery

j) DFS[26]

k) TPC[27]

l) Higher layer timer synchronization (QoS[28] facility only)

m) QoS traffic scheduling (QoS facility only)

n) Radio measurement

o) DSE[29]

Este conjunto de servicios se divide en dos grupos: SS y DSS. El SS es parte de cada estación y el DSS es proporcionado por el DS.

Hay muchos servicios especificados por IEEE 802.11. Seis de los servicios se utilizan para dar soporte en la entrega de la Unidad de Datos de Servicio MAC (MSDU) entre STAs. Tres de los servicios se utilizan para controlar el acceso WLAN y su confidencialidad. Dos de los servicios se utilizan para proporcionar la gestión del espectro. Uno de los servicios proporciona soporte para aplicaciones LAN con requerimientos de QoS. Otro de los servicios brinda soporte para capas superiores en cuanto a sincronización de tiempo. Uno de los servicios también se utiliza para la medición de radio.

Los servicios se presentan en un orden diseñado para ayudar a construir una comprensión de la funcionalidad de una red ESS. Como resultado tenemos que los servicios que comprenden la SS y DSS se entremezclan en orden en lugar de ser agrupados por categorías.

---

[25] **MSDU** Medium Access Control (MAC) Service Data Unit
[26] **DFS** Dynamic Frequency Selection
[27] **TPC** Transmit Power Control
[28] **QoS** Quality of Service
[29] **DSE** Dynamic Station Enablement

Cada uno de los servicios está soportado por uno o más tipos de trama[30] MAC. Algunos de los servicios son compatibles con mensajes de gestión MAC y algunos mensajes de datos MAC. La subcapa MAC de IEEE 802.11 utiliza tres tipos de mensajes: datos, gestión y control. Los mensajes de datos se manejan a través de la ruta de servicio de datos MAC.

Los mensajes de gestión MAC son utilizados para dar soporte a los servicios y se manejan a través de la ruta de servicio de gestión MAC, mientras que los mensajes de control MAC se utilizan para respaldar la entrega de datos y los mensajes de gestión.

1.4.2.1. SS (STATION SERVICE)

El servicio que es proporcionado por las estaciones se le conoce como SS. El SS está presente en cada estación (incluyendo APs, como los puntos de acceso que incluyen la funcionalidad en cada estación). El SS esta especificado para su uso por entidades de la subcapa MAC. Todas las estaciones conformadas proporcionan SS.

Los servicios de estación son los siguientes:

a) Autenticación
b) Desautenticación
c) Confidencialidad de Datos
d) Entrega de MSDU
e) DFS (Dynamic Frequency Selection)
f) TPC (Transmit Power Control)
g) Capas superiores de sincronización de temporización (Higher layer timer synchronization)
h) Programación de tráfico de QoS (QoS traffic scheduling)
i) Mediciones de Radio (Radio measurement)
j) DSE (Dynamic Station Enablement)

1.4.2.2. DDS (DISTRIBUTION SYSTEM SERVICE)

El servicio que es proporcionado por el DS se le conoce como DSS. Este servicio es parte de la arquitectura IEEE 802.11. Los DSSs están especificados para uso de las entidades de subcapa MAC.

[30] **Trama** La Unidad de Datos de Protocolo (PDU) de la capa enlace de datos del modelo OSI

Los servicios que comprende el DSS son los siguientes:

a) Asociación
b) Disociación
c) Distribución
d) Integración
e) Reasociación
f) Programación de tráfico de QoS (QoS traffic scheduling)
g) DSE (Dynamic Station Enablement)
h) Interfuncionamiento con el DS

La FIGURA 7 combina los componentes de las figuras anteriores con ambos tipos de servicios para mostrar la arquitectura completa de IEEE 802.11.

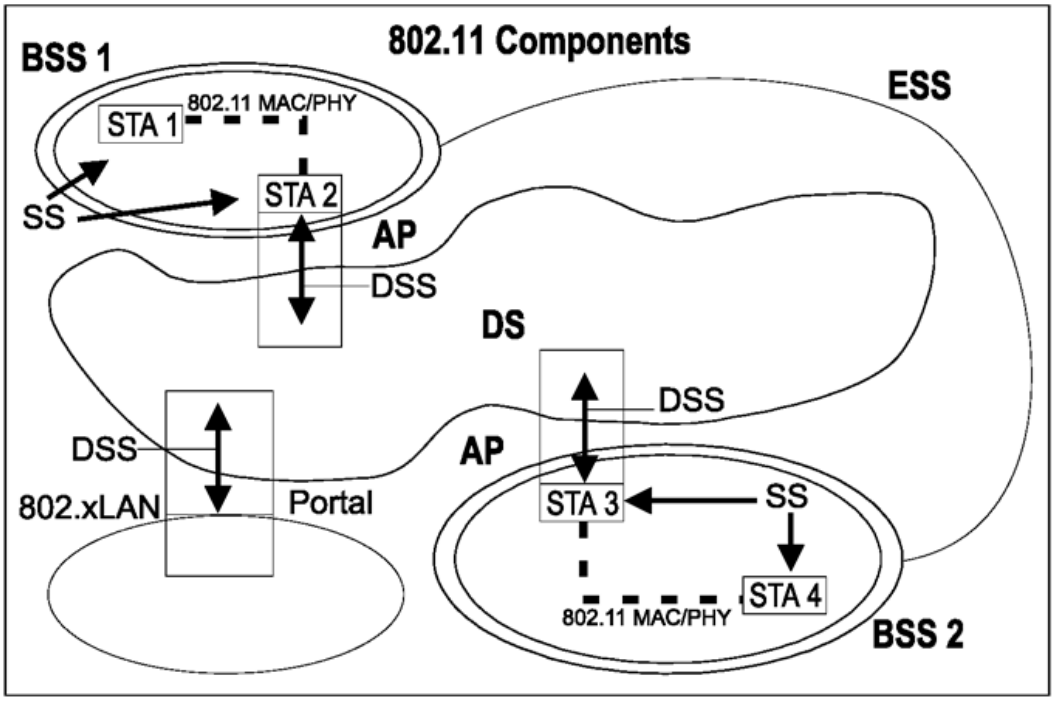


FIGURA 7 Arquitectura Completa de IEEE 802.11

Fuente: (IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007, 2012, pág. 69)

1.4.2.3. MENSAJES DE DISTRIBUCIÓN DENTRO DE UN DS

1.4.2.3.1. DISTRIBUCIÓN (DISTRIBUTION)

Este es el servicio más utilizado por las estaciones inalámbricas. Es conceptualmente solicitado por cada mensaje de datos hacia o desde una estación operando en un ESS (cuando se envía la trama a través del DS). El servicio de distribución es a través del DSS.
Como el mensaje se distribuye dentro del DS, no está especificado por el estándar IEEE 802.11. Todo el estándar es requerido para proporcionar al DS la información suficiente para que este pueda determinar el punto de salida que corresponde al destinatario. La información necesaria es proporcionada al DS por la relación de los tres servicios de asociación (asociación, re-asociación y des-asociación).

1.4.2.3.2. INTEGRACIÓN (INTEGRATION)

Si el servicio de distribución determina que el destinatario de un mensaje es un miembro de una LAN integrada, el punto de salida del DS sería un portal en lugar de un AP.
Los mensajes que se distribuyen a un portal, causa al DS solicitar la función de Integración después del servicio de distribución. La función de integración es responsable de llevar a cabo lo que sea necesario para entregar un mensaje desde el DSM a la LAN Integrada[31] (incluyendo cualquier medio de comunicación requerido o traducciones de espacio de direcciones). La integración es uno de los servicios en el DSS.

1.4.2.3.3. PROGRAMACIÓN DE TRÁFICO DE QOS

La programación de tráfico de QoS proporciona transferencias de trama de calidad de servicio intra-BSS bajo el Hybrid Coordination Function (HCF[32]), utilizando canales de acceso basados en contención o control.

1.4.2.4. SERVICIOS QUE SOPORTA EL DS

El propósito primario de una subcapa MAC es transferir MSDUs entre las entidades de la subcapa MAC. La información requerida por el servicio de distribución para funcionar está proporcionada por los servicios de asociación. Antes de que un mensaje de datos pueda ser manejado por el servicio de distribución, una estación inalámbrica es asociada. Para entender el concepto de asociación, es necesario primero entender el concepto de movilidad.

---

[31] **Integrada** se refiere a una LAN alámbrica físicamente conectada al DS
[32] **HCF** combina y mejora los aspectos de los métodos de acceso contention-based y contention-free

1.4.2.4.1. TIPOS DE MOVILIDAD

Los tres tipos de transición importantes en el estándar IEEE 802.11 que describen la movilidad de las estaciones inalámbricas (STAs) dentro de una red son las siguientes:

a) **Sin Transición:** En este tipo, tenemos dos subclases identificados:
1) Estático: sin movimiento.
2) Movimiento Local: movimiento dentro del rango PHY de las comunicaciones entre STAs, es decir, el movimiento se realiza dentro del área de servicios básicos (BSA).

b) **Transición BSS:** Este tipo se define como el movimiento de una STA desde un BSS a otro BSS dentro del mismo ESS.

c) **Transición ESS:** Este tipo se define como el movimiento de una STA desde un BSS en un ESS a un BSS en un diferente ESS. Este caso sólo se admite en el sentido de que la STA se puede mover.

Los diferentes servicios de asociación soportan las diferentes categorías de movilidad

1.4.2.4.2. ASOCIACIÓN (ASSOCIATION)

El servicio de asociación se encarga de establecer una asociación inicial entre una determinada estación y un AP. Esta información se proporciona al DS por el concepto de asociación. Este servicio no es suficiente para soportar movilidad de transición BSS sino movilidad sin transición.

Antes de que a una estación inalámbrica se le permita transmitir o recibir mensajes de datos a través de un AP, primero debe estar asociada con el AP.

(IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007, 2012) Afirma:

Dentro de una red de seguridad robusta (RSN[33]), el servicio de asociación se maneja de manera diferente. En un RSNA[34], el puerto IEEE 802.1x[35] determina cuándo permitir el tráfico de datos a través de un enlace IEEE 802.11. Un solo puerto IEEE 802.1x se asigna a una asociación, y cada asociación de mapas a un puerto IEEE 802.1x. Un puerto IEEE 802.1x consta de un puerto IEEE 802.1x controlado y un puerto IEEE 802.1x no controlado. El puerto IEEE 802.1x controlado está bloqueado el paso general de tráfico de datos entre dos STAs hasta que un procedimiento de autenticación IEEE 802.1x se realiza satisfactoriamente en el puerto IEEE 802.1X no controlado. (pág. 72)

---

[33] **RSN** Robust Security Network
[34] **RSNA** Robust Security Network Association
[35] **IEEE 802.1x** Port-Based Network Access Control. Estándar diseñado para proveer funciones de control de acceso para redes alámbricas e inalámbricas

1.4.2.4.3. REASOCIACIÓN (REASSOCIATION)

La Asociación es suficiente para entrega de mensajes sin transición entre STAs. La funcionalidad adicional es necesaria para soportar movilidad de transición BSS proporcionado por el servicio de reasociación.

El servicio de reasociación permite transferir una asociación existente desde un AP a otro. Esto mantiene al DS informado de la asignación actual entre el AP y STA a medida que el STA se mueve desde un BSS a otro BSS dentro de un ESS.

1.4.2.4.4. DISOCIACIÓN (DISASSOCIATION)

El servicio de disociación se invoca cuando una asociación existente se ha terminado, es por ello que el servicio de disociación es una notificación más no una solicitud.

1.4.2.5. SERVICIOS DE CONTROL DE ACCESO Y CONFIDENCIALIDAD DE DATOS

Dos servicios son requeridos por el estándar IEEE 802.11 para proporcionar funcionalidades similares en relación a las LANs cableadas, que basan su diseño en asumir los atributos físicos del cable. En una WLAN que no soporta RSNA se definen dos servicios, autenticación y confidencialidad de datos. La autenticación IEEE 802.11 se utiliza en lugar de una conexión física de medios cableados; mientras que la confidencialidad de datos y la integridad de los datos son proporcionadas por la gestión de claves RSN junto con los mecanismos de encapsulación de cifrado de datos mejorados.

1.4.2.5.1. AUTENTICACIÓN (AUTHENTICATION)

La autenticación opera en el nivel de enlace entre estaciones inalámbricas. El estándar IEEE 802.11 no proporciona cualquier tipo de autenticación end to end (origen del mensaje al destino del mensaje) o usuario a usuario.

La Autenticación es un SS. Este servicio puede ser utilizado por todas las STAs para establecer su identidad a las STAs con las que se comunican, tanto en redes IBSS como ESS. Si un nivel de autenticación no ha sido establecido entre dos STA, la asociación de uno de ellos no se ha establecido.

1.4.2.5.2. DESAUTENTICACIÓN (DEAUTHENTICATION)

El servicio de desautenticación se utiliza cuando existe un Sistema Abierto, clave compartida, o la autenticación se ha terminado, donde la STA quiere desasociarse. La Desautenticación es un SS.

En un ESS, debido a que la autenticación es un prerrequisito para la asociación, el acto de desautenticación causa la desasociación de una STA. La Desautenticación no es una respuesta, tan solo es una notificación. La asociación en la transmisión STA es terminada cuando la STA envía un aviso de desautenticación a un STA asociado.

1.4.2.5.3. CONFIDENCIALIDAD DE DATOS (DATA CONFIDENTIALITY)

En una LAN cableada, sólo las estaciones físicamente conectadas al cable pueden enviar o recibir tráfico de la LAN. Con un medio inalámbrico compartido, no hay ninguna conexión física, y todas las STAs y otros dispositivos de Radio Frecuencia (RF) que se encuentran cerca de la LAN pueden ser capaz de enviar, recibir e interferir con el tráfico LAN. De esta manera, la conexión de un solo enlace inalámbrico (sin confidencialidad de los datos) a una LAN cableada existente puede degradar seriamente el nivel de seguridad de la LAN cableada.

Para llevar la seguridad de la WLAN hasta el nivel comprendido en el diseño LAN cableado, el estándar IEEE 802.11 proporciona la capacidad para proteger el contenido de los mensajes. Esta funcionalidad es proporcionada por el servicio de confidencialidad de datos, el mismo que pertenece a un SS.

(IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007, 2012) Proporciona: “Varios algoritmos criptográficos para proteger el tráfico de datos, incluyendo: WEP[36] (Wired Equivalent Privacy), TKIP[37] (Temporal Key Integrity Protocol) y CCMP[38] (Counter mode with Cipher-block chaining Message authentication code Protocol). WEP y TKIP se basa en el algoritmo ARC419[39], y CCMP se basa en el Estándar de Encriptación Avanzado (AES[40])” (p.75). Un medio es proporcionado por STAs para seleccionar el algoritmo o algoritmos que se utilizará para una determinada asociación.

1.4.2.6. SERVICIOS DE GESTIÓN DEL ESPECTRO

Dos servicios son necesarios para satisfacer los requerimientos de algunos dominios de regulación para el funcionamiento en la banda de 5 GHz. Estos servicios se denominan control de potencia de transmisión (TPC) y selección de frecuencias dinámicas (DFS).

---

[36] **WEB** Algoritmo criptográfico obsoleto para confidencialidad de los datos especificados por el estándar
[37] **TKIP** Protocolo de seguridad usado en WPA (Wi-Fi Protected Access) para mejorar el cifrado de datos en redes inalámbricas
[38] **CCMP** Protocolo de encriptación diseñado para productos Wireless LAN que implementan el estándar de IEEE 802.11i
[39] **ARC419** 19 detalles del algoritmo ARC4 están disponibles a partir de la Seguridad RSA
[40] **AES** Es una técnica de cifrado de clave simétrica que remplazará el Estándar de Encriptación de Datos (DES) utilizado habitualmente.

1.4.2.6.1. TPC (CONTROL DE POTENCIA DE TRANSMISIÓN)

El servicio de TPC establece lo siguiente:

- La Asociación de STAs con un AP en un BSS se basa en la capacidad de potencia de las estaciones inalámbricas.
- La especificación de regulación y niveles de potencia de transmisión máxima local para el canal actual.
- La selección de una potencia de transmisión para cada transmisión en un canal dentro de las limitaciones impuestas por los requerimientos regulatorios.
- La adaptación de potencia de transmisión basada en una amplia gama de información, incluyendo la pérdida de trayectoria (path loss) y las estimaciones de margen del enlace.

1.4.2.6.2. DFS (SELECCIÓN DE FRECUENCIAS DINÁMICAS)

El servicio de DFS establece lo siguiente:

- La Asociación de STAs con un AP en un BSS se basa en los canales soportados por las estaciones inalámbricas.
- Canales de prueba para radar antes de utilizar un canal y cuando se transmite en un canal.
- La interrupción de las operaciones después de la detección del radar en el canal actual para evitar la interferencia con el radar.
- La detección del radar en los canales actuales se basa en los requerimientos regulatorios.
- La solicitud y notificación de mediciones en los canales actuales.
- La selección y publicación de un nuevo canal para ayudar a la migración de un BSS después de haber sido detectado el radar.

1.4.2.7. SERVICIO DE MEDICIÓN DE RADIO

El servicio proporciona las siguientes características:

- La capacidad de solicitar y reportar mediciones de radio en canales admitidos.
- La capacidad de realizar mediciones de radio en canales soportados.

- Una interfaz para aplicaciones de capa superior para obtener mediciones de radio utilizando primitivas MLME[41] y/o el acceso MIB[42].
- Información sobre los APs vecinos.

1.4.3. CAPA FÍSICA (PHY)

La capa física es la primera capa en el modelo de referencia OSI[43] (Open Systems Interconnection) en la cual se define la relación entre un dispositivo y el medio de comunicación físico. Se divide en dos subcapas:

- Subcapa de Procedimiento de Convergencia de Capa Física (PLCP, Physical Layer Convergence Procedure)
- Subcapa Dependiente del Medio Físico (PMD, Physical Medium Dependent)

La capa física de IEEE 802.11 se ha emitido en cuatro etapas. La primera parte, llamada simplemente IEEE 802.11 incluye la capa MAC y tres especificaciones de capa física, dos de ellas en la banda de 2.4 GHz (ISM) y uno en infrarrojo, todos se encuentran funcionando a 1 y 2 Mbps como se muestra en la FIGURA 8.

[41] **MLME** MAC Sublayer Management Entity
[42] **MIB** Management Information Base
[43] **OSI** Interconexión de Sistemas Abiertos

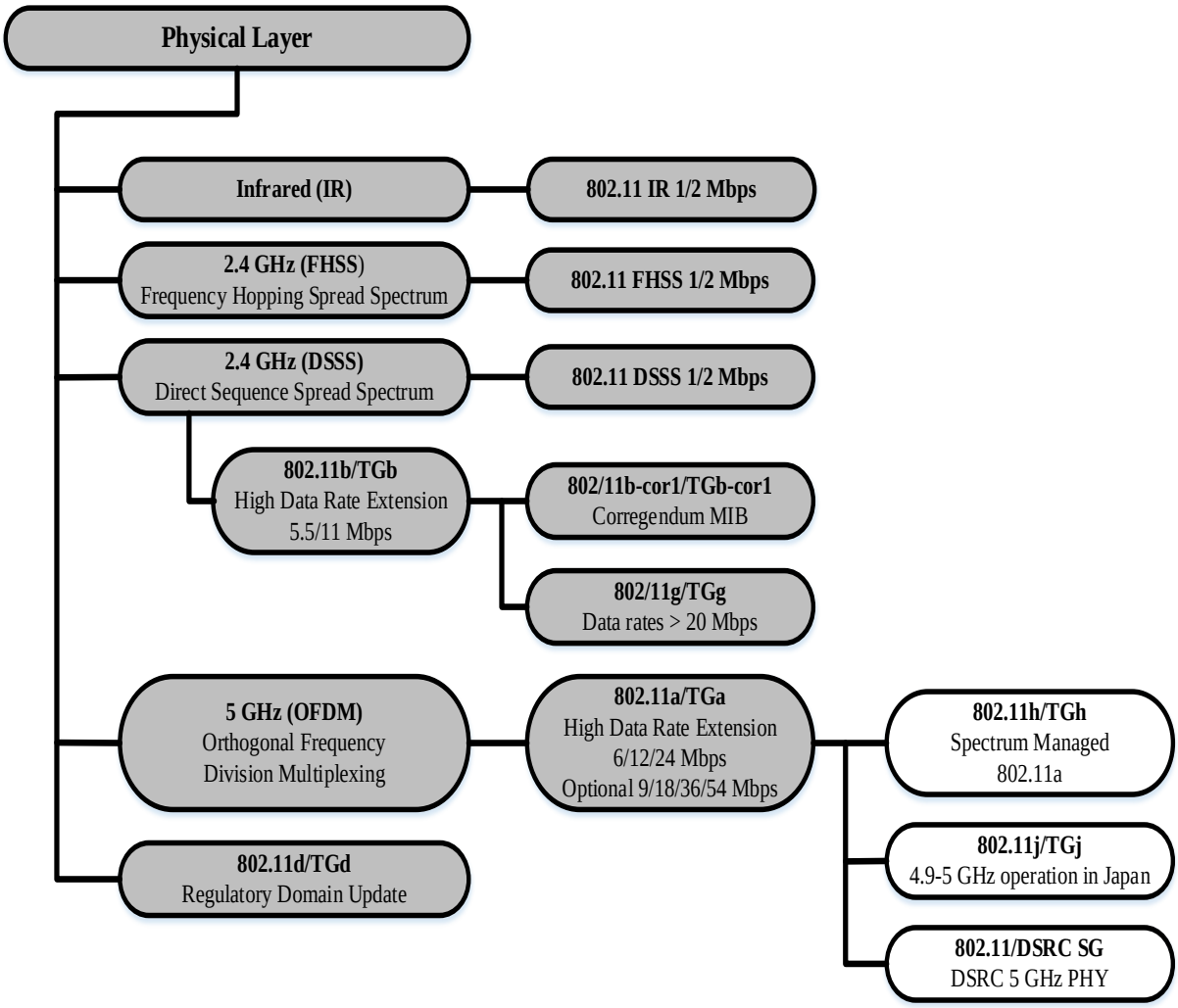


FIGURA 8 IEEE 802.11 Actividades de Capa Física

Fuente: (Stallings, 2005, pág. 443)

El estándar IEEE 802.11a opera en la banda de 5 GHz a velocidades de datos de hasta 54 Mbps y el estándar IEEE 802.11b opera en la banda de 2,4 GHz a 1, 2, 5.5, 11 Mbps. IEEE 802.11g también opera en la banda de 2.4 GHz, con velocidades de datos de hasta 54 Mbps. En la FIGURA 8 podemos notar la relación entre los diversos estándares desarrollados para la capa física, y en la FIGURA 9 resaltamos el modelo de referencia 802.11.

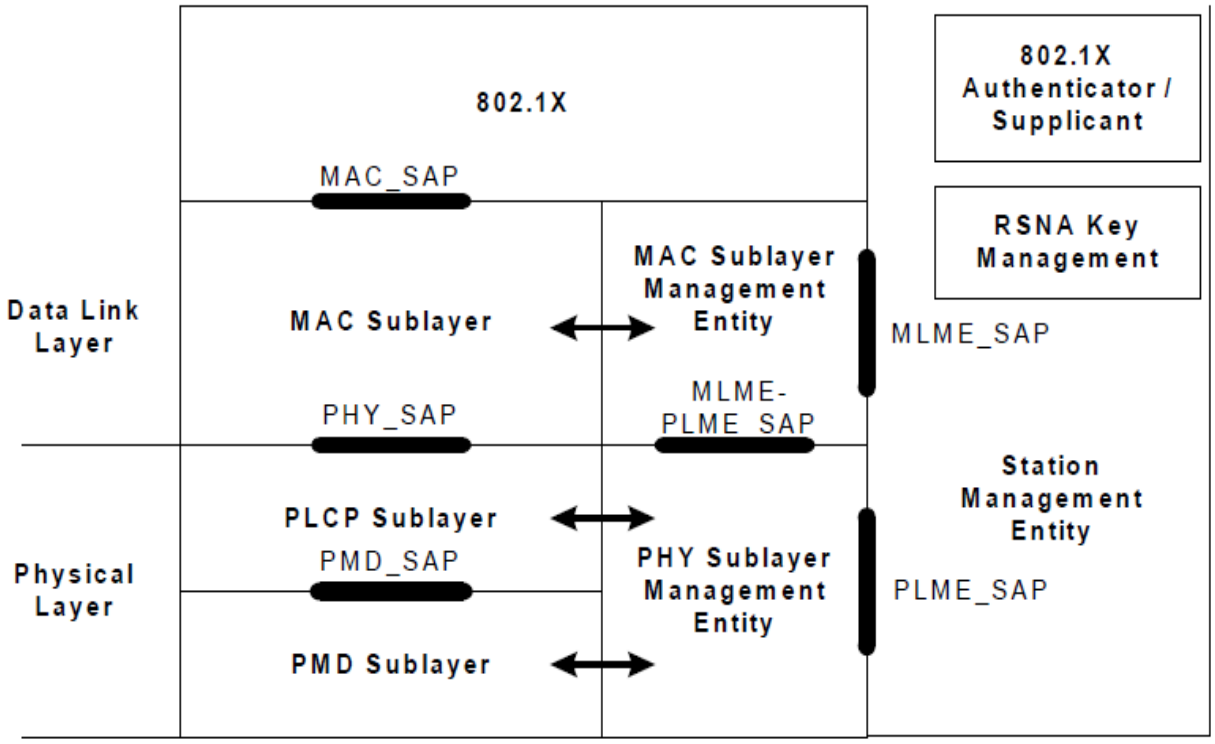


FIGURA 9 Modelo de Referencia 802.11

Fuente: (IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007, 2012, pág. 82)

1.4.3.1. PLCP (SUBCAPA DE PROCEDIMIENTO DE CONVERGENCIA DE CAPA FÍSICA)

La función de la subcapa PLCP es la de proporcionar un mecanismo para la transferencia de MPDUs[44] dentro de un formato de trama adecuado para enviar y recibir datos de usuario e información de gestión entre dos o más estaciones inalámbricas sobre la subcapa PMD adaptando sus capacidades al servicio de la capa física (PHY).

1.4.3.2. PMD (SUBCAPA DEPENDIENTE DEL MEDIO FÍSICO)

La subcapa PMD es responsable de implementar el esquema de codificación de transmisión, sistema el cual tiene como función definir ciertas características y los métodos de transmisión y recepción de datos a través de un WM entre dos o más STAs. Cada subcapa PMD puede requerir la definición de un PLCP único donde la subcapa PMD proporciona servicios PHY definidos como soporte de múltiples esquemas de modulación. La función de PHY puede ser nula.

[44] **MPDU** Medium Access Control (MAC) Protocol Data Unit

Varios organismos reguladores de algunos países se dedican a controlar y administrar como se implementa la capa PHY de los dispositivos inalámbricos. Por lo tanto, los administradores de redes inalámbricas deben asegurarse que sus dispositivos se configuren apropiadamente y se utilicen para que no violen las leyes que regulan la transmisión y recepción de señales de RF. Por la misma razón los fabricantes de dispositivos inalámbricos deben asegurarse que estén bien diseñados y debidamente etiquetados para su uso dentro de una región.

La capa PHY especifica las técnicas de señalización inalámbricas utilizadas para transmitir y recibir información a través de ondas de radio tal y como se muestra en la siguiente TABLA 2.

TABLA 2 Técnicas de Señalización (Modulación)

TÉCNICA DE SEÑALIZACIÓN	DESCRIPCIÓN
FHSS[45] (Frequency-Hopping Spread Spectrum)	Está técnica de modulación especifica su uso en 2.4 GHz en la banda de frecuencia ISM (Industrial, Scientific, and Medical). El rango de frecuencia específica es 2.402-2.480 GHz. Es una de las técnicas de modulación utilizadas en las primeras implementaciones WLAN siendo hoy en día muy poco manejadas. Es compatible con velocidades de datos de 1 a 2 Mbps. Trabaja haciendo las señales de salto a través de los canales de frecuencia permitidos en una secuencia predeterminada. Por ejemplo una secuencia predeterminada puede ser tan simple como decir que cada 5 segundos el sistema va a saltar a un nuevo canal dentro del rango de frecuencia ISM. El sistema FHSS usa dos modulaciones: ◈ FSK Gaussiana (GFSK) de dos niveles para 1 Mbps. ◈ FSK Gaussiana (GFSK) de cuatro niveles para 2 Mbps.
DSSS[46] (Direct-Sequence Spread Spectrum)	Está técnica de modulación especifica su uso en 2.4 GHz en la banda de frecuencia ISM. El rango de frecuencia específica es 2.400-2.497 GHz. Puede soportar velocidades de datos de 1 a 2 Mbps.

[45] **FHSS** Espectro Ensanchado por Salto de Frecuencia
[46] **DSSS** Espectro Ensanchado por Secuencia Directa

	Se han definido 14 canales cada uno de 5 MHz. El número de canales disponibles depende del ancho de banda ubicado por las agencias nacionales de regulación. El sistema DSSS usa dos modulaciones: ◈ DBPSK[47] (Differential Binary Phase Shift Keying) para 1Mbps. ◈ DQPSK[48] (Differential Quadrature Shift Keying) para 2 Mbps.
IR[49] (Infrared)	Longitudes de onda entre 850 nm y 950 nm Soporta velocidades de 1 y 2 Mbps. Omnidireccional. Utiliza técnicas de modulación 16-PPM[50] y 4-PPM para velocidades de transmisión de 1 y 2 Mbps respectivamente. La transmisión final utiliza un esquema de intensidad: ◈ La presencia de señal corresponde a un 1. ◈ La ausencia de señal corresponde a un 0.
HR/DSSS[51] (High Rate Direct Sequence Spread Spectrum)	Una extensión o mejora del DSSS. Funciona a 2.4 GHz en las bandas de frecuencia ISM. La implementación de sistemas puede proporcionar velocidades de datos de 1, 2, 5.5 y 11 Mbps.
OFDM[52] (Orthogonal Frequency Division Multiplexing)	Especifica el uso de 5 MHz en la bandas de frecuencia UNII[53] (Unlicensed National Information Infrastructure) y 2.4 GHz en las bandas ISM. La mayoría de los estándares recientes IEEE 802.11 implementan PHY y sus variantes.

[47] **DBPSK** Modulación por Desplazamiento Diferencial de Fase Binario
[48] **DQPSK** Modulación por Desplazamiento Diferencial de Fase por Cuadratura
[49] **IR** Infrarrojo
[50] **PPM** Pulse Position Modulation
[51] **HR/DSSS** Espectro Ensanchado por Secuencia Directa de Alta Velocidad
[52] **OFDM** Multiplexación por División de Frecuencias Ortogonales
[53] **UNII** Infraestructura de Información Nacional sin Licencia

	Soporta velocidades de datos más altas de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.
ERP[54] (Extended Rate PHY)	Proporciona extensiones a las especificaciones existentes de capa física como DSSS y OFDM. Las extensiones tienen la intención de mejorar la compatibilidad y coexistencia con la PHY existente. Trabaja en la banda de frecuencia de 2.4 GHz. Algunas variaciones populares de ERP son: **ERP-DSSS:** Proporciona soporte para sistemas que necesitan implementar ERP pero también deben ser compatibles con versiones anteriores de DSSS PHY. **ERP-OFDM:** Se implementa para el funcionamiento en la banda de 2.4 GHz. La implementación de sistemas de PHY puede soportar velocidades de datos de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. **DSSS-OFDM:** Proporciona un modo mixto para para la operación de los sistemas DSSS y OFDM. Los sistemas DSSS antiguos pueden interpretar partes de la comunicación (como la cabecera) y los sistemas más recientes basados en OFDM pueden interpretar la cabecera y el payload de datos reales.

Fuente: (Soyinka, 2010, pág. 81)

1.4.4. SUBCAPA MAC

Para mantener las comunicaciones de datos y comunicaciones humanas, ciertas reglas y directrices deben ser establecidas y cumplidas. Esto es especialmente importante en las comunicaciones inalámbricas debido a la naturaleza de los medios utilizados por aire o el espacio. Las normas y directrices se especifican en las diferentes capas del modelo OSI.

MAC es la subcapa de la capa de Enlace de Datos del modelo OSI, o conocida como capa 2. La subcapa MAC es responsable de proporcionar mecanismos de direccionamiento y control de acceso al medio que hace posible que varios nodos se comuniquen en la red.

[54] **ERP** Capa Física (PHY) de Velocidad Extendida

"*Las funciones MAC se utilizan para controlar y gestionar el acceso al medio de transmisión en un sistema de comunicaciones*" (Soyinka, 2010, pág. 82).

Para coordinar el acceso al medio LAN, una colisión ocurre si dos o más dispositivos intentan enviar un mensaje al mismo tiempo, de esta manera las estaciones LAN utilizan Acceso Múltiple por Detección de Portadora con Detección de Colisiones (CSMA/CD[55]).

En lugar de tratar de detectar cuando el medio está disponible para su uso, los sistemas basados en 802.11 toman un rumbo diferente tratando de evitar cualquier tipo de colisión al no poder transmitir y escuchar al mismo tiempo como en una red cableada. Este es el Acceso Múltiple por Detección de Portadora con Prevención de Colisiones (CSMA/CA[56]).

1.4.4.1. ARQUITECTURA MAC

En las especificaciones del estándar IEEE 802.11 la arquitectura de la subcapa MAC incluye ciertas funciones:

- La Función de Coordinación Distribuida (DCF[57])
- La Función de Coordinación Puntual (PCF[58])
- La Función de Coordinación Híbrida (HCF[59])
- La Función de Coordinación Mesh (MCF[60])

Una representación de la arquitectura MAC se muestra en la FIGURA 10 en la cual los servicios PCF y HCF se proporcionan utilizando los servicios del DCF. Se debe tener en cuenta que en una estación inalámbrica (STA) sin QoS, HCF no está presente; mientras, en una implementación de QoS en un STA, tanto DCF y HCF están presentes. PCF es opcional en todas las STAs.

[55] **CSMA/CD** Carrier Sense Multiple Access with Collision Detection
[56] **CSMA/CA** Carrier Sense Multiple Access with Collision Avoidance
[57] **DCF** Distributed Coordination Function
[58] **PCF** Point Coordination Function
[59] **HCF** Hybrid Coordination Function
[60] **MCF** Mesh Coordination Function

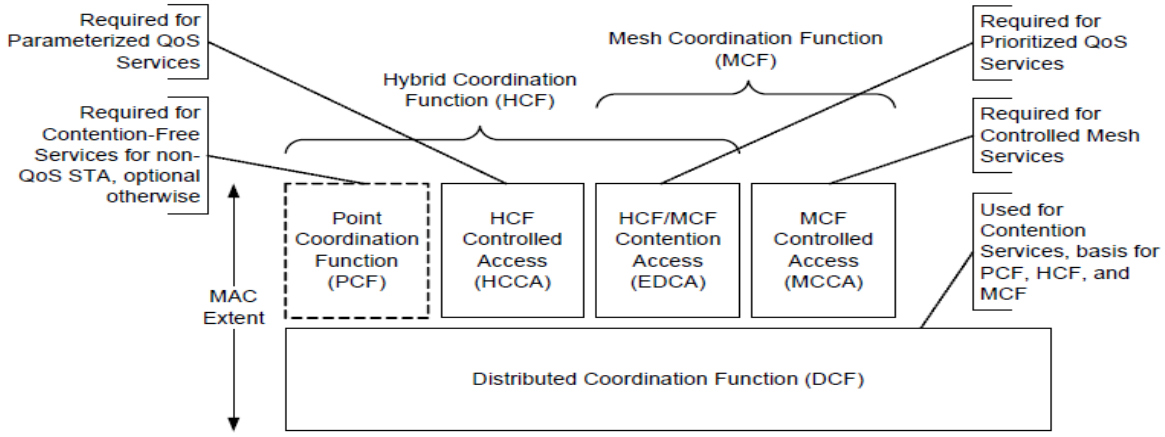


FIGURA 10 Arquitectura MAC

Fuente: (IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007, 2012, pág. 818)

1.4.4.1.1. FUNCIÓN DE COORDINACIÓN DISTRIBUIDA

La Función de Coordinación Distribuida es un protocolo básico de acceso al medio el cual permite compartir automáticamente el medio entre PHYs compatibles a través de la utilización de CSMA/CA y un tiempo de backoff[61] de envío aleatorio en un medio ocupado. Adicionalmente, todos los paquetes enviados a recepción se confirman mediante una trama de Acknowledgment (ACK[62]), donde se prevé una retransmisión si no se recibe el ACK.

1.4.4.1.2. FUNCIÓN DE COORDINACIÓN PUNTUAL

Una clase de posibles funciones de coordinación, en la cual la función de coordinación lógica está activa en solo una estación (STA) en un conjunto de servicios básicos (BSS) en un momento dado en que la red esté en funcionamiento.

1.4.4.1.3. FUNCIÓN DE COORDINACIÓN HÍBRIDA

Una de las funciones de coordinación que combina y refuerza los aspectos de los métodos de acceso como son Contention-based[63] y Contention-free[64] para proporcionar calidad de servicio (QoS) a las estaciones cumpliendo ciertos parámetros en el medio inalámbrico (WM).

[61] Algoritmo de Backoff (Algoritmo de Retroceso Exponencial Binario)
[62] **ACK** Acuse de Recibo
[63]**Contention-based** Es un protocolo de comunicaciones para el funcionamiento de equipos de telecomunicaciones inalámbricos que permiten a muchos usuarios utilizar el mismo canal de radio.
[64] **Contention-free** Usa un acceso centralizado como método de control

1.4.4.1.4. FUNCIÓN DE COORDINACIÓN MESH

Una función de coordinación que combina aspectos de los métodos de acceso de contention-based y programación. El MCF incluye la funcionalidad proporcionada por el Acceso al Canal de Distribución Mejorado (EDCA[65]) y Acceso al Canal Controlado de la Función de Coordinación Mesh (MCCA[66]).

1.4.4.2. FORMATO DE LA TRAMA MAC

Dependiendo de su función, los tipos de tramas MAC que define el estándar IEEE 802.11 se pueden agrupar en tres categorías: tramas de control, tramas de gestión y tramas de datos.

1.4.4.2.1. TRAMAS DE CONTROL

Son muy importantes para todas las comunicaciones WLAN y se utilizan para soportar la entrega de los otros tipos de tramas MAC. Todas las estaciones inalámbricas deben ser capaces de analizar las tramas de control, en otras palabras la información no debe ser secreta o peor aún clasificada. Las tramas de control son utilizadas por ejemplo, cuando una estación inalámbrica necesita realizar una negociación y obtener acceso a una WLAN usando CSMA/CA. Otros tipos de tramas de control son el Request to Send (RTS), Clear to Send (CTS), y Acknowledgment (ACK).

- **RTS:** Proporciona algunos mecanismos de prevención de colisiones para WLANs, de cierta manera es una forma de comprobar que el medio de comunicación se encuentra en uso por otras estaciones inalámbricas.
- **CTS:** Enviado por las estaciones inalámbricas en respuesta a la trama RTS.
- **ACK:** Enviado por la estación inalámbrica receptora para confirmar que la trama ha llegado exitosamente.

1.4.4.2.2. Tramas de Gestión

Este tipo de trama se utiliza con propósitos de gestión en una WLAN donde cumplen con un papel muy importante. Las tramas de gestión son utilizadas por estaciones inalámbricas siempre y cuando un STA quiera oficialmente participar o suspender su participación en la red. A continuación algunos tipos de tramas de gestión:

[65] **EDCA** El tráfico de alta prioridad tiene más probabilidad de ser enviado antes que el tráfico de baja prioridad
[66] **MCCA** Una función de coordinación para el conjunto de servicios básicos mesh (MBSS)

- **Trama Beacon:** Lleva a cabo diversas funciones, tal como la sincronización de tiempo entre estaciones inalámbricas, almacena el valor del SSID, especifica la PHY que está utilizando y los tipos de datos soportados en la WLAN.
- **Trama de Solicitud de Asociación:** Estas tramas son enviadas por la estación inalámbrica para solicitar asociación con el AP.
- **Trama de Respuesta de Asociación:** Estas tramas contienen las respuestas de los APs a los STAs respecto a la solicitud de asociación.
- **Trama de Solicitud de Reasociación:** Estas tramas son utilizadas por estaciones inalámbricas siempre que necesitan ser reasociados con el AP.
- **Trama de Respuesta de Reasociación:** Estas tramas son enviadas por el AP en respuesta a la solicitud de STAs de reasociarse con el AP.
- **Trama de Autenticación:** Estas tramas se utilizan cada vez que un STA necesita participar o integrarse a un BSS. La estación inalámbrica emplea tramas de autenticación para confirmar su identidad.
- **Trama de Desautenticación:** Las estaciones inalámbricas autenticadas utilizan estos tipos de tramas para señalar su intención de terminar las comunicaciones autenticadas.
- **Trama de Disociación:** Esta trama se envía por un STA que está asociado con un AP para informar al AP que se quiere interrumpir la asociación.
- **Trama de Solicitud de Sondeo:** Los STAs envían tramas de solicitud de sondeo siempre que lo necesiten para descubrir información de otras estaciones inalámbricas.
- **Trama de Respuesta de Sondeo:** Esta trama transporta las respuestas de solicitudes de sondeo.

1.4.4.2.3. Tramas de Datos

Estos tipos de tramas son responsables de transportar el payload[67] real de los datos hacia y desde los puntos finales de comunicación.

1.4.4.3. Trama MAC Completa

En la siguiente

FIGURA **11** se muestra el formato de la trama MAC. La TABLA 3 explica algunas partes de la trama MAC que pueden ser interesantes desde el punto de vista de un administrador de red inalámbrica.

[67] **Payload** Carga útil, contiene los datos que se desean trasladar.

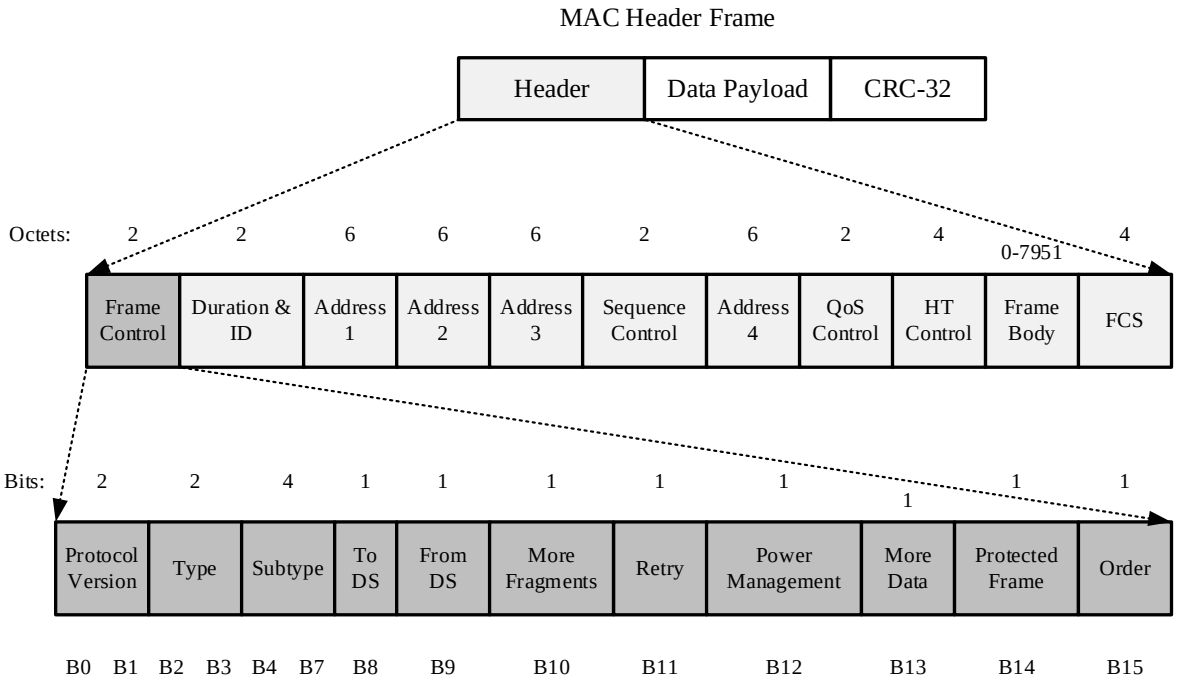


FIGURA 11 Trama MAC Completa

Fuente: (Soyinka, 2010, pág. 85)

TABLA 3 Campos de la Trama MAC IEEE 802.11

CAMPO	DESCRIPCIÓN
Frame Control	Muestra la información que se almacena en el campo de la trama de control que relaciona la versión del protocolo que está en uso: tipo de trama (control, gestión o datos), etc.
Duration / ID	Utilizado por los dispositivos WLAN para reservar o especificar el período de tiempo durante el cual el medio de RF[68] estará en uso.
Address 1	Dirección Origen (SA[69]): una dirección MAC de 48 bits. Actúa con el mismo propósito que la SA de capa 2 utilizada en redes Ethernet; es

[68] **RF** Radiofrecuencia
[69] **SA** Source Address

	decir, se trata de la dirección de la STA que ha creado la trama original que será transmitida.
Address 2	Dirección Destino (DA[70]): una dirección MAC de 48 bits. Actúa con el mismo propósito que la DA de capa 2 utilizada en redes Ethernet; es decir, se trata de la dirección del destinatario final de la trama IEEE 802.11
Address 3	Dirección del Receptor (RA[71]): puede ser la dirección del siguiente salto del dispositivo de radio en la WLAN que reenviará el paquete a su destino final.
Sequence Control	Contiene el fragmento y números de secuencia de cada trama.
Address 4	Dirección del Transmisor (TA[72]): puede ser una intermedia STA que transmite la trama.
QoS Control	El campo de control de calidad de servicio es un campo de 16 bits que identifica el TC[73] o TS[74] al que pertenece la trama, así como varios otros relacionados con QoS.
HT Control	El campo de HT[75] Control tiene un tamaño de 4 octetos, se encuentra presente en la tramas Control Wrapper, Datos de QoS y gestión determinados por el orden de los bits del campo de la trama de control.
Frame Body	El cuerpo de la trama es un campo de longitud variable que contiene información específica de los tipos y subtipos de tramas. La longitud mínima es de 0 octetos, la longitud máxima es ahora de 7955 octetos y se define por el tamaño máximo de MSDU (2304 octetos) más la

[70] **DA** Destination Address
[71] **RA** Receiver Address (Rx STA)
[72] **TA** Transmitter Address (Tx STA)
[73] **TC** Traffic Category
[74] **TS** Traffic Stream
[75] **HT** High-Throughput

	longitud del campo de Control Mesh (6, 12, 18 octetos) si está presente, el tamaño máximo MMPDU[76] sin cifrar excluye la cabecera MAC y FCS (2304 octetos) o el tamaño máximo A-MSDU[77] (3839 o 7935 octetos dependiendo de la capacidad de las estaciones inalámbricas) más cualquier sobrecarga de encapsulación de seguridad.
Frame Check Sequence (FCS)	Secuencia de chequeo de trama: se utiliza para comprobar o verificar que la trama no ha sido interrumpida durante la transmisión, mediante el chequeo de redundancia cíclica (CRC).
Protocol Version	El campo es de 2 bits de longitud. Para este estándar, el valor de la versión del protocolo es 0. Todos los demás valores posibles de este campo son reservados para cambios grandes en el actual estándar. El nivel de revisión se incrementa cuando existe una incompatibilidad fundamental entre una nueva revisión y una edición anterior del estándar.
Type and Subtype	Los campos juntos identifican la función de la trama. Hay tres tipos de tramas: control, datos y gestión. Cada uno de los tipos de tramas tiene varios subtipos definidos.
To DS and From DS	Hacia DS y Desde DS. El significado de estos campos varían de acuerdo a las posibles combinaciones entre 1 y 0: ***To DS = 0 y From DS = 0*** Implica que la trama ha sido enviada desde un STA a otro STA dentro de la misma red IBSS tal como una red ad-hoc. ***To DS = 1 y From DS = 0*** Implica que la trama está destinada al DS o que una trama será enviada por una STA asociada a un AP.

[76] **MMPDU** Medium Access Control (MAC) Management Protocol Data Unit
[77] **A-MSDU** Aggregate Medium Access Control (MAC) Service Data Unit

	To DS = 0 y From DS = 1 Implica que la trama viene desde un DS. ***To DS = 1 y From DS = 1*** La trama utiliza el formato de cuatro direcciones pero actualmente no se encuentra definido por el estándar IEEE 802.11 a pesar de ser una combinación posible.
More Fragments	Este campo indica que todavía existen fragmentos por transmitir.
Retry	El campo establecido permite evitar el procesamiento de tramas duplicadas. Un valor de 1 en una trama de datos o gestión significa que la trama es una retransmisión de una trama anterior.
Power Management	Indica el modo de gestión de energía de una STA. Un valor de 1 significa que la STA estará en modo de ahorro de energía y un valor en 0 estará en modo activo. Para tramas transmitidas por los APs este campo será siempre 0.
More Data	El AP usa este bit, en modo de gestión de energía, para especificarle a una STA que existen tramas adicionales almacenadas temporalmente en estado de espera.
Protected Frame	Indica cuando el campo del cuerpo de la trama contiene información que ha sido procesada por un algoritmo criptográfico. Un valor de 1 significa que el cuerpo de la trama está cifrado. Un valor de 1 solo es posible dentro de unos tipos de tramas de datos y algunos tipos de tramas de gestión. El valor de 0 se utiliza para los demás tipos de tramas.
Order	Indica que la trama se ha enviado a través de una clase de servicio de orden estricto (Strictly-Ordered Service Class).

Fuente: (Soyinka, 2010, pág. 86)

1.4.5. Estándares LAN Inalámbricos

Todos los estándares WLAN están incluidos en las series IEEE 802.11. Definen el funcionamiento de capa 1 y 2, que incluye las frecuencias, los canales inalámbricos, el rendimiento, la seguridad, la movilidad, etc.

1.4.5.1. Estándar IEEE 802.11a

El estándar 802.11a permite que la velocidad de transmisión sea escalable desde 6, 9, 12, 18, 24, 36, 48 y 54 Mbps, sin embargo típicamente el rendimiento máximo suele ser de 28 Mbps. Transmite en un rango de frecuencia de 5 GHz y utiliza 8 canales no superpuestos. Utiliza la misma modulación OFDM que IEEE 802.11g. Para complementar OFDM soporta una variedad de esquemas de modulación y codificación como se puede ver en la TABLA 4 junto a varias características del estándar.

Es por esto que los dispositivos 802.11a son incompatibles con los dispositivos 802.11b. De esta manera existen dispositivos que incorporan ambos chips los cuales tienen el nombre de banda dual.

TABLA 4 OFDM 802.11ª

Velocidad de Transmisión (Mbps)	Modulación	Índice de Codificación	Bits Codificados por Sub-portadora	Bits Codificados por Símbolo OFDM	Bits de Datos por Símbolo
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

Fuente: (Stallings, 2005, pág. 445)

1.4.5.2. Estándar IEEE 802.11b

El estándar 802.11b permite velocidades de transmisión de 1, 2, 5.5 y 11 Mbps en un rango de 100 metros aproximadamente en ambientes cerrados, más de 200 metros al aire libre e inclusive mayores distancias con el uso de antenas. El estándar específica el uso de la modulación DSSS en la banda de 2.4 GHz.

El Chipping Rate es 11 MHz igual que la versión original, donde para obtener una mayor velocidad de transmisión en el mismo ancho de banda y con la misma velocidad de chipping se utiliza un esquema de modulación CCK[78] que fue adoptado para complementar el código Barker en las redes digitales inalámbricas para lograr velocidades de datos mayor a 2 Mbps como se tiene en la TABLA 5. El estándar también plantea una alternativa a CCK (opcional y no implementado frecuentemente) como lo es PBCC[79] que alcanza una trasmisión más eficiente a cambio de mayor procesamiento en el receptor.

TABLA 5 DSSS (802.11 y 802.11b)

Data Rate	Chipping code length	Modulation	Symbol rate	Bits / symbol
1 Mbps	11 (Barker sequence)	DBPSK	1 Msps	1
2 Mbps	11 (Barker sequence)	DQPSK	1 Msps	2
5.5 Mbps	8 (CCK)	DQPSK	1.375 Msps	4
11 Mbps	8 (CCK)	DQPSK	1.375 Msps	8

Fuente: (Stallings, 2005, pág. 445)

[78] **CCK** Complementary Code Keying
[79] **PBCC** Packet Binary Convolutional Coding

Un AP y un cliente pueden negociar la tasa de transferencia de datos que se intercambiarán una vez realizada la asociación. Consiste en 14 canales de 22 MHz de amplitud como nos muestra la FIGURA 12 y una separación de 5 MHz entre sí, que podemos analizar en la

TABLA 6 junto con sus dominios regulatorios. “Es por ello que se recomienda optar por los canales disjuntos 1, 6 y 11, que no representan solapamientos, produciéndose interferencias mínimas” (Herrera Ramírez, Días Ramírez, & Calafate, 2008, pág. 2).

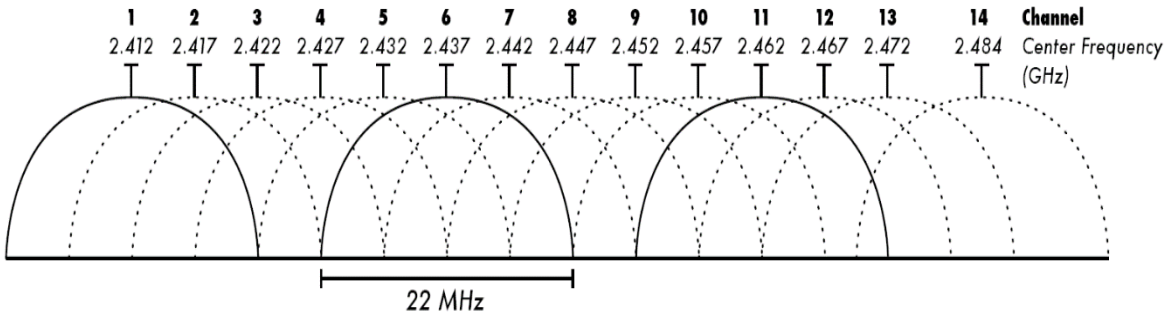


FIGURA 12 Canales 802.11 b/g en la banda de 2.4 GHz
Fuente: http://blog.alvarezp.org/2009/07/10/el-mito-de-los-11-canales-de-80211bg/

TABLA 6 Canales de Frecuencia de 802.11b

DOMINIOS REGULATORIOS							
Identificador de Canal	**Frecuencia**	**Norte América**		**Europa**			**Japón**
	en MHz	FCC	IC	ETSI	España	Francia	MKK
1	2412	X	X	X	-	-	-
2	2417	X	X	X	-	-	-
3	2422	X	X	X	-	-	-
4	2427	X	X	X	-	-	-
5	2432	X	X	X	-	-	-
6	2437	X	X	X	-	-	-
7	2442	X	X	X	-	-	-

8	2447	X	X	X	-	-	-
9	2452	X	X	X	-	-	-
10	2457	X	X	X	X	X	-
11	2462	X	X	X	X	X	-
12	2467	-	-	X	-	X	-
13	2472	-	-	X	-	X	-
14	2484	-	-	-	-	-	X

Fuente: (Magaña, 2013)

1.4.5.3. Estándar IEEE 802.11g

El estándar 802.11g permite un máximo de transferencia de datos de 54 Mbps en rangos comparables a los del estándar antecesor 802.11b, permitiendo interoperabilidad entre dispositivos. Ofrece una mayor variedad de velocidades de transmisión y esquemas de modulación.

Para velocidades de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps, 802.11g adopta el esquema OFDM de 802.11a adaptado para 2.4 GHz y se define como ERP-OFDM[80], adicionalmente el esquema ERP-PBCC[81] es utilizado para proporcionar velocidades de datos de 22 y 33 Mbps.

El estándar ofrece una mayor variedad de opciones de velocidad de datos y esquemas de modulación como se muestra en la TABLA 7. 802.11g proporciona compatibilidad con la revisión original de 802.11 y 802.11b especificando la misma modulación y esquemas de entramado para velocidades de 1, 2, 5.5 y 11 Mbps.

[80] **ERP-OFDM** Extended Rate Physical Layer OFDM
[81] **ERP-PBCC** Extended Rate Physical Layer PBCC

TABLA 7 Opciones de Capa Física para 802.11g

VELOCIDAD DE DATOS (MBPS)	ESQUEMA DE MODULACIÓN
1	DSSS
2	DSSS
5.5	CCK o PBCC
6	ERP-OFDM
9	ERP-OFDM
11	CCK o PBCC
12	ERP-OFDM
18	ERP-OFDM
22	ERP-PBCC
24	ERP-OFDM
33	ERP-PBCC
36	ERP-OFDM
48	ERP-OFDM
54	ERP-OFDM

Fuente: (Stallings, 2005, pág. 450)

1.4.5.4. Estándar IEEE 802.11n

802.11n está ganando rápidamente una gran aceptación, la mayoría de los fabricantes de equipos incluyen varios productos que implementan el uso del estándar de una u otra forma. El estándar especifica la operación en las bandas de frecuencias de 2.4 GHz y 5 GHz, en lo que concierne a la máxima velocidad de datos sería de 300 Mbps utilizando un esquema de modulación basado en OFDM.

Ofrece mejoras globales 802.11n en comparación a los estándares anteriores. Un cambio significativo que facilita alguna de estas mejoras es el uso de la tecnología MIMO[82]. "De hecho muchos identifican a 802.11n como el estándar MIMO. Esta es una tecnología que, mediante el empleo de varias antenas, ofrece la posibilidad de resolver información coherentemente desde varias rutas de señales mediantes antenas receptoras separadas espacialmente" (Herrera Ramírez, Días Ramírez, & Calafate, 2008, pág. 5).

1.5. ELEMENTOS BÁSICOS DE LAS COMUNICACIONES INALÁMBRICAS

"Las comunicaciones inalámbricas hacen uso de las ondas electromagnéticas para enviar señales a través de largas distancias. Desde la perspectiva del usuario, las conexiones inalámbricas no son particularmente diferentes de cualquier otra conexión" (Delgado Ortiz, 2009, pág. 57).

1.5.1. Conceptos básicos de Antenas

1.5.1.1. Definición de Antena

(Stallings, 2005) Define: "Una antena como un conductor eléctrico o sistema de conductores eléctricos utilizados para radiar o recolectar energía electromagnética" (pág. 96). Dicho de otro modo, la antena es la transición entre un medio guiado y el espacio libre.

Las ondas electromagnéticas se caracterizan por su frecuencia (f) y longitud de onda (λ) donde c es la velocidad de propagación en el medio ($3 \times 10^8\ m/s$ en el espacio libre):

$$\lambda = \frac{c}{f}$$

[82] **MIMO** Múltiples Entradas / Múltiples Salidas

Las antenas también son elementos esenciales de todo equipamiento que utiliza radios, tanto para transmisión como recepción con el fin de acoplar su conexión eléctrica con el campo electromagnético.

1.5.1.2. Patrones de Radiación

Una antena puede radiar energía en todas las direcciones pero por lo general no lo realiza de manera uniforme en todas las direcciones. Una manera común de caracterizar el rendimiento de una antena es el patrón de radiación que no es más que una representación gráfica de las propiedades de radiación de una antena como una función de las coordenadas espaciales (Stallings, 2005). El patrón de radiación puede ser representado en dos planos perpendiculares conocidos como Elevación y Azimut.

1.5.1.3. Ganancia

Es una característica importante en una antena donde viene a ser la potencia de amplificación de la señal; es decir, que cuan mayor es la ganancia mejor es la antena. La ganancia de la antena se mide en dB[83] isotrópicos y se representa en dBi[84]; esto significa que la ganancia de potencia con respecto a un modelo teórico de antena isotrópica, radia la misma energía en todas las direcciones del espacio.

1.5.1.4. Relación Señal / Ruido

Uno de los mayores inconvenientes de los sistemas de radio son las señales de ruido. “Obviamente, cuan menor sea la relación de ruido con respecto a la señal, más óptima se considerará la señal. Incluso en las transmisiones digitales, se tienen que usar métodos de modulación que reduzcan el ruido y amplifiquen la señal de radio” **(Delgado Ortiz, 2009, pág. 62).**

La relación se expresa en dB y en escala exponencial, lo que se demuestra que con un valor de 10 dB la señal es 10 veces mayor que la del ruido, mientras que con 20 dB es 100 veces mayor.

1.5.1.5. Apertura del Haz

Representa la separación angular entre los dos puntos del lóbulo principal del patrón de radiación. Se suele representar en el plano horizontal y se expresa en grados.

---

[83] **dB** Decibelio, es una unidad que se utiliza para medir la intensidad del sonido y otras magnitudes físicas.
[84] **dBi** Decibelio isótropo, es una unidad para medir la ganancia de una antena en referencia a una antena isótropa teórica.

1.5.1.6. Polarización

Nos indica la orientación de los campos electromagnéticos que emite o recibe una antena. “La polarización de las antenas de ambos extremos de la comunicación debe ser la misma para minimizar la pérdida de ganancia” (Carlos, 2010). Las más comunes son: vertical, horizontal, circular y elíptica.

1.5.1.7. Zona de Fresnel

El proceso de propagación de radio entre 2 puntos se puede considerar como un tubo virtual por donde viaja la mayor parte de la energía entre el transmisor y receptor como se muestra en la FIGURA 13. Con el fin de evitar pérdidas no debería haber obstáculos dentro de esta zona porque un obstáculo alteraría el flujo de energía (Delgado Ortiz, 2009, pág. 65).

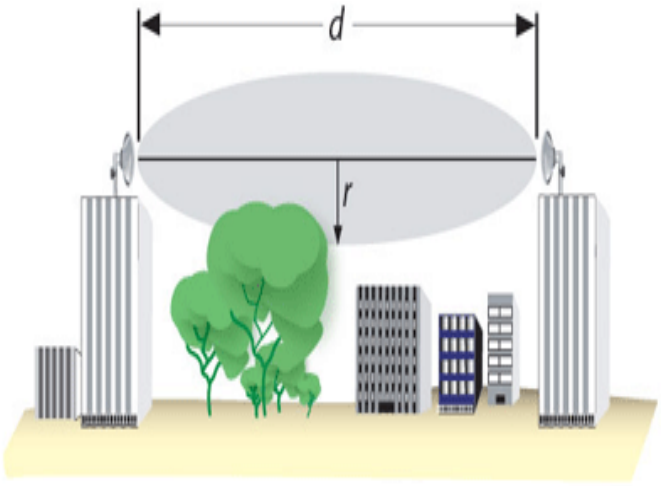


FIGURA 13 Representación de la Zona de Fresnel
Fuente: (Magnetoxx24, 2012)

1.5.2. Tipos de Antenas

De acuerdo al área de radiación las antenas de redes inalámbricas se pueden dividir en tres tipos principales:

1.5.2.1. Antenas Omnidireccionales

Orientan la señal en todas las direcciones con un haz amplio pero de corto alcance, también envían la información teóricamente a los 360° por lo que es posible establecer comunicación independiente del punto en el que se esté (FIGURA 14). “El alcance viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor” (Carlos, 2010).

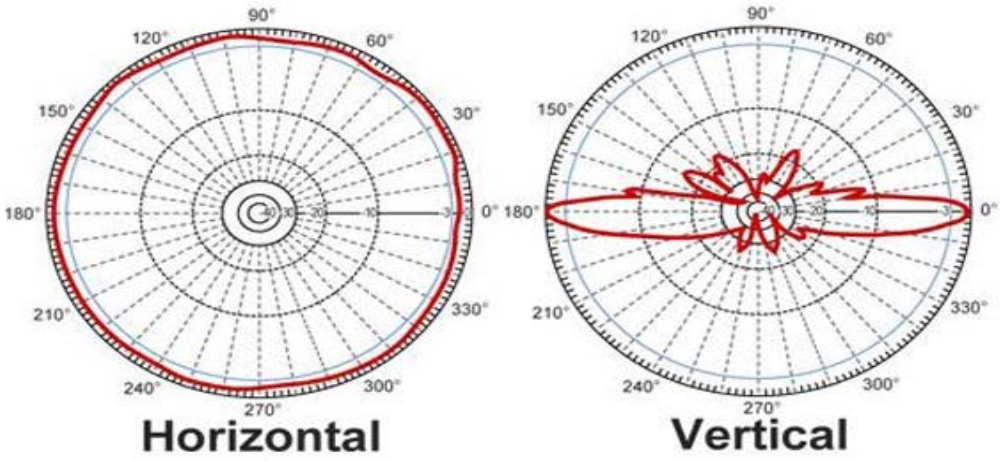


FIGURA 14 Patrón de radiación antena omnidireccional

Fuente: (Monsalve, 2011)

1.5.2.2. Antenas Direccionales

Orientan la señal en una dirección muy determinada con una haz estrecho pero de largo alcance; envían la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se puede establecer comunicación (FIGURA 15). “El alcance viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor” (Carlos, 2010).

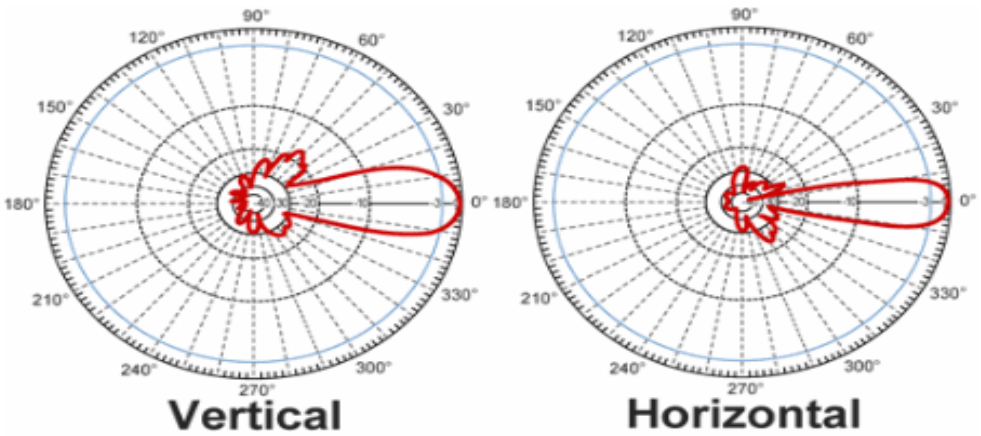


FIGURA 15 Patrón de radiación antena direccional

Fuente: (Monsalve, 2011)

1.5.2.3. Antenas Sectoriales

Son la mezcla de las antenas direccionales y las omnidireccionales. Se encargan de emitir un haz más amplio que una direccional pero no tan amplio como una omnidireccional. El alcance de una sectorial es mayor que la omnidireccional pero algo menor que la direccional. “Para tener una cobertura de 360° (como una antena omnidireccional) y un largo alcance (como una antena direccional) deberemos instalar o tres antenas sectoriales de 120° ó 4 antenas sectoriales de 80°” (Monsalve, 2011). El diagrama de radiación se muestra en la FIGURA 16.

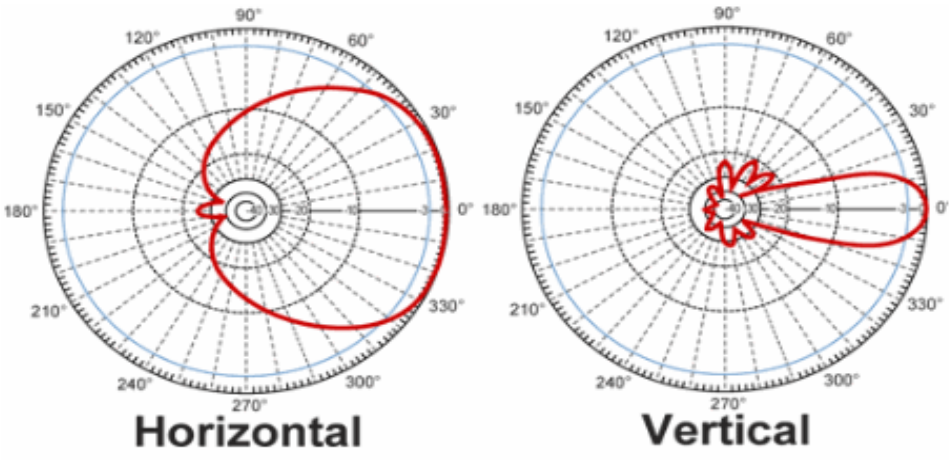


FIGURA 16 Patrón de radiación antena sectorial
Fuente: (Monsalve, 2011)

1.5.3. Propagación de Ondas de Radio

Las ondas presentan propiedades de propagación las cuales se indica a continuación:

1.5.3.1. Absorción

“Cuando una onda de radio se topa con un obstáculo, parte de su energía se absorbe y se convierte en otro tipo de energía, mientras que otra parte se atenúa y sigue propagándose, de esta manera es posible que otra parte se refleje” (Kioskea ES, 2013).

1.5.3.1.1. Atenuación

Atenuación significa la pérdida de potencia de la señal sufrida en el momento de viajar por cualquier medio de transmisión. La atenuación aumenta cuando se incrementa la frecuencia o la distancia.

1.5.3.2. Difracción

Se refiere a varios fenómenos que se producen cuando una onda se encuentra con un obstáculo, o visto de otro modo “difracción es el comportamiento de las ondas cuando al incidir en un objeto dan la impresión de doblarse, causando el efecto de ondas doblando las esquinas” (Delgado Ortiz, 2009, pág. 67).

1.5.3.3. Reflexión

“Cuando una onda de radio choca con un obstáculo, parte o la totalidad de la onda se refleja y se observa una pérdida de la intensidad. La reflexión es tal que el ángulo de incidencia equivale al ángulo de reflexión” (Kioskea ES, 2013).

1.5.3.4. Refracción

Es el cambio de dirección de una onda cuando cruza el límite entre dos medios en los cuales la onda viaja con diferente velocidad; este fenómeno supone un cambio en la velocidad de propagación de la onda el mismo que es asociado a un medio hacia otro de diferente naturaleza (Delgado Ortiz, 2009, pág. 69).

1.5.4. Ondas (Waves)

Una onda es algo difícil de definir pero un fenómeno fácil de entender. Resulta difícil, porque una onda se puede definir de diferentes maneras basándose en alguna aplicación o escenario específico y resulta fácil entender porque se puede ver sus efectos en la vida cotidiana sin tener demasiado conocimiento técnico.

Una onda es un tipo de perturbación que viaja a través de un medio en un determinado tiempo; además, una transferencia de energía siempre está asociada con dicho medio de transporte.

Las comunicaciones inalámbricas se realizan a través de ondas de radio; por lo tanto, podemos definir que una onda de radio es una perturbación que se desplaza a través del aire o el espacio en un momento dado (Soyinka, 2010, pág. 16).

1.5.4.1. Frecuencia

La frecuencia es una característica central y medible de una onda. Genéricamente hablando, es una magnitud que mide el número de repeticiones de un evento por unidad de tiempo fijo. La frecuencia se mide en hertzios (Hz), donde un Hertz es una unidad de frecuencia igual a un ciclo por segundo.

1.5.4.2. Longitud de Onda (Wavelenght)

La longitud de onda (algunas veces denotada como lambda λ) es la distancia medida desde un punto en una onda hasta la parte equivalente de la siguiente, es decir, desde la cima de un pico hacia otro pico. La longitud de onda está relacionada con la frecuencia y la relación es inversamente proporcional, cuanto mayor sea la frecuencia más corta es la longitud de onda y mientras más baja es la frecuencia más larga es la longitud de onda.

1.5.4.3. Amplitud

La amplitud es una magnitud de medida de una onda, se define formalmente como el desplazamiento máximo de una onda periódica y afecta el rendimiento que permanece en una señal después de viajar sobre una cierta distancia (Soyinka, 2010, pág. 19). En sistemas de comunicaciones inalámbricas la amplitud se puede medir en los extremos de transmisión y recepción de las entidades que se comunican.

1.5.4.4. Fase

La fase es el desplazamiento de una onda desde un punto de referencia; asimismo es una medida relativa entre una cantidad conocida y otra desconocida con profunda influencia en las comunicaciones de radiofrecuencia. También tenemos como particularidad que la fase afecta a la amplitud de una onda, aunque es una diferencia verdadera de tiempo que se mide en términos de ángulo, grados o radianes.

1.5.4.5. Bandas

El espectro radioeléctrico se divide en diferentes frecuencias de comunicación a las que se les conoce con el nombre de bandas. Existen varios modelos para la agrupación en bandas de frecuencia, las mismas que se indican a continuación:

- **Banda de Onda Media (MW[85]):** Esta banda se utiliza principalmente para la radiodifusión AM. En la mayoría de las partes del mundo el rango de frecuencias es 531-1602 kHz.
- **Banda de Muy Alta Frecuencia (VHF[86]):** Se trata de las frecuencias de radio en el rango de 30 a 300 MHz, es muy común dentro de este rango la banda de radio FM. En la mayoría de las partes del mundo, la banda FM está en el rango de 87.5-108 MHz; pero, la banda en Japón es de 76-90 MHz.
- **Banda K NATO[87]:** Esta banda comprende frecuencias entre 20 y 40 GHz.
- **Banda K IEEE:** Esta banda incluye el rango de frecuencias de microondas de 18 a 27 GHz.
- **Banda Industrial, Científica y Médica (ISM):** Las bandas de frecuencias ISM están definidas por la UIT-R[88], donde cada país controla el uso de las frecuencias conjuntamente con su ente regulador. Estándares de la IEEE muy populares como 802.11b y 802.11g operan en la gama de frecuencias ISM. A continuación en la
- TABLA 8 se presenta los rangos de frecuencias disponibles en la banda ISM:

TABLA 8 Frecuencias ISM

RANGO DE FRECUENCIA	FRECUENCIA CENTRAL
6.765 – 6.795 MHz	6.780 MHz
13.553 – 13.567 MHz	13.560 MHz
26.957 – 27.283 MHz	27.120 MHz
40.66 – 40.70 MHz	40.68 MHz
433.05 – 434.79 MHz	433.92 MHz
902 – 928 MHz	915 MHz
2.400 – 2500 GHz	2.450 GHz
5.725 – 5.875 GHz	5.800 GHz

[85] **MW** Medium Wave Band
[86] **VHF** Very High Frecuency
[87] **NATO - OTAN** Organización del Tratado del Atlántico Norte
[88] **UIT-R** Unión Internacional de Telecomunicaciones para el Sector de las Radiocomunicaciones

24 – 24.25 GHz	24.125 GHz
61 – 61.5 GHz	61.25 GHz
122-123 GHz	122.5 GHz
244 – 246 GHz	245 GHz

Fuente: (Soyinka, 2010, pág. 21)

- **Banda de Infraestructura de Información Nacional sin Licencia (UNII):** Las frecuencias y los límites de potencia en la banda UNII son definidos por la FCC en los Estados Unidos. Esta banda se subdivide en grupos de frecuencias que son cada uno de 100 MHz de ancho, se utiliza generalmente para aplicaciones de gran ancho de banda (por ejemplo VoIP y video) debido a su capacidad de manejar este tipo de aplicaciones. Mayor ancho de banda significa utilizar velocidades más altas. El popular estándar IEEE 802.11a opera en la banda de frecuencia UNII (TABLA 9).

TABLA 9 Frecuencias UNII

NOMBRE	RANGO DE FRECUENCIAS
UNII Low (Bajo)	5.15 – 5.25 GHz
UNII Mid (Medio)	5.25 – 5.35 GHz
UNII Worldwide (En todo el Mundo)	5.47 – 5.725 GHz
UNII Uper (Alto)	5.725 – 5.825 GHz

Fuente: (Soyinka, 2010, pág. 22)

1.5.4.6. Canales

Un canal en el lenguaje de las comunicaciones es la ruta mediante la cual se envía la información. Las bandas del espectro de radiofrecuencia se dividen en canales dando las facilidades correspondientes antes que citar frecuencias de radios reales. Por ejemplo: “si se le pide a una persona sintonizar su televisión en el canal 3 es más fácil que solicitarle que

sintonice su televisión en la frecuencia de 61.25 a 65.75 MHz para recibir los componentes de audio y video de una emisión de televisión" (Soyinka, 2010, pág. 22).

La **TABLA 10** muestra como los canales se asignan a frecuencias reales en la banda ISM. Estas frecuencias se utilizan en las comunicaciones WLAN basándose en los estándares de la IEEE 802.11b, 802.11g y 802.11n.

TABLA 10 Canales de Frecuencia de la Banda ISM

CANAL	FRECUENCIA BAJA (GHZ)	FRECUENCIA CENTRAL (GHZ)	FRECUENCIA ALTA (GHZ)
1	2.401	2.412	2.423
2	2.404	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.451	2.457	2.468
11	2.451	2.462	2.473

Fuente: (Soyinka, 2010, pág. 23)

1.5.5. Handoff / Roaming

Actualmente los entornos de comunicación inalámbrica son complejos debido al exitoso despliegue de diferentes tecnologías como Wi-Fi, WiMAX[89] y LTE[90] (Long Term Evolution) que operan de manera independiente brindando soporte a diferentes aplicaciones dentro y fuera de Internet (Ramírez Pérez, 2011, pág. 1).

[89] **WiMAX** Se refiere a las implementaciones interoperables de la familia inalámbrica IEEE 802.16 por el Foro WiMAX.
[90] **LTE** Es un estándar de tecnología inalámbrica para comunicaciones de datos y una evolución de los estándares GSM/UMTS.

Handoff es el movimiento de un nodo móvil entre Access Points, mientras que Roaming se refiere al movimiento de un nodo móvil entre redes. Las estaciones inalámbricas deberían permitir que el protocolo MAC utilizado en las WLANs se desplace de una celda[91] a otra.

1.5.5.1. Paradigma ABC

El paradigma ABC (Always Best Connected) de siempre la mejor conexión implica optimizar el desempeño de aplicaciones y brindar movilidad transparente a los usuarios, es decir que durante la conmutación entre redes el usuario no debería percibir un deterioro en la calidad y continuidad de las aplicaciones (Ramírez Pérez, 2011, pág. 2)

1.5.5.2. Handoff Vertical

En este esquema de red se requiere de un mecanismo que sea capaz de responder a las necesidades de comunicación de los usuarios a través de la selección eficiente de redes. Tradicionalmente en un escenario homogéneo, la necesidad de Handoff surge cuando la potencia de la señal de la estación base (estación inalámbrica) que actualmente soporta un servicio está por debajo de cierto umbral[92]. En un entorno heterogéneo los usuarios pueden moverse entre diferentes accesos de red correspondientes a diferentes tecnologías como se indica en la

FIGURA **17** para aprovechar las diferentes características de las redes que no pueden ser comparadas directamente (cobertura, ancho de banda, latencia[93], consumo de potencia, costo) (Ramírez Pérez, 2011, pág. 4).

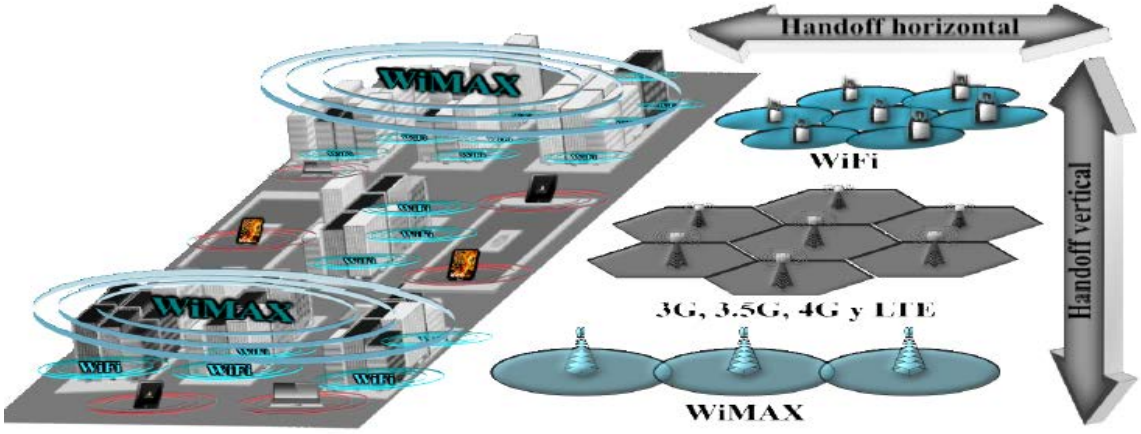


FIGURA 17 Escenario de Red

Fuente: (Ramírez Pérez, 2011, pág. 4)

[91] **Celda** Es una pequeña área geográfica de cobertura de una estación base.
[92] **Umbral** Es la cantidad mínima de señal que ha de estar presente para ser registrada por un sistema.
[93] **Latencia** Suma de retardos temporales dentro de una red.

1.5.5.3. PROCESO DE HANDOFF VERTICAL

El Handoff vertical puede definirse como un proceso para mejorar o mantener el rendimiento y la calidad en las aplicaciones de un dispositivo terminal; en este proceso las aplicaciones se mantienen activas mientras se realiza el cambio de AP. La principal diferencia entre el handoff vertical y el tradicional handover, es que en el primero se consideran y comparan redes de diferentes tecnologías para seleccionar a la mejor; mientras que en el segundo solo se seleccionan APs pertenecientes a una misma tecnología (Kassar, Kervella, & Pujolle, 2008). Esto da lugar a una clasificación de acuerdo a las razones que pueden motivar el proceso de handoff:

- **Handoff forzado o imperativo:** Activados por eventos físicos de acuerdo a la disponibilidad de interfaces de red.
- **Handoff de usuario o alternativo:** Activado por políticas o bien por preferencias de usuario.

1.5.5.4. GESTIÓN DE HANDOFF VERTICAL

La diversidad de los elementos involucrados en la realización del handoff vertical incrementa considerablemente su complejidad con respecto al tradicional handover. Esto ha dado lugar al desarrollo del concepto de gestión de handoff que engloba todos aquellos aspectos relacionados con este proceso (Kassar, Kervella, & Pujolle, 2008).

Como se observa en la FIGURA 18 el concepto de gestión de handoff comprende tres fases (Ramírez Pérez, 2011):

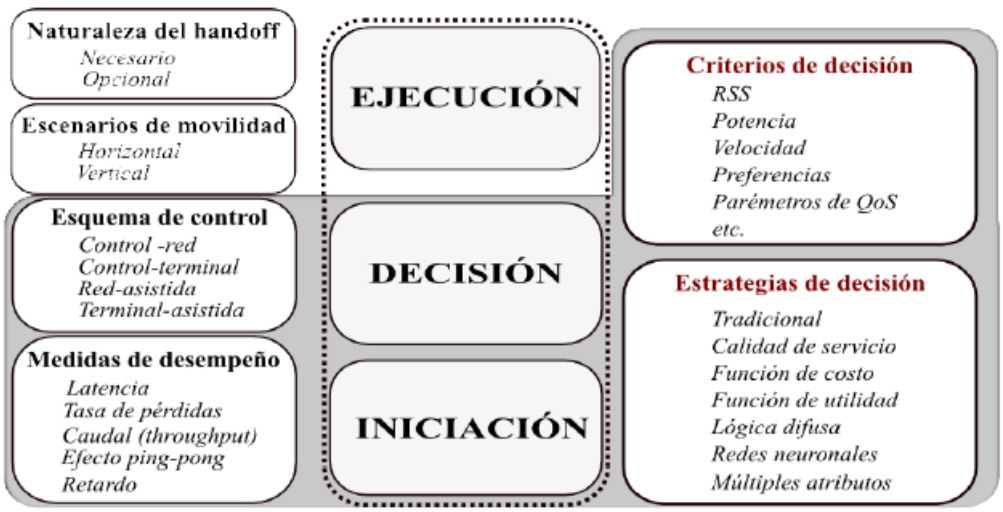


FIGURA 18 Aspectos principales en la Gestión de Handoff Vertical

Fuente: (Ramírez Pérez, 2011, pág. 6)

- **Iniciación:** Consiste en recolectar toda la información requerida para identificar la necesidad de handoff y poder próximamente iniciarlo.
- **Decisión:** Su función es procesar los datos proporcionados por la fase de iniciación para seleccionar el acceso de red más adecuado.
- **Ejecución:** Esta fase es la encargada de realizar los cambios necesarios configurando parámetros de transmisión conforme a los detalles resueltos durante la fase de decisión.

1.6. SEGURIDAD EN REDES INALÁMBRICAS

(Delgado Ortiz, 2009, pág. 211) Considera:

En la actualidad, gracias a la movilidad y reducción de costes que aporta la tecnología Wi-Fi, han surgido un gran número de redes inalámbricas en oficinas, centros de trabajo y lugares públicos (hot-spots[94]). Sin embargo muchas veces no se tiene en cuenta la vulnerabilidad de estas redes tanto respecto a la privacidad de las comunicaciones como frente a intrusiones en la red. Por tanto, a la hora de afrontar el reto de la movilidad, es imprescindible conocer los diferentes protocolos y mecanismos de seguridad existentes y tomar las medidas adecuadas.

1.6.1. Objetivos de Seguridad de Comunicaciones

1.6.1.1. Confidencialidad

Los datos son protegidos frente a la intercepción de personas no autorizadas para evitar que nadie pueda capturar las comunicaciones y acceder a su contenido, por ello es necesario tener en cuenta el cifrado de las comunicaciones.

1.6.1.2. Integridad

Garantizar que los datos no han sido modificados.

1.6.1.3. Autenticación

Garantizar que los datos vienen de quien se supone deben venir (origen de los datos).

1.6.1.4. Autorización y Control de Acceso

- Ambas se implementan sobre autenticación.
- Antes de garantizar acceso a los datos se debe encontrar:

[94] **Hot-Spots** Lugar que ofrece acceso a Internet a través de una red inalámbrica y un enrutador conectado a un proveedor de servicios de Internet.

- ✓ ¿Quién es el usuario (autenticación)?
- ✓ ¿La operación de acceso está permitida (autorización)?

1.6.2. Mecanismos de Seguridad Básicos

1.6.2.1. WEB (Wired Equivalent Protocol)

Se trata del primer mecanismo de seguridad implementado, fue diseñado para ofrecer un cierto grado de privacidad, pero no puede compararse con protocolos de redes más seguros tales como IPSec[95] para la creación de Virtual Private Networks (VPN[96]). WEP comprime y cifra los datos que se envían a través de las ondas de radio. WEP usa una clave secreta, utilizada para el cifrado de los paquetes antes de su retransmisión. El algoritmo utilizado para el cifrado es RC4. (Delgado Ortiz, 2009, pág. 212)

1.6.2.2. Firewall

"Sistema de defensa basado en la instalación de un muro entre una computadora, un AP o un router y la red por la que circulan todos los datos. Este tráfico es autorizado o denegado por el firewall, siguiendo instrucciones previamente configuradas" (Delgado Ortiz, 2009, pág. 212).

1.6.2.3. ACL (Access Control List)

"Si bien no forma parte del estándar, la mayor parte de los productos dan soporte al mismo. Se utiliza como mecanismo de autenticación la dirección MAC de cada estación, permitiendo el acceso únicamente a aquellas estaciones cuya MAC figura en la lista de control de acceso (ACL)" (Delgado Ortiz, 2009, pág. 212).

1.6.2.4. Closed Network Access Control

Se debe permitir solamente el acceso a la red a aquellos que conozcan el nombre de la red o SSID.

1.6.2.5. Filtrado de direcciones MAC

"Los APs deben tener una relación de las direcciones MAC que pueden conectarse. No es un método que ofrezca un alto grado de seguridad, pero es una medida básica para evitar que cualquier usuario pueda acceder a la red" (Delgado Ortiz, 2009, pág. 212).

---

[95] IPSec Es un conjunto de características que protegen los datos IP cuando éstos viajan desde una entidad a otra.

[96] VPN Es una tecnología de red que permite una extensión segura de la red local sobre una red pública no controlada como Internet.

1.6.2.6. Open System Authentication

“Es el mecanismo de autenticación definido por el estándar 802.11 y consiste en autenticar todas las peticiones que reciben. El principal problema de este mecanismo es que no realiza ninguna comprobación y, además, todas las tramas de gestión son enviadas sin ningún tipo de cifrado, incluso cuando se ha activado WEP” (Delgado Ortiz, 2009, pág. 212).

1.6.2.7. Antivirus

Se encarga de detectar y destruir virus los mismos que son software totalmente diseñados con un solo propósito de dañar los sistemas. Cuenta además con procedimientos de eliminación, detección, reconstrucción de los archivos y las áreas del sistema que han sido infectadas. Es importante aclarar que un antivirus es una herramienta útil para el usuario pero no será una protección total.

1.6.3. Mecanismos de Seguridad Avanzados

1.6.3.1. TKIP (Protocolo de Integridad de Clave Temporal)

“Con este protocolo se pretende resolver las deficiencias del algoritmo WEP, este protocolo posee un código de integración de mensajes (MIC[97]) el cual cifra el checksum[98] incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11 protegiendo con esto cualquier ataque por falsificación” (Delgado Ortiz, 2009, pág. 212).

1.6.3.2. VPN (Virtual Private Network)

La conexión VPN a través de internet es técnicamente una Red de Área Extensa (WAN) que ofrece conectividad punto a punto con validación jerárquica de usuarios y host conectados remotamente. “Sistema para simular una red privada sobre una pública, como por ejemplo Internet, La idea es que la red pública sea vista desde dentro de la red privada como un cable lógico que une dos o más redes que pertenecen a la red privada” (Delgado Ortiz, 2009, pág. 212).

1.6.3.3. Estándar IEEE 802.1X

El estándar 802.1x está diseñado para mejorar la seguridad de las redes WLAN que siguen el estándar IEEE 802.11. 802.1x proporciona una autenticación para redes LAN inalámbricas, lo que permite a un usuario ser autenticado por una autoridad central. 802.1x utiliza EAP[99] que funciona en Ethernet, Token Ring o en redes LAN inalámbricas, generando un intercambio de mensajes durante el proceso de autenticación.

---

[97] **MIC** Message Integrity Code
[98] **Checksum** Comprobación de suma, realiza cálculos sobre cadenas de texto.
[99] **EAP** Protocolo de Autenticación Extensible (RFC 2284)

En una LAN inalámbrica con 802.1x, un usuario (conocido como el Suplicante) genera las solicitudes de acceso a un AP (conocido como el Autenticador) como se indica en la

FIGURA **19**. El AP obliga al usuario no autorizado en un estado que permite al cliente enviar solo un mensaje de inicio de EAP. El punto de acceso EAP devuelve un mensaje solicitando la identidad del usuario. El cliente devuelve la identidad que se transmite por el AP al servidor de autenticación, que utiliza un algoritmo para autenticar el usuario y devuelve un mensaje de confirmación o denegación de vuelta al AP. El AP cambia el estado del cliente a ser autorizado y de esta manera el tráfico normal ya podrá circular. (Delgado Ortiz, 2009, pág. 220)

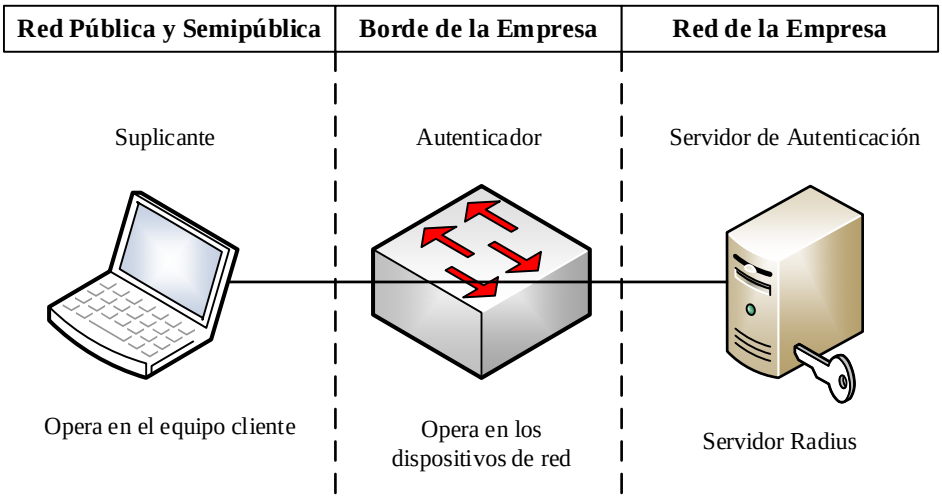


FIGURA 19 Control de Acceso IEEE 802.1x

Fuente: (Delgado Ortiz, 2009, pág. 220)

El Autenticador no tiene por qué ser una máquina inteligente, por lo que pequeños APs podrán utilizar este estándar 802.1x.

La adopción de 802.11i propone hacer frente a las actualizaciones de firmware de las estaciones inalámbricas. En caso de que el hardware haya quedado obsoleto para el soporte de la nueva norma, habrá que comprar APs capaces de soportar AES; dado que, 802.11i puede operar con cualquier otra técnica de encriptación, el soporte de esta especificación es su principal ventaja sobre WPA.

1.6.3.4. WPA (Wi-Fi Protected Access)

El estándar IEEE 802.11i se centra en resolver los problemas de seguridad en las WLAN, incluso abarca más allá que la autenticación del cliente utilizando claves WEB. WPA utiliza varios de los componentes del estándar 802.11 proporcionando las siguientes medidas de seguridad:

- Autenticación de cliente utilizando 802.1x o llave precompartida (PSK[100]).
- Autenticación mutua entre cliente y servidor.
- Privacidad de los datos con TKIP.
- Integridad de los datos utilizando MIC.

1.6.3.5. WPA2 (Wi-Fi Protected Access Version 2)

WPA2 está basado en el estándar 802.11i final el cual elimina muchas de las debilidades de sus predecesores tanto en la autenticación de usuarios como en la robustez de los métodos de encriptación. (Ariganello & Barrientos Sevilla, 2010) Afirma: “Se extiende mucho más en las medidas de seguridad que WPA. Para la encriptación de los datos se utiliza AES que es un método robusto y escalable adoptado para utilizarlo por muchas organizaciones gubernamentales. Soporta TKIP para la encriptación de los datos y tiene compatibilidad con WPA” (pág. 500).

Con WPA o con autenticación EAP un usuario inalámbrico tiene que autenticarse al AP el cual solicita la petición, de esta forma si el usuario se está moviendo de un AP a otro el continuo proceso de autenticación puede llegar a ser tedioso. Es por ello que WPA2 resuelve este problema utilizando PKC[101], una técnica de roaming rápida donde el usuario se autentica solo una vez en el primer AP que realiza la petición de conexión. Si el resto de los APs soportan WPA2 y están configurados como un grupo lógico, la autenticación se pasa automáticamente de un AP a otro.

1.6.4. Encriptación y Autenticación en Redes Inalámbricas

1.6.4.1. 802.1X y Autenticación EAP

EAP o 802.1x es un protocolo estándar desarrollado por la IEEE que permite a los switches realizar autenticación por puerto. Algunas de las características de 802.1x son las siguientes:

[100] **PSK** (Pre-Shared Key) Se define una clave secreta en el cliente y en el AP.
[101] **PKC** Proactive Key Caching

- Utiliza un servidor RADIUS[102] como método de autenticación, almacenando así la base de datos de usuarios y contraseñas en una localización centralizada.
- La autenticación entre el cliente y el servidor RADIUS es mutua.
- Puede usar diferentes tipos de encriptación tales como AES, WPA, TKIP, WEP.
- Si no hay intervención manual, entonces y de forma automática utiliza llaves dinámicas WEB para la encriptación, las cuales son derivadas después de pasar la autenticación.
- Soporta roaming.
- Las políticas de control están centralizadas.

Los componentes necesarios para implementar una arquitectura 802.1x se presentan en la

FIGURA **20** y son los siguientes:

- Suplicante (Supplicant)
  - Estaciones Inalámbricas.
- Autenticador (Authenticator)
  - AP o Router Inalámbrico
- Servidor de Autenticación (Authentication Server)
  - Accesible a través del sistema de distribución.
  - Puede estar en el AP o Router Inalámbrico.
  - La solicitud de login acompañado de su password es comparado con una base de datos para garantizar el acceso al usuario.

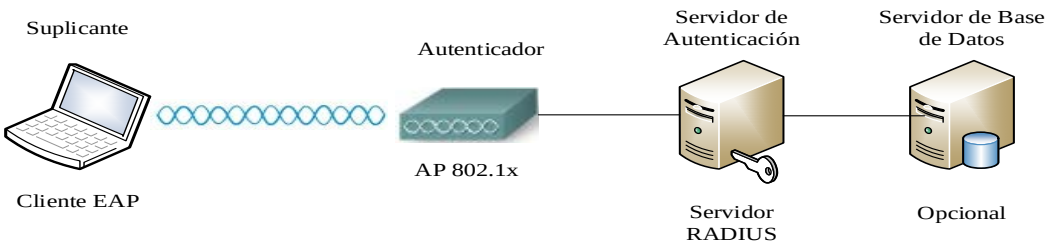


FIGURA 20 Componentes necesarios para implementar una arquitectura 802.1x

Fuente: (Ariganello & Barrientos Sevilla, 2010, pág. 874)

[102] **RADIUS** Remote Access Dial-In User Service

1.6.4.2. EAP-LEAP

LEAP[103] es uno de los tipos de autenticación de 802.1x desarrollado por Cisco para redes inalámbricas. Soporta autenticación manual entre el servidor y cliente mediante el ingreso de usuario y contraseña; además proporciona distribución de clave de sesión segura y dinámica para cada usuario.

Las características más sobresalientes de LEAP son las siguientes:

- Roaming rápido y seguro a nivel de capa 2 y 3.
- Soporta una amplia gama de sistemas operativos.

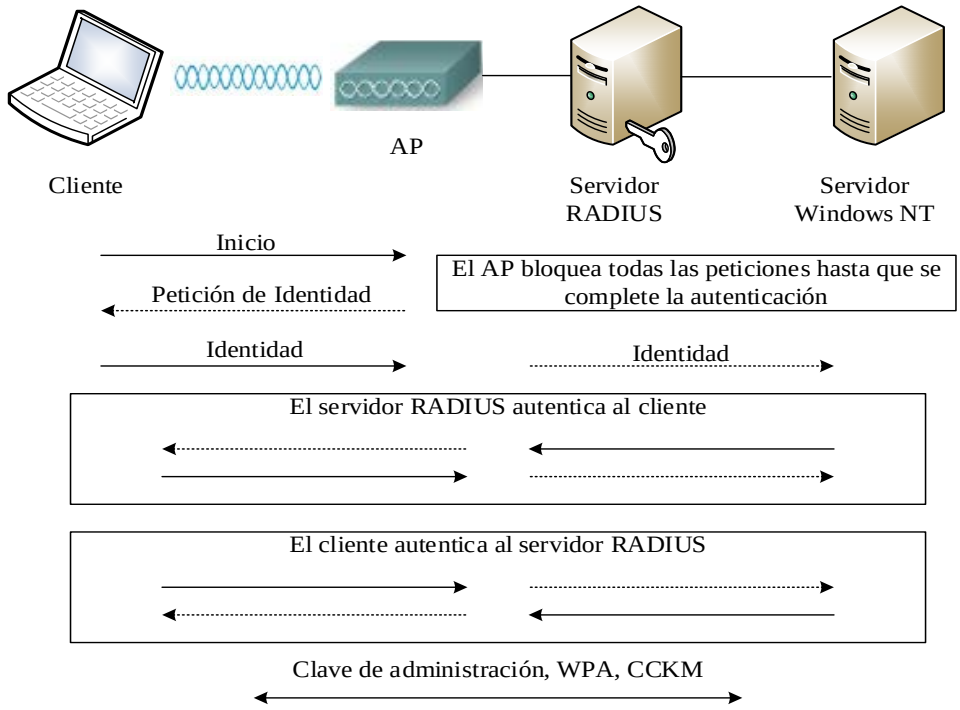


FIGURA 21 Proceso de Autenticación de Cisco LEAP

Fuente: (Ariganello & Barrientos Sevilla, 2010, pág. 875)

La **FIGURA 21** muestra el proceso de autenticación de LEAP donde el cliente solamente puede transmitir tráfico EAP hasta que es autenticado por el servidor RADIUS. Se debe tomar en cuenta que la autenticación puede ser iniciada tanto por el cliente como por el AP, en cualquiera de los dos casos el cliente responde al AP con un usuario, por medio del cual el AP lo encapsula en un mensaje RADIUS y los envía al servidor de autenticación.

[103] **LEAP** Lightweight Extensible Authentication Protocol

1.6.4.3. EAP-FAST

EAP-FAST[104] fue inicialmente desarrollado por Cisco y posteriormente estandarizado, muy apropiada para clientes que no pueden implementar contraseñas complejas y el uso de certificados digitales.

Características:

- Compatible con el sistema de validación única de Windows.
- No requiere certificados o el uso de PKI[105] en los clientes.
- Soporta clientes Windows 2000, XP, CE.
- Proporciona soporte para 802.11i, 802.1x, TKIP y AES.
- Soporta WPA en clientes Windows 2000, XP.
- Soporta WDS[106], roaming rápido y seguro con CCKM[107].

La FIGURA 22 muestra el proceso de autenticación EAP-FAST donde el cliente solamente puede transmitir tráfico EAP hasta que es autenticado por el servidor RADIUS. Una vez autenticado se generan unas llaves que son utilizadas dinámicamente para cifrar tráfico por el tiempo que dure la sesión.

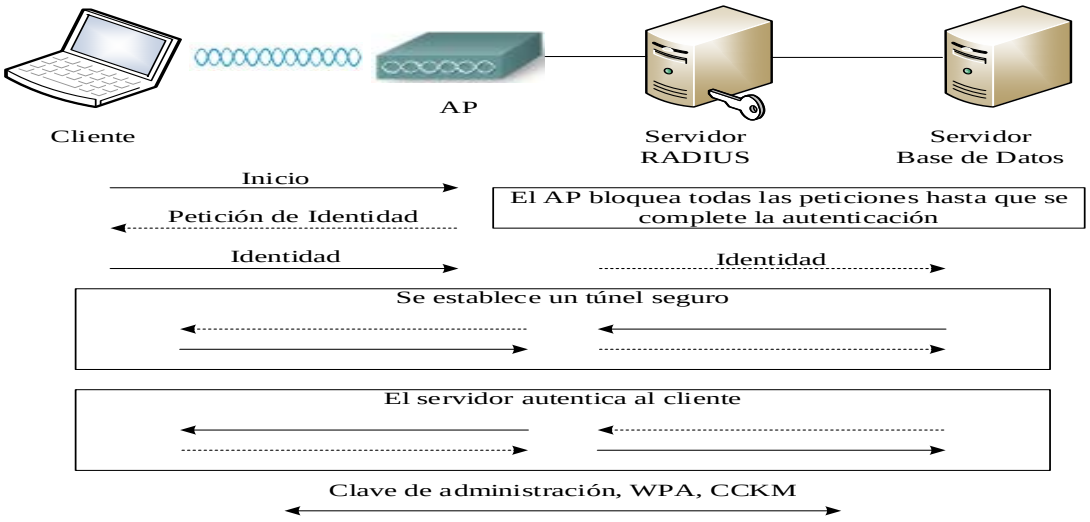


FIGURA 22 Proceso de Autenticación EAP-FAST

Fuente: (Ariganello & Barrientos Sevilla, 2010, pág. 877)

[104] **EAP-FAST** Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling.
[105] **PKI** Public Key Infrastructure: involucra el proceso de intercambio y mantenimiento de llaves.
[106] **WDS** Wireless Domain Services
[107] **CCKM** Cisco Centralized Key Management

1.6.4.4. EAP-TLS

EAP-TLS[108] es un método de autenticación muy seguro que utiliza el protocolo TLS[109] para proporcionar transferencia de datos en redes públicas, conjuntamente utiliza PKI donde el cliente y el servidor obtienen un certificado digital desde una Autoridad Certificadora reemplazando de esta manera claves demasiado simples.

La FIGURA 23 muestra el proceso de autenticación de EAP-TLS donde el cliente se asocia al AP y sólo se le permite enviar tráfico EAP cuando es autenticado por el servidor RADIUS. Una vez realizada la autenticación se negocian las llaves para la encriptación de la sesión que puede ser WEB o 802.11i.

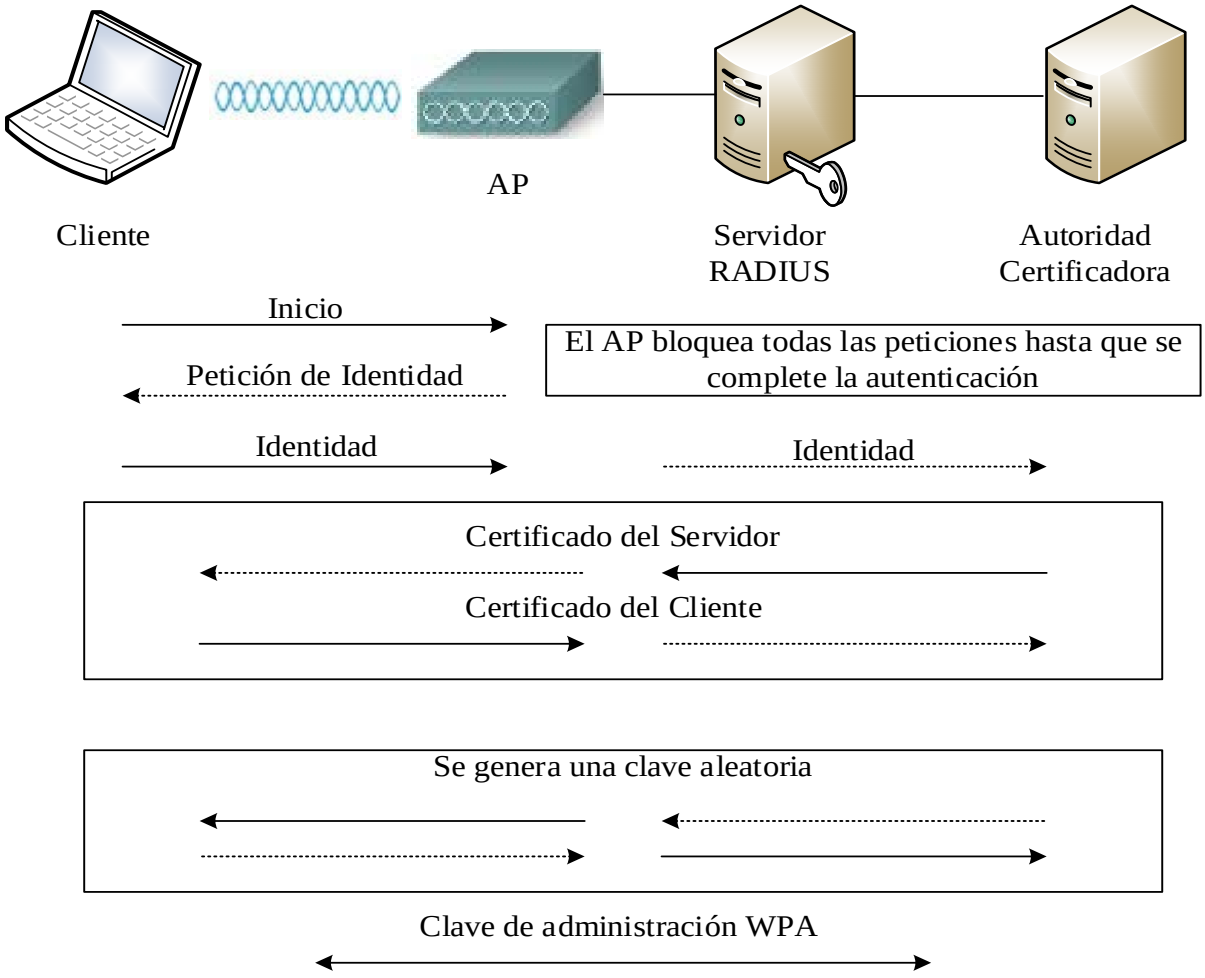


FIGURA 23 Proceso de Autenticación de EAP-TLS

Fuente: (Ariganello & Barrientos Sevilla, 2010, pág. 878)

[108] **EAP-TLS** Extensible Authentication Protocol-Transport Layer Security
[109] **TLS** Transport Layer Security

1.6.4.5. EAP-PEAP

PEAP[110] es otro tipo de autenticación 802.1x desarrollada por Cisco Systems, Microsoft y RSA Security, posteriormente estandarizado por la IEEE. “Soporta métodos EAP a través del túnel, pero a diferencia de TTLS, no soporta otros métodos para la negociación de la autenticación del cliente” (Espinoza & Loayza, 2013, pág. 3). “PEAP utiliza una infraestructura PKI pero solo es obligatorio instalar los certificados digitales en el servidor, no es necesario en los clientes” (Fernández Hansen, Ramos Varón, & García Moran, 2009, pág. 65). La FIGURA 24 muestra el proceso de autenticación de EAP-PEAP.

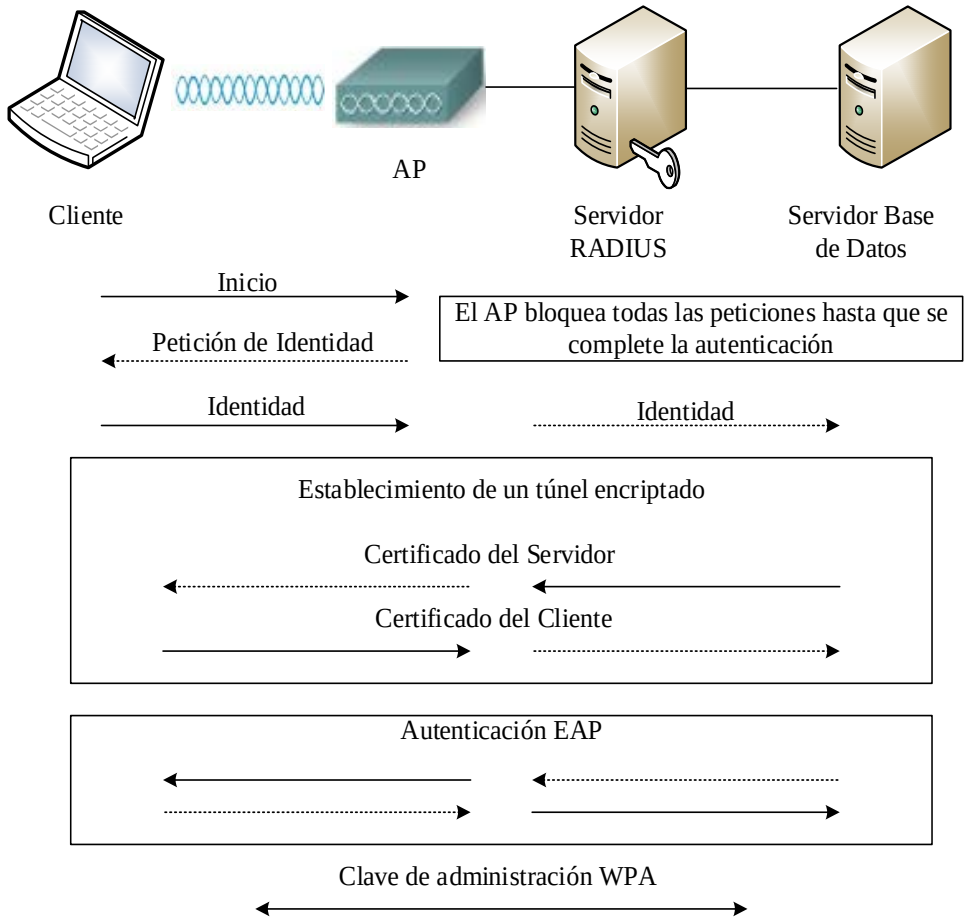


FIGURA 24 Proceso de Autenticación EAP-PEAP
Fuente: (Ariganello & Barrientos Sevilla, 2010, pág. 879)

[110] **PEAP** Protected Extensible Authentication Protocol

1.6.4.6. WPA, 802.11i y WPA2

WPA es una solución estándar para proporcionar seguridad y cubrir los defectos de WEB.

En la FIGURA 25 se muestra el proceso de autenticación de WPA y 802.11i mediante el cual el cliente y el AP intercambian una petición de asociación inicial y se ponen de acuerdo en el uso de cierta capacidad con un tipo de seguridad específica. Posteriormente el cliente y el servidor RADIUS llevan a cabo la autenticación 802.1x, si dicha autenticación resulta satisfactoria el servidor genera y envía una llave maestra al AP mientras que el cliente por su parte genera la misma llave (estas llaves son llamadas PMK[111]). A continuación el cliente y el AP realizan un saludo de 4 vías para verificar la validez del AP creando una sesión de confianza entre el AP y el cliente. El paso final es un saludo de 2 vías entre cliente y AP que tiene como objetivo derivar las llaves GTK[112] y MIC. (Ariganello & Barrientos Sevilla, 2010, pág. 879)

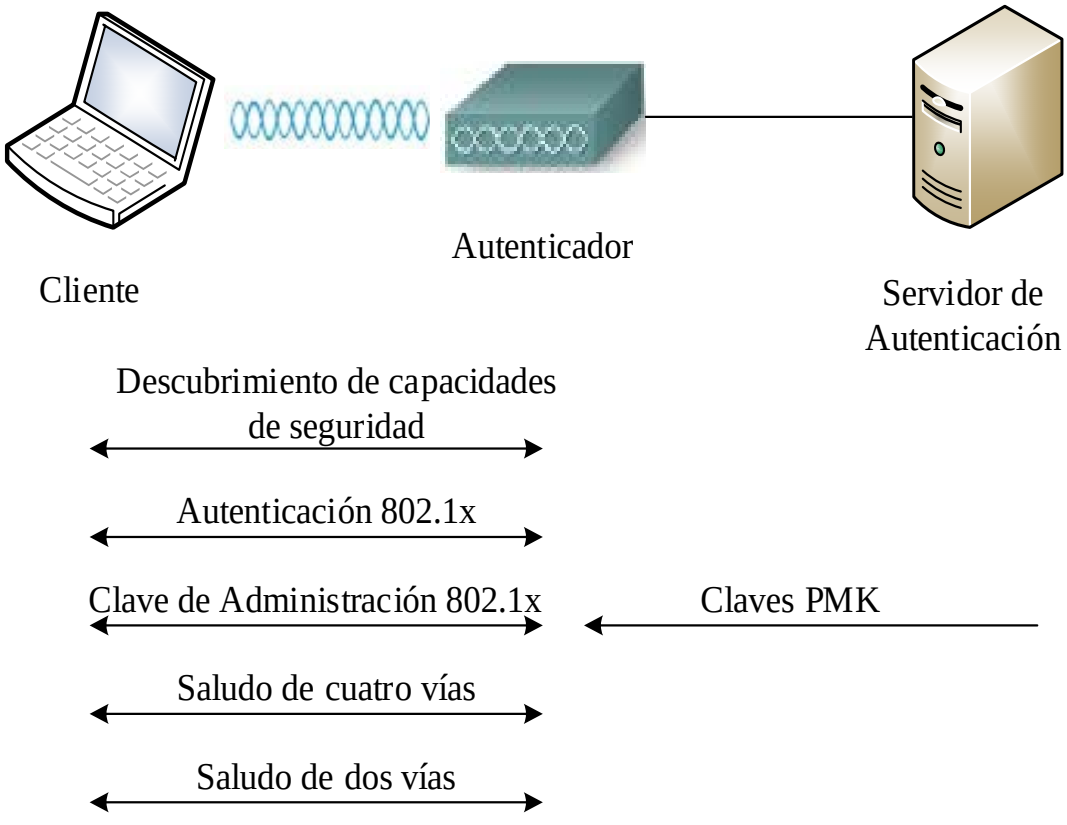


FIGURA 25 Proceso de Autenticación de WPA y 802.11i
Fuente: (Ariganello & Barrientos Sevilla, 2010, pág. 880)

[111] **PMK** Pairwise Master Key
[112] **GTK** Group Transient Ke

Aunque WPA es un método seguro puede presentar algunas desventajas:

- WPA utiliza TKIP y confía en la encriptación RC4 que no es de las opciones existentes más seguras.
- WPA requiere soporte de firmware de los controladores y del sistema operativo.
- WPA es susceptible a un ataque DoS conocido.

Poco después de que WPA estuviera disponible la IEEE ratificó el estándar 802.11i, el cual proporciona autenticación, encriptación y gestión de llaves de manera más segura. Los principales componentes añadidos con 802.11i son:

- Autenticación 802.1x.
- Encriptación AES.
- Gestión de llaves.

WPA2 es el sucesor de WPA y es capaz de interoperar con 802.11i, incorpora AES como algoritmo de escriptación.

Las principales características de WPA2 son las siguientes:

- Utiliza 802.1x para el proceso de autenticación.
- Utiliza un método de renovación y distribución de llaves similar al de WPA.
- Soporta PKC (Proactive Key Caching).
- Soporta IDS[113] (Intrusion Detection System).

WPA y WPA2 tienen dos modos de funcionamiento, personal y enterprise. La siguiente tabla muestra los métodos de autenticación y encriptación usados en cada uno de ellos:

[113] **IDS** Programa usado para detectar accesos no autorizados a un computador o a una red.

TABLA 11 Métodos de autenticación y encriptación de WPA y WPA2

MODO	WPA	WPA2
Enterprise	Autenticación: IEEE 802.1x/EAP Encriptación: TKIP/MIC	Autenticación: IEEE 802.1x/EAP Encriptación: AES-CCMP
Personal	Autenticación: PSK Encriptación: TKIP/MIC	Autenticación: PSK Encriptación: AES-CCMP

Fuente: (Ariganello & Barrientos Sevilla, 2010, pág. 881)

Aunque WPA2 es mucho más seguro que WPA todavía tiene algunos por menores:

- El cliente necesita un controlador compatible con EAP.
- El servidor RADIUS tiene que soportar EAP.
- Consume más recursos de CPU que WPA, por lo que en algún caso quizás sea necesario actualizar el hardware.

1.6.4.7. COMPARATIVA DE MÉTODOS DE AUTENTICACIÓN EAP

Una comparación de los métodos de autenticación EAP se muestra en la TABLA 12.

TABLA 12 Comparación de los Métodos de Autenticación EAP

TEMA	MD5	LEAP (CISCO)	TLS (MS)	TTLS (FUNK)	PEAP (VARIOS)	FAST (CISCO)
Solución de Seguridad	Estándar	Patente	Estándar	Estándar	Estándar	Estándar
Certificado Cliente	No	N/A	Sí	No (opcional)	No (opcional)	No
Certificado Servidor	No	N/A	Sí	Sí	Sí	No/Si
Credenciales de Seguridad	Ninguna	Deficiente	Buena	Buena	Buena	Depende

Soporta Autentificación de Base de Datos	Requiere borrar la Base de Datos	Active Directory, NT Domains	Active Directory	Act. Dir. NT Domains, Token Systems, SQL, LDAP	Act. Dir. NT Domains, LDAP, Novell NDS, Token	Act. Dir. NT Domains, LDAP
Intercambio de llaves dinámicas	No	Sí	Sí	Sí	Sí	No
Autenticación Mútua	No	Sí	Sí	Sí	Sí	Sí

Fuente: (Delgado Ortiz, 2009, pág. 225)

1.6.5. RADIUS

"RADIUS (Remote Authentication Dial-In User Server) es un protocolo definido por el IETF[114] en el documento RFC[115] 2865 y se utiliza para gestionar el acceso a los recursos de la red. También es conocido como un protocolo cliente/servidor que se ejecuta en la capa aplicación utilizando UDP como transporte" (Soyinka, 2010, pág. 142). El protocolo ha existido durante mucho tiempo y se utiliza de una u otra forma en innumerables aplicaciones. RADIUS hace su trabajo, proporcionando un medio para la gestión centralizada de usuarios, puede ser en forma de una base de datos o podría contener una lista de requisitos que se deben cumplir para permitir el acceso a un usuario.

Utilizan el protocolo AAA[116] (Authentication, Authorization, Accounting) lo cual permite un manejo adecuado de todos los clientes que hacen uso del servidor. Cuando el usuario intenta acceder a la misma red, necesita identificarse por medio de un nombre de usuario y una contraseña. Esta información es recibida por el servidor RADIUS el cual valida una petición de autentificación contra la información almacenada en su base de datos. Si la petición fue aceptada, el servidor se encargará de asignar una dirección IP y los demás parámetros necesarios para la conexión y registro.

---

[114] **IETF** Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet).
[115] **RFC** Request for Comments: conjunto de documentos que sirven de referencia para la comunidad de Internet.
[116] **AAA** Autentificación, Autorización y Registro

1.6.5.1. Entidades RADIUS

La FIGURA 28 muestra la ubicación de cada una de las entidades RADIUS en una red inalámbrica:

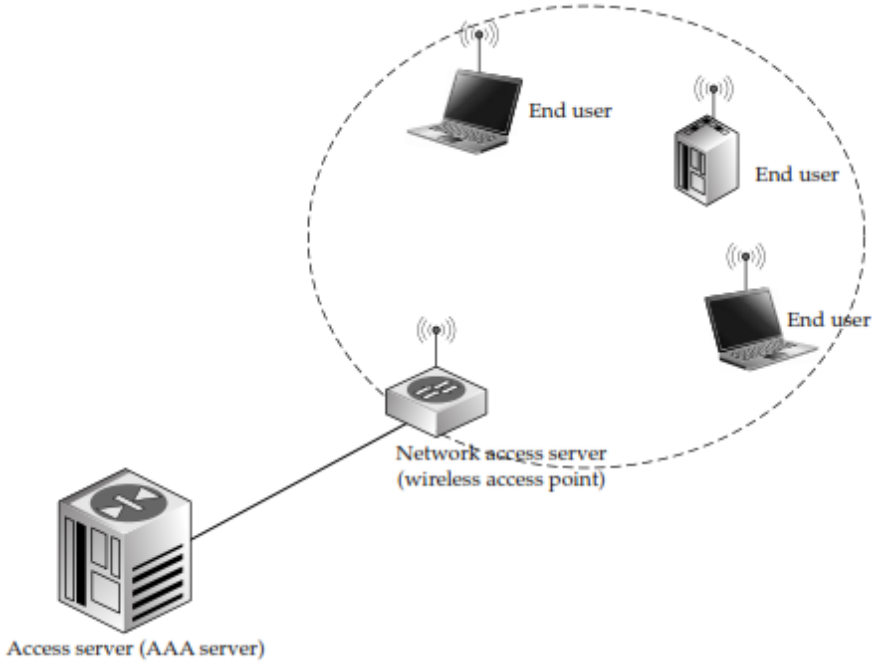


FIGURA 26 Una simple Red RADIUS

Fuente: (Soyinka, 2010, pág. 143)

1.6.5.1.1. End User (Usuario Final)

Entidad que tiene acceso a los recursos de la red después de haber sido autenticado por un servidor de autenticación encargado de gestionar los usuarios, tal como una estación inalámbrica. Desde el punto de vista del protocolo RADIUS el usuario final no es necesariamente la misma entidad que el cliente RADIUS (autenticador); de hecho, el usuario final es a menudo distinto del cliente RADIUS.

1.6.5.1.2. NAS (Network Access Server)

Este dispositivo proporciona acceso a la red tal como un AP, donde el usuario final se conecta al NAS[117] cada vez que necesita acceder a los recursos de la red. El NAS a su vez se basa en un servidor de acceso para determinar si se debe permitir o denegar el ingreso al usuario final. El NAS se conoce comúnmente como el cliente RADIUS o el autenticador.

[117] **NAS** Servidor de Acceso a la Red

1.6.5.1.3. AS (Access Server)

El NAS envía peticiones de los usuarios finales que desean acceder a los recursos de la red en el AS[118]. El servidor de acceso toma la decisión final de permitir o denegar la conexión al usuario.

1.6.5.2. AAA

El documento RFC 2903 propone una arquitectura para el desarrollo de la Autentificación, Autorización y Accounting en un servidor que provea estos tres servicios (Servidor AAA). El documento entrega las bases y las reglas generales para establecer estos tres servicios de manera integrada. Además el servidor AAA es definido como una entidad que es capaz de autentificar usuarios, manejar requests de autorizaciones y recolectar datos de las cuenta.

1.6.5.2.1. Autenticación (Authentication)

La autenticación es el proceso de validación de identidad y credenciales de los usuarios para permitir o denegar el acceso a la red a determinados recursos. Entre los métodos más comunes de autenticación se tiene el uso de contraseñas, sin embargo cada vez es más requerido el uso de ciertos elementos de autenticación como tokens[119] o biometría[120]. El componente de autenticación se establece en el puerto 1812 UDP.

1.6.5.2.2. Autorización (Authorization)

La autorización define qué derechos y servicios tiene el usuario final una vez que su acceso ha sido identificado y aceptado. También es posible configurar restricciones a la autorización de determinados servicios en función de ciertos parámetros como la hora del día, la localización del usuario, o incluso la posibilidad o imposibilidad de realizar múltiples logins de un mismo usuario.

1.6.5.2.3. Registro (Accounting)

El registro de los usuarios permite mantener la información de los servicios que han sido utilizados por el usuario final para determinados propósitos tales como facturación, auditoría y planes de capacitación; sin embargo, el registro suele incluir parámetros como la identidad del usuario y tiempo de inicialización y finalización de uso del servicio. El componente de registro se establece en el puerto 1813 UDP.

---

[118] **AS** Servidor de Acceso
[119] **Token** Es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.
[120] **Biometría** Es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo.

1.6.5.3. Requerimientos para el uso de RADIU

Un administrador de red inalámbrica como parte esencial de su infraestructura necesita conocer ciertos requerimientos para utilizar RADIUS, es por ello que la siguiente lista ayudará a responder esta pregunta:

- Se usa RADIUS cuando se necesite administrar un gran número de usuarios que utilicen la red inalámbrica desde una ubicación central.
- Se usa RADIUS como complemento de cualquiera de las dos soluciones de seguridad inalámbrica de modo Enterprise (Empresarial) donde WPA2 es el sucesor de WPA por ser un método muy seguro al utilizar AES como algoritmo de encriptación.
- Se usa RADIUS para mantener un registro de usuarios inalámbricos para propósitos de auditoría y facturación.
- Se usa RADIUS cuando se requiere cumplir o definir características basadas en políticas avanzadas tal como el acceso limitado por tiempo a los usuarios de la red inalámbrica.
- Se usa RADIUS cuando la red inalámbrica este destinada para uso público como hotspots[121] inalámbricos.
- Se usa RADIUS principalmente cuando la integración del servidor a los recursos de la red se puede realizar fácilmente sin ningún tipo de problemas.
- Se usa RADIUS cuando se esté manejando un gran número de clientes inalámbricos que poseen diferentes plataformas tales como Linux, Windows, Macintosh, BSD, etc.

1.7. PORTALES CAUTIVOS

1.7.1. Definición

Una herramienta común de autenticación utilizada en las redes inalámbricas es el portal cautivo, el mismo que utiliza una página Web con la cual un usuario de una red pública y/o privada tiene la posibilidad de presentar sus credenciales de registro garantizando su acceso a las funciones normales de la red.

“También puede utilizarse para presentar información a los usuarios antes de permitirles el acceso. Mediante el uso de un navegador web en lugar de un programa personalizado de

[121] **HotSpot** Es una zona de alta demanda de tráfico, que por tanto el dimensionamiento de su cobertura está condicionado a cubrir esta demanda por parte de un AP o varios.

autenticación, los portales cautivos funcionan en prácticamente todas las computadoras portátiles y sistemas operativos" (wndw.net, 2008, pág. 165).

Estos portales son generalmente utilizados por centros de negocios, aeropuertos, museos, hoteles, restaurantes, cafés Internet y otros proveedores que ofrecen HotSpot de Wi-Fi para usuarios de Internet.

1.7.2. Ventajas de los Portales Cautivos

- Puede funcionar tanto en redes inalámbricas como en redes cableadas.
- Seguridad basada en identidades.
- Configuración sencilla.
- Estadísticas de uso por usuario.
- Mejor despliegue que VPN: no necesita cliente, solo es necesario un navegador.
- Más rápidos: no hay latencia por cifrado.
- Pueden utilizar autenticación centralizada.
- Permite aplicar políticas por usuario.
- No se compromete todo el sistema.
- Muchas soluciones comerciales y libres.

1.7.3. Desventajas de los Portales Cautivos

- Menos seguros que otras soluciones (se puede combinar con WEB/WPA).
- Vulnerables a spoofing de MAC e IP.
- No se cifra el tráfico (depende de los protocolos de aplicación: https, ssh, etc.)
- Si el dispositivo no tiene navegador no es posible autenticarse.
- Los clientes asociados al AP tienen visibilidad entre ellos aunque no estén autenticados.

1.7.4. Funcionalidades de los Portales Cautivos

La funcionalidad de un portal cautivo es simple, el usuario es el encargado de conectarse a la red inalámbrica donde se le asigna una dirección IP por DHCP[122] (Dynamic Host Configuration Protocol) para que pueda hacer uso de la red. Es así que el usuario desde su navegador web solicita cualquier página de internet como se muestra en la FIGURA 27.

[122] **DHCP** Protocolo de red que permite a los clientes de una red obtener sus parámetros IP de configuración automáticamente.

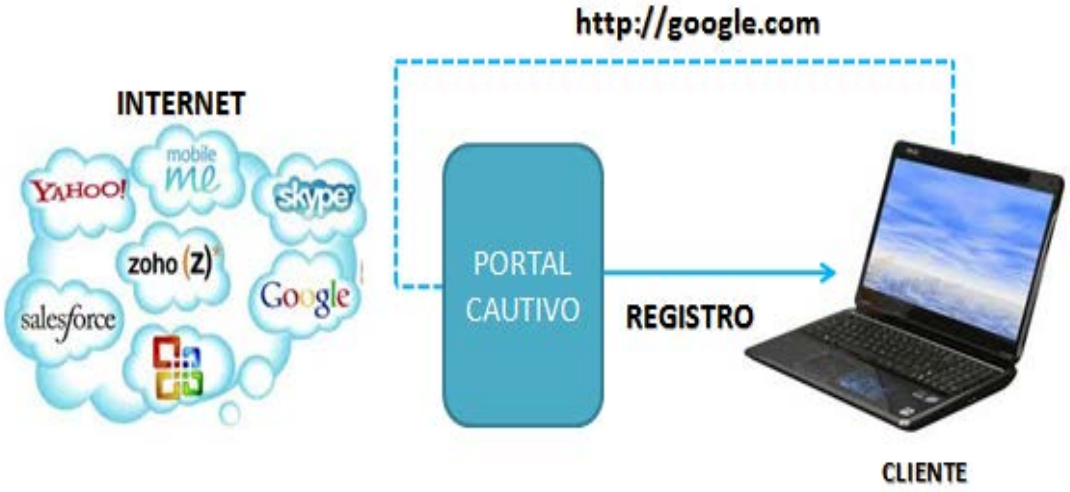


FIGURA 27 El usuario solicita una página web y es redireccionado

Fuente: (wndw.net, 2008, pág. 165)

Una vez que ha solicitado el usuario su página de internet inmediatamente se le redireccionará a una página de registro donde tendrá que ingresar su usuario y contraseña para poder tener privilegios de acceso a Internet. El AP y el servidor de autenticación se encargarán de la verificación de los datos del usuario (

FIGURA **28**).

FIGURA 28 Verificación de credenciales

Fuente: (wndw.net, 2008, pág. 165)

Finalmente, gracias al servidor de autenticación el usuario ha sido autenticado, por lo tanto se le permitirá el acceso a los recursos de la red (FIGURA 29).

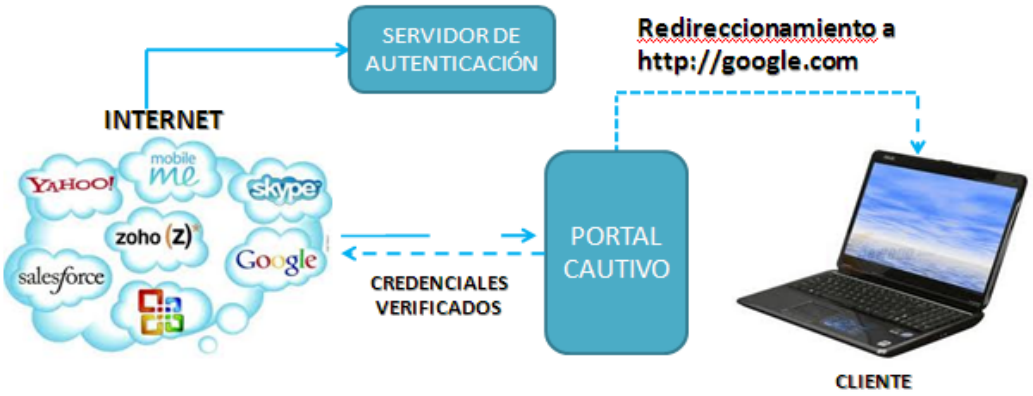


FIGURA 29 Después de que el usuario es autenticado, se le permite el acceso
Fuente: (wndw.net, 2008, pág. 165)

1.7.5. Portales Cautivos por Software

Son programas que crean un punto de acceso a Internet implementando un portal cautivo a través de un servidor o computador, el cual debe tener dos tarjetas de red como mínimo: la una como salida al Internet y la otra para conectarse a la red de acceso inalámbrico con recursos compartidos.

Para poder seleccionar un portal cautivo por software dependerá del sistema operativo del servidor o computador a utilizarse. A continuación indicaremos los más importantes:

- Chillispot
- Wifidog
- m0n0wall
- PfSense
- Zeroshell
- PepperSpot

1.7.5.1. Chillispot

FIGURA 30 Logo identificador de Chillispot
Fuente: (Chillispot, 2013)

Chillispot es un portal cautivo de código abierto o también el controlador de un AP inalámbrico dentro de una LAN. Se utiliza para la autenticación de usuarios de una red inalámbrica, su compatibilidad se basa en el inicio de sesión mediante una página WEB que es el modelo actual para la autenticación de los HotSpots públicos donde cada usuario al ingresar sus credenciales podrá utilizar los recursos de la red (Chillispot, 2013). Adicionalmente se podría decir que EasyHotspot[123] utiliza como aplicación de portal cautivo Chillispot, con una base de datos MySQL[124] para almacenamiento de los usuarios y de la información registrada.

1.7.5.2. Wifidog

FIGURA 31 Logo identificador de Wifidog
Fuente: (Île Sans Fil, 2013)

Wifidog más que todo es utilizado para controlar el acceso a redes Wi-Fi de acceso público; dicho software opera bajo un Portal Cautivo. Un Portal Cautivo es como un cortafuego que bloquea el acceso a la red de los usurarios no registrados en dicho portal, a través de su página de inicio. Una vez registrado el usuario en el portal, puede tener acceso a internet y a los recursos de la red. El portal cautivo se instala en la puerta de enlace de la red (puede ser un servidor o un hardware) (Linux-OS, 2013).

1.7.5.3. m0n0wall

FIGURA 32 Logo identificador de m0n0wall
Fuente: (Kasper, 2013)

[123] **EasyHotspot** es una aplicación que corre sobre una distribución de Ubuntu.
[124] **MySQL** es un sistema de administración de bases de datos.

Es un sistema operativo embebido completo basado en FreeBSD junto con un servidor web, PHP[125] (Hypertext Preprocessor) y algunas otras utilidades. Toda la configuración del sistema se almacena en un único archivo de texto XML[126] (Extensible Markup Language) para mantener las cosas transparentes. Cuando se utiliza junto con una PC embebido proporciona todas las características importantes de firewalls comerciales incluyendo la facilidad de uso en fracción del precio.

M0n0wall es probablemente el primer sistema UNIX que ha hecho su configuración en tiempo de arranque con PHP en lugar de los habituales Shell scripts y que tiene toda la configuración del sistema almacenada en formato XML (Kasper, 2013).

1.7.5.4. PfSense

FIGURA 33 Logo identificador PfSense
(Electric Sheep Fencing LLC., 2013)

El proyecto PfSense es una distribución libre de firewall de red, basado en el sistema operativo FreeBSD con un kernel personalizado e incluyendo paquetes de software de terceros para funcionalidades adicionales. A través de este sistema de paquetes de software PfSense, es capaz de proporcionar la mayor parte de funcionalidades de firewalls comerciales comunes (Electric Sheep Fencing LLC., 2013).

1.7.5.5. Zeroshell

FIGURA 34 Logo identificador Zeroshell
(Ricciardi, 2013)

[125] **PHP** Lenguaje de código abierto especialmente adecuado para el desarrollo WEB.
[126] **XML** Lenguaje de Marcas Extensible

Zeroshell es una distribución Linux para servidores y dispositivos embebidos orientados a proveer los servicios y recursos de red. Zeroshell es una distribución Live CD. Esto significa que no es necesario instalarlo en el disco duro para que funcione, ya que es capaz de funcionar desde el CD ROM. Lógicamente la base de datos de la red, puede ser almacenada en discos ATA, SATA, SCSI y USB. Se puede descargar para formatos en tarjetas Compact Flash para instalarla en dispositivos embebidos. Es un firewall gratuito que tiene las características de los equipos complejos que se encargan de la seguridad (Ricciardi, 2013).

1.7.5.6. PepperSpot

FIGURA 35 Logo identificador PepperSpot
Fuente: (Vincent & Vançon, 2013)

PepperSpot es un portal cautivo o controlador de APs de una LAN inalámbrica que soporta el protocolo IPv6. Es compatible con el inicio de sesión basado en WEB y soporta WPA. La autenticación se puede manejar con el servidor RADIUS preferido (sobre IPv4[127]/IPv6[128]). PepperSpot ofrece una potente herramienta para la administración de una red. Posee una gran variedad de servicios, como son: DHCP, DNS[129] (Domain Name System), Freeradius[130], Apache2, Firewall, Radvd[131] (Router Advertisement Daemon) entre otros.

1.7.6. Portales Cautivos por Hardware

Son dispositivos que llevan el software de control y portal cautivo internamente permitiendo la administración del acceso de usuarios a Internet y en áreas públicas, no necesitan de equipos adicionales para su funcionamiento como un servidor o computador. A continuación indicaremos los más importantes:

---

[127] **IPv4** Protocolo de Internet versión 4 definido en el RFC 791.
[128] **IPv6** Protocolo de Internet versión 6 definido en el RFC 2460.
[129] **DNS** Sistema de Nombres de Dominio definido en los RFCs 1034 y 1035.
[130] **Freeradius** Servidor RADIUS de código abierto.
[131] **Radvd** es un demonio en IPv6 que informa a los nodos que se conectan a la subred cuál es la dirección de esa subred, y cuál es su prefijo.

- Antamedia Hotspot Gateway
- Aptilo Access Gateway
- Mikrotik RouterOS
- 4ipnet Hotspot Gateway

CAPITULO II

2. SITUACIÓN ACTUAL DE LA RED LAN INALÁMBRICA Y RECURSOS

En este capítulo se identificó como se encuentra actualmente la red inalámbrica de la Universidad Técnica del Norte, que permita establecer los requerimientos actuales y futuros a ser considerados en el diseño de la Red LAN Inalámbrica.

2.1. LA UNIVERSIDAD TÉCNICA DEL NORTE

2.1.1. Ubicación

La Universidad está situada en la ciudad de Ibarra, en la provincia de Imbabura, en la República del Ecuador. Pertenece a la región 1, zona norte del país (Imbabura, Carchi, Norte de Pichincha, Esmeraldas y Sucumbíos).

FIGURA 36 Vista Superior de la Universidad Técnica del Norte
Fuente: Imagen proporcionada de Google Earth

La ubicación exacta es al noroeste de la ciudad Avenida 17 de Julio 5-21 sector el Olivo, su ubicación geográfica es 0°21'28.59" N 78°06'40.59" O.

2.1.2. Antecedentes

El aumento significativo de aplicaciones en la red ha provocado en la Universidad Técnica del Norte (UTN) muchas falencias en el rendimiento y la capacidad de sus servicios y recursos. Indudablemente el crecimiento tecnológico adquirido ha permitido mejorar de una u otra forma las prestaciones de la universidad, lo que ha generado ventajas como la digitalización de la información y desventajas como el congestionamiento de tráfico por innumerables paquetes de información que se encuentran cursando en la red.

Los estudiantes requieren tener acceso a una red LAN Inalámbrica en el interior de cada una de las facultades de la UTN, pero dadas las circunstancias no se ha logrado establecer buenas políticas sobre el uso, consumo y capacidad donde los procesos realizados garanticen su funcionalidad. En puntos estratégicos de los alrededores de la institución se implementaron 9 Access Points (APs), los mismos que no abastecen a cubrir un área de cobertura eficiente y mucho menos movilidad.

Toda fuente de información confiable es un complemento de consulta para la educación académica de los alumnos de la UTN; por ello los recursos de biblioteca, repositorios y acceso a Internet son una herramienta metodológica para los partícipes del aprendizaje y la enseñanza; identificando los criterios y procedimientos de estudio.

2.1.3. INFRAESTRUCTURA FÍSICA DE LA UTN

El campus de la UTN es una de las infraestructuras más modernas, de la región norte del país, lo que ha permitido mantenerse a la vanguardia; formando entes que generen soluciones y aporten ideas para el mejoramiento del país.

La Universidad Técnica del Norte está conformada por algunos edificios, encargados tanto de la parte académica como administrativa los cuales son:

- Edificio de Administración Central
- Edificio de Bienestar Universitario
- Facultad de Ingeniería en Ciencias Aplicadas
- Facultad de Ingeniería en Ciencias Agropecuarias y Ambientales
- Facultad de Ciencias Administrativas y Económicas
- Facultad de Ciencias de la Salud
- Facultad de Educación, Ciencia y Tecnología

A más de las facultades citadas, forman parte de la casona universitaria el Instituto de Postgrado en su nueva edificación. Cabe recalcar que las instalaciones donde antes funcionaba el Instituto de Postgrado se encuentran siendo utilizadas por el Centro Académico de Idiomas, Centro de Educación Continua (CEC) y la Escuela de Conducción UTN.

Entre otras estructuras que conforman el campus UTN tenemos la Biblioteca, el Auditorio Agustín Cueva, el polideportivo, el complejo acuático, el gimnasio y comedor universitario, la mecánica de la universidad, parqueaderos y canchas deportivas para la recreación de la comunidad universitaria.

2.1.4. ADMINISTRACIÓN Y UBICACIÓN DE LAS EDIFICACIONES DE LA UTN

El estudio realizado de la red de la UTN nos ayuda a determinar cómo se encuentran distribuidas cada una de las edificaciones que conforman las instalaciones de la casona universitaria (**¡Error! No se encuentra el origen de la referencia.**).

2.1.4.1. EDIFICIO DE ADMINISTRACIÓN CENTRAL

En este edificio se ubican la mayoría de los departamentos administrativos de la universidad, también se encuentra el departamento de informática desenvolviendo roles importantes en lo que respecta al control y administración de la red de la universidad, también se encuentra el cuarto de equipos con toda su infraestructura de comunicaciones. El área de desarrollo de software se encarga de cada uno de los sistemas utilizados en los diferentes procesos que maneja la institución.

Dos entidades importantes que también se encuentran en el edificio central son la Radio y la Televisora Universitaria.

2.1.4.2. Facultad de Ingeniería en Ciencias Aplicadas (FICA)

“La Facultad de Ingeniería en Ciencias Aplicadas, es una unidad académica que contribuye al desarrollo del conocimiento, forma profesionales especializados de manera científica y humanista en armonía con el medio ambiente y conciencia social” (FICA, 2013). Actualmente la facultad cuenta con un número de estudiantes definido en la siguiente TABLA 13

TABLA 13 Distribución del número de estudiantes en la FICA

FICA	PRESENCIAL		SEMIPRESENCIAL		TOTAL
CARRERAS	**FEMENINO**	**MASCULINO**	**FEMENINO**	**MASCULINO**	
Carrera de Ingeniería en Electrónica y Redes de Comunicación	127	235			362
Carrera de Ingeniería en Mecatrónica	61	306			367
Carrera de Ingeniería en Sistemas Computacionales	89	237			326
Carrera de Ingeniería en Textil	69	46			115
Carrera de Ingeniería Industrial	79	138			217
Carrera de Ingeniería en Diseño Textil y Modas	11	1			12
Total Estudiantes	**436**	**963**			**1399**

Fuente: Información establecida por el personal de Desarrollo del Sistema UTN periodo académicos 2012-2013

2.1.4.3. Facultad de Ingeniería en Ciencias Agropecuarias y Ambientales (FICAYA)

"La Facultad de Ingeniería en Ciencias Agropecuarias y Ambientales, forma profesionales emprendedores. Defendemos el desarrollo sostenible de recursos naturales, la producción limpia, principios de equidad, que den seguridad y soberanía alimentaria" (FICAYA, 2013). Actualmente la facultad cuenta con un número de estudiantes definido en la siguiente TABLA **14**.

TABLA 14 Distribución del número de estudiantes en la FICAYA

FICAYA	PRESENCIAL		SEMIPRESENCIAL		TOTAL
CARRERAS	**FEMENINO**	**MASCULINO**	**FEMENINO**	**MASCULINO**	
Carrera de Ingeniería Agroindustrial	127	112			239
Carrera de Ingeniería en Agronegocios Avalúos y Catastros			51	82	133
Carrera de Ingeniería en Agropecuaria	83	125			208
Carrera de Ingeniería en Biotecnología	17	13			30
Carrera de Ingeniería en Energías Renovables	6	7			13
Carrera de Ingeniería en Recursos Naturales Renovables	161	152			313
Carrera de Ingeniería Forestal	56	100			156
Total Estudiantes	**450**	**509**	**51**	**82**	**1092**

Fuente: Información establecida por el personal de Desarrollo del Sistema UTN periodo académicos 2012-2013

2.1.4.4. Facultad de Educación, Ciencia y Tecnología (FECYT)

"La Facultad Educación Ciencia y Tecnología es una unidad académica, que contribuye al desarrollo integral de la sociedad, forma profesionales emprendedores, competitivos, comprometidos con el desarrollo sustentable" (FECYT, 2013). Actualmente la facultad cuenta con un número de estudiantes definido en la siguiente TABLA **15**.

TABLA 15 Distribución del número de estudiantes en la FECYT

FECYT	PRESENCIAL		SEMIPRESENCIAL		TOTAL
CARRERAS	FEMENINO	MASCULINO	FEMENINO	MASCULINO	
Carrera de Ingeniería en Gestión y Desarrollo Social	8	15			23
Carrera de Ingeniería en Mantenimiento Automotriz	12	276			288
Carrera de Ingeniería en Mantenimiento Eléctrico	6	131			137
Carrera de Licenciatura en Artes Plásticas	10	6			16
Carrera de Licenciatura en Diseño Gráfico	39	88	3	8	138
Carrera de Licenciatura en Diseño y Publicidad			25	51	76
Carrera de Licenciatura en Relaciones Públicas	8	10			18
Carrera de Licenciatura en Secretariado Ejecutivo en Español			129	5	134
Carrera de Psicología	38	17			55
Carrera de Ingeniería en Turismo	131	8			229
Carrera de Licenciatura en Contabilidad y Computación	60	33			93
Carrera de Licenciatura en Educación Física	29	117			146
Carrera de Licenciatura en Entrenamiento Deportivo			14	93	107
Carrera de Licenciatura en Físico Matemático	40	37			77
Carrera de Licenciatura en Inglés	71	36			107

Carrera de Licenciatura en Parvularia			354	12	366
Carrera de Licenciatura en Psicología Educativa y O. V.	102	36			138
Total Estudiantes	**554**	**900**	**525**	**169**	**2148**

Fuente: Información establecida por el personal de Desarrollo del Sistema UTN periodo académicos 2012-2013

2.1.4.5. Facultad de Ciencias Administrativas y Económicas (FACAE)

"La Facultad de Ciencias Administrativas y Económicas de la Universidad Técnica del Norte, contribuye a dinamizar el desarrollo en los campos administrativos, contables, económicos y de mercado de la región y del País" (FACAE, 2013). Actualmente la facultad cuenta con un número de estudiantes definido en la siguiente TABLA 16

TABLA 16 Distribución del número de estudiantes en la FACAE

FACAE	PRESENCIAL		SEMIPRESENCIAL		TOTAL
CARRERAS	**FEMENINO**	**MASCULINO**	**FEMENINO**	**MASCULINO**	
Carrera de Ingeniería Comercial	232	115	17	10	374
Carrera de Ingeniería en Administración Pública de Gobiernos Seccionales	24	15			39
Carrera de Ingeniería en Contabilidad y Auditoría CPA	576	105	239	61	981
Carrera de Ingeniería en Economía Mención Finanzas	143	69			212
Carrera de Ingeniería en Mercadotecnia	130	96			226
Total Estudiantes	**1105**	**400**	**256**	**71**	**1832**

Fuente: Información establecida por el personal de Desarrollo del Sistema UTN periodo académicos 2012-2013

2.1.4.6. Facultad de Ciencias de la Salud

"Contribuyendo al desarrollo local, regional y nacional a través de la formación de profesionales críticos y creativos altamente capacitados, con el fin de apoyar problemas en salud, alimentación y nutrición" (FCCSS, 2013). Actualmente la facultad cuenta con un número de estudiantes definido en la siguiente TABLA **17**.

TABLA 17 Distribución del número de estudiantes en la FCCSS

FCCSS	PRESENCIAL		SEMIPRESENCIAL		TOTAL
CARRERAS	**FEMENINO**	**MASCULINO**	**FEMENINO**	**MASCULINO**	
Carrera de Licenciatura en Enfermería	486	106			592
Carrera de Licenciatura en Terapia Física Médica	201	72			273
Carrera de Gastronomía	90	93			183
Carrera de Licenciatura en Nutrición y Salud Comunitaria	175	35			210
Total Estudiantes	**952**	**306**			**1258**

Fuente: Información establecida por el personal de Desarrollo del Sistema UTN periodo académicos 2012-2013

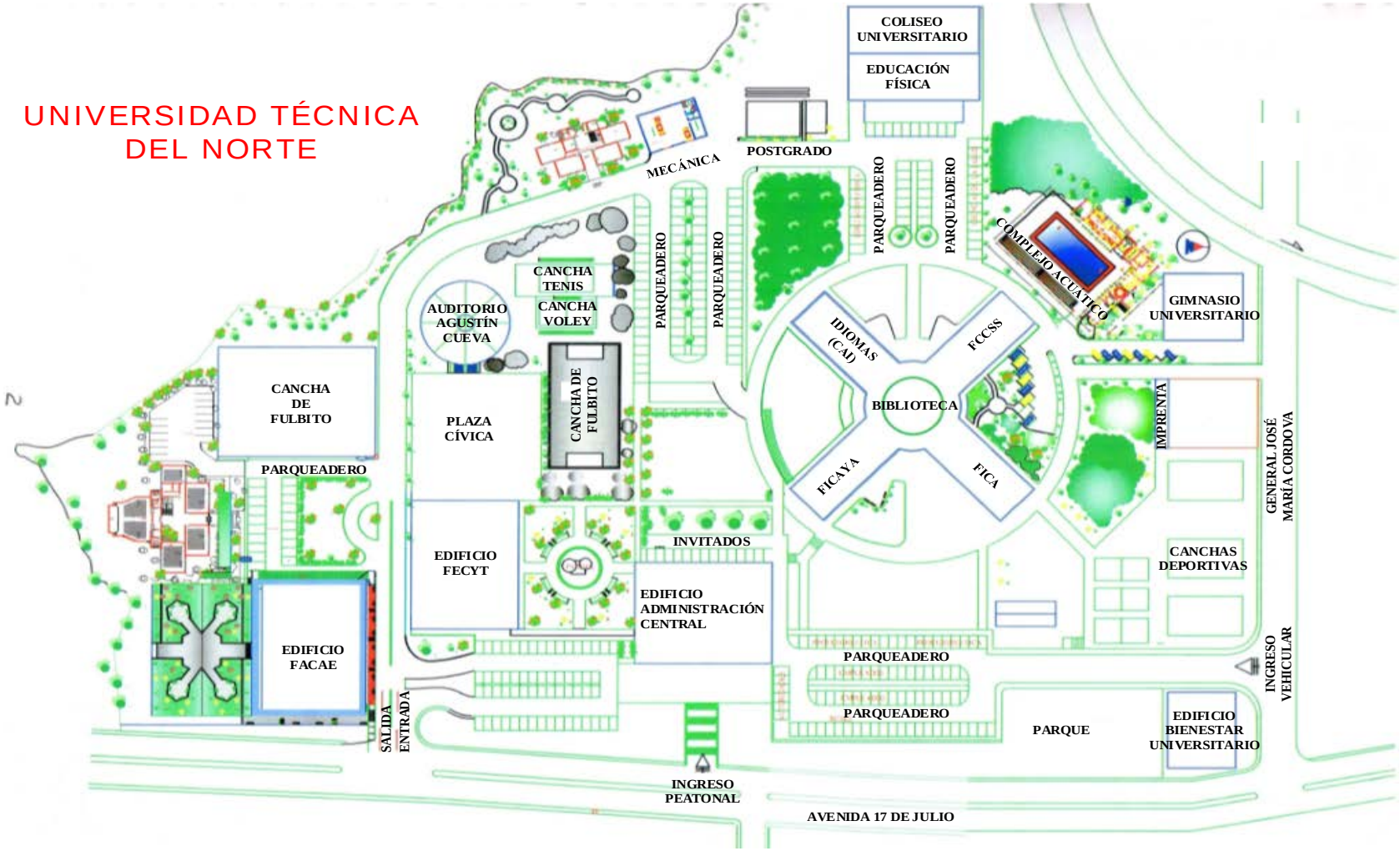


FIGURA 37 Ubicación de las Edificaciones de la UTN

Fuente: Universidad Técnica del Norte

2.2. DESCRIPCIÓN DE LA INFRAESTRUCTURA DE LA RED UTN

La Universidad Técnica del Norte ha realizado fuertes inversiones en un proceso de actualización de toda la infraestructura tecnológica que se encontraba obsoleta, lo que no permitía satisfacer las nuevas necesidades que demandaba el crecimiento de la red de datos y comunicaciones. El acceso al Internet y a los recursos de la red en toda universidad tecnológica es imprescindible, más aun al contar con más de 9000 usuarios entre estudiantes, docentes, administrativos y empleados, pertenecientes a la casona universitaria, al colegio universitario, al antiguo hospital San Vicente de Paúl y a las Granjas de Yuyucocha y la Pradera respectivamente.

2.2.1. Situación Actual de la Red

La red de la UTN como se indica en la

FIGURA **38** presenta un diseñó lógico basado en un modelo de redes jerárquicas que ha permitido una mejor administración y mayores facilidades de expansión de la red, es así que los problemas se solucionan con mayor rapidez. Según el contrato de prestación de servicios otorgado por CEDIA[132] el Ancho de Banda (AB[133]) para Internet Comercial ofertado es de 87.00 Mbps inicialmente y se incrementará a 98.00 Mbps. El proveedor proporciona un router cisco de la serie 7604 que se conecta internamente a la red de la universidad. Se implementó como protocolo de enrutamiento BGP[134] y con soporte MPBGP[135].

[132] **CEDIA** Fundación Consorcio Ecuatoriano para el Desarrollo del Internet Avanzado
[133] **AB (Ancho de Banda)** Cantidad de datos que se pueden transmitir en una unidad de tiempo.
[134] **BGP** (Border Gateway Protocol) protocolo mediante el cual se intercambia información de ruteo entre sistemas autónomos.
[135] **MPBGP** (Multiprotocol BGP) es una extensión de BGP que permite diferentes tipos de direcciones.

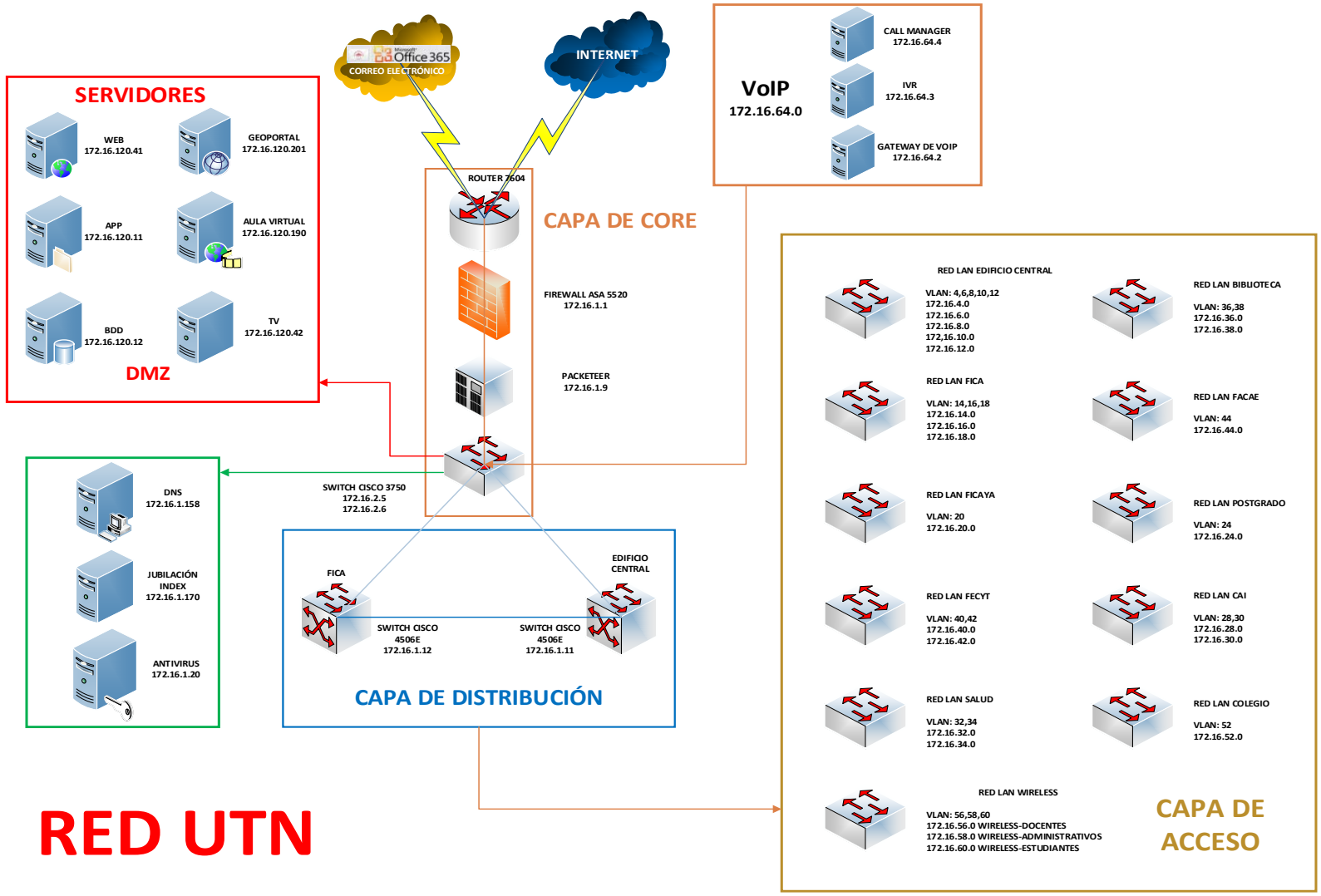


FIGURA 38 Diseño Lógico de la Red UTN

Fuente: Dirección de Desarrollo Tecnológico e Informático

El router se conecta a un Firewall ASA 5520 encargado de la seguridad de la red cuya finalidad es garantizar la confidencialidad, autenticidad, integridad de los datos y prevención de intrusos.

Actualmente la red de datos y comunicaciones está formada por 2 Switches de Core Catalyst 4506-E, que permiten administrar de mejor manera las comunicaciones garantizando el correcto funcionamiento de la red de forma constante junto con el servicio de redundancia.

Estos conmutadores de capa 3[136] tienen las siguientes ubicaciones: el primero se encuentra en la planta baja del Edificio Central en el cuarto frío dentro del Departamento de Informática y el segundo se encuentra en la Facultad de Ingeniería en Ciencias Aplicadas (FICA) en la planta 1 dentro de un pequeño cuarto de equipos.

Además de los 2 switches de core que están en la capa de distribución se dispone de 53 conmutadores adicionales en la capa de acceso ubicados dentro de las edificaciones de la universidad, a los cuales se llega con dos enlaces de fibra óptica, uno como principal y el secundario para redundancia como se muestra en la **¡Error! No se encuentra el origen de la referencia.**. Mediante enlaces de radio forman parte de la red de la UTN el Colegio Universitario, el Antiguo Hospital San Vicente de Paúl y las Granjas de Yuyucocha y la Pradera (**¡Error! No se encuentra el origen de la referencia.**), sumando 5 conmutadores en capa de acceso con un total de 58 switches.

El PacketShaper 3500 controla y administra la distribución del ancho de banda, optimizandolas aplicaciones, servicios y recursos de una red segmentada hasta 45 Mbps; además, nos permite monitorear el tráfico de entrada y salida que se genera en toda la red. Debido al crecimiento constante de la red y los altos costos de licenciamiento del equipo ha provocado bastantes problemas por el consumo inconsciente de los usuarios.

[136] **Capa 3** Se encarga de identificar el enrutamiento existente entre una o más redes.

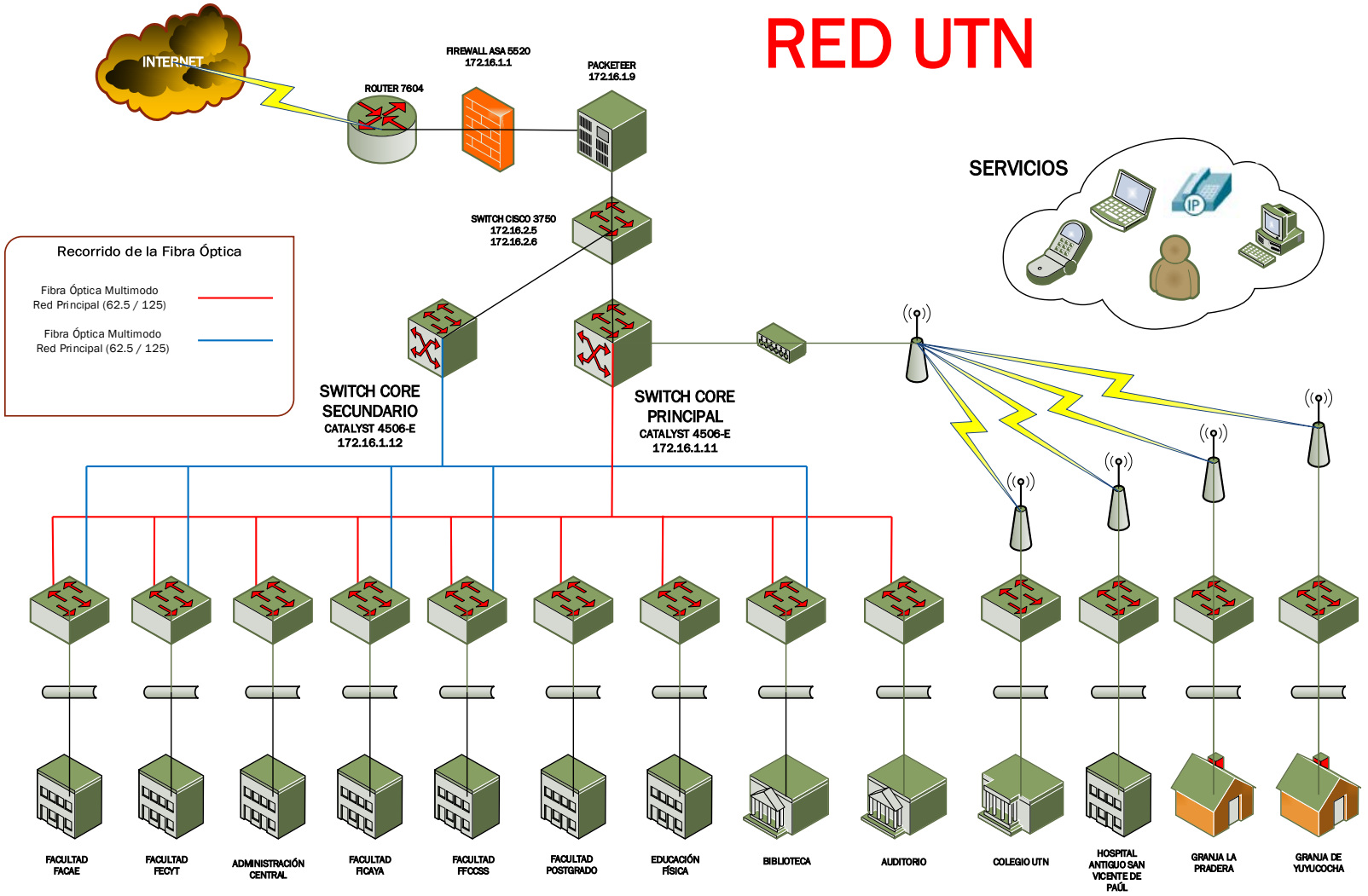


FIGURA 39 Topología Física de la Red UTN

Fuente: Dirección de Desarrollo Tecnológico e Informático

La implementación de una red de telefonía IP por medio de un Call Manager de Cisco ha permitido una adecuada organización en las comunicaciones internas, entre los diferentes departamentos y facultades de la institución utilizando la misma infraestructura de red y permitiendo reducir el costo de comunicación interna.

2.2.2. Administración de las VLANS

La segmentación con que cuenta la UTN ha mejorado significativamente la red de la misma.

El rendimiento de la red puede ser un factor en la productividad de una organización y su reputación para realizar sus transmisiones en la forma prevista. Una de las tecnologías que contribuyen al excelente rendimiento de la red es la división de los grandes dominios de broadcast en dominios más pequeños con las VLAN[137]. Los dominios de broadcast más pequeños limitan el número de dispositivos que participan en los broadcasts y permiten que los dispositivos se separen en agrupaciones funcionales, como servicios de base de datos para un departamento contable y transferencia de datos a alta velocidad para un departamento de ingeniería. (Cisco Networking Academy, 2008)

Para la creación de todas las VLANs se tomó en cuenta el peso del tráfico de cada una de las facultades y dependencias administrativas y académicas que integran el campus universitario. Las VLANs son administradas por el switch de core localizado en el cuarto frío del edificio central, el mismo que se encuentra configurado en modo de servidor VTP[138] lo que permite propagar las configuraciones de las VLAN hacia los otros switches en la red en el mismo dominio que funcionarán en modo cliente VTP (estos modos VTP solo soportan los switches de la marca cisco).

La distribución de VLANs de la red interna de la UTN está dada por subredes de clase B disponibles desde la dirección 172.16.0.0 donde de acuerdo a los requerimientos cada subred tiene la capacidad de cambiar su máscara de subred dependiendo del espacio de división entre cada una de las subredes (

TABLA 18).

[137] **VLAN** Virtual Local Area Network (Red de Área Local Virtual)
[138] **VTP** VLAN Trunk Protocol (Protocolo de Enlace Troncal VLAN)

TABLA 18 Distribución de VLANs de la Red UTN

VLAN	DESCRIPCIÓN	DIRECCIÓN DE SUBRED	MÁSCARA	UBICACIÓN
1	Servidores	172.16.1.0	255.255.255.0	Edificio Central
2	Equipos Activos	172.16.2.0	255.255.255.0	Toda la UTN
4	Financiero	172.16.4.0	255.255.255.0	Edificio Central
6	Departamento Informática	172.16.6.0	255.255.255.0	Edificio Central
7	CECI	172.16.7.0	255.255.255.0	Biblioteca
8	Autoridades	172.16.8.0	255.255.255.0	Edificio Central
10	Administrativos	172.16.10.0	255.255.255.0	Edificio Central
12	Comunicación Organizacional	172.16.12.0	255.255.255.0	Edificio Central
14	Administrativos	172.16.14.0	255.255.255.0	FICA
16	Laboratorios	172.16.16.0	255.255.254.0	FICA
18	Cisco	172.16.18.0	255.255.255.0	FICA
20	Administrativos	172.16.20.0	255.255.255.0	FICAYA
22	Laboratorios	172.16.22.0	255.255.255.0	FICAYA
24	Administrativos	172.16.24.0	255.255.255.0	POSTGRADO
26	Laboratorios	172.16.26.0	255.255.255.0	POSTGRADO
28	Administrativos	172.16.28.0	255.255.255.0	CAI
30	Laboratorios	172.16.30.0	255.255.255.0	CAI
32	Administrativos	172.16.32.0	255.255.255.0	FFCCSS
34	Estudiantes	172.16.34.0	255.255.255.0	FFCCSS
36	Administrativos	172.16.36.0	255.255.255.0	Biblioteca
38	Estudiantes	172.16.38.0	255.255.254.0	Biblioteca

40	Administrativos	172.16.40.0	255.255.255.0	FECYT - ED. FÍSICA
42	Laboratorios	172.16.42.0	255.255.255.0	FECYT
44	Administrativos	172.16.44.0	255.255.254.0	FACAE
46	Laboratorios	172.16.46.0	255.255.255.0	FACAE
48	Auditorio	172.16.48.0	255.255.255.0	Agustín Cueva
52	Administrativos	172.16.52.0	255.255.255.0	Colegio UTN
54	Laboratorios	172.16.54.0	255.255.255.0	Colegio UTN
56	Docentes	172.16.56.0	255.255.255.0	Wireless
58	Administrativos	172.16.58.0	255.255.255.0	Wireless
60	Estudiantes	172.16.60.0	255.255.254.0	Wireless
64	Telefonía IP	172.16.64.0	255.255.254.0	Toda la UTN
66	Copiadora	172.16.66.0	255.255.255.0	Edificio Central
68	Wireless	172.16.68.0	255.255.255.0	FICA
120	NAT DMZ Interno	172.16.120.0	255.255.255.0	Edificio Central
168	Banco del Pacífico	192.168.100.0	255.255.255.0	Edificio Central

Fuente: Información establecida por el Administrador de Redes y Comunicaciones de la UTN

Se cuenta con 30 IPs públicas con máscara /27[139] distribuidos para los diferentes servicios, aplicaciones y recursos que demanda la red de la universidad.

2.2.3. Monitoreo del Tráfico de Datos

El tráfico de datos que cursa por la Universidad Técnica del Norte desde sus instalaciones internas como externas, se refleja en el ancho de banda contratado con CEDIA el mismo que no se encuentra controlado y administrado, es por ello que las aplicaciones que ofrece la UTN y el consumo sin restricción alguna de los usuarios han provocado ciertas falencias en el funcionamiento de la red.

[139] **/27** Máscara 255.255.255.224

El PacketShaper debido a su limitación de poder controlar un AB de más de 45 Mbps funciona como un analizador de consumo de cada una de las VLANs pertenecientes a la red universitaria. A continuación se muestran los reportes gráficos generales del tráfico Inbound[140] y Outbound[141]:

- **Tráfico de Entrada del mes de Enero 2013**

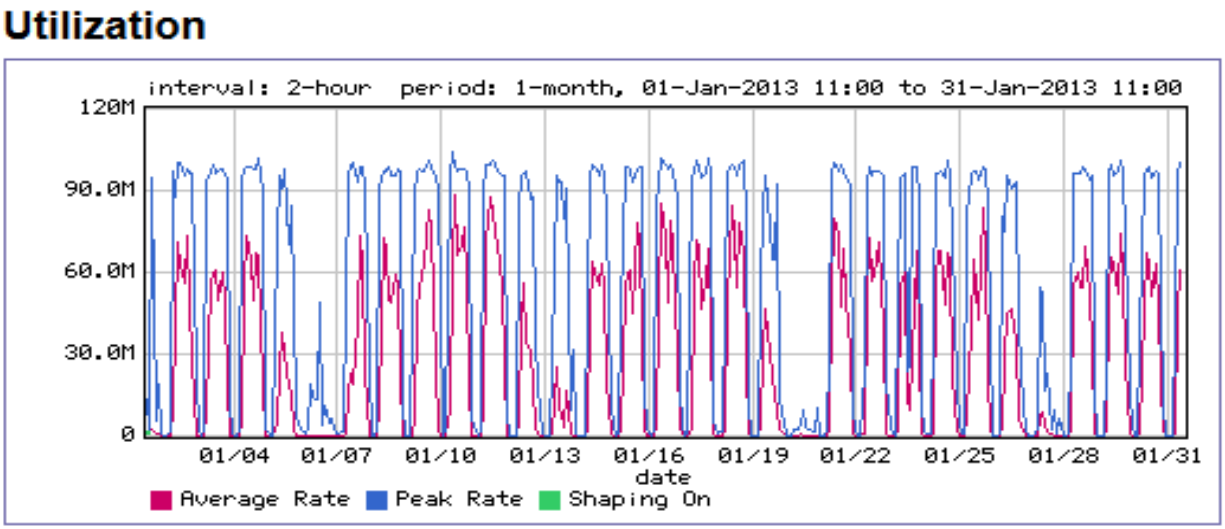


FIGURA 40 Utilización del Tráfico Inbound del mes de enero

Fuente: Reportes realizados por el controlador de ancho de banda PacketShaper 3500

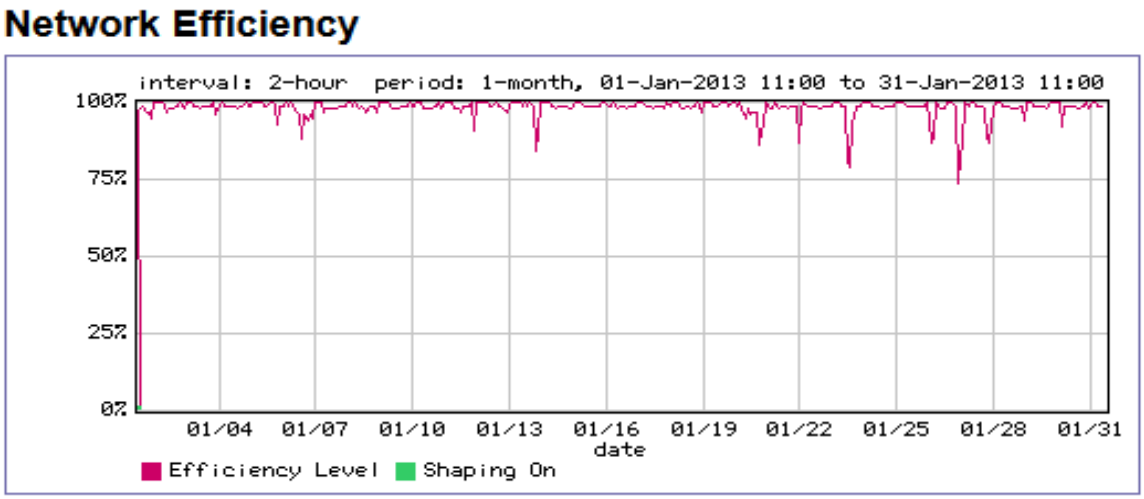


FIGURA 41 Eficiencia de Red del Tráfico Inbound del mes de enero

Fuente: Reportes realizados por el controlador de ancho de banda PacketShaper 3500

[140] **Inbound** Tráfico de entrada
[141] **Outbound** Tráfico de Salida

En el mes de enero 2013 el total de bytes recibidos es 8197.9GB, donde se tiene una capacidad de utilización:

$$Cuce = \frac{8197.9GB}{1mes} \times \frac{8bits}{1B} \times \frac{1mes}{2678400s}$$

$$Cuce = 24.48\ Mbps$$

Cuce: Capacidad de utilización del canal de entrada

- **Tráfico de Salida del mes de Enero 2013**

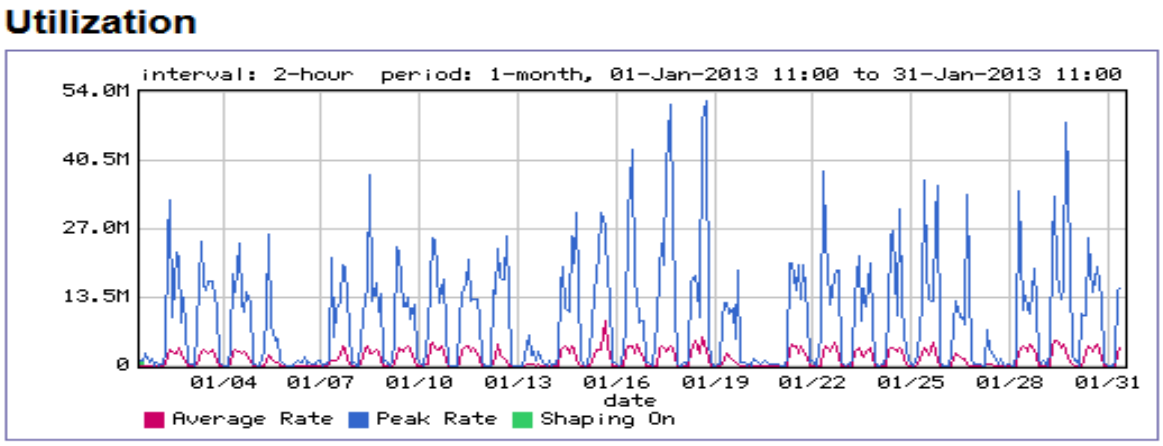


FIGURA 42 Utilización del Tráfico Outbound del mes enero

Fuente: Reportes realizados por el controlador de ancho de banda PacketShaper 3500

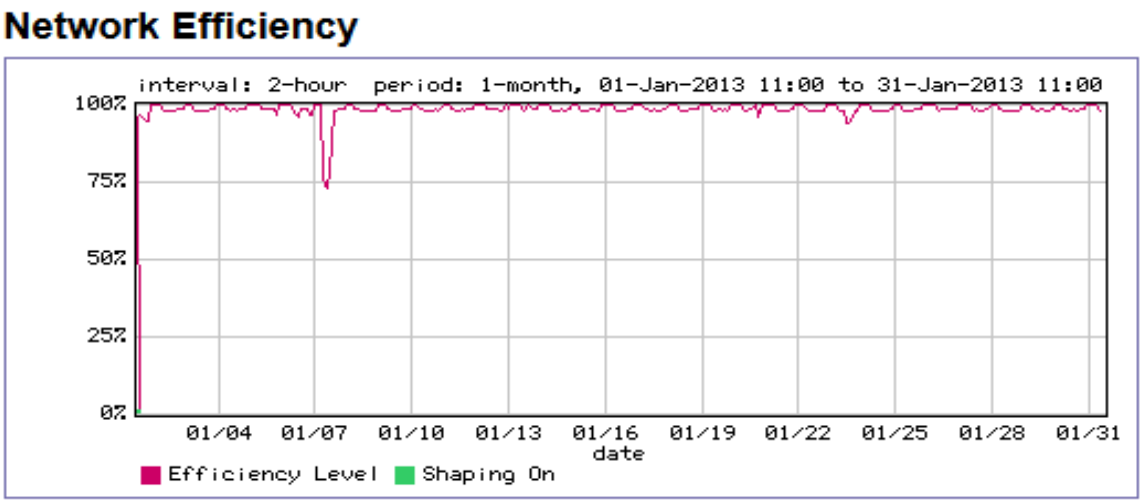


FIGURA 43 Eficiencia de Red del Tráfico Outbound del mes enero

Fuente: Reportes realizados por el controlador de ancho de banda PacketShaper 3500

En el mes de enero 2013 el total de bytes enviados es 443,8GB, donde se tiene una capacidad de utilización:

$$Cucs = \frac{443.8GB}{1mes} \times \frac{8bits}{1B} \times \frac{1mes}{2678400s}$$

$$Cucs = \ 1.32\ Mbps$$

Cucs: Capacidad de utilización del canal de salida

- **Tráfico de Entrada del mes de Febrero 2013**

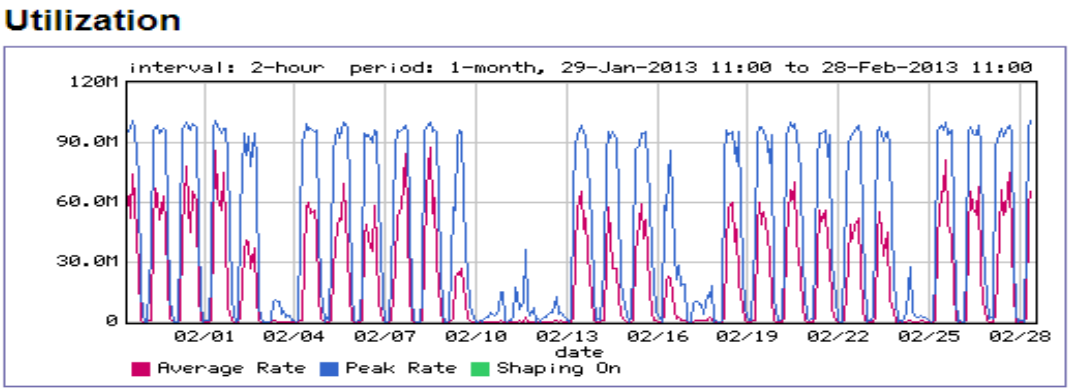


FIGURA 44 Utilización del Tráfico Inbound del mes de febrero

Fuente: Reportes realizados por el controlador de ancho de banda PacketShaper 3500

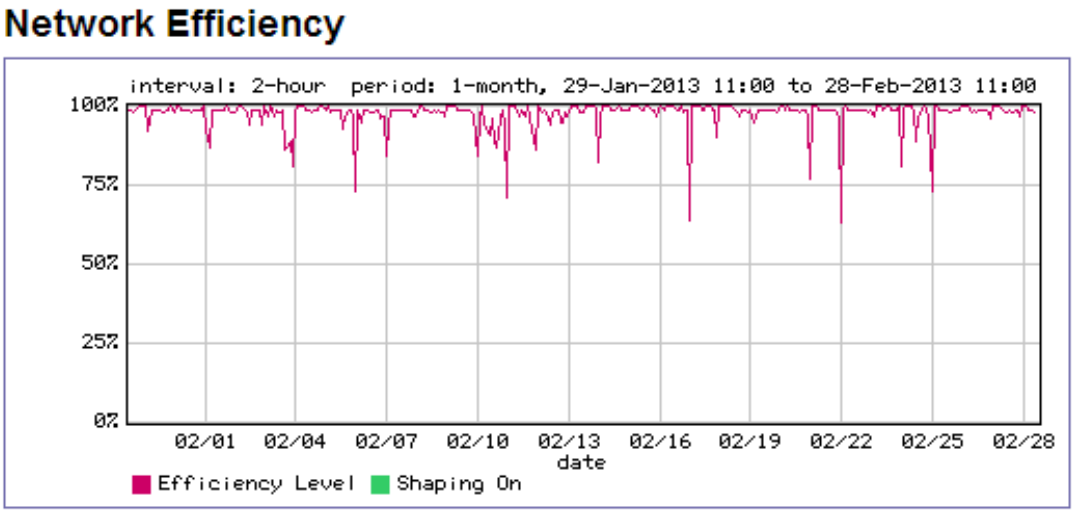


FIGURA 45 Eficiencia de Red del Tráfico Inbound del mes febrero

Fuente: Reportes realizados por el controlador de ancho de banda PacketShaper 3500

En el mes de febrero 2013 el total de bytes recibidos es 6280.1GB, donde se tiene una capacidad de utilización:

$$Cuce = \frac{6280.1GB}{1mes} \times \frac{8bits}{1B} \times \frac{1mes}{2678400s}$$

$$Cuce = \ 18.76\ Mbps$$

Cuce: Capacidad de utilización del canal de entrada

- **Tráfico de Salida del mes de Febrero 2013**

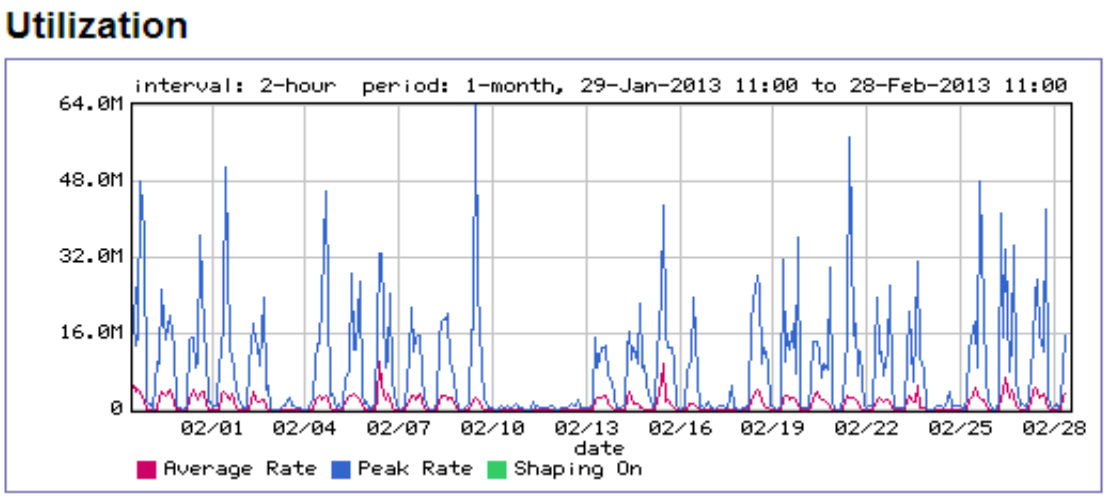


FIGURA 46 Utilización del Tráfico Outbound del mes febrero

Fuente: Reportes realizados por el controlador de ancho de banda PacketShaper 3500

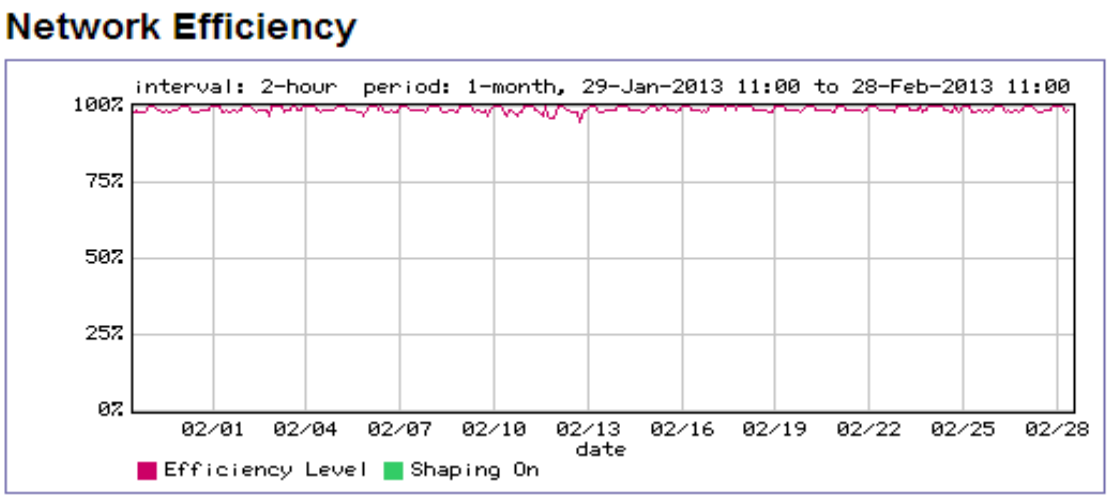


FIGURA 47 Eficiencia de Red del Tráfico Outbound del mes de febrero

Fuente: Reportes realizados por el controlador de ancho de banda PacketShaper 3500

En el mes de febrero 2013 el total de bytes enviados es 360.1GB, donde se tiene una capacidad de utilización:

$$Cucs = \frac{360.1GB}{1mes} \times \frac{8bits}{1B} \times \frac{1mes}{2678400s}$$

$$Cucs = \ 1.07\ Mbps$$

Cucs: Capacidad de utilización del canal de salida

2.2.4. Servicios de la Red

Algunos de los componentes se encuentran funcionando al servicio de la Universidad y de sus usuarios internos y externos, otros trabajan a prueba, mientras algunos más, se encuentran en proceso de implementación y son los siguientes:

- Sistema de Información Integrado
  - Módulo de Gestión Académica
  - Módulo de Gestión Presupuestaria
  - Módulo de Adquisiciones
  - Módulo de Activos Fijos
  - Módulo de Inventarios
  - Módulo de Gestión de Clientes
  - Módulo de Gestión de Proveedores
  - Módulo de Tesorería y Bancos
  - Módulo de Anexos del SRI
  - Módulo de Contabilidad Gerencial
  - Módulo de Planeamiento y Evaluación Integral
  - Módulo de Inventario de Hardware y Software
  - Módulo de Costeo Basado en Actividades
  - Módulo de Gestión Bibliotecaria
  - Módulo de Gestión de Órganos Colegiados y Normativa Universitaria
  - Módulo de Gestión del Talento Humano
  - Módulo de Vinculación con la Colectividad
  - Módulo de Evaluación Integral Universitaria
  - Módulo de Gestión en las Recaudaciones Arancelarias
  - Módulo de Auditoría de Bases de Datos
  - Módulo de Seguridades

- Módulo de Gestión de Vehículos
- Módulo de Nómina
- Módulo de Bienestar Universitario

  - Submódulo de Gestión Médica
  - Submódulo de Gestión Odontológica
  - Submódulo de Laboratorio Clínico

- Gestión de Infraestructura Tecnológica, Redes y Comunicaciones
- Gestión de Correos Electrónicos
- Gestión de Aulas Virtuales
- Gestión de Zonas Wi-fi y Autentificación de usuarios Inalámbricos
- Gestión de Operación y Control de Infraestructura Tecnológica
- Repositorio Digital Institucional
- Implantación de Nuevas Tecnologías de Información y Comunicación (TICs)
- Inteligencia de Negocios

2.3. DESCRIPCIÓN DE LA INFRAESTRUCTURA DE LA RED LAN INALÁMBRICA UTN

La Universidad Técnica del Norte actualmente cuenta con una red LAN Inalámbrica de poco alcance que no abastece a cubrir todo el campus universitario y todo lo que implica la gestión de áreas académicas como aulas, asociaci ones estudiantiles, biblioteca, etc.

El equipo que se encarga de la administración de la red inalámbrica es un Cisco 5500 Series Wireless Controller modelo 5508, mediante el cual se enganchan los Access Points en modo lightweight[142] con toda la información de configuración mantenida dentro del WLC[143].

2.3.1. Ubicación de los Access Point

El campus universitario consta de varias edificaciones, en la figura se determina las áreas de cobertura y la ubicación de cada AP. En la siguiente TABLA 19, se detalla el lugar con el equipo y antenas respectivas (omnidireccionales y sectoriales).

---

[142] **Lightweight** Los AP en este modo de configuración funcionan en conjunción con un Cisco Wireless LAN Controller

[143] **WLC** Wireless LAN Controller

TABLA 19 Información actual de los Access Points de la WLAN UTN

NOMBRE DEL EQUIPO	PRODUCT ID	MAC ADDRESS	TIPO DE ANTENA	UBICACIÓN
WLC-UTN	AIR-CT5508-K9	50:3d:e5:19:ac:80	-	Planta Central
AP-UTN-FICA	AIR-BR1310GA-K9-R	00:21:d8:f6:1e:80	Omnidireccional 15 dBi	Terraza FICA
AP-UTN-POSTGRADO	AIR-BR1310GA-K9-R	00:22:90:72:65:98	Omnidireccional 15 dBi	Terraza Postgrado
AP-UTN-BIBLIOTECA	AIR-BR1310GA-K9-R	00:22:90:72:65:58	Sectorial 120, 14 dBi	Biblioteca UTN
AP-UTN-AUDITORIO	AIR-BR1310GA-K9-R	00:21:d8:f6:1e:60	Sectorial 120, 14 dBi	Terraza Auditorio
AP-UTN-EDFISICA	AIR-BR1310GA-K9-R	00:23:04:ef:93:84	Sectorial 120, 14 dBi	Terraza Educación Física
AP-UTN-CENTRAL	AIR-BR1310GA-K9-R	00:23:33:95:32:ec	Omnidireccional 15 dBi	Terraza Planta Central
AP-UTN-FACAE	AIR-BR1310GA-K9-R	00:21:d8:f6:18:56	Omnidireccional 15 dBi	Terraza FACAE
AP-UTN-ENTRADA	AIR-BR1310GA-K9-R	00:21:d8:f6:1e:a2	Sectorial 120, 14 dBi	Entrada Norte UTN
AP-UTN-FECYT	AIR-BR1310GA-K9-R	00:22:90:12:25:b2	Omnidireccional 15 dBi	Terraza FECYT

Fuente: Información establecida por el equipo WLC y el Administrador de Redes y Comunicaciones de la UTN

En el WLC se instaló la versión de software 6.0.199.4 la misma que se cargó a los diferentes APs en modo de configuración lightweight. A continuación se muestra en la TABLA 20 la siguiente información real con dos de los APs en estado down que se encontraban sin funcionar en el estudio de la situación actual de la red inalámbrica:

TABLA 20 Versión y Estado de los APs

NOMBRE DEL EQUIPO	SOFTWARE VERSION	IOS VERSION	STATUS
WLC-UTN	6.0.199.4	-	UP
AP-UTN-FICA	6.0.199.4	12.4(21a)JHB1	DOWN
AP-UTN-POSTGRADO	6.0.199.4	12.4(21a)JHB1	UP
AP-UTN-BIBLIOTECA	6.0.199.4	12.4(21a)JHB1	UP
AP-UTN-AUDITORIO	6.0.199.4	12.4(21a)JHB1	UP
AP-UTN-EDFISICA	6.0.199.4	12.4(21a)JHB1	UP
AP-UTN-CENTRAL	6.0.199.4	12.4(21a)JHB1	UP
AP-UTN-FACAE	6.0.199.4	12.4(21a)JHB1	UP
AP-UTN-ENTRADA	6.0.199.4	12.4(21a)JHB1	DOWN
AP-UTN-FECYT	6.0.199.4	12.4(21a)JHB1	UP

Fuente: Información establecida por el equipo WLC

2.3.2. Cobertura de la Red LAN Inalámbrica

En el estudio realizado de la situación actual, la cobertura en todo el campus universitario es deficiente, donde cada uno de los APs se encuentran ubicados en lugares específicos tal como se indica en la TABLA 19 que no abastecen del servicio de Internet a los usuarios pertenecientes a la institución.

Los APs que utilizan antenas omnidireccionales, los cuales están ubicados en las edificaciones de: Planta Central, FACAE, FECYT, POSTGRADO y FICA; no tienen una amplia cobertura y es por ello que no se podría garantizar el área descrita por la **¡Error! No se encuentra el origen de la referencia.**. Con respecto al AP cuya ubicación es en el Auditorio Agustín Cueva, cubrirá unas pocas áreas que dejan con una mínima señal los APs vecinos.

De igual manera, se puede decir que los APs que utilizan las antenas sectoriales tienen un área de cobertura menor a 120° dependiendo del posicionamiento de la antena (horizontal o vertical), los mismos que están ubicados en: las Canchas de la Entrada UTN, Auditorio Agustín Cueva, Educación Física, entre POSTGRADO-FICAYA (Biblioteca) como se describe el área de cobertura en la **¡Error! No se encuentra el origen de la referencia.**.

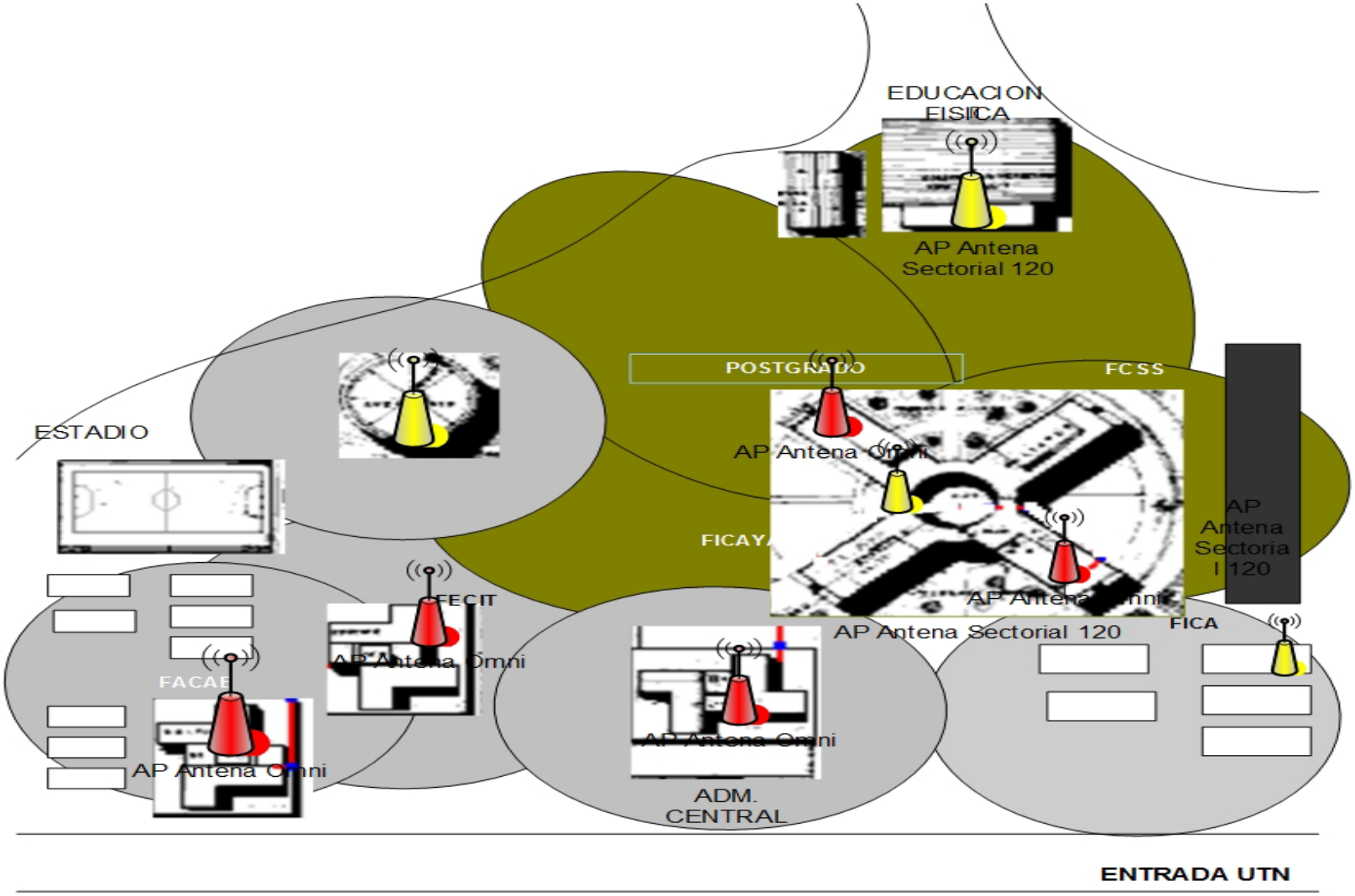


FIGURA 48 Esquema general actual de la cobertura de la red WLAN UTN

Fuente: Información establecida por el Administrador de Redes y Comunicaciones de la

2.3.3. Direccionamiento de la Red LAN Inalámbrica

Los equipos activos que funcionan para la red inalámbrica se encuentran en una misma VLAN, el WLC permite configurar uno o varios SSIDs creando interfaces de VLANs diferentes para poder propagarlas en la red WLAN UTN.

En la TABLA 21 se detalla a parte del direccionamiento IP que incluye máscara, Gateway y el canal mediante el cual se encuentran propagando las redes inalámbricas cada AP.

TABLA 21 Direccionamiento de la Red LAN Inalámbrica

NOMBRE DEL EQUIPO	IP ESTÁTICA	MÁSCARA	GATEWAY	CANAL
WLC-UTN	172.16.2.100	255.255.255.0	172.16.2.1	-
AP-UTN-FICA	172.16.2.101	255.255.255.0	172.16.2.1	6
AP-UTN-POSTGRADO	172.16.2.102	255.255.255.0	172.16.2.1	1
AP-UTN-BIBLIOTECA	172.16.2.103	255.255.255.0	172.16.2.1	6
AP-UTN-AUDITORIO	172.16.2.104	255.255.255.0	172.16.2.1	11
AP-UTN-EDFISICA	172.16.2.105	255.255.255.0	172.16.2.1	1
AP-UTN-CENTRAL	172.16.2.106	255.255.255.0	172.16.2.1	6
AP-UTN-FACAE	172.16.2.107	255.255.255.0	172.16.2.1	11
AP-UTN-ENTRADA	172.16.2.108	255.255.255.0	172.16.2.1	1
AP-UTN-FECYT	172.16.2.109	255.255.255.0	172.16.2.1	6

Fuente: Información establecida por el equipo WLC

El controlador de la red inalámbrica tiene configurado tres nombres de perfiles de WLAN SSID (TABLA 22); uno para docentes, otro para administrativos y por último para estudiantes. No se maneja ninguna política de seguridad por el momento, el acceso es totalmente libre.

TABLA 22 SSIDs actual de la WUTN

WLAN ID	PROFILE NAME	WLAN SSID	ADMIN STATUS	SECURITY POLICIES
1	Docentes UTN	WUTN.Docentes	Enabled	None
2	Administrativos UTN	WUTN.Admin	Enabled	None
3	Estudiantes UTN	WUTN.Estudiantes	Enabled	None

Fuente: Información establecida por el equipo WLC

2.4. PROBLEMAS DE LA RED ACTUAL UTN

Una de las razones más populares de las redes WLAN es el acceso sin necesidad de cables, pero a la vez es el problema más grande si nos referimos a la seguridad donde cualquier dispositivo inalámbrico que capte la señal del AP, tendrá la posibilidad de navegar gratis en la Internet, emplear la red como punto de ataque hacia otras redes y luego desconectarse para no ser detectado, robar software o información e introducir virus o software maligno.

Las ondas de radio que generan los puntos de acceso pueden salir fuera del área del campus universitario en el que cualquier persona que posea un equipo móvil y entre en la zona de cobertura podría conectarse a la red inalámbrica.

El consumo de ancho de banda juega un papel importante, debido a que el hardware PacketShaper por su licencia obsoleta no permite tener un control sofisticado del AB, por ello cabe destacar que el crecimiento de la red institucional ha aumentado significativamente en cuanto a sus aplicaciones y servicios.

2.5. REQUERIMIENTOS

En base al estudio de la situación actual de la red inalámbrica de la UTN surgieron algunos requerimientos que serán muy importantes para el diseño de la misma, los cuales se indican a continuación:

- Un mayor número de APs para llegar a zonas donde la red inalámbrica actual no abastece a cubrir ciertas áreas de cobertura.
- Control de acceso de los usuarios lo que dará mayor seguridad a la red ante cualquier tipo de infiltraciones maliciosas, ataques Man-in-the-Middle[144], etc.
- Gestión de los Servicios.
- Roaming que se refiere al cambio de conexión que ejecuta un usuario en movimiento entre dos coordinadores de red inalámbricos.
- Control de ancho de banda.

[144] **Man-in-the-Middle** Método por el cual el atacante solo necesita situarse en medio de las dos partes que intentan comunicarse, interceptando los mensajes enviados e imitando al menos a una de ellas.

CAPITULO III

3. DISEÑO DE LA INFRAESTRUCTURA DE MOVILIDAD DE LA RED LAN INALÁMBRICA PARA LA UNIVERSIDAD TÉCNICA DEL NORTE

Se diseñó la red LAN Inalámbrica de acuerdo al análisis estudiado de frecuencias, canales de operación, ubicación de los Access Points (AP), área de cobertura de los APs en todo el campus de la UTN y en cada una de las facultades como también el dimensionamiento del AAA y el portal cautivo.

3.1. REQUERIMIENTOS DEL DISEÑO

Se debe tomar en cuenta ciertas consideraciones en el diseño de una red inalámbrica encargada de proveer servicio de Internet a un determinado número de usuarios, los mismos que pertenecen a la universidad desenvolviéndose en diferentes cargos como son: autoridades, administrativos, docentes y estudiantes.

El presente diseño debe satisfacer las necesidades de conectividad desde el campus universitario que como ente educativo requiere para mejorar el aprendizaje y la enseñanza de sus catedráticos a sus alumnos.

El diseño debe garantizar ciertos parámetros importantes los cuales se enuncian a continuación:

- Disponibilidad
- Escalabilidad
- Confiabilidad
- Seguridad
- Interoperabilidad
- Número de Usuarios
- Autenticación de Usuarios
- Disponibilidad de Ancho de banda
- Gestión y Administración centralizada
- Movilidad

3.2. TECNOLOGÍA DE LA RED INALÁMBRICA

Existen varias tecnologías que son utilizadas en redes inalámbricas, el empleo de cada una de ellas depende mucho de la aplicación. Una WLAN permite que los usuarios terminales que se encuentran dentro del área de cobertura puedan conectarse entre sí.

La tecnología a utilizar en el presente diseño lleva el nombre de Wi-Fi o IEEE 802.11 con el respaldo de WECA[145], ofreciendo una velocidad máxima de 54 Mbps y capaz de soportar los siguientes estándares IEEE 802.11a, b, g y n.

Las estaciones inalámbricas y los equipos terminales trabajan en las banda de frecuencia a 2.4 GHz y 5.8 GHz en nuestro país, motivo por el cual el uso de estas frecuencias del espectro radioeléctrico no tienen ningún costo de licenciamiento y tienen la capacidad de integrarse fácilmente a una red cableada.

[145] **WECA** Wireless Ethernet Compatibility Alliance

3.3. DISEÑO DE MODELO JERÁRQUICO

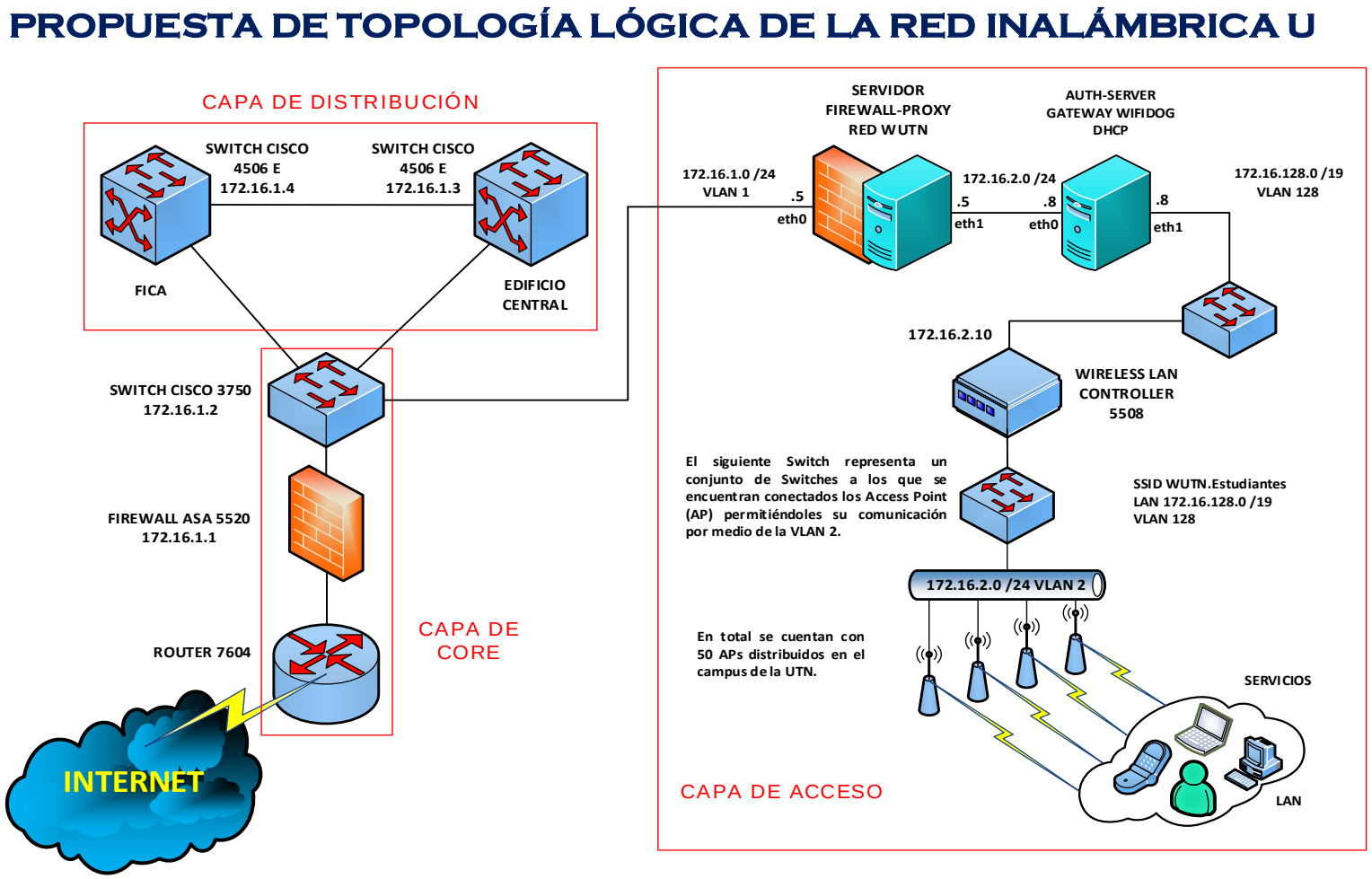


FIGURA 49 Diseño de Modelo Jerárquico Red Inalámbrica UTN

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

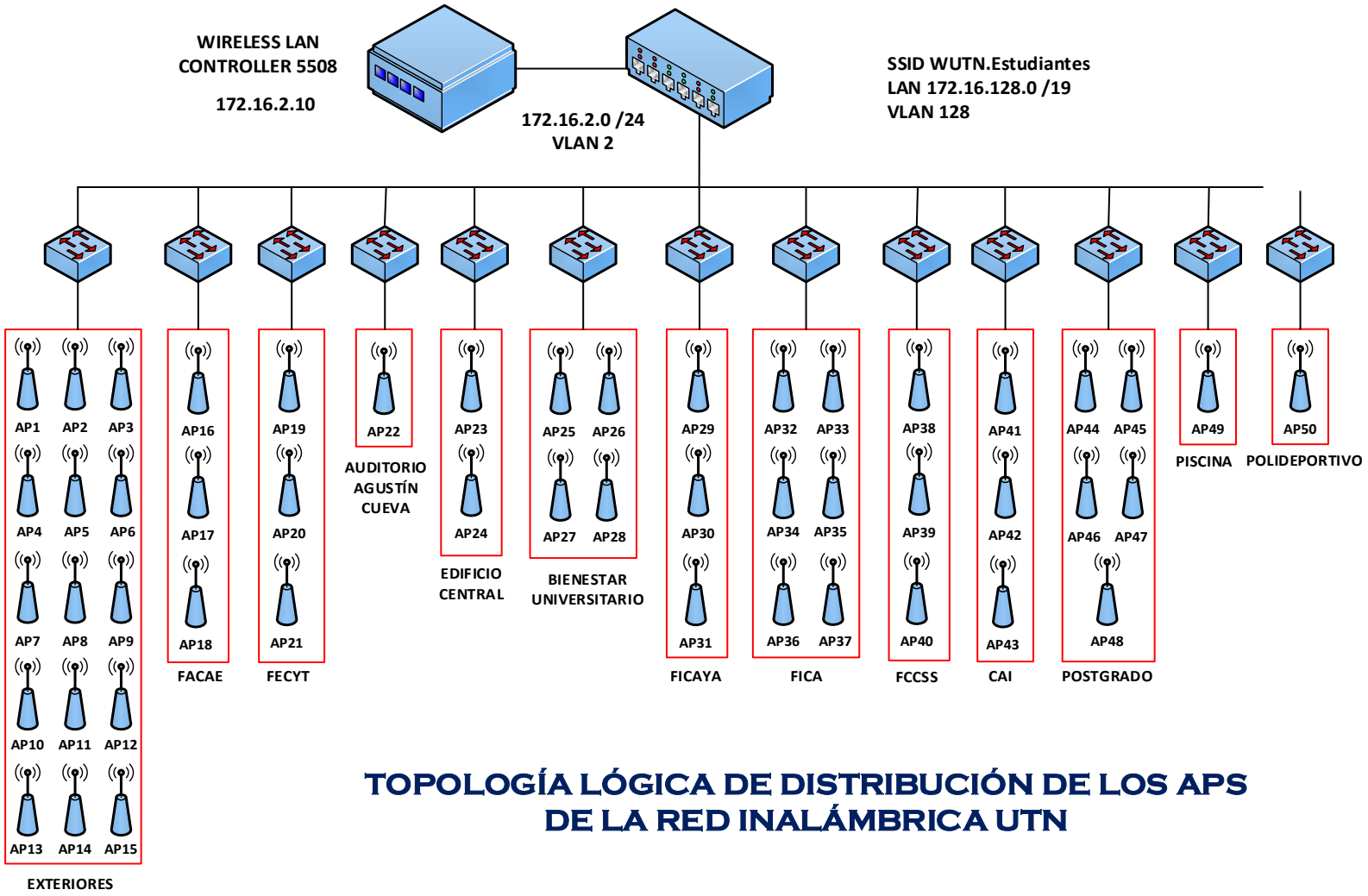


FIGURA 50 Diseño Lógico de Distribución de los APs de la Red Inalámbrica UTN

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.4. DIRECCIONAMIENTO DE LA RED

De acuerdo al estudio y diseño realizado se ha optado porque el direccionamiento de los equipos activos de la red inalámbrica (APs y WLC) se encuentre dentro de una misma VLAN tal como se tenía en su funcionamiento actual.

3.4.1. Direccionamiento IP APs de Exteriores (OUTDOOR AP 1310G)

TABLA 23 Direccionamiento de APs de Exteriores WUTN

# AP	NOMBRE	UBICACIÓN	IP ESTÁTICA	MÁSCARA	GATEWAY
AP1	AP-UTN-FICA-FICAYA	Terraza entre FICA - FICAYA	172.16.2.80	255.255.255.0	172.16.2.1
AP2	AP-UTN-CAI-FICAYA	Terraza entre CAI-FICAYA	172.16.2.81	255.255.255.0	172.16.2.1
AP3	AP-UTN-FICA-FFCCSS	Terraza entre FICA - FFCCSS	172.16.2.82	255.255.255.0	172.16.2.1
AP4	AP-UTN-EDFISICA	Este - Instituto Educación Física	172.16.2.83	255.255.255.0	172.16.2.1
AP5	AP-UTN-ESTE-AUDITORIO	Este - Auditorio Agustín Cueva	172.16.2.84	255.255.255.0	172.16.2.1
AP6	AP-UTN-NORTE-AUDITORIO	Norte - Auditorio Agustín Cueva	172.16.2.85	255.255.255.0	172.16.2.1
AP7	AP-UTN-SUR-CENTRAL	Terraza Planta Central Sur	172.16.2.86	255.255.255.0	172.16.2.1
AP8	AP-UTN-NORTE-CENTRAL	Terraza Planta Central Norte	172.16.2.87	255.255.255.0	172.16.2.1

AP9	AP-UTN-CAI-TERRAZA	Terraza CAI	172.16.2.88	255.255.255.0	172.16.2.1
AP10	AP-UTN-SUR-FACAE	Terraza Planta 1 Sur FACAE	172.16.2.89	255.255.255.0	172.16.2.1
AP11	AP-UTN-NORTE-FACAE	Terraza Planta 1 Norte FACAE	172.16.2.90	255.255.255.0	172.16.2.1
AP12	AP-UTN-FECYT	Terraza Planta 1 NorEste FECYT	172.16.2.91	255.255.255.0	172.16.2.1
AP13	AP-UTN-OESTE-CENTRAL	Terraza Planta 1 Oeste Edificio Central	172.16.2.92	255.255.255.0	172.16.2.1
AP14	AP-UTN-NORTE-ENTRADA	Entrada Norte	172.16.2.93	255.255.255.0	172.16.2.1
AP15	AP-UTN-PISCINA	Exterior Complejo Acuático	172.16.2.94	255.255.255.0	172.16.2.1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.4.2. Direccionamiento IP APs de Interiores FACAE (INDOOR AP 1262N)

Tabla 24 Direccionamiento de APs de Interiores FACAE WUTN

# AP	NOMBRE	UBICACIÓN	IP ESTÁTICA	MÁSCARA	GATEWAY
AP16	AP-FACAE-PA1	Planta Alta 1 FACAE	172.16.2.100	255.255.255.0	172.16.2.1
AP17	AP-FACAE-PA2	Planta Alta 2 FACAE	172.16.2.101	255.255.255.0	172.16.2.1
AP18	AP-FACAE-PA3	Planta Alta 3 FACAE	172.16.2.102	255.255.255.0	172.16.2.1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.4.3. Direccionamiento IP APs de Interiores FECYT (INDOOR AP 1262N)

TABLA 25 Direccionamiento de APs de Interiores FECYT WUTN

# AP	NOMBRE	UBICACIÓN	IP ESTÁTICA	MÁSCARA	GATEWAY
AP19	AP-FECYT-PA1	Planta Alta 1 FECYT	172.16.2.110	255.255.255.0	172.16.2.1
AP20	AP-FECYT-PA2	Planta Alta 2 FECYT	172.16.2.111	255.255.255.0	172.16.2.1
AP21	AP-FECYT-PA3	Planta Alta 3 FECYT	172.16.2.112	255.255.255.0	172.16.2.1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.4.4. Direccionamiento IP APs de Interiores Agustín Cueva (INDOOR AP 1262N)

TABLA 26 Direccionamiento de APs de Interiores Agustín Cueva WUTN

# AP	NOMBRE	UBICACIÓN	IP ESTÁTICA	MÁSCARA	GATEWAY
AP22	AP-AUDITORIO-INTERIOR	Auditorio Agustín Cueva Interior	172.16.2.120	255.255.255.0	172.16.2.1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.4.5. Direccionamiento IP APs de Interiores Edificio Central (INDOOR AP 1262N)

TABLA 27 Direccionamiento de APs de Interiores Edificio Central WUTN

# AP	NOMBRE	UBICACIÓN	IP ESTÁTICA	MÁSCARA	GATEWAY
AP23	AP-CENTRAL-PB	Planta Baja Edificio Central	172.16.2.130	255.255.255.0	172.16.2.1
AP24	AP-CENTRAL-PA2	Planta Alta 2 Edificio Central	172.16.2.131	255.255.255.0	172.16.2.1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.4.6. Direccionamiento IP APs de Interiores Edificio Bienestar (INDOOR AP 1262N)

Tabla 28 Direccionamiento de APs de Interiores Edificio Bienestar WUTN

# AP	NOMBRE	UBICACIÓN	IP ESTÁTICA	MÁSCARA	GATEWAY
AP25	AP-BIENESTAR-PB	Planta Baja BIENESTAR	172.16.2.140	255.255.255.0	172.16.2.1
AP26	AP-BIENESTAR-PA1	Planta Alta 1 BIENESTAR	172.16.2.141	255.255.255.0	172.16.2.1
AP27	AP-BIENESTAR-PA2	Planta Alta 2 BIENESTAR	172.16.2.142	255.255.255.0	172.16.2.1
AP28	AP-BIENESTAR-PA3	Planta Alta 3 BIENESTAR	172.16.2.143	255.255.255.0	172.16.2.1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.4.7. Direccionamiento IP APs de Interiores FICAYA (INDOOR AP 1262N)

TABLA 29 Direccionamiento de APs de Interiores FICAYA WUTN

# AP	NOMBRE	UBICACIÓN	IP ESTÁTICA	MÁSCARA	GATEWAY
AP29	AP-FICAYA-PA1	Planta Alta 1 FICAYA	172.16.2.150	255.255.255.0	172.16.2.1
AP30	AP-FICAYA-PA2	Planta Alta 2 FICAYA	172.16.2.151	255.255.255.0	172.16.2.1
AP31	AP-FICAYA-PA3	Planta Alta 3 FICAYA	172.16.2.152	255.255.255.0	172.16.2.1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.4.8. Direccionamiento IP APs de Interiores FICA (INDOOR AP 1131AG)

TABLA 30 Direccionamiento de APs de Interiores FICA WUTN

# AP	NOMBRE	UBICACIÓN	IP ESTÁTICA	MÁSCARA	GATEWAY
AP32	AP-FICA-PB	Planta Baja FICA	172.16.2.160	255.255.255.0	172.16.2.1
AP33	AP-FICA-PA2D	Planta Alta 2 Derecha FICA	172.16.2.161	255.255.255.0	172.16.2.1
AP34	AP-FICA-PA2I	Planta Alta 2 Izquierda FICA	172.16.2.162	255.255.255.0	172.16.2.1
AP35	AP-FICA-PA3D	Planta Alta 3 Derecha FICA	172.16.2.163	255.255.255.0	172.16.2.1
AP36	AP-FICA-PA3I	Planta Alta 3 Izquierda FICA	172.16.2.164	255.255.255.0	172.16.2.1
AP37	AP-FICA-PA4	Planta Alta 4 FICA	172.16.2.165	255.255.255.0	172.16.2.1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.4.9. Direccionamiento IP APs de Interiores FCCSS (INDOOR AP 1262N)

Tabla 31 Direccionamiento de APs de Interiores FCCSS WUTN

# AP	NOMBRE	UBICACIÓN	IP ESTÁTICA	MÁSCARA	GATEWAY
AP38	AP-FCCSS-PA1	Planta Alta 1 FCCSS	172.16.2.170	255.255.255.0	172.16.2.1
AP39	AP-FCCSS-PA2	Planta Alta 2 FCCSS	172.16.2.171	255.255.255.0	172.16.2.1
AP40	AP-FCCSS-PA3	Planta Alta 3 FCCSS	172.16.2.172	255.255.255.0	172.16.2.1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.4.10. Direccionamiento IP APs de Interiores CAI (INDOOR AP 1262N)

TABLA 32 Direccionamiento de APs de Interiores CAI WUTN

# AP	NOMBRE	UBICACIÓN	IP ESTÁTICA	MÁSCARA	GATEWAY
AP41	AP-CAI-PA1	Planta Alta 1 CAI	172.16.2.180	255.255.255.0	172.16.2.1
AP42	AP-CAI-PA2	Planta Alta 2 CAI	172.16.2.181	255.255.255.0	172.16.2.1
AP43	AP-CAI-PA3	Planta Alta 3 CAI	172.16.2.182	255.255.255.0	172.16.2.1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.4.11. Direccionamiento IP APs de Interiores POSTGRADO (INDOOR AP 1262N)

Tabla 33 Direccionamiento de APs de Interiores POSTGRADO WUTN

# AP	NOMBRE	UBICACIÓN	IP ESTÁTICA	MÁSCARA	GATEWAY
AP44	**AP-POSTGRADO-PB1**	Planta Baja POSTGRADO Cubículos	172.16.2.190	255.255.255.0	172.16.2.1
AP45	**AP-POSTGRADO-PB2**	Planta Baja POSTGRADO	172.16.2.191	255.255.255.0	172.16.2.1
AP46	**AP-POSTGRADO-PB-AUDITORIO**	Planta Baja Auditorio POSTGRADO	172.16.2.192	255.255.255.0	172.16.2.1
AP47	**AP-POSTGRADO-PA1**	Planta Alta 1 POSTGRADO	172.16.2.193	255.255.255.0	172.16.2.1
AP48	**AP-POSTGRADO-PA2**	Planta Alta 2 POSTGRADO	172.16.2.194	255.255.255.0	172.16.2.1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.4.12. Direccionamiento IP APs de Interiores Complejo Acuático (INDOOR AP 62N)

Tabla 34 Direccionamiento de APs de Interiores Complejo Acuático WUTN

# AP	NOMBRE	UBICACIÓN	IP ESTÁTICA	MÁSCARA	GATEWAY
AP49	AP-PISCINA-INTERIOR	Interior Complejo Acuático	172.16.2.200	255.255.255.0	172.16.2.1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.4.13. Direccionamiento IP APs de Interiores POLIDEPORTIVO (INDOOR AP 1262N)

Tabla 35 Direccionamiento de APs de Interiores POLIDEPORTIVO WUTN

# AP	NOMBRE	UBICACIÓN	IP ESTÁTICA	MÁSCARA	GATEWAY
AP50	AP-POLIDEPORTIVO	Polideportivo UTN	172.16.2.210	255.255.255.0	172.16.2.1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.5. ANÁLISIS DE ESCALABILIDAD DE LA RED

Las prestaciones de la red de la Universidad Técnica del Norte son bien estructuradas debido a su capacidad de adaptarse al medio y acoplarse a nuevos requerimientos en cuanto a estándares y nuevas tecnologías.

Uno de los grandes beneficios de las redes inalámbricas es la escalabilidad que tienen por ciertos factores como son:

- El incremento de ancho de banda suficiente para brindar servicios a un determinado número de usuarios.
- El incremento de la zona de cobertura que dependería de la potencia de señal que tengan los APs o posiblemente en la instalación de más APs que puedan cubrir ciertos lugares donde se pierde señal.

Uno de los inconvenientes por resolver sigue siendo la limitación del espectro de radiofrecuencia que en muchas situaciones ocasiona pérdidas de la señal por interferencias producidas en los sectores que se tienen instalados los APs.

De acuerdo a la propuesta de diseño que se plantea se requiere que conforme incremente el número de usuarios y el área de cobertura de la red, se tendrá que aumentar cierto número de APs tomando en cuenta la licencia del Wireless LAN Controller y el máximo de APs que nos permite controlar este equipo.

3.6. DETERMINACIÓN DE EQUIPOS DE LA RED INALÁMBRICA

En base al diseño propuesto para el mejoramiento de la Red Inalámbrica describiremos equipos que soporten los estándares 802.11 b/g/n, los cuales son utilizados actualmente por sus compatibilidad y escalabilidad con un sin número de dispositivos inalámbricos. Las características de estos equipos nos permitirán tener un buen diseño de distribución de equipos inalámbricos que brinden el servicio de internet a los usuarios.

3.6.1. Access Point de Exteriores

3.6.1.1. Cisco Aironet 1300 Series Outdoor Access Point (ANEXO 1)

FIGURA 51 Cisco Aironet 1300 Series
Fuente: (Cisco, 2013)

Los Access Point de la Serie 1300 (FIGURA 51) como característica importante soportan 802.11g y proporcionan alta velocidad y conectividad inalámbrica entre múltiples redes y clientes fijos o móviles. La construcción de una infraestructura inalámbrica con el Cisco Aironet 1300 provee al personal de implementación una solución flexible y fácil de utilizar que cumple con los requisitos de seguridad.

Está diseñado en base a una carcasa compacta y resistente para el despliegue en ambientes al aire libre, se encuentra disponible en dos versiones: La serie Cisco Aironet 1300 con antena integrada que se puede instalar rápidamente y la serie Cisco Aironet 1300 con conectores de antena las cuales son compatibles con una diversidad de antenas a 2.4 GHz ofreciendo variedad y versatilidad de cobertura.

La serie Cisco Aironet 1300 está disponible como parte de la Cisco Unified Wireless Network (Red Inalámbrica Unificada de Cisco) o como un AP autónomo. La red inalámbrica unificada de Cisco es una solución completa que ofrece una red integrada cableada e inalámbrica. Los APs unificados funcionan con el protocolo LWAPP[146] en conjunción con un Cisco Wireless LAN Controller y un Cisco Wireless Control System (WCS[147]).

3.6.1.2. Cisco Aironet 1400 Series Wireless Bridge

FIGURA 52 Cisco Aironet 1400 Series
Fuente: (Cisco, 2013)

Los Access Point de la Serie 1400 (FIGURA 62) crean un nuevo punto de referencia para la extensión inalámbrica, proporcionando una solución de alto rendimiento para conectar varias LAN en un área metropolitana. La construcción de una infraestructura inalámbrica con el Cisco Aironet 1400 provee al personal de implementación una solución flexible y fácil de utilizar que cumple con los requisitos de seguridad.
Diseñado para ser una alternativa rentable para las líneas arrendadas, específicamente creada para entornos de exteriores hostiles, pero también funciona bien en despliegue de interiores, proporcionando características tales como:

- Soporte de configuraciones punto a punto o punto a multipunto.
- Admite velocidades de datos de hasta 54 Mbps.

[146] **LWAPP** Protocolo Ligero de Punto de Acceso
[147] **WCS** Sistema de Control Inalámbrico

- Los mecanismos de seguridad mejorados se basan en el estándar IEEE 802.11i.
- Optimizado para áreas de exteriores hostiles.
- Desarrollo de flexibilidad en cuanto a antenas externas e integradas.
- Diseñado para a facilidad de instalación y operación.

Los Cisco Aironet tienen un historial probado en la industria en lo que respecta a las características de seguridad avanzadas. Sobre la seguridad inalámbrica básica, el apoyo de Cisco Wireless Security se incluye en la Serie Cisco Aironet 1400 que ofrece soporte para autenticación mutua IEEE 802.1X y cifrado de alta seguridad.

3.6.1.3. Comparación de Access Point de Exteriores

TABLA 36 Especificaciones técnicas para Access Point de Exteriores

ESPECIFICACIONES	CISCO	CISCO
Modelo	Aironet 1300 Series	Aironet 1400 Series
Estándares	IEEE 802.11b/g	IEEE 802.11a
Certificación Wi-Fi	Si	Si
Velocidades	✓ 802.11b: 1, 2, 5.5 y 11 Mbps ✓ 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 y 54 Mbps	802.11a: 6, 9, 12, 18, 24, 36, 48 y 54 Mbps
Banda de Frecuencia	✓ 2.412 a 2.462 GHz (FCC) ✓ 2.412 a 2.472 GHz (ETSI) ✓ 2.412 a 2.472 GHz (TELEC)	5.725 a 5.825 GHz (FCC UNII 3)
Modulación	✓ 802.11b: DSSS ✓ 802.11g: OFDM	802.11a: COFDM[148]
Canales que no se superponen	3	4
Gestión SNMP[149]	Versión 1 y 2	Versión 1 y

[148] **COFDM** Coded Orthogonal Frecuency Division Multiplexing
[149] **SNMP** Simple Network Management Protocol

Seguridad	✓ Autenticación 802.1X ✓ Encriptación WPA-TKIP y AES (802.11i)	✓ Autenticación 802.1X ✓ Encriptación WEB, WPA-TKIP
Soporte de configuración	Telnet, HTTP, FTP, TFTP, SNMP	Telnet, HTTP, FTP, TFTP, SNMP
Soporte DHCP	Si	Si
Soporte RADIUS	Si	Si
Soporte VLAN	Si	Si
Soporte QoS	Si	Si
Soporte PoE	Si	Si
Sensibilidad de Recepción	✓ 1 Mbps: -94 dBm ✓ 2 Mbps: -91 dBm ✓ 5.5 Mbps: -89 dBm ✓ 11 Mbps: -85 dBm ✓ 6 Mbps: -90 dBm ✓ 9 Mbps: -89 dBm ✓ 12 Mbps: -86 dBm ✓ 18 Mbps: -84 dBm ✓ 24 Mbps: -81 dBm ✓ 36 Mbps: -77 dBm ✓ 48 Mbps: -73 dBm ✓ 54 Mbps: -72 dBm	✓ 6 Mbps: -83 dBm ✓ 9 Mbps: -83 dBm ✓ 12 Mbps: -83 dBm ✓ 18 Mbps: -82 dBm ✓ 24 Mbps: -79 dBm ✓ 36 Mbps: -76 dBm ✓ 48 Mbps: -72 dBm ✓ 54 Mbps: -70 dBm
Máximo Nivel de Recepción Operacional	-20 dBm	-19 dBm
Máximo Nivel de Recepción de Survivable	10 dBm	0 dBm

Fuente: Datasheets del Cisco Aironet 1300 Series y Cisco Aironet 1400 Series

3.6.1.4. Selección del Access Point de Exteriores

Para la elección del AP de exteriores se tomó en cuenta algunas especificaciones importantes como los estándares IEEE que soporta, las velocidades, la banda de frecuencia en la que trabaja y la integración con antenas externas. Con estos parámetros importantes se llegó a determinar que el Cisco Aironet 1300 Series Access Point es el más idóneo para implementarse en la Red Inalámbrica de la Universidad Técnica del Norte.

3.6.2. Access Point de Interiores

3.6.2.1. Cisco Aironet 1130AG Series Access Point (ANEXO 2)

FIGURA 53 Cisco Aironet 1130AG Series
Fuente: (Cisco, 2013)

Los Access Point de la Serie 1130AG (FIGURA 53) proporcionan alta capacidad, alta seguridad, funciones de diseño para áreas de oficina y entrega total de acceso WLAN. El Cisco Aironet 1130AG utiliza las características de un radio y la gestión de red para su implementación junto con las antenas omnidireccionales que proporcionan una determinada área de cobertura para entornos de oficinas y RF.

El Cisco Aironet 1130AG Series Access Point está disponible en dos tipos de configuraciones “Autonomous” y “Lightweight”. Los Access Points en modo Autonomous pueden soportar configuraciones independientes en la red con todas las opciones de configuración que se mantienen dentro de los Access Points. Los Access Points en modo Lightweight funcionan en conjunción con un Cisco Wireless LAN Controller con toda la información de configuración mantenida dentro del Controlador.

Estos APs se pueden instalar en el techo para proporcionar a los usuarios una cobertura continua, como por ejemplo para edificios y establecimientos educativos. Son equipos que se pueden montar de forma sencilla y segura en las paredes o techos según el área de cobertura que se requiera conectividad con un costo de instalación mínimo.

3.6.2.2. Cisco Aironet 1260 Series Access Point (ANEXO 3)

FIGURA 54 Cisco Aironet 1260 Series Access Point
Fuente: (Cisco, 2013)

Los Access Point de la Serie 1260 (FIGURA 54) proporciona cobertura inalámbrica para interiores con soporte para IEEE 802.11n. Estos APs son capaces de ofrecer hasta nueve veces el rendimiento de las redes IEEE 802.11 a/b/g. Diseñado específicamente para los entornos más exigentes, la serie 1260 es compatible con las antenas externas y una amplia gama de temperaturas.

Cisco también ofrece la más amplia selección de la industria de antenas IEEE 802.11n ofreciendo una cobertura óptima para una variedad de escenarios de implementación. La serie 1260 es un componente de la Red Inalámbrica Unificada de Cisco proporcionando una arquitectura más flexible, resistente y escalable, ofreciendo un acceso seguro a los servicios de movilidad, como también a la protección de la inversión mediante la integración sin ningún problema con la red cableada existente.

3.6.2.3. Comparación de Access Point de Interiores

TABLA 37 Especificaciones técnicas para Access Point de Interiores

ESPECIFICACIONES	CISCO	CISCO
Modelo	Aironet 1130AG Series	Aironet 1260 Series
Estándares	IEEE 802.11a/b/g	IEEE 802.11a/b/g/n
Certificación Wi-Fi	Si	Si
Velocidades	✓ 802.11a: 6, 9, 12, 18, 24, 36, 48 y 54 Mbps ✓ 802.11b: 1, 2, 5.5 y 11 Mbps ✓ 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 y 54 Mbps	✓ 802.11a: 6, 9, 12, 18, 24, 36, 48 y 54 Mbps ✓ 802.11b: 1, 2, 5.5 y 11 Mbps ✓ 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 y 54 Mbps ✓ 802.11n: Hasta 300 Mbps
Banda de Frecuencia	Americas (FCC) ✓ 2.412 a 2.462 GHz (11 canales) ✓ 5.15 a 5.35, 5.725 a 5.825 GHz (12 canales) ETSI ✓ 2.412 a 2.472 GHz (13 canales) ✓ 5.15 a 5.725 GHz (19 canales) Japan (TELEC) ✓ 2.412 a 2.472 GHz (13 canales OFDM) ✓ 2.412 a 2.484 GHz (14 canales CCK)	A (A Regulatory Domain) ✓ 2.412 a 2.462 GHz (11 canales) ✓ 5.180 a 5.320 GHz (8 canales) ✓ 5.500 a 5.700 GHz (8 canales excluidos 5.600 a 5.640 GHz) ✓ 5.745 a 5.825 GHz (5 canales) E (E Regulatory Domain) ✓ 2.412 a 2.472 GHz (13 canales) ✓ 5.180 a 5.320 GHz (8 canales)

	✓ 5.15 a 5.25 GHz (4 canales)	✓ 5.500 a 5.700 GHz (8 canales excluidos 5.600 a 5.640 GHz) Q (Q Regulatory Domain) ✓ 2.412 a 2.472 GHz (13 canales) ✓ 5.180 a 5.320 GHz (8 canales) ✓ 5.500 a 5.700 GHz (11 canales)
Modulación	✓ 802.11a: OFDM ✓ 802.11b: DSSS ✓ 802.11g: OFDM	✓ 802.11a: OFDM ✓ 802.11g: OFDM ✓ 802.11n: OFDM
Canales que no se superponen	✓ 802.11a: Hasta 19 ✓ 802.11b/g: 3	2.4 GHz ✓ 802.11b/g: • 20 MHz: 3 ✓ 802.11n: • 20 MHz: 3 5 GHz ✓ 802.11a: • 20 MHz: 21 ✓ 802.11n: • 20 MHz: 21 • 40 MHz: 9
Gestión SNMP	Versión 1 y 2	Versión 1, 2 y 3
Seguridad	✓ 802.11i, WPA2, WPA ✓ Autenticación 802.1X ✓ Encriptación AES, TKIP	✓ 802.11i, WPA2, WPA ✓ Autenticación 802.1X ✓ Encriptación AES, TKIP.
Soporte de configuración	Telnet, HTTP, FTP, TFTP, SNMP	Telnet, HTTP, FTP, TFTP, SNMP
Soporte DHCP	Si	Si

Soporte RADIUS	Si	Si
Soporte VLAN	Si	Si
Soporte QoS	Si	Si
Soporte PoE	Si	Si
Sensibilidad de Recepción	802.11a: ✓ 6 Mbps: -87 dBm ✓ 9 Mbps: -86 dBm ✓ 12 Mbps: -85 dBm ✓ 18 Mbps: -84 dBm ✓ 24 Mbps: -80 dBm ✓ 36 Mbps: -78 dBm ✓ 48 Mbps: -73 dBm ✓ 54 Mbps: -71 dBm 802.11g: ✓ 1 Mbps: -93 dBm ✓ 2 Mbps: -91 dBm ✓ 5.5 Mbps: -88 dBm ✓ 6 Mbps: -86 dBm ✓ 9 Mbps: -85 dBm ✓ 11 Mbps: -85 dBm ✓ 12 Mbps: -84 dBm ✓ 18 Mbps: -83 dBm ✓ 24 Mbps: -79 dBm ✓ 36 Mbps: -77 dBm ✓ 48 Mbps: -72 dBm ✓ 54 Mbps: -70 dBm	802.11a (non HT20): ✓ 6 Mbps: -93 dBm ✓ 9 Mbps: -93 dBm ✓ 12 Mbps: -92 dBm ✓ 18 Mbps: -90 dBm ✓ 24 Mbps: -87 dBm ✓ 36 Mbps: -84 dBm ✓ 48 Mbps: -79 dBm ✓ 54 Mbps: -79 dBm 802.11b (CCK): ✓ 1 Mbps: -101 dBm ✓ 2 Mbps: -98 dBm ✓ 5.5 Mbps: -92 dBm ✓ 11 Mbps: -89 dBm 802.11g (non HT20): ✓ 6 Mbps: -92 dBm ✓ 9 Mbps: -92 dBm ✓ 12 Mbps: -92 dBm ✓ 18 Mbps: -90 dBm ✓ 24 Mbps: -86 dBm ✓ 36 Mbps: -84 dBm ✓ 48 Mbps: -79 dBm ✓ 54 Mbps: -78 dBm
Configuración de la Potencia de Transmisión Disponible	802.11a (OFDM): ✓ 17 dBm (50 mW) ✓ 15 dBm (30 mW) ✓ 14 dBm (25 mW) ✓ 11 dBm (12 mW)	2.4 GHz ✓ 23 dBm (200 mW) solo CCK ✓ 20 dBm (100 mW) ✓ 17 dBm (50 mW)

	✓ 8 dBm (6 mW) ✓ 5 dBm (3 mW) ✓ 2 dBm (2 mW) ✓ -1 dBm (1 mW) 802.11b (CCK): ✓ 20 dBm (100 mW) ✓ 17 dBm (50 mW) ✓ 14 dBm (25 mW) ✓ 11 dBm (12 mW) ✓ 8 dBm (6 mW) ✓ 5 dBm (3 mW) ✓ 2 dBm (2 mW) ✓ -1 dBm (1 mW) 802.11g (OFDM): ✓ 17 dBm (50 mW) ✓ 14 dBm (25 mW) ✓ 11 dBm (12 mW) ✓ 8 dBm (6 mW) ✓ 5 dBm (3 mW) ✓ 2 dBm (2 mW) -1 dBm (1 mW)	✓ 14 dBm (25 mW) ✓ 11 dBm (12.5 mW) ✓ 8 dBm (6.25 mW) ✓ 5 dBm (3.13 mW) ✓ 2 dBm (1.56 mW) ✓ -1 dBm (0.78 mW) 5 GHz ✓ 20 dBm (100 mW) ✓ 17 dBm (50 mW) ✓ 14 dBm (25 mW) ✓ 11 dBm (12.5 mW) ✓ 8 dBm (6.25 mW) ✓ 5 dBm (3.13 mW) ✓ 2 dBm (1.56 mW) ✓ -1 dBm (0.78 mW)

Fuente: Datasheets Cisco Aironet 1130AG Series y Cisco Aironet 1260 Series

3.6.2.4. Selección del Access Point de Interiores

Para la elección del AP de interiores se tomó en cuenta algunas especificaciones importantes como los estándares IEEE que soporta, las velocidades, la banda de frecuencia en la que trabaja y la integración con antenas externas. Con estos parámetros importantes se llegó a determinar que el Cisco Aironet 1260 Series Access Point es el más idóneo para implementarse en la Red Inalámbrica de la Universidad Técnica del Norte.

3.6.3. Wireless LAN Controller (ANEXO 4)

FIGURA 55 Cisco Wireless LAN Controller 5508
Fuente: (Cisco, 2014)

El Cisco Wireless LAN Controllers 5508 que se indica en la FIGURA 55 es una plataforma altamente escalable y flexible que permite manejar un sistema con amplios servicios para redes inalámbricas dirigidas a ambientes empresariales como también a campus de tamaño medio y grandes. Diseñado para soportar el estándar IEEE 802.11n mejorando considerablemente su rendimiento y escalabilidad. Ofrece características importantes como:

- Capacidad de administrar simultáneamente hasta 500 APs dependiendo del tipo de licenciamiento que se haya adquirido.
- Visibilidad y protección de RF.
- Excelente rendimiento para la voz y streaming video.

El WLC de la serie 5500 es recomendable para redes inalámbricas de alto rendimiento, ofrece mayor movilidad, automatiza las funciones de administración, gestión y configuración del equipo de manera eficaz y segura.

3.6.3.1. Selección del Wireless LAN Controller

No se hizo ninguna comparación de Controladoras porque la universidad actualmente cuenta con el equipo Cisco Wireless LAN Controller 5508 que nos brinda escalabilidad, alto rendimiento, flexibilidad de crecimiento.

3.7. COBERTURA DE LOS APS DE LA RED INALÁMBRICA

3.7.1. Cálculo del Área de Cobertura

En base a las especificaciones técnicas el alcance o radio de una antena sectorial es de 100 metros, de una antena omnidireccional es de 50 metros, de una antena dipolo es de 90 metros y de una antena interna es de 137 metros.

3.7.1.1. Antena Sectorial

Para encontrar el área de un sector circular, en realidad se está tratando de encontrar una parte fraccional del área de todo el círculo donde se representa el lóbulo de radiación de la antena sectorial. La fracción se determina por la relación del ángulo central del sector, con el ángulo central de todo el círculo, que es 360º; o por la relación de la longitud del arco y la longitud de la circunferencia entera como se visualiza en la FIGURA 56.

El Área es igual al ángulo central (120°) multiplicado por Pi y por radio al cuadrado, el resultado será dividido para 360.

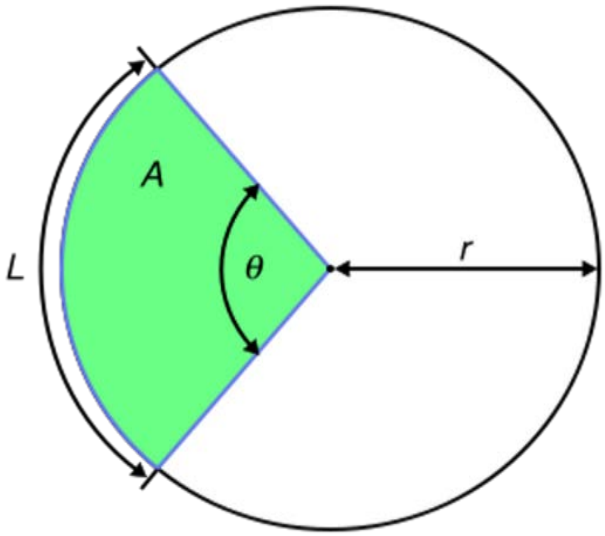


FIGURA 56 Área de cobertura de una Antena Sectorial
Fuente: (Diego, 2014)

A: Área

θ: Ángulo central

r: radio

$$A = \frac{\theta^\circ}{360^\circ}\pi r^2$$

$$A = \frac{120^\circ}{360^\circ}\pi(100m)^2$$

$$A = 10471.97551\ m^2$$

$$\boldsymbol{A \approx 10472\ m^2}$$

TABLA 38 APs con tipo de Antena Sectorial

# AP	NOMBRE	UBICACIÓN	MODELO AP	TIPO DE ANTENA	RADIO DE COBERTURA
AP2	AP-UTN-CAI-FICAYA	Terraza entre CAI-FICAYA	AIR-BR1310G-A-K9-R	Sectorial	100 metros
AP4	AP-UTN-EDFISICA	Este - Instituto Educación Física	AIR-BR1310G-A-K9-R	Sectorial	100 metros
AP5	AP-UTN-ESTE-AUDITORIO	Este - Auditorio Agustín Cueva	AIR-BR1310G-A-K9-R	Sectorial	100 metros
AP8	AP-UTN-NORTE-CENTRAL	Terraza Planta Central Norte	AIR-BR1310G-A-K9-R	Sectorial	100 metros

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.7.1.2. Antena Omnidireccional

Para encontrar el área circular, en realidad se está tratando de encontrar toda el área del círculo donde se representa el lóbulo de radiación de la antena omnidireccional como se indica en la FIGURA 57. El Área es igual a Pi multiplicado por radio al cuadrado.

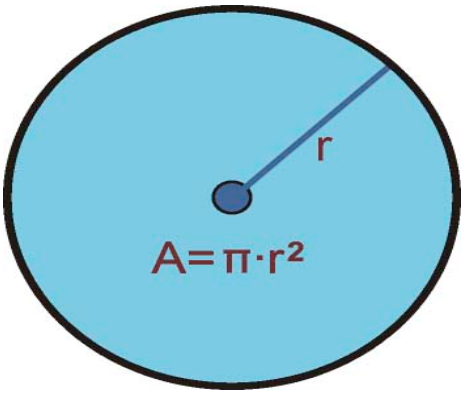


FIGURA 57 Área de cobertura de una Antena Omnidireccional
Fuente: (Adeva Brito, 2014)

A: Área

r: radio

$$A = \pi r^2$$

$$A = \pi(50m)^2$$

$$A = 7853.981634\ m^2$$

$$\boldsymbol{A \approx 7854\ m^2}$$

TABLA 39 APs con tipo de Antena Omnidireccional

# AP	NOMBRE	UBICACIÓN	MODELO AP	TIPO DE ANTENA	RADIO DE COBERTURA
AP10	AP-UTN-SUR-FACAE	Terraza Planta 1 Sur FACAE	AIR-BR1310G-A-K9-R	Omnidireccional	50 metros
AP11	AP-UTN-NORTE-FACAE	Terraza Planta 1 Norte FACAE	AIR-BR1310G-A-K9-R	Omnidireccional	50 metros
AP12	AP-UTN-FECYT	Terraza Planta 1 NorEste FECYT	AIR-BR1310G-A-K9-R	Omnidireccional	50 metros
AP13	AP-UTN-OESTE-CENTRAL	Terraza Planta 1 Oeste Edificio Central	AIR-BR1310G-A-K9-R	Omnidireccional	50 metros
AP14	AP-UTN-NORTE-ENTRADA	Entrada Norte	AIR-BR1310G-A-K9-R	Omnidireccional	50 metros

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.7.1.3. Antena Dipolo

Para encontrar el área circular, en realidad se está tratando de encontrar toda el área del círculo donde se representa el lóbulo de radiación de la antena dipolo que se asemeja al lóbulo de radiación de una antena omnidireccional como se indica en la FIGURA 58 donde lo único que varía es el radio de cobertura. El Área es igual a Pi multiplicado por radio al cuadrado.

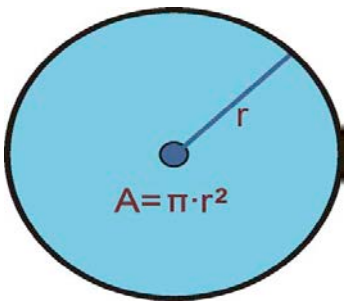


FIGURA 58 Área de cobertura de una Antena Dipolo

Fuente: (Adeva Brito, 2014)

A: Área

r: radio

$$A = \pi r^2$$

$$A = \pi(90m)^2$$

$$A = 25446.90049\ m^2$$

$$\boldsymbol{A \approx 25447\ m^2}$$

TABLA 40 APs con tipo de Antena Dipolo

# AP	NOMBRE	UBICACIÓN	MODELO AP	TIPO DE ANTENA	RADIO DE COBERTURA
AP16	AP-FACAE-PA1	Planta Alta 1 FACAE	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP17	AP-FACAE-PA2	Planta Alta 2 FACAE	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP18	AP-FACAE-PA3	Planta Alta 3 FACAE	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP19	AP-FECYT-PA1	Planta Alta 1 FECYT	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP20	AP-FECYT-PA2	Planta Alta 2 FECYT	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP21	AP-FECYT-PA3	Planta Alta 3 FECYT	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP22	AP-AUDITORIO-INTERIOR	Auditorio Agustín Cueva Interior	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP23	AP-CENTRAL-PB	Planta Baja Edificio Central	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP24	AP-CENTRAL-PA2	Planta Alta 2 Edificio Central	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP25	AP-BIENESTAR-PB	Planta Baja BIENESTAR	AIR-LAP1262N-A-K9	Dipolo	90 metros

AP26	AP-BIENESTAR-PA1	Planta Alta 1 BIENESTAR	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP27	AP-BIENESTAR-PA2	Planta Alta 2 BIENESTAR	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP28	AP-BIENESTAR-PA3	Planta Alta 3 BIENESTAR	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP25	AP-BIENESTAR-PB	Planta Baja BIENESTAR	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP29	AP-FICAYA-PA1	Planta Alta 1 FICAYA	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP30	AP-FICAYA-PA2	Planta Alta 2 FICAYA	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP31	AP-FICAYA-PA3	Planta Alta 3 FICAYA	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP38	AP-FCCSS-PA1	Planta Alta 1 FCCSS	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP39	AP-FCCSS-PA2	Planta Alta 2 FCCSS	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP40	AP-FCCSS-PA3	Planta Alta 3 FCCSS	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP41	AP-CAI-PA1	Planta Alta 1 CAI	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP42	AP-CAI-PA2	Planta Alta 2 CAI	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP43	AP-CAI-PA3	Planta Alta 3 CAI	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP44	AP-POSTGRADO-PB1	Planta Baja POSTGRADO Cubículos	AIR-LAP1262N-A-K9	Dipolo	90 metros

AP45	AP-POSTGRADO-PB2	Planta Baja POSTGRADO	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP46	AP-POSTGRADO-PB-AUDITORIO	Planta Baja Auditorio POSTGRADO	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP47	AP-POSTGRADO-PA1	Planta Alta 1 POSTGRADO	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP48	AP-POSTGRADO-PA2	Planta Alta 2 POSTGRADO	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP49	AP-PISCINA-INTERIOR	Interior Complejo Acuático	AIR-LAP1262N-A-K9	Dipolo	90 metros
AP50	AP-POLIDEPORTIVO	Polideportivo UTN	AIR-LAP1262N-A-K9	Dipolo	90 metros

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.7.1.4. Antena Interna

Para encontrar el área circular, en realidad se está tratando de encontrar toda el área del círculo donde se representa el lóbulo de radiación de la antena interna de un AP para Indoor que se asemeja al lóbulo de radiación de una antena omnidireccional como se indica en la FIGURA 59 donde lo único que varía es el radio de cobertura. El Área es igual a Pi multiplicado por radio al cuadrado.

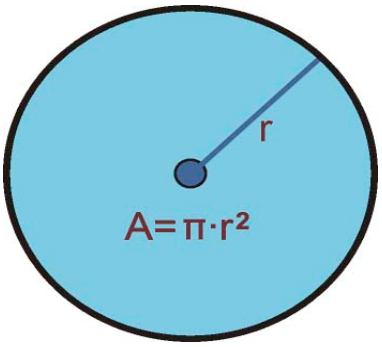


FIGURA 59 Área de cobertura de una Antena Interna

Fuente: (Adeva Brito, 2014)

A: Área

r: radio

$$A = \pi r^2$$

$$A = \pi(137m)^2$$

$$A = 58964.55252\ m^2$$

$$\boldsymbol{A \approx 58964\ m^2}$$

TABLA 41 APs con tipo de Antena Dipolo

# AP	NOMBRE	UBICACIÓN	MODELO AP	TIPO DE ANTENA	RADIO DE COBERTURA
AP32	AP-FICA-PB	Planta Baja FICA	AIR-LAP1131AG-A-K9	Interna	137 metros
AP33	AP-FICA-PA2D	Planta Alta 2 Derecha FICA	AIR-LAP1131AG-A-K9	Interna	137 metros
AP34	AP-FICA-PA2I	Planta Alta 2 Izquierda FICA	AIR-LAP1131AG-A-K9	Interna	137 metros
AP35	AP-FICA-PA3D	Planta Alta 3 Derecha FICA	AIR-LAP1131AG-A-K9	Interna	137 metros
AP36	AP-FICA-PA3I	Planta Alta 3 Izquierda FICA	AIR-LAP1131AG-A-K9	Interna	137 metros
AP37	AP-FICA-PA4	Planta Alta 4 FICA	AIR-LAP1131AG-A-K9	Interna	137 metros

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.7.2. Access Points de Exteriores

En el siguiente diseño de área de cobertura se describe la ubicación de cada uno de los APs instalados en lugares estratégicos correspondientes a la infraestructura de la universidad, distinguiendo tres series de APs para entorno de exteriores los mismos que se diferencian por el tipo de antena que poseen tal como se indica en la **¡Error! No se encuentra el origen de la referencia.**.

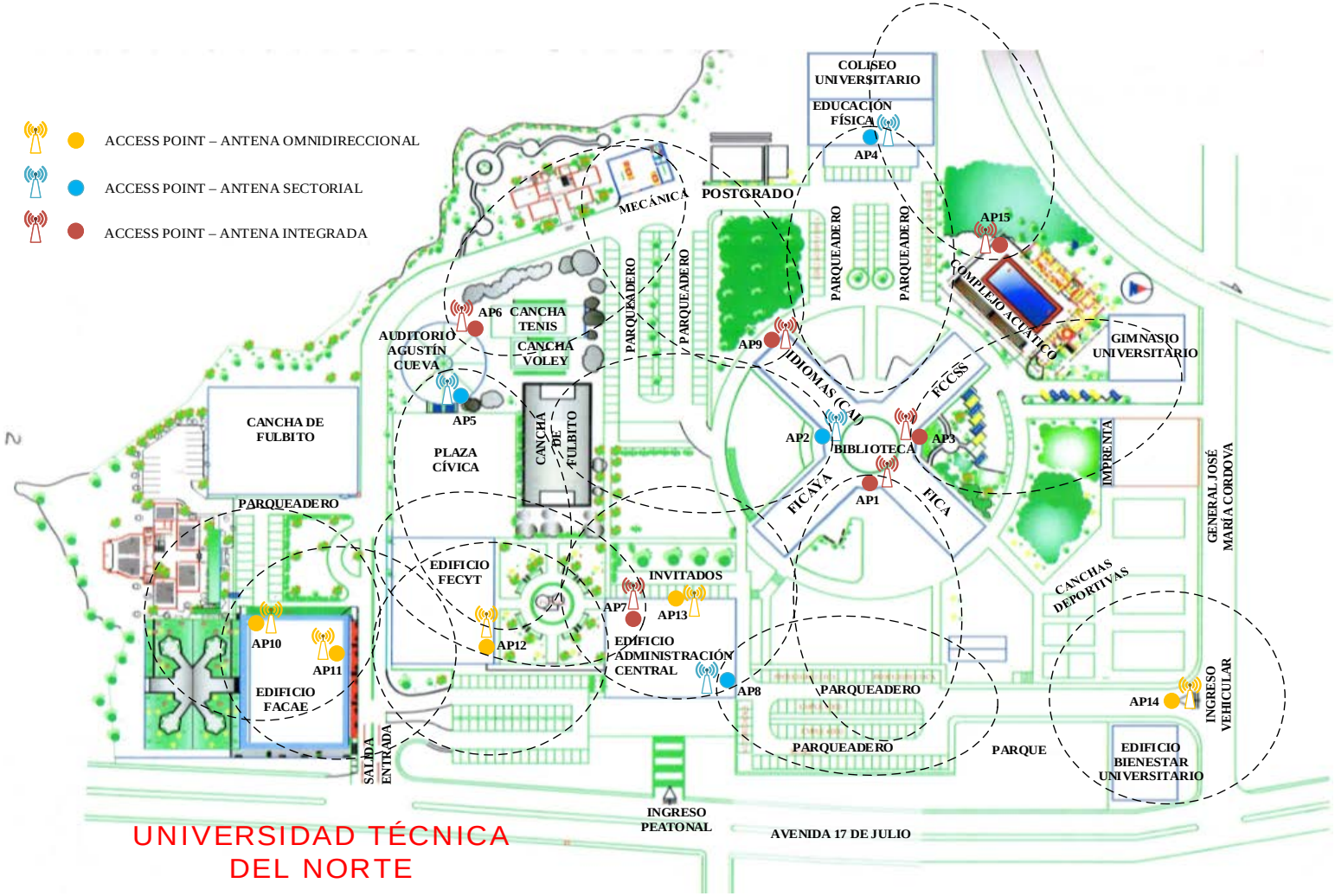


FIGURA 60 Diseño de Área de Cobertura de los APs de la Red Inalámbrica UTN

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.7.3. Access Points de Interiores

En el siguiente diseño utilizaremos la siguiente descripción para diferenciar los diferentes canales de propagación que fueron configurados en cada uno de los APs de acuerdo al análisis de cobertura realizado que se mostrará a continuación:

- Canal 1 (Color Verde)
- Canal 6 (Color Azul)
- Canal 11 (Color Naranja)

3.7.3.1. FACAE

- PLANTA PRIMER PISO ALTO FACAE

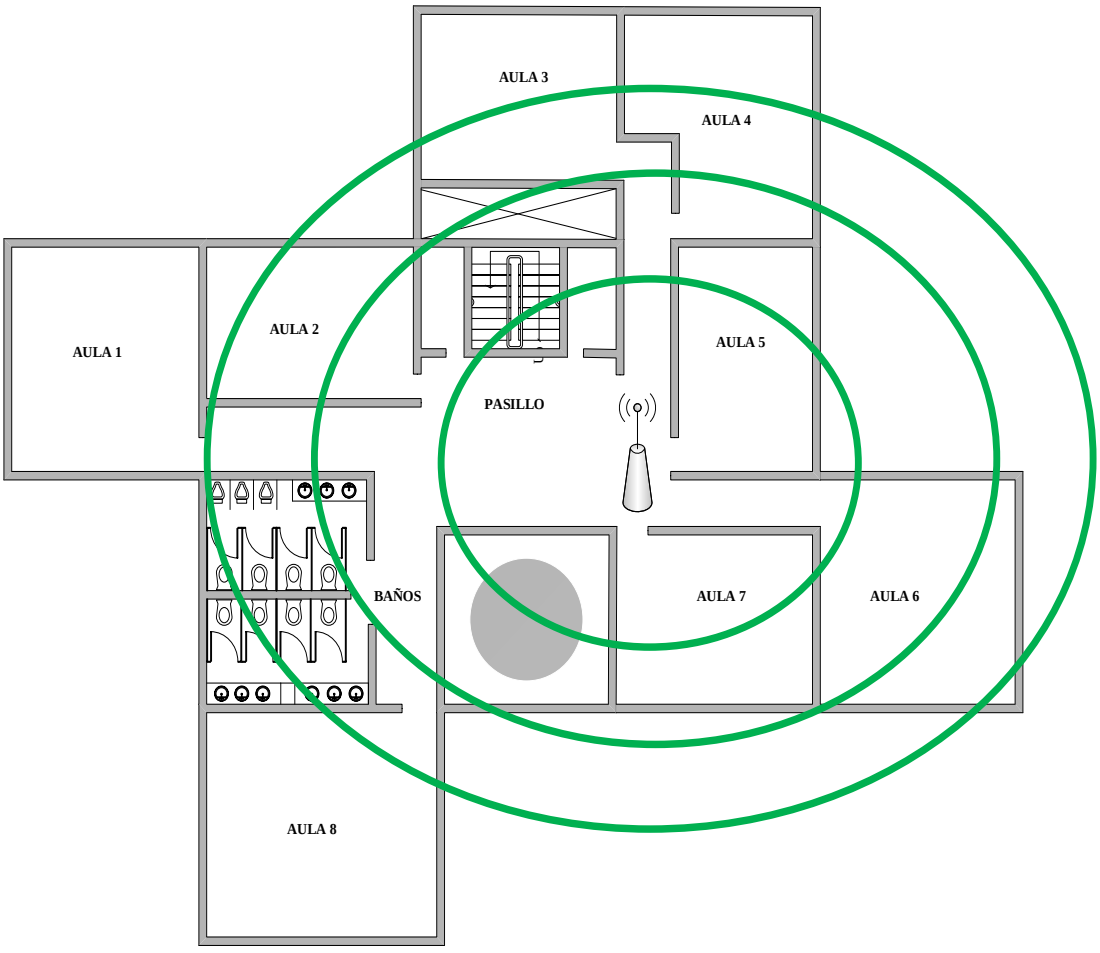


FIGURA 61 Planta primer piso alto FACAE

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA SEGUNDO PISO ALTO FACAE

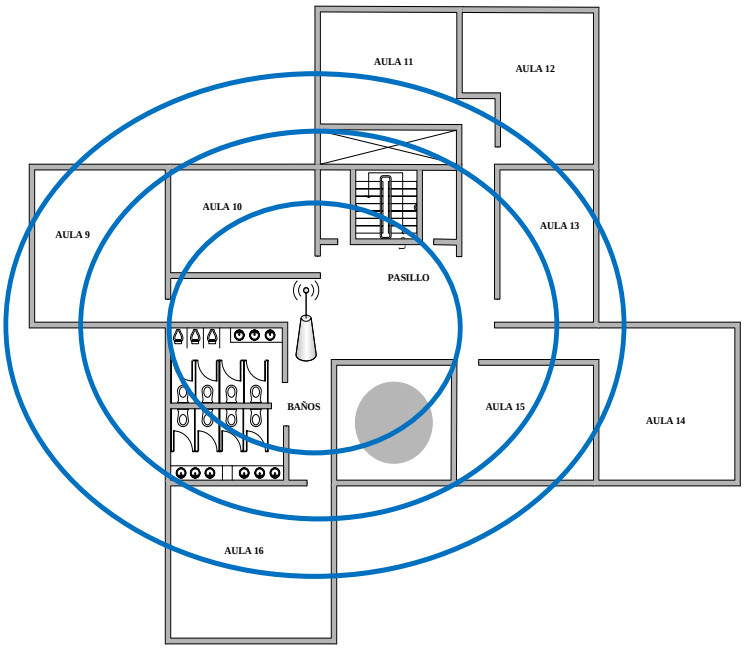


FIGURA 62 Planta segundo piso alto FACAE

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA TERCER PISO ALTO FACAE

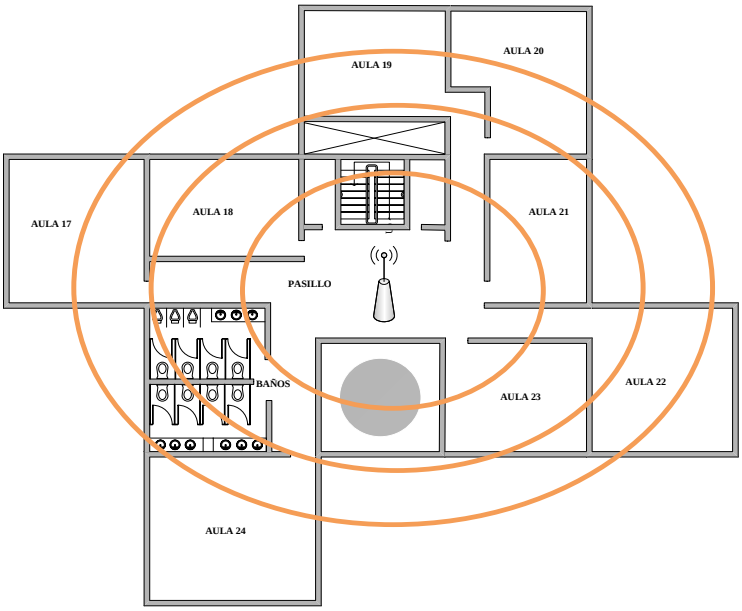


FIGURA 63 Planta tercer piso alto FACAE

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.7.3.2. FECYT

- PLANTA PRIMER PISO ALTO FECYT

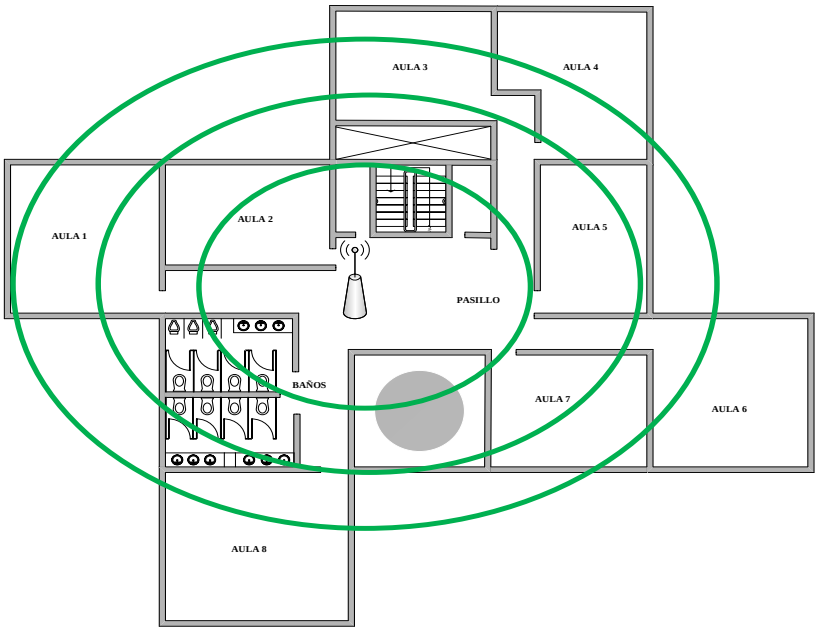


FIGURA 64 Planta primer piso alto FECYT

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA SEGUNDO PISO ALTO FECYT

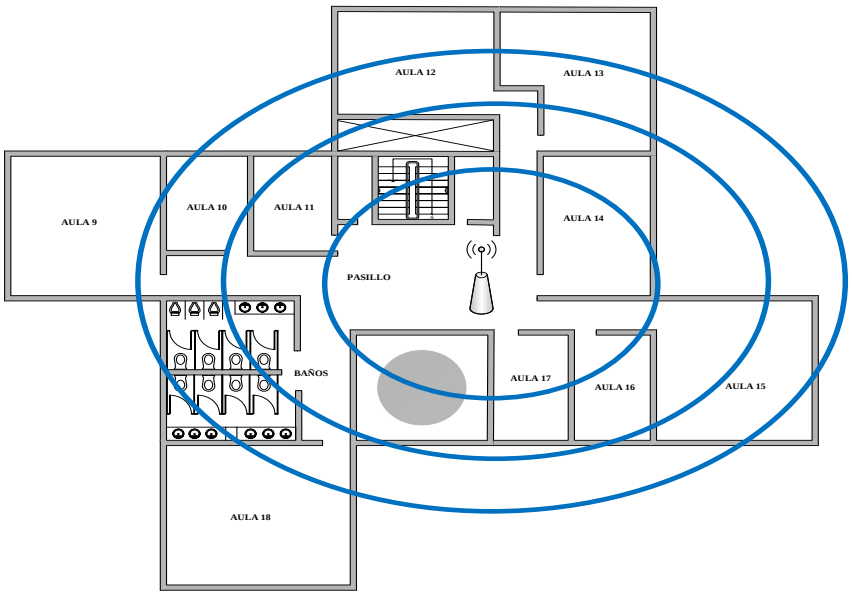


FIGURA 65 Planta segundo piso alto FECYT

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA TERCER PISO ALTO FECYT

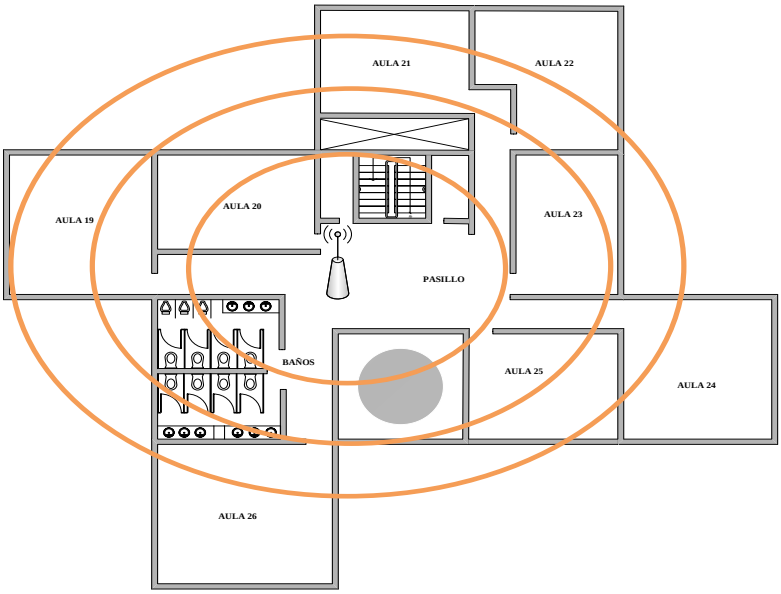


FIGURA 66 Planta tercer piso alto FECYT

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.7.3.3. FICAYA

- PLANTA PRIMER PISO ALTO FICAYA

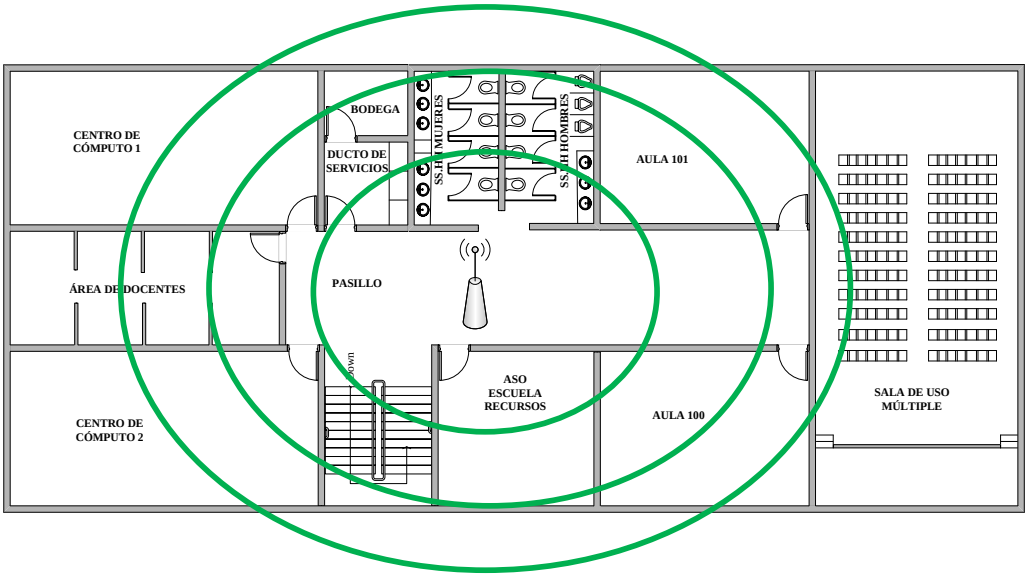


FIGURA 67 Planta primer piso alto FICAYA

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA SEGUNDO PISO ALTO FICAYA

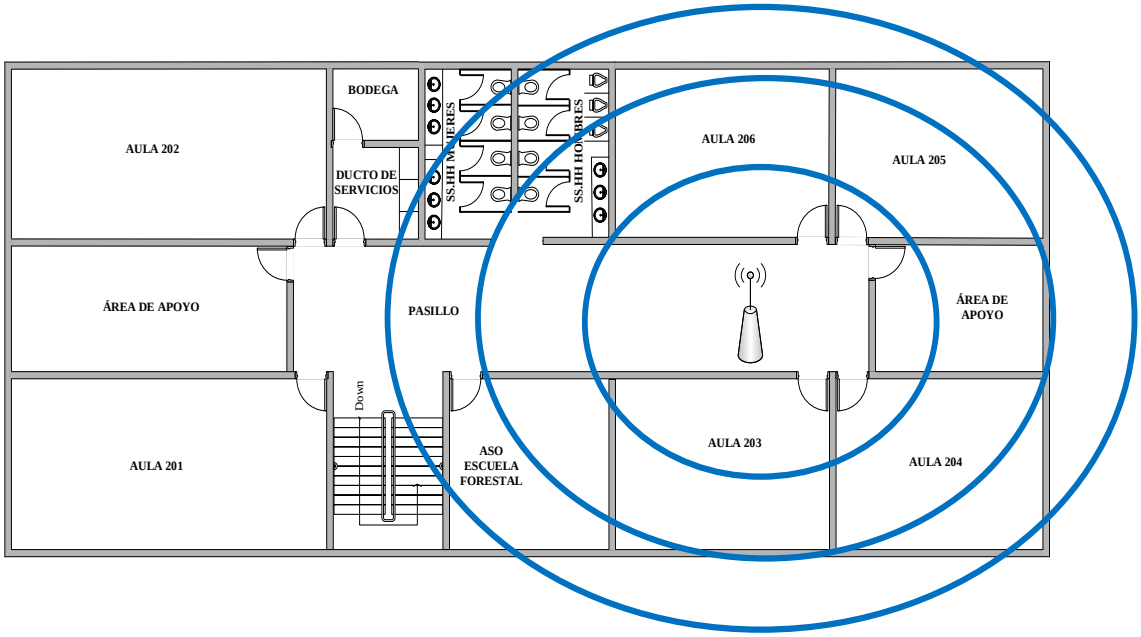


FIGURA 68 Planta segundo piso alto FICAYA

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA TERCER PISO ALTO FICAYA

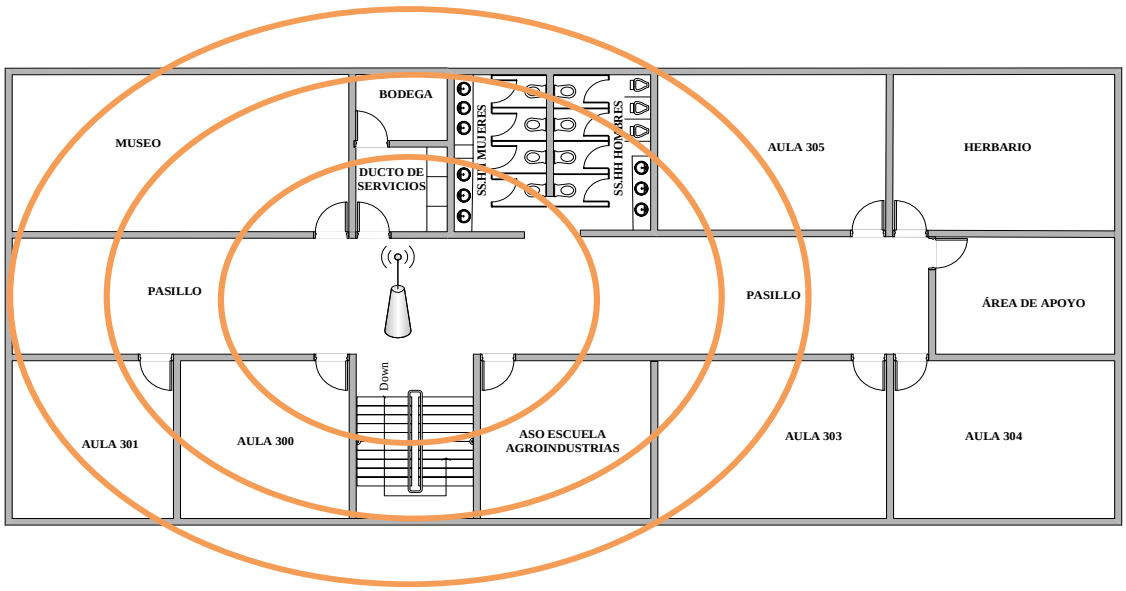


FIGURA 69 Planta tercer piso alto FICAYA

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.7.3.4. FICA

- PLANTA BAJA FICA

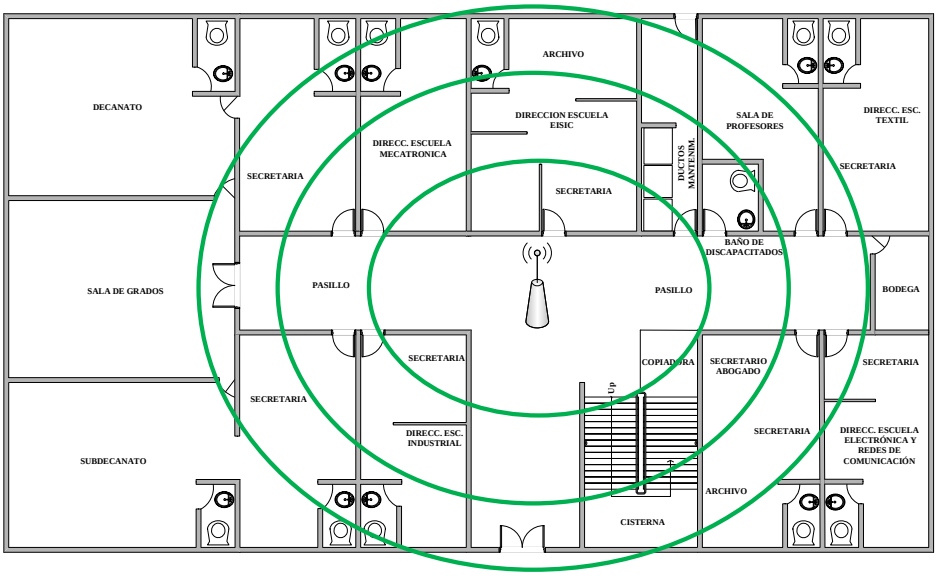


FIGURA 70 Planta baja FICA

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA SEGUNDO PISO ALTO FICA

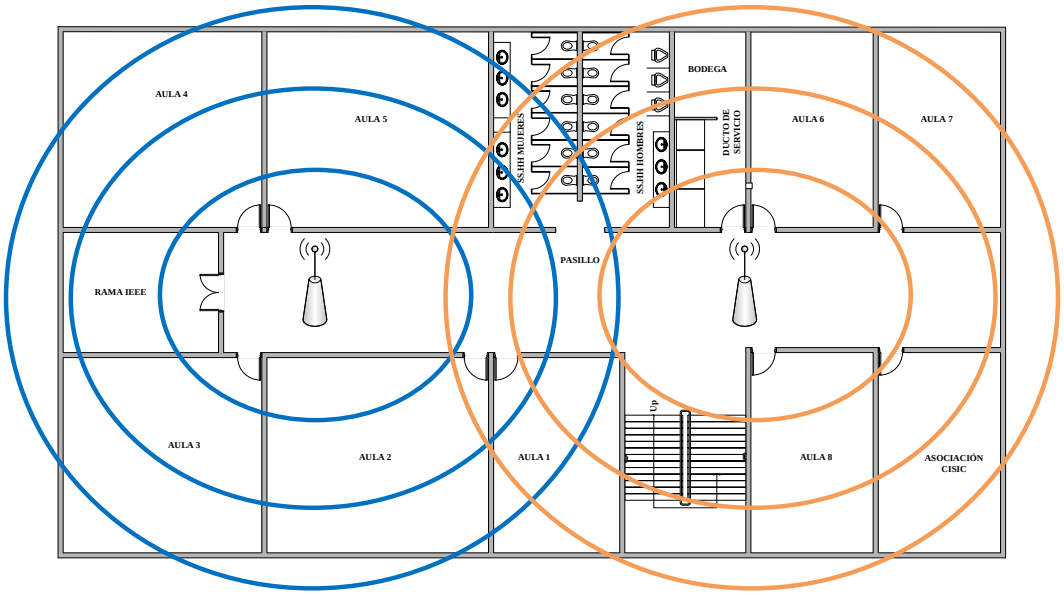


FIGURA 71 Planta segundo piso alto FICA

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA TERCER PISO ALTO FICA

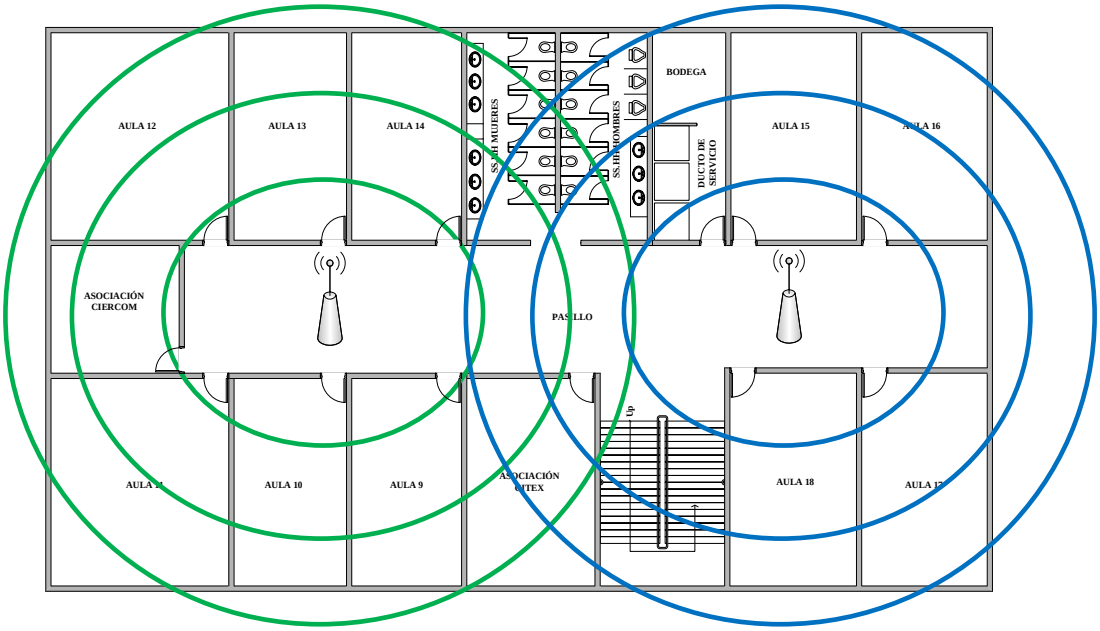


FIGURA 72 Planta tercer piso alto FICA

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA CUARTO PISO ALTO FICA

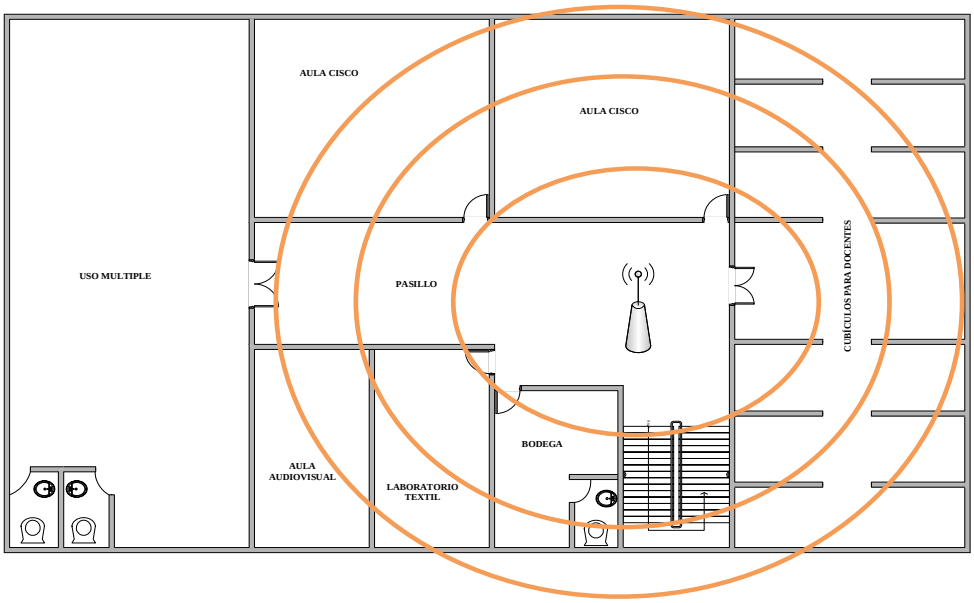


FIGURA 73 Planta cuarto piso alto FICA

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.7.3.5. FCCSS

- PLANTA PRIMER PISO ALTO FCCSS

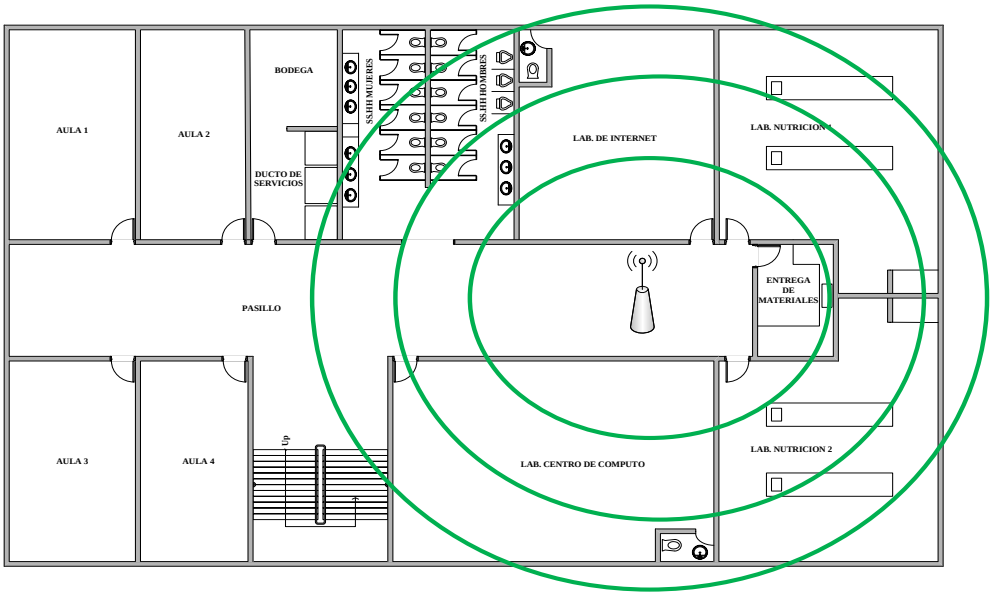


Figura 74 Planta primer piso alto FCCSS

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA SEGUNDO PISO ALTO FCCSS

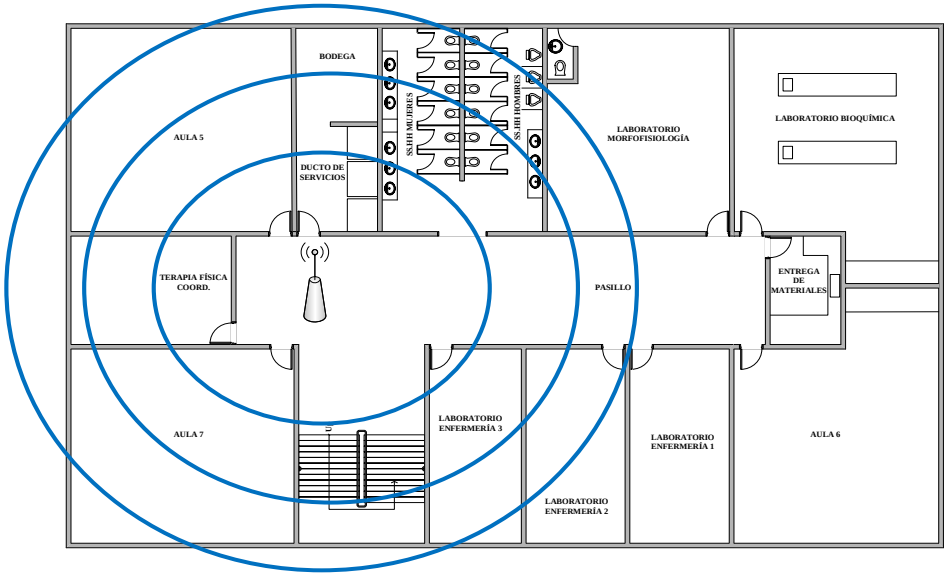


FIGURA 75 Planta segundo piso alto FCCSS

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA TERCER PISO ALTO FCCSS

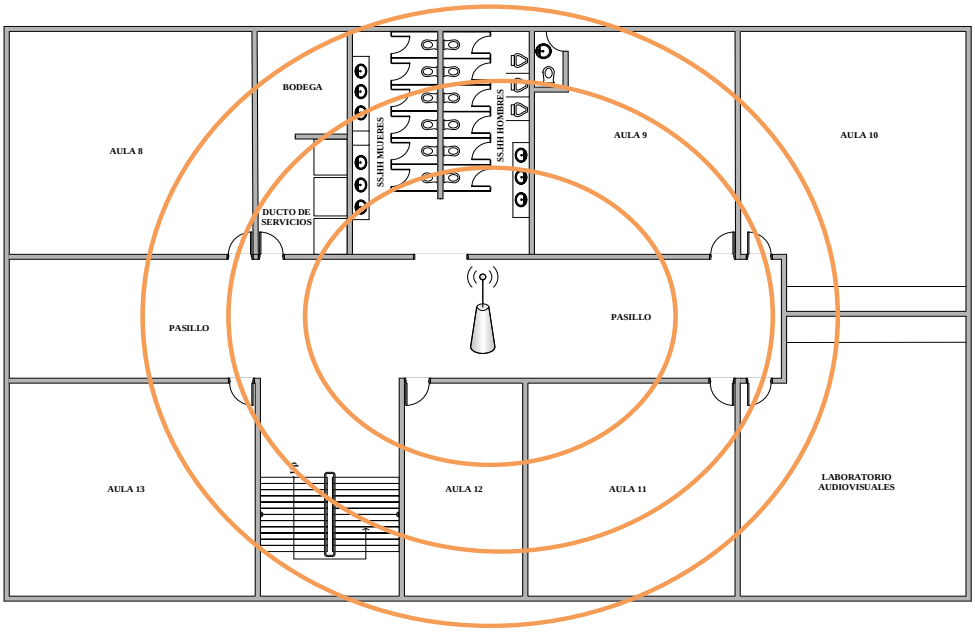


FIGURA 76 Planta tercer piso alto FCCSS

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.7.3.6. CAI

- PLANTA PRIMER PISO ALTO CAI

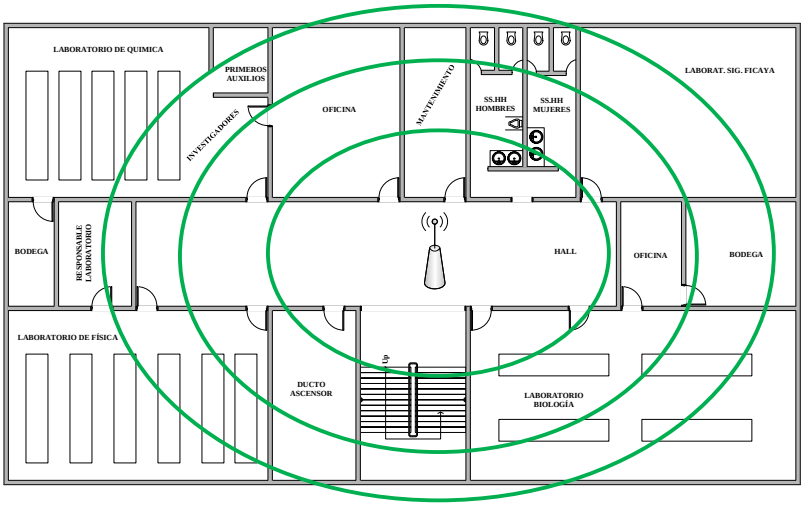


FIGURA 77 Planta primer piso alto CAI

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA SEGUNDO PISO ALTO CAI

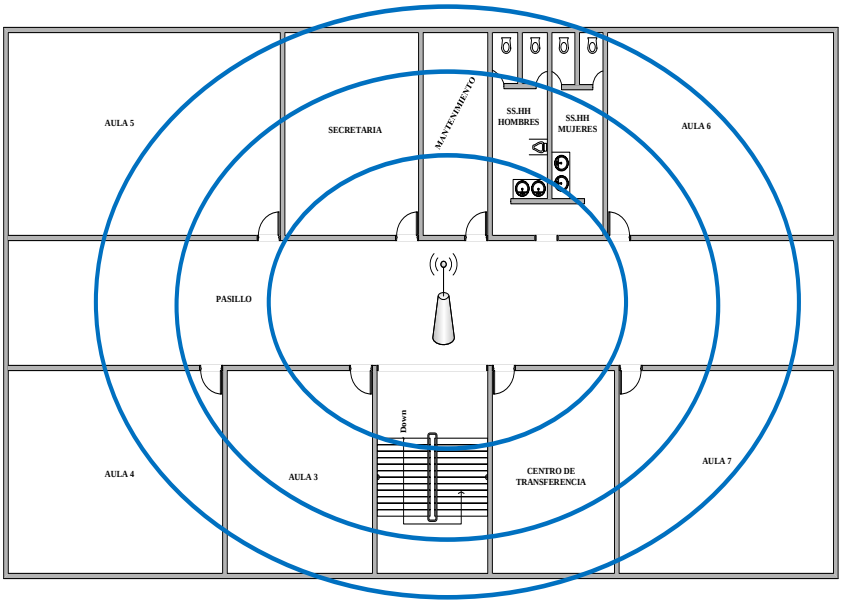


FIGURA 78 Planta segundo piso alto CAI

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA TERCER PISO ALTO CAI

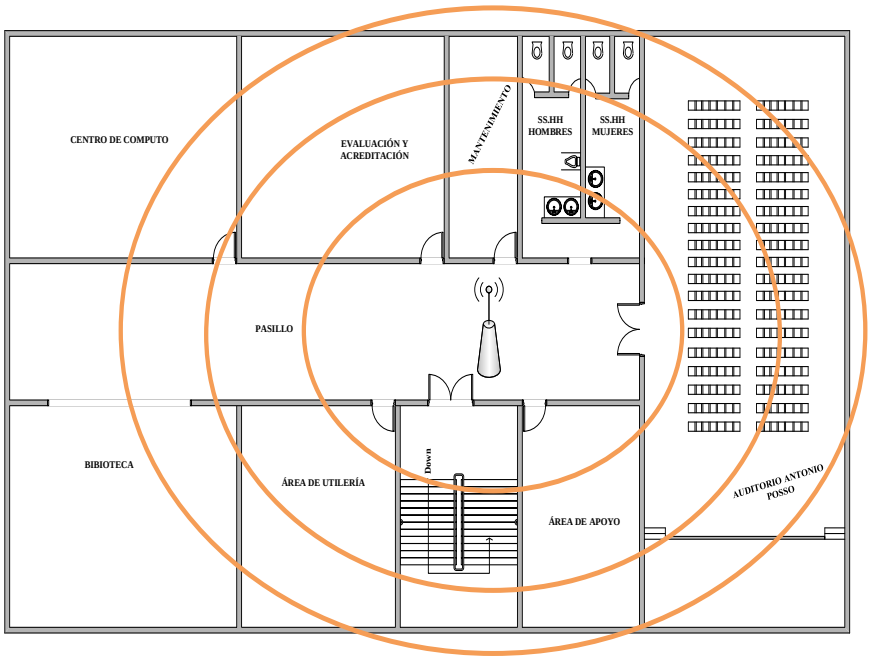


FIGURA 79 Planta tercer piso alto CAI

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.7.3.7. POSTGRADO

- PLANTA BAJA POSTGRADO

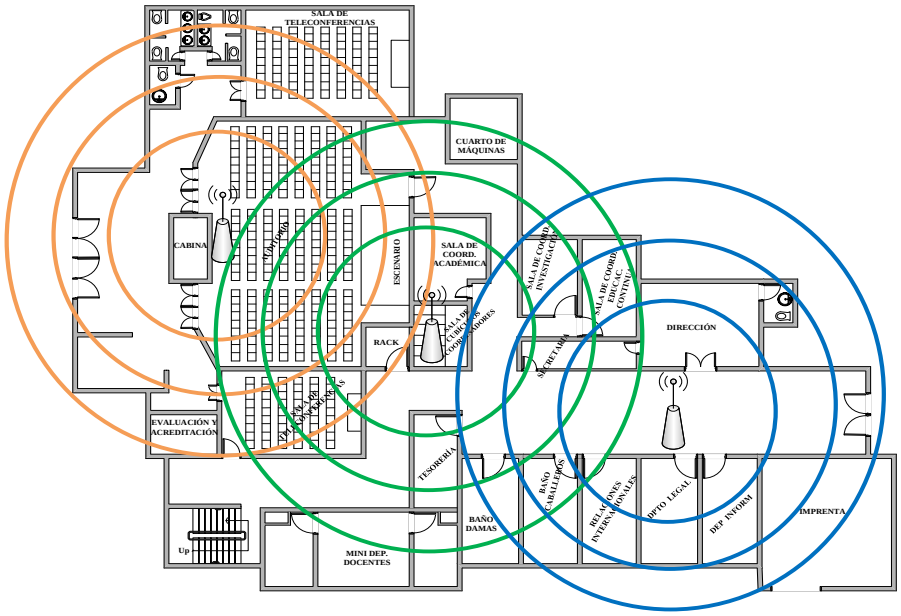


FIGURA 80 Planta baja POSTGRADO

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático

de la UTN

- PLANTA PRIMER PISO ALTO POSTGRADO

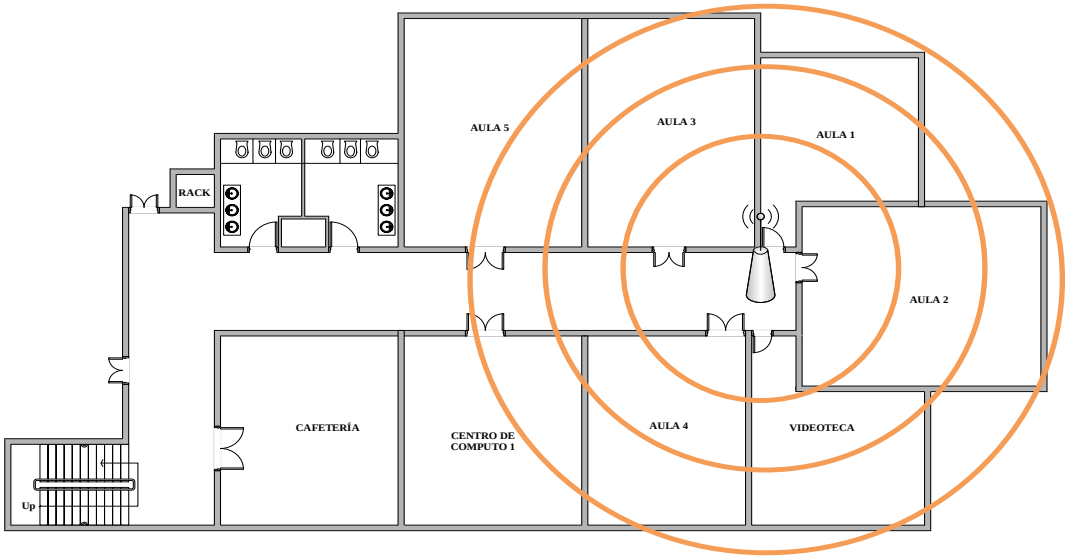


FIGURA 81 Planta primer piso alto POSTGRADO

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA SEGUNDO PISO ALTO POSTGRADO

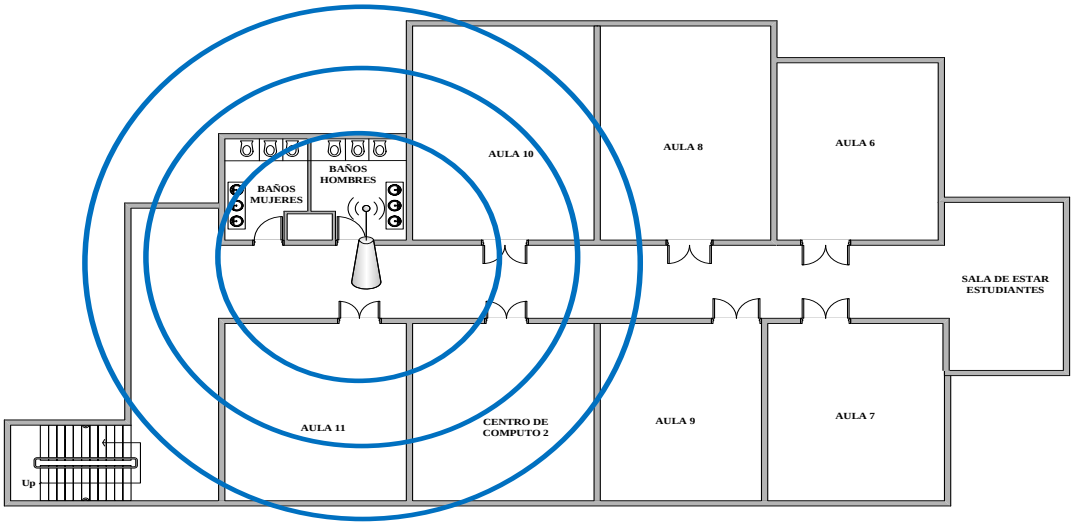


FIGURA 82 Planta segundo piso alto POSTGRADO

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.7.3.8. EDIFICIO BIENESTAR UNIVERSITARIO

- PLANTA BAJA BIENESTAR

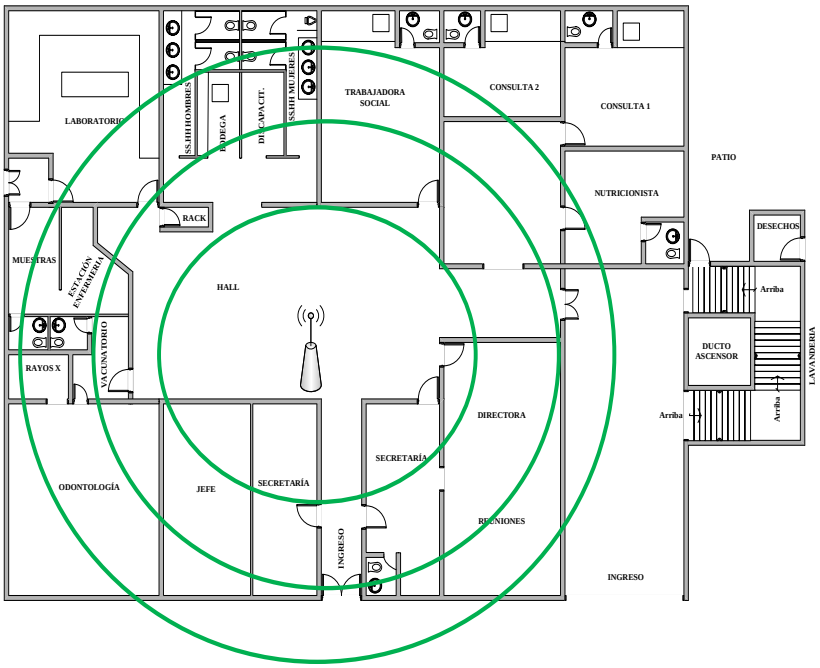


FIGURA 83 Planta baja BIENESTAR

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA PRIMER PISO ALTO BIENESTAR

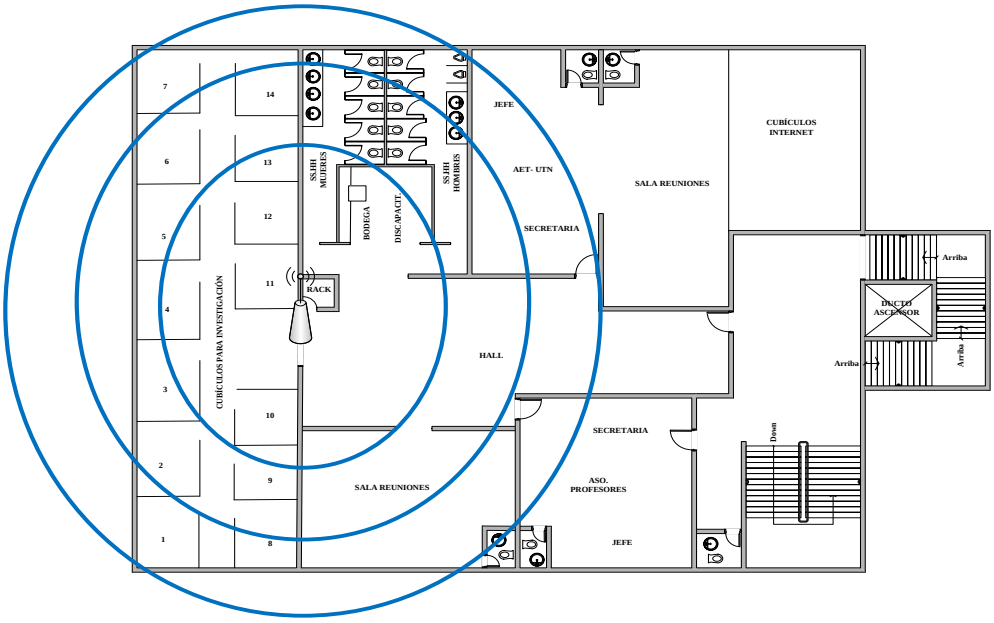


FIGURA 84 Planta primer piso alto BIENESTAR

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA SEGUNDO PISO ALTO BIENESTAR

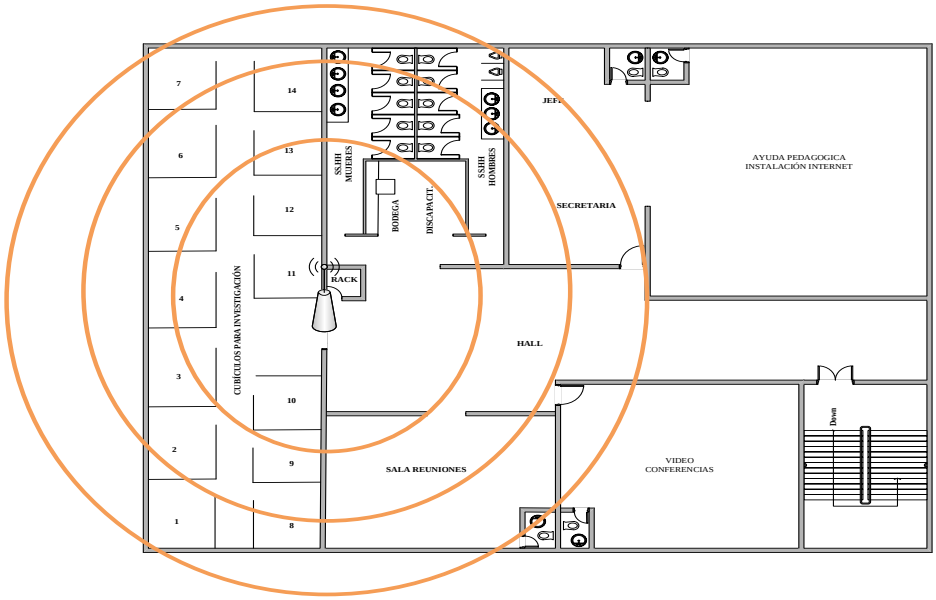


FIGURA 85 Planta segundo piso alto BIENESTAR

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA TERCER PISO ALTO BIENESTAR

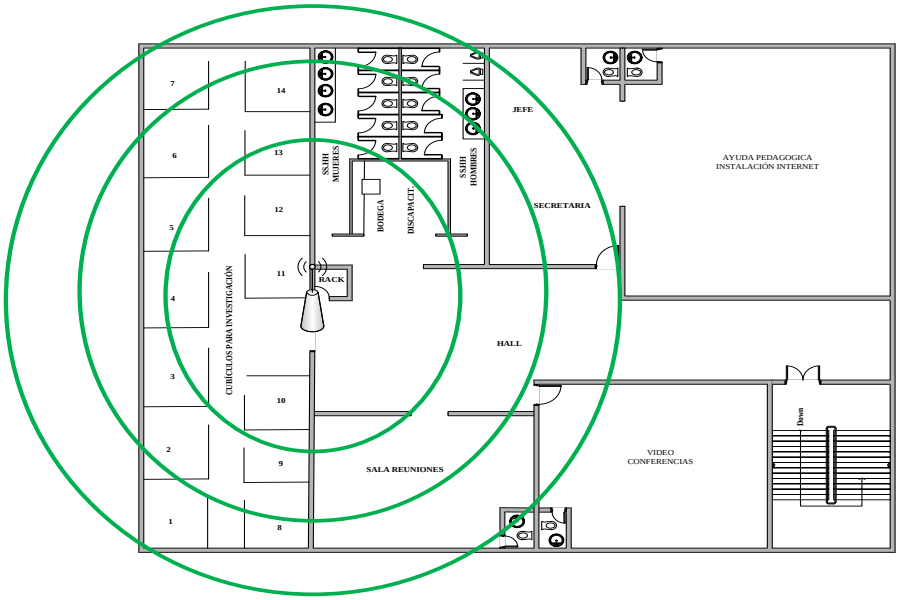


FIGURA 86 Planta tercer piso alto BIENESTAR

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.7.3.9. EDIFICIO CENTRAL

- PLANTA BAJA EDIFICIO CENTRAL

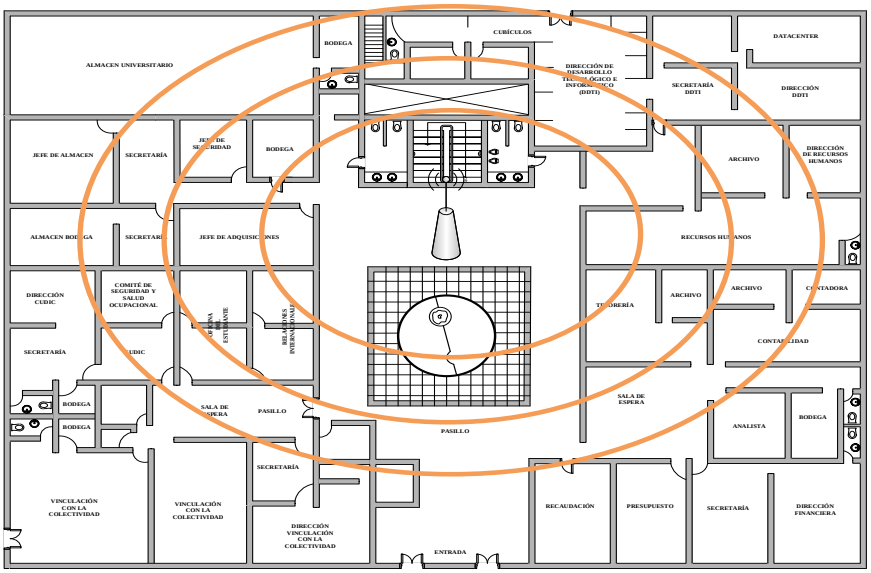


FIGURA 87 Planta baja EDIFICIO CENTRAL

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

- PLANTA SEGUNDO PISO ALTO EDIFICIO CENTRAL

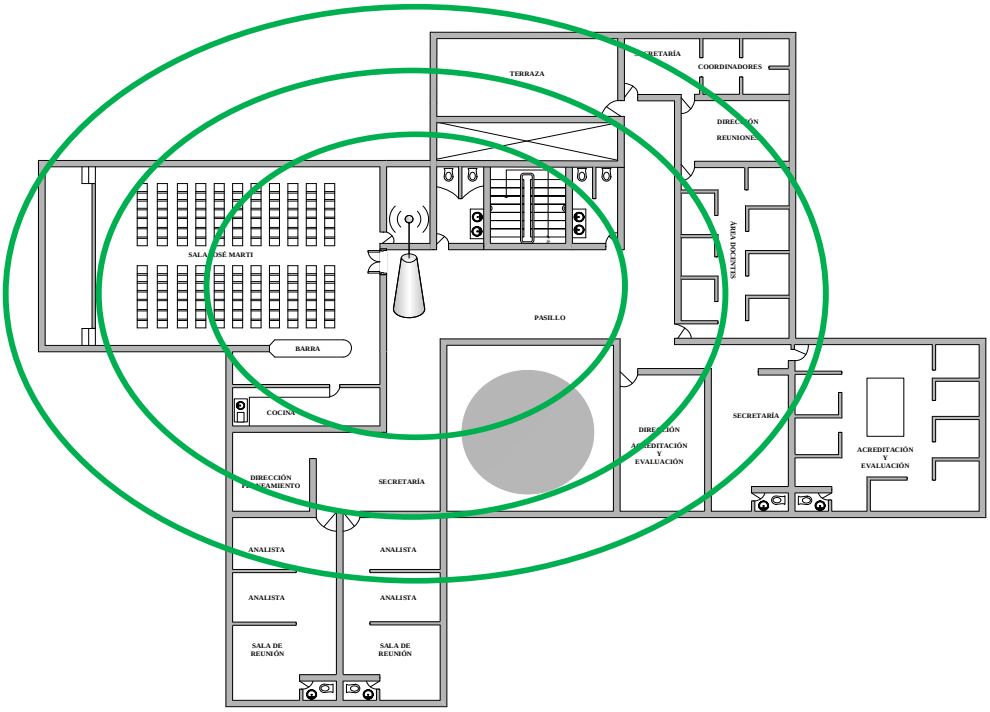


FIGURA 88 Planta segundo piso alto EDIFICIO CENTRAL

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8. DISTRIBUCIÓN DE CANALES

En toda implementación de redes inalámbricas para que no existan interferencias en la comunicación por intermedio de los APs, se considera configurar los canales de trabajo 1, 6 y 11 en base a la distribución de los APs con el propósito de solventar posibles inconvenientes que podrían causar solapamientos de la señales y por ende problemas de conexión por parte de los usuarios al querer acceder a utilizar los recursos de la Internet.

3.8.1. Access Points de Exteriores

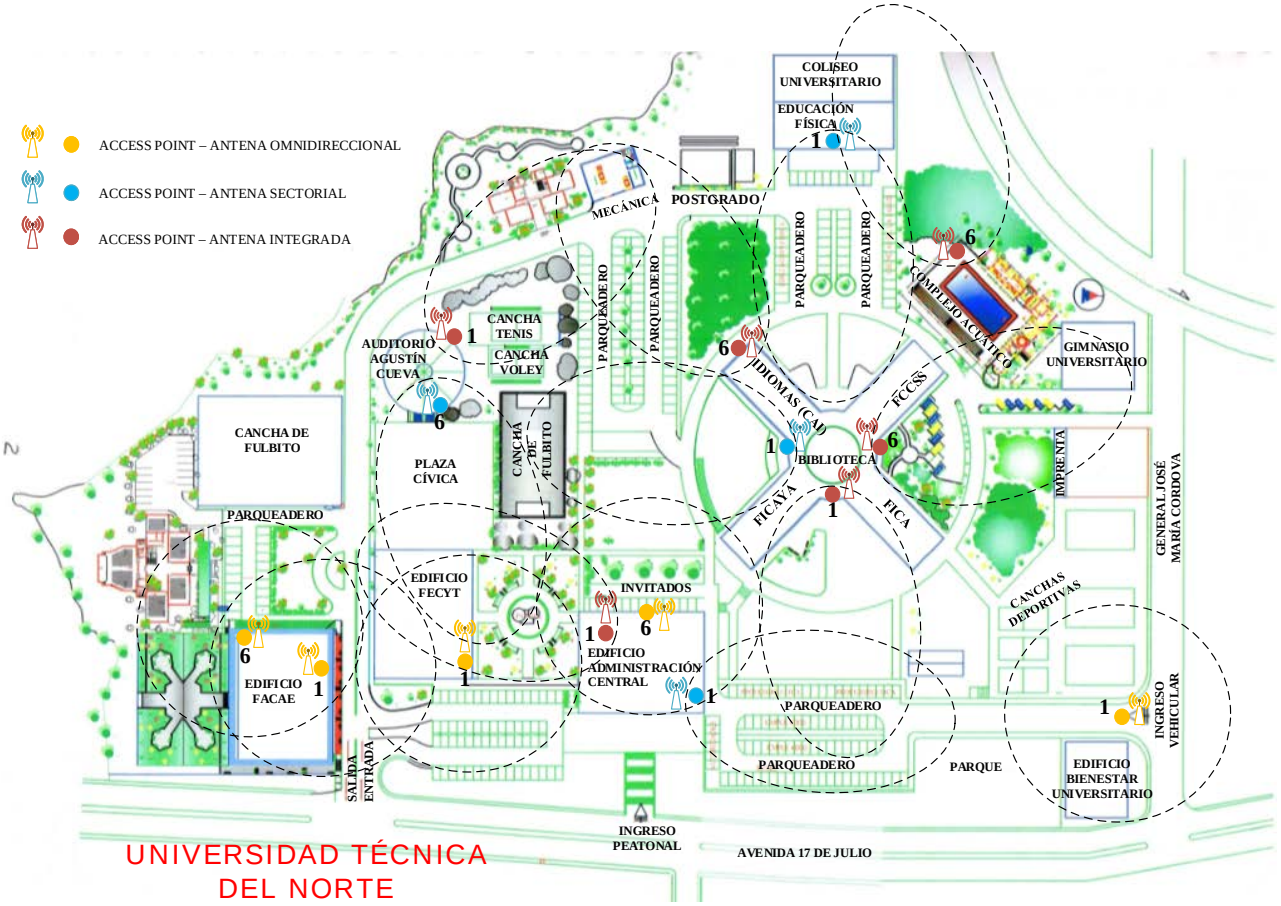


FIGURA 89 Diseño de Canales del Área de Cobertura de los APs de la Red Inalámbrica UTN

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

TABLA 42 Distribución de Canales de los APs de Exteriores

# AP	NOMBRE	UBICACIÓN	MODELO AP	CANALES
AP1	AP-UTN-FICA-FICAYA	Terraza entre FICA - FICAYA	**AIR-LAP1310G-A-K9**	11
AP2	AP-UTN-CAI-FICAYA	Terraza entre CAI-FICAYA	**AIR-BR1310G-A-K9-R**	1
AP3	AP-UTN-FICA-FFCCSS	Terraza entre FICA - FFCCSS	**AIR-LAP1310G-A-K9**	6
AP4	AP-UTN-EDFISICA	Este - Instituto Educación Física	**AIR-BR1310G-A-K9-R**	11
AP5	AP-UTN-ESTE-AUDITORIO	Este - Auditorio Agustín Cueva	**AIR-BR1310G-A-K9-R**	6
AP6	AP-UTN-NORTE-AUDITORIO	Norte - Auditorio Agustín Cueva	**AIR-LAP1310G-A-K9**	11
AP7	AP-UTN-SUR-CENTRAL	Terraza Planta Central Sur	**AIR-LAP1310G-A-K9**	11
AP8	AP-UTN-NORTE-CENTRAL	Terraza Planta Central Norte	**AIR-BR1310G-A-K9-R**	1
AP9	AP-UTN-CAI-TERRAZA	Terraza CAI	**AIR-LAP1310G-A-K9**	6
AP10	AP-UTN-SUR-FACAE	Terraza Planta 1 Sur FACAE	**AIR-BR1310G-A-K9-R**	6
AP11	AP-UTN-NORTE-FACAE	Terraza Planta 1 Norte FACAE	**AIR-BR1310G-A-K9-R**	11

AP12	AP-UTN-FECYT	Terraza Planta 1 NorEste FECYT	**AIR-BR1310G-A-K9-R**	1
AP13	AP-UTN-OESTE-CENTRAL	Terraza Planta 1 Oeste Edificio Central	**AIR-BR1310G-A-K9-R**	6
AP14	AP-UTN-NORTE-ENTRADA	Entrada Norte	**AIR-BR1310G-A-K9-R**	11
AP15	AP-UTN-PISCINA	Exterior Complejo Acuático	**AIR-LAP1310G-A-K9**	6

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.2. Access Points de Interiores

3.8.2.1. FACAE

TABLA 43 Distribución de Canales de los APs de la FACAE

# AP	NOMBRE	UBICACIÓN	MODELO AP	CANALES
AP16	AP-FACAE-PA1	Planta Alta 1 FACAE	AIR-LAP1262N-A-K9	1
AP17	AP-FACAE-PA2	Planta Alta 2 FACAE	AIR-LAP1262N-A-K9	6
AP18	AP-FACAE-PA3	Planta Alta 3 FACAE	AIR-LAP1262N-A-K9	11

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.2.2. FECYT

TABLA 44 Distribución de Canales de los APs de la FECYT

# AP	NOMBRE	UBICACIÓN	MODELO AP	CANALES
AP19	AP-FECYT-PA1	Planta Alta 1 FECYT	AIR-LAP1262N-A-K9	1
AP20	AP-FECYT-PA2	Planta Alta 2 FECYT	AIR-LAP1262N-A-K9	6
AP21	AP-FECYT-PA3	Planta Alta 3 FECYT	AIR-LAP1262N-A-K9	11

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.2.3. Auditorio Agustín Cueva

TABLA 45 Distribución de Canales de los APs del Auditorio Agustín Cueva

# AP	NOMBRE	UBICACIÓN	MODELO AP	CANALES
AP22	AP-AUDITORIO-INTERIOR	Auditorio Agustín Cueva Interior	AIR-LAP1262N-A-K9	1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.2.4. Edificio Central

TABLA 46 Distribución de Canales de los APs del Edificio Central

# AP	NOMBRE	UBICACIÓN	MODELO AP	CANALES
AP23	AP-CENTRAL-PB	Planta Baja Edificio Central	AIR-LAP1262N-A-K9	11
AP24	AP-CENTRAL-PA2	Planta Alta 2 Edificio Central	AIR-LAP1262N-A-K9	1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.2.5. Edificio de Bienestar Universitario

TABLA 47 Distribución de Canales de los APs del Edificio de Bienestar Universitario

# AP	NOMBRE	UBICACIÓN	MODELO AP	CANALES
AP25	AP-BIENESTAR-PB	Planta Baja BIENESTAR	AIR-LAP1262N-A-K9	1
AP26	AP-BIENESTAR-PA1	Planta Alta 1 BIENESTAR	AIR-LAP1262N-A-K9	6
AP27	AP-BIENESTAR-PA2	Planta Alta 2 BIENESTAR	AIR-LAP1262N-A-K9	11
AP28	AP-BIENESTAR-PA3	Planta Alta 3 BIENESTAR	AIR-LAP1262N-A-K9	1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.2.6. FICAYA

TABLA 48 Distribución de Canales de los APs de la FICAYA

# AP	NOMBRE	UBICACIÓN	MODELO AP	CANALES
AP29	AP-FICAYA-PA1	Planta Alta 1 FICAYA	AIR-LAP1262N-A-K9	1
AP30	AP-FICAYA-PA2	Planta Alta 2 FICAYA	AIR-LAP1262N-A-K9	6
AP31	AP-FICAYA-PA3	Planta Alta 3 FICAYA	AIR-LAP1262N-A-K9	11

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.2.7. FICA

TABLA 49 Distribución de Canales de los APs de la FICA

# AP	NOMBRE	UBICACIÓN	MODELO AP	CANALES
AP32	AP-FICA-PB	Planta Baja FICA	AIR-LAP1131AG-A-K9	1
AP33	AP-FICA-PA2D	Planta Alta 2 Derecha FICA	AIR-LAP1131AG-A-K9	11
AP34	AP-FICA-PA2I	Planta Alta 2 Izquierda FICA	AIR-LAP1131AG-A-K9	6
AP35	AP-FICA-PA3D	Planta Alta 3 Derecha FICA	AIR-LAP1131AG-A-K9	6
AP36	AP-FICA-PA3I	Planta Alta 3 Izquierda FICA	AIR-LAP1131AG-A-K9	1
AP37	AP-FICA-PA4	Planta Alta 4 FICA	AIR-LAP1131AG-A-K9	11

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.2.8. FCCSS

TABLA 50 Distribución de Canales de los APs de FCCSS

# AP	NOMBRE	UBICACIÓN	MODELO AP	CANALES
AP38	AP-FCCSS-PA1	Planta Alta 1 FCCSS	AIR-LAP1262N-A-K9	1
AP39	AP-FCCSS-PA2	Planta Alta 2 FCCSS	AIR-LAP1262N-A-K9	6
AP40	AP-FCCSS-PA3	Planta Alta 3 FCCSS	AIR-LAP1262N-A-K9	11

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.2.9. CAI

TABLA 51 Distribución de Canales de los APs del CAI

# AP	NOMBRE	UBICACIÓN	MODELO AP	CANALES
AP41	AP-CAI-PA1	Planta Alta 1 CAI	AIR-LAP1262N-A-K9	6
AP42	AP-CAI-PA2	Planta Alta 2 CAI	AIR-LAP1262N-A-K9	11
AP43	AP-CAI-PA3	Planta Alta 3 CAI	AIR-LAP1262N-A-K9	1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.2.10. POSTGRADO

TABLA 52 Distribución de Canales de los APs de POSTGRADO

# AP	NOMBRE	UBICACIÓN	MODELO AP	CANALES
AP44	AP-POSTGRADO-PB1	Planta Baja POSTGRADO Cubículos	AIR-LAP1262N-A-K9	1
AP45	AP-POSTGRADO-PB2	Planta Baja POSTGRADO	AIR-LAP1262N-A-K9	6
AP46	AP-POSTGRADO-PB-AUDITORIO	Planta Baja Auditorio POSTGRADO	AIR-LAP1262N-A-K9	11
AP47	AP-POSTGRADO-PA1	Planta Alta 1 POSTGRADO	AIR-LAP1262N-A-K9	11
AP48	AP-POSTGRADO-PA2	Planta Alta 2 POSTGRADO	AIR-LAP1262N-A-K9	6

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.2.11. Complejo Acuático

TABLA 53 Distribución de Canal del AP del Complejo Acuático

# AP	NOMBRE	UBICACIÓN	MODELO AP	CANALES
AP49	AP-PISCINA-INTERIOR	Interior Complejo Acuático	AIR-LAP1262N-A-K9	6

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.2.12. POLIDEPORTIVO

TABLA 54 Distribución de Canal del AP del POLIDEPORTIVO

# AP	NOMBRE	UBICACIÓN	MODELO AP	CANALES
AP50	AP-POLIDEPORTIVO	Polideportivo UTN	AIR-LAP1262N-A-K9	1

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.3. Diagramas Unifilares de los Access Points de Interiores

En los siguientes diagramas unifilares utilizaremos la siguiente descripción para diferenciar los diferentes canales de propagación que fueron configurados en cada uno de los APs de acuerdo al análisis de cobertura realizado que se mostrará a continuación:

- Canal 1 (Color Verde)
- Canal 6 (Color Azul)
- Canal 11 (Color Naranja)

3.8.3.1. FACAE

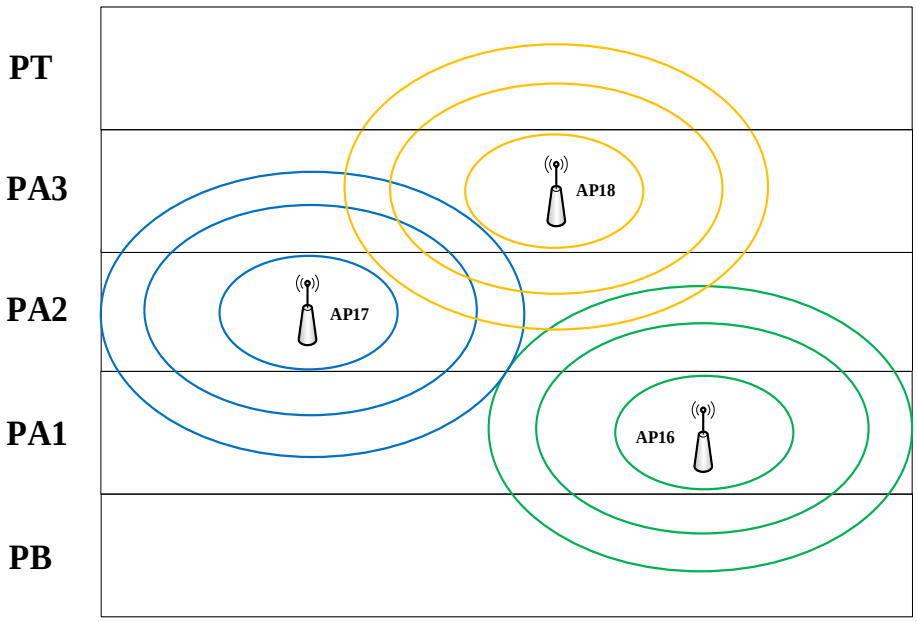


FIGURA 90 Diagrama Unifilar FACAE

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.3.2. FECYT

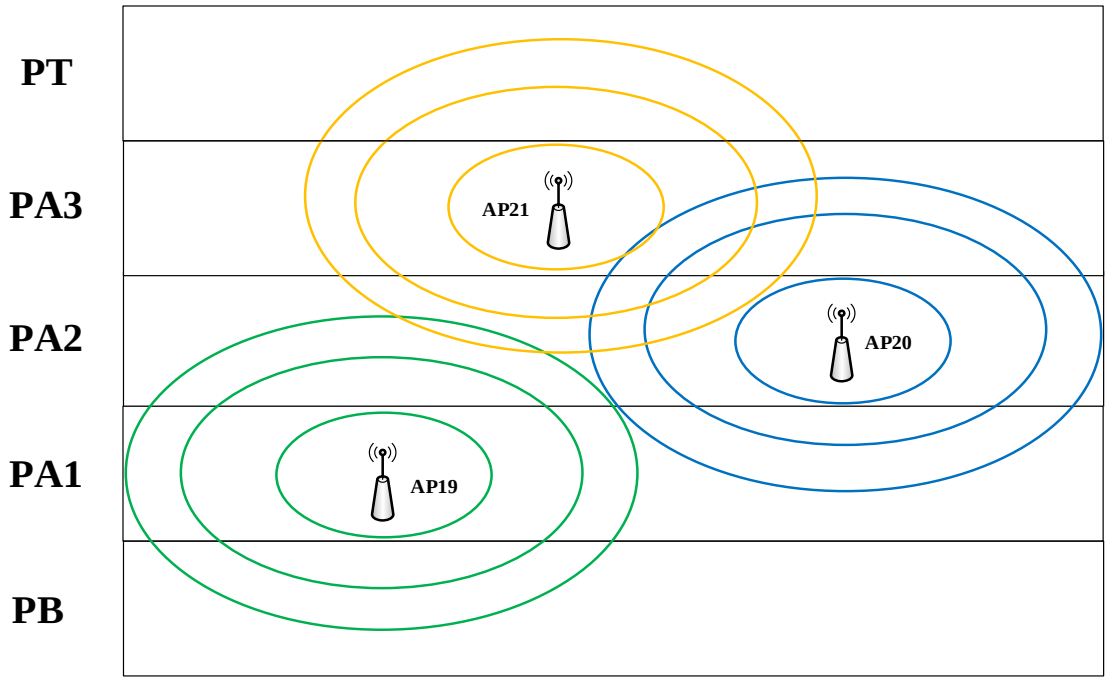


FIGURA 91 Diagrama Unifilar FECYT

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.3.3. Edificio Central

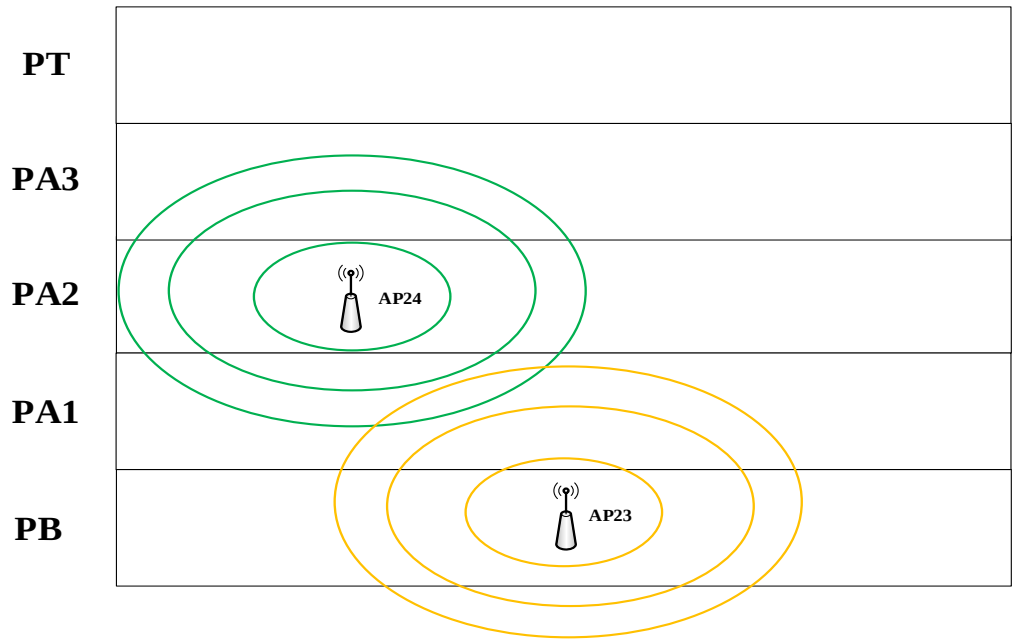


FIGURA 92 Diagrama Unifilar Edificio Central

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.3.4. Edificio de Bienestar Universitario

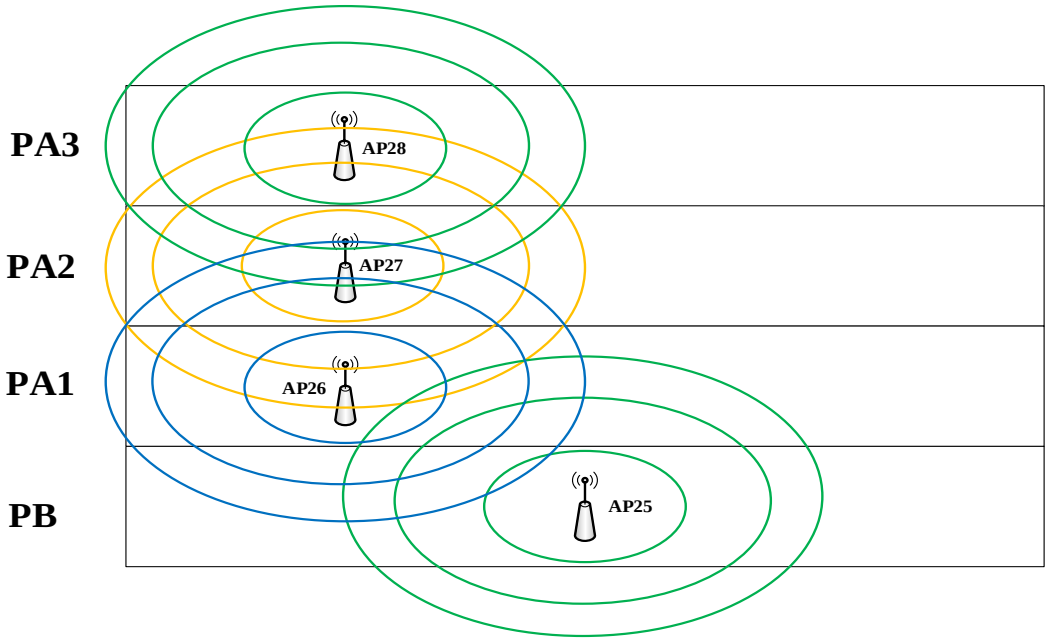


FIGURA 93 Diagrama Unifilar Edificio de Bienestar Universitario

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.3.5. FICAYA

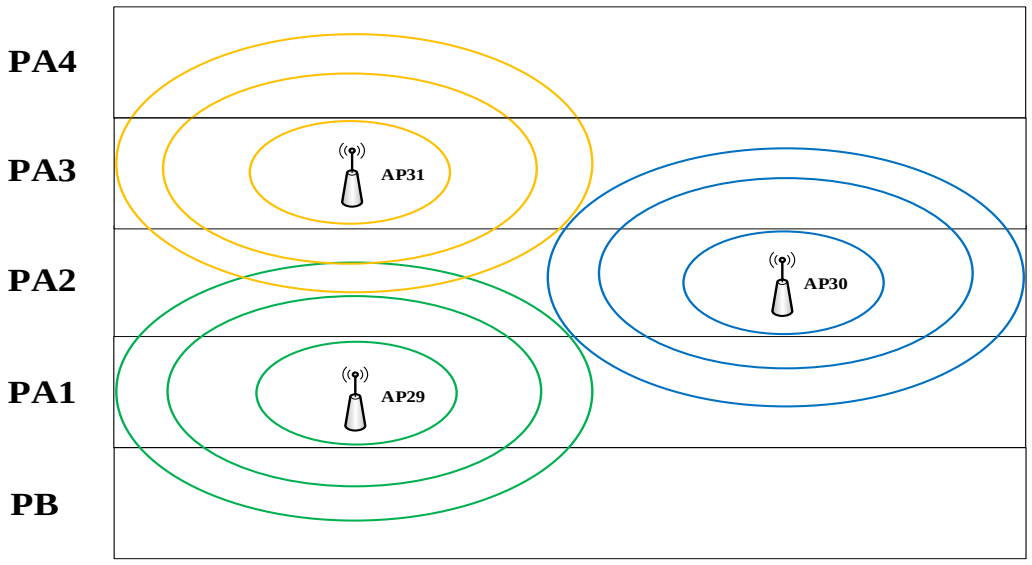


FIGURA 94 Diagrama Unifilar FICAYA

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.3.6. FICA

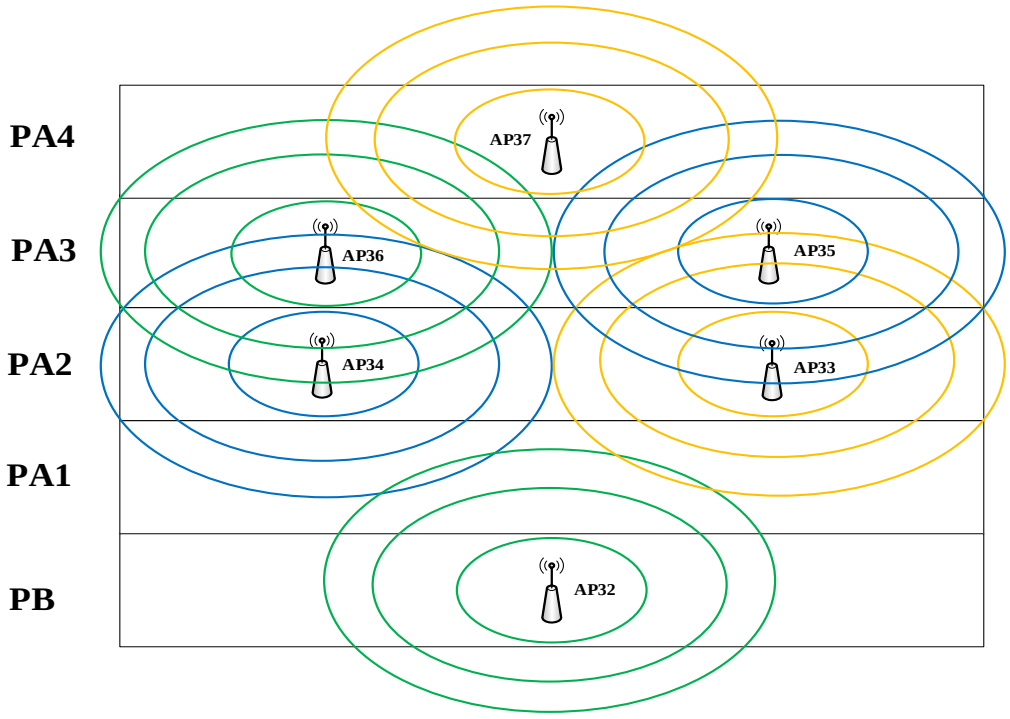


FIGURA 95 Diagrama Unifilar FICA

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.3.7. FCCSS

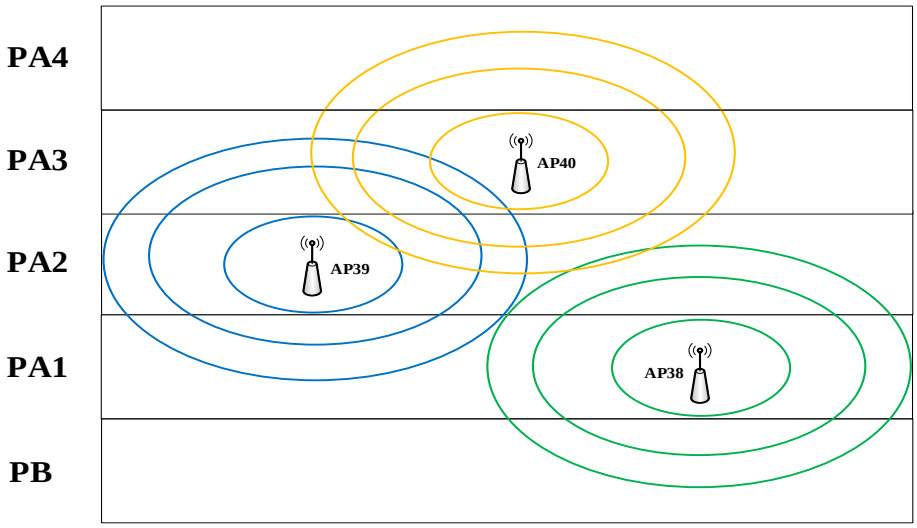


FIGURA 96 Diagrama Unifilar FCCSS

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.3.8. CAI

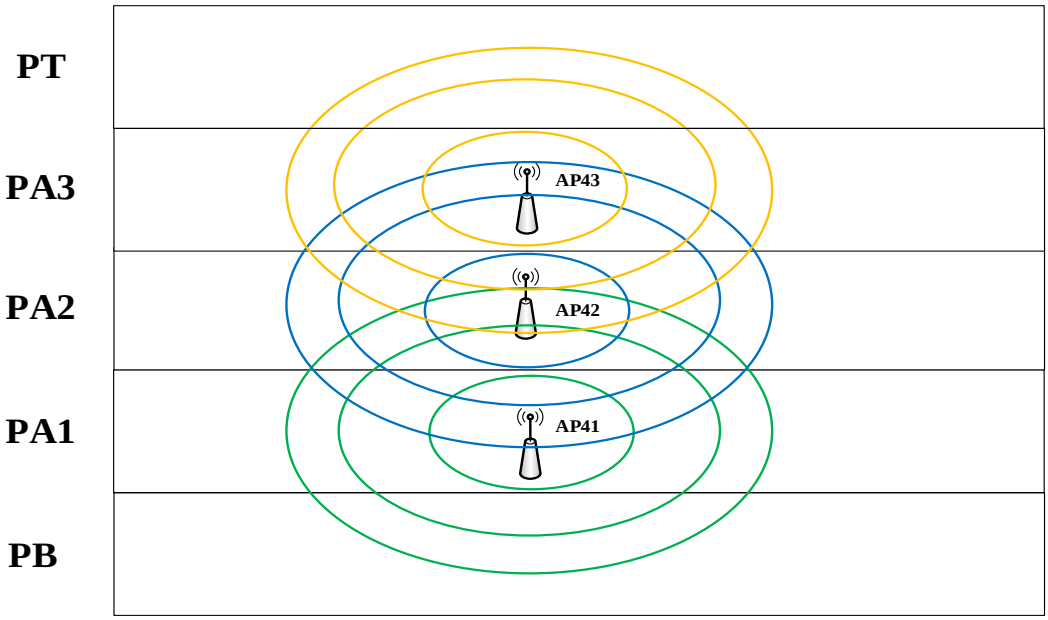


FIGURA 97 Diagrama Unifilar CAI

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.8.3.9. POSTGRADO

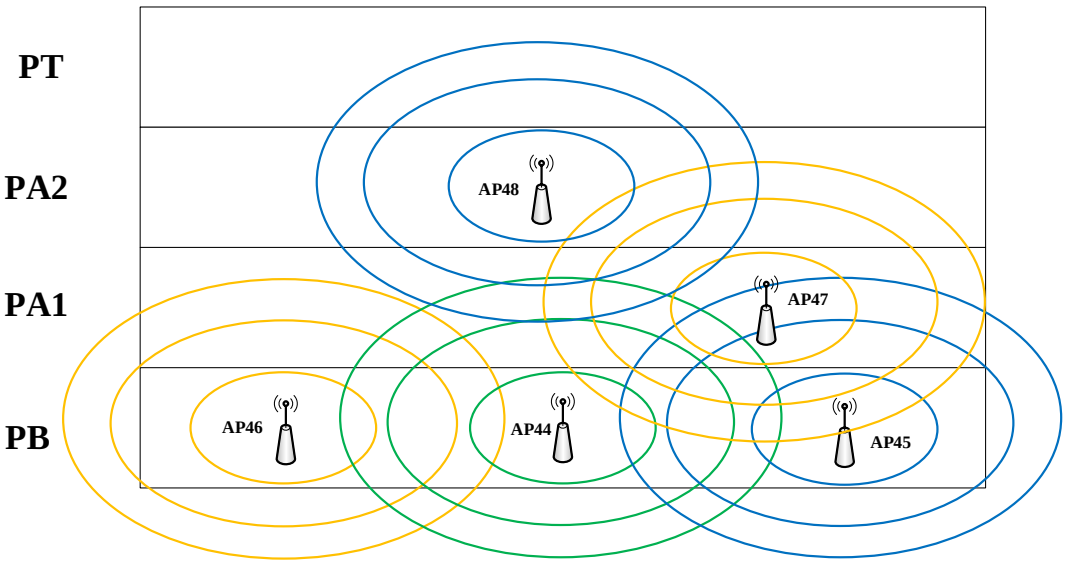


FIGURA 98 Diagrama Unifilar POSTGRADO

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

3.9. GESTIÓN DEL WIRELESS LAN CONTROLLER

Las funciones de gestión se llevan a cabo por medio de un WLC que integra un determinado número de APs en base al soporte de licenciamiento adquirido para la controladora. Las funciones del WLC son la administración de APs, autenticación de usuarios, estadística de los usuarios, política de seguridad, administración de canales, niveles de potencia de salida, etc.

"El proceso de asociación del LAP[150] con el WLC se produce a través de un túnel para pasar los mensajes relativos a 802.11 y los datos de los clientes. Los LAP y el WLC pueden estar localizados en la misma subred o VLAN pero no tiene que ser siempre así. El túnel hace posible el encapsulado de los datos entre ambos AP dentro de nuevos paquetes IP. Los datos tunelizados pueden ser conmutados o enrutados a través de la red del campus según muestra la siguiente

FIGURA 99" (Ariganello & Barrientos Sevilla, 2010, pág. 507).

[150] **LAP** Lightweight Access Point

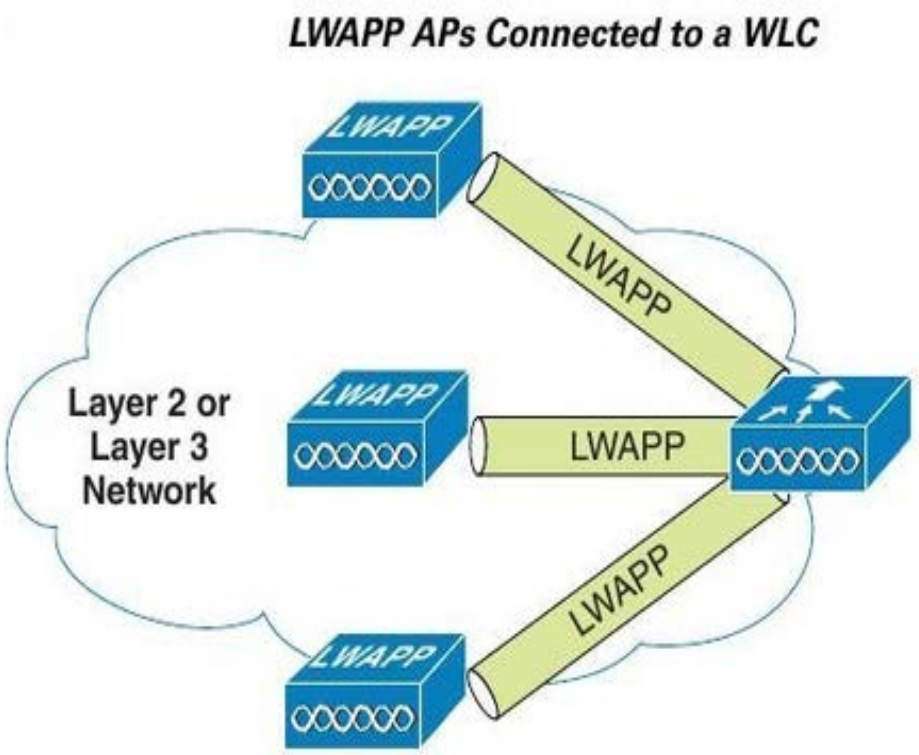


FIGURA 99 LWAPP Access Points
Fuente: (Fürman, 2014)

El LAP y el WLC utilizan el LWAPP[151] como mecanismo de tuneling dividido en dos modos diferentes:

- Mensajes de control LWAPP: son mensajes utilizados para la configuración del LAP y gestionan la operación. Estos mensajes están autenticados y encriptados de tal manera que el LAP es controlado de manera segura solamente por el WLC.
- Datos LWAPP: Los paquetes hacia y desde los clientes Wireless son asociados con el LAP. Los datos son encapsulados dentro de LWAPP pero no están encriptados entre el AP y el WLC.

3.9.1. Funciones del WLC

Una vez que los túneles LWAPP se construyen desde el WLC a uno o más LAP, el WLC puede comenzar a ofrecer una cantidad de funciones adicionales:

- **Asignación de canales dinámicos:** el WLC elige la configuración de los canales de RF que usará cada LAP basándose en otros AP activos en el área.

[151] **LWAPP** Lightweight Access Point Protocol

- **Optimización del poder de transmisión:** el WLC configura el poder de transmisión para cada LAP en función de la cobertura de área necesaria. El poder de transmisión también se ajusta automáticamente de manera periódica.
- **Solución de fallos en la cobertura:** si un LAP deja de funcionar, el agujero que deja la falta de cobertura es solucionado aumentando el poder de transmisión en los LAP que hay alrededor de manera automática.
- **Roaming flexible:** los clientes pueden moverse libremente en capa 2 o en capa 3 con un tiempo de roaming muy rápido.
- **Balanceo de carga dinámico:** cuando 2 o más LAP están posicionados para cubrir la misma área geográfica el WLC puede asociar los clientes con el LAP menos usado distribuyendo la carga de clientes entre los LAP.
- **Monitorización de RF:** el WLC gestiona cada LAP de manera que pueda buscar los canales y monitorizar el uso de la RF. Escuchando en un canal el WLC puede conseguir información sobre interferencias, ruido, señales de diversos tipos.
- **Gestión de la seguridad:** el WLC puede requerir a los clientes Wireless que obtengan una dirección IP de un servidor DHCP confiable antes de permitirles su asociación con la WLAN.

3.9.2. Funciones del LAP

El LAP lleva una configuración muy básica, el AP debe encontrar un WLC para recibir la configuración de tal manera que nunca necesite ser configurado por el puerto de consola (Ariganello & Barrientos Sevilla, 2010, pág. 508).

Los siguientes pasos detallan el proceso de inicio que el LAP tiene que completar antes de entrar en actividad:

1. Se obtiene una dirección de un servidor DHCP.
2. El LAP aprende la dirección IP de los WLC disponibles.
3. Envía una petición de unión al primer WLC que encuentra en la lista de direcciones. Si el primero no responde se intenta con el siguiente. Cuando el WLC acepta al LAP envía una respuesta para hacer efectiva la unión.
4. El WLC compara el código de imagen del LAP con el código que tiene localmente almacenado, el LAP descarga la imagen y se reinicia.
5. El WLC y el AP construyen un túnel seguro LWAPP para tráfico de gestión y otro similar no seguro para los datos del cliente.

3.9.3. Asociación y Roaming del LAP

"Los clientes inalámbricos tienen que negociar una asociación con el LAP, como ocurre en 802.11, pero la arquitectura MAC dividida tiene un efecto diferente en el proceso de asociación con los clientes. Un LAP maneja en tiempo real todas las tareas inalámbricas intercambiando información con el WLC. En efecto, los clientes negocian su asociación con el WLC directamente" (Ariganello & Barrientos Sevilla, 2010, pág. 511).

- Todas las asociaciones de clientes pueden ser gestionadas desde una ubicación centralizada.
- El roaming de los clientes se lleva a cabo de una manera más rápida y más fácil.

La asociación de un cliente se produce con el WLC a través del LAP, cuando el cliente se mueve cambiando de celda cambia de LAP y de túnel LWAPP. Si los LAP pertenecen al mismo controlador el WLC será el mismo aun cuando se mueva de celda en celda.

3.10. ANÁLISIS COMPARATIVO DE PORTALES CAUTIVOS

A continuación se describe los parámetros a evaluar en el análisis comparativo, para ello se ha considerado tres principales portales cautivos de software los cuales se analizarán con cada uno de los parámetros establecidos a continuación:

3.10.1. Descripción de Parámetros

TABLA 55 Descripción de Parámetros

PARÁMETROS	DESCRIPCIÓN
Open Source	Es un término que se utiliza en el software libre donde los usuarios tienen la absoluta libertad de modificar y distribuir el código.
Requerimientos de Instalación	Muy importante al momento de elegir el software a utilizar tanto para la instalación y configuración del portal cautivo.
Configuración	El administrador debe ser capaz de configurar el portal cautivo de manera fácil y sin límite de tiempo.

Seguridad en la Comunicación	La seguridad es una parte fundamental a la hora de elegir el portal cautivo a utilizar, por ello debemos tener en consideración que el servidor podría recibir ataques internos o externos.
Conectividad de Usuarios	Se describe la forma en que el portal cautivo verifica y mantiene la conectividad de un cliente.
Versión	Son mejoras que se realizan en los elementos de configuración que forman la línea base de un software.
Funcionalidad	El usuario debe conocer los pasos a seguir para que no existan inconvenientes y funcione satisfactoriamente.
Descripción del Portal	Indica el principio y fin por el cual fue creado cada portal cautivo.
Lenguaje que soporta	Se basa básicamente en códigos que son interpretados por un ordenador para expresar procesos.
Monitoreo de la Red	El administrador no solo necesita funcionalidad de los portales cautivos, sino también llevar un control de tráfico de la red como estadísticas.
Interfaz del Administrador	Se refiere a la manera en que el administrador puede comunicarse con una computadora y de esta manera poder interactuar entre el usuario y el equipo. Sus principales funciones son: - Administrar la configuración del portal cautivo. - Verificar que usuarios se encuentran conectados.
Interfaz del Usuario	Se refiere a la manera en que el usuario puede autenticarse y acceder al servicio de Internet a través del portal cautivo.

Fuente: (Solano Jiménez & Oña Garcés, 2010)

3.10.2. Comparación entre Portales Cautivos

TABLA 56 Comparación de los principales Portales Cautivos

PARÁMETROS	CHILLISPOT	WIFIDOG	PEPPERSPOT
Open Source	Es una aplicación para portal cautivo con todas las características de Open Source.	Producto Open Source desarrollado por la comunidad de hotspots públicos de Quebec (Canadá) Île Sans Fil.	Está disponible gratuitamente bajo los términos de GNU General Public License version 2.
Requerimientos de Instalación	Este portal requiere de un PC o servidor con Linux más dos tarjetas de red, Freeradius, Apache, MySQL y soporte SSL para el servidor WEB.	Este portal requiere de un servidor GNU/Linux o un router Linksys WRT54G con Open WRT. El servidor de autenticación requiere también de Apache2 y PHP. Los características de hardware mínimo son una PC o servidor con CDROM, procesador de 486 o más, 32 MB en RAM, 1 GB de disco duro y 2 tarjetas Ethernet de 10/100.	Este portal requiere de un servidor WEB que permita redireccionar a un cliente a la página principal de login. El servidor de autenticación requiere soporte del protocolo RADIUS para procedimientos de autenticación y registro. Finalmente requiere de un servicio de enrutamiento.
Configuración	Es un portal sencillo y fácil de configurar porque mantiene soporte de lenguajes por medio del cual los desarrolladores pueden adaptarlo dependiendo de las necesidades.	Es un portal que necesita conocimientos básicos de Linux por su compleja configuración, posee gran soporte de lenguajes y permite configurar las plantillas HTML y los archivos CSS más no el código fuente de la misma.	Se recomienda configurar e instalar el RADIUS y el servicio de enrutamiento en distintos servidores, pero se podría integrar en un solo servidor. Dependiendo del modo que se elija, donde se decida

			instalar PepperSpot necesita ser configurado para IPv4 o IPv6.
Seguridad en la Comunicación	Chillispot con la autenticación UAM soporta SSL. Describe un control administrativo de los clientes.	Posee una seguridad SSL para la comunicación del portal cautivo, esta opción viene por defecto en la instalación del software. El Gateway redirige tráfico de un usuario hacia la Internet solo si el Auth-Server a autenticado correctamente a dicho usuario, de esa manera la contraseña nunca es vista por el Gateway.	PepperSpot utilizará las reglas de algunos Netfilter para continuar la comunicación del cliente hacia la Internet. Así que el sistema debe ser compatible con Netfilter, si no es el caso modificar la configuración de su kernel: Para IPv4 se necesita habilitar soporte para Nat, Mangle y tracking; mientras que para IPv6 solo el soporte básico.
Conectividad de usuarios	Utiliza una conexión en tiempo real.	Mantiene una conexión con los clientes comprobando su actividad en la red. Puede ser una ventaja o desventaja que el propio usuario se registre en el portal para tener acceso a los recursos de la red.	PepperSpot está destinado para ser utilizado por clientes inalámbricos.
Versión	chillispot 1.1.0	wifidog-20090925	pepperspot-0.4
Funcionalidad	Su funcionamiento es comprendido por el cliente.	Su funcionamiento es comprendido por el cliente.	Su funcionamiento es comprendido por el cliente.

Descripción del Portal	Portal Cautivo creado para su aplicación pública o privada.	Portal Cautivo creado para su aplicación pública o privada.	Portal Cautivo creado para su aplicación pública o privada.
Lenguaje que soporta	Está desarrollado en Lenguaje C y la autenticación en lenguaje PERL.	Está desarrollado totalmente en lenguaje C, el portal principal del Servidor de Autenticación está codificado en PHP y usa PostgreSQL como su motor base de datos.	Está desarrollado en Lenguaje PERL.
Monitoreo de la Red	Permite el monitoreo de la red con cuadros estadísticos básicos del tiempo de uso de la red por usuario y el ancho de banda utilizado.	Es una aplicación que permite el monitoreo de la red en tiempo real, con informes y estadísticas que incluyen: los 10 consumidores más altos del ancho de banda, los 10 usuarios más frecuentes, los 10 usuarios más móviles, exportación de los datos a SQL, cuantos usuarios utilizan realmente la red, registro de la conexión, gráfico de uso de la red (por hora, día laborable y mes), informe individual del usuario, ubicación geográfica de los usuarios conectados mediante google maps, información de los nodos más populares por visita, información del estado de la red, estado del nodo, registro interno e informe del registro del usuario.	Carece de monitoreo de la red.
Interfaz del Administrador	No existe interfaz	Amigable y Fácil de utilizar.	Amigable y Fácil de utilizar.
Interfaz del Usuario	Amigable y Fácil de utilizar.	Amigable y Fácil de utilizar.	Amigable y Fácil de utilizar.

Fuente: (Fierro Fierro & González Bonifaz, 2012)

3.11. POLÍTICAS DE SEGURIDAD

- El mantenimiento de la seguridad de la red inalámbrica de la universidad requiere métodos que aseguren que sólo los usuarios autorizados puedan tener acceso al mismo. De tal manera, el equipo debe tener las seguridades físicas necesarias para evitar que se vean afectados los servicios de la red inalámbrica.
- Todos los puntos de acceso deben de ser registrados y aprobados por el administrador de la Red.
- La instalación, administración y uso de los dispositivos de la red inalámbrica debe estar de acuerdo con las especificaciones y normas de redes inalámbricas y con las políticas implantadas en la universidad.
- El SSID debe estar configurado para que sea identificado con la universidad.
- Ningún individuo debe conectar ni instalar cualquier equipo de comunicaciones a la red sin la previa autorización del administrador.
- Las comunicaciones inalámbricas no proveen codificación de los datos transmitidos. La protección de los datos es responsabilidad del usuario y de la aplicación que utilice para transmitir los datos.
- No se debe permitir ni fomentar el uso de la red inalámbrica para utilizar los sistemas administrativos de la Universidad donde se transmiten o reciben datos confidenciales.
- El equipo del usuario conectado a la red inalámbrica, está sujeto a monitoreo, pruebas de penetración y auditorías de seguridad.
- Cualquier equipo que represente un riesgo de seguridad para la red de comunicaciones del campus universitario, podrá ser desconectado de la red y la persona que tenga registrado el equipo será notificado.
- Cualquier situación que no se pueda resolver con usuarios referente al sistema de red inalámbrica, será referido al DDTI[152] ubicado en el Edificio Central de la UTN específicamente al Área de Redes y Comunicaciones para tomar la decisión que sea necesaria.

[152] **DDTI** Dirección de Desarrollo Tecnológico e Informático

CAPITULO IV

4. IMPLEMENTACIÓN DE LA RED LAN INALÁMBRICA Y PRUEBAS DE FUNCIONALIDAD EN LA UNIVERSIDAD TÉCNICA DEL NORTE

En el siguiente capítulo se procedió con la configuración de los equipos a utilizar y las pruebas de funcionalidad que demuestren el mejoramiento de la performance de acceso de los usuarios y la confiabilidad de la solución planteada en la implementación de la red LAN Inalámbrica en la UTN.

4.1. CONFIGURACIÓN DEL WIRELESS LAN CONTROLLER

4.1.1. Propiedades de Puerto Serial

Conectar la fuente de alimentación al WLC. Utilizando Hyperterminal, conectar al puerto de consola de la controladora usando la siguiente configuración que se muestra en la FIGURA 100

FIGURA 100

FIGURA 100 Propiedades del Puerto serial

Fuente: Software Hyperterminal

4.1.2. Borrar y Reiniciar la Configuración

Borramos la configuración del WLC, seguido del reinicio del sistema para poder escribir la nueva configuración para esto utilizamos los siguientes comandos:

(Cisco Controller) >**clear config**

Are you sure you want to clear the configuration? (y/n) y

Configuration Cleared!

(Cisco Controller) >**reset system**

The system has unsaved changes.

Would you like to save them now? (y/N) n

Configuration Not Saved!

Are you sure you would like to reset the system? (y/N) y

System will now restart!

4.1.3. Atributos Básicos de Configuración

La primera vez que reinicie el controlador WLAN, un asistente de configuración le pedirá que introduzca los atributos básicos de configuración. Usted sabrá que ha introducido la interfaz del asistente cuando vea “Welcome to the Cisco Wizard Configuration Tool”. Pulsar la tecla de retorno permite utilizar las opciones de configuración por defecto. La opción de configuración por defecto estará entre corchetes según el asistente que se pida. El primer indicador que se pide es el nombre del sistema (System Name), pulse Intro para mantener el valor por defecto. El siguiente le pide solicitar el nombre de usuario y contraseña administrativa.

Welcome to the Cisco Wizard Configuration Tool

Use the '-' character to backup

System Name [Cisco_49:43:c0]: **WLC-UTN**

Enter Administrative User Name (24 characters max): ********

Enter Administrative Password (24 characters max): <********>

Introduzca la información de la interfaz de administración

Management Interface IP Address: **172.16.2.10**

Management Interface Netmask: **255.255.255.0**

Management Interface Default Router: **172.16.2.1**

Management Interface VLAN Identifier (0 = untagged): **0**

Management Interface Port Num [1 to 8]: **1**

Management Interface DHCP Server IP Address: **172.16.128.8**

Configure la dirección IP del Virtual Gateway con 1.1.1.1 (esto es aceptable porque no se está usando esto para enrutamiento). La dirección IP del Virtual Gateway es por lo general una dirección ficticia, sin asignación de IP, tal como la dirección que estamos usando aquí.

Virtual Gateway IP Address: **1.1.1.1**

Configurar el grupo de la movilidad y el nombre de la red como "WUTN.Estudiantes". Permitir las direcciones IP estáticas, pero no configurar un servidor RADIUS ahora.

Mobility/RF Group Name: **WLC-UTN**

Network Name (SSID): **WLC-UTN**

Configure DHCP Bridging Mode [yes][NO]: NO

Allow Static IP Addresses [YES][no]: **YES**

Configure a RADIUS Server now? [YES][no]: **no**

Warning! The default WLAN security policy requires a RADIUS server.

Please see documentation for more details.

Utilice los valores predeterminados para el resto de la configuración. (Pulsar Intro en cada pregunta).

Enter Country Code (enter 'help' for a list of countries) [US]: EC

Enable 802.11b Network [YES][no]:

Enable 802.11a Network [YES][no]:

Enable 802.11g Network [YES][no]:

Enable Auto-RF [YES][no]:

Configure a NTP server now? [YES][no]: no

Configure the system time now? [YES][no]: no

Warning! No AP will come up unless the time is set.

Please see documentation for more details.

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes

Configuration saved!

Resetting system with new configuration...

Cuando el WLC ha terminado de reiniciarse, se debe iniciar sesión con el nombre de usuario "*******" y la contraseña "*******".

User: ***********

Password: <***********>

Cambiar el controlador del sistema a "WLC_CONTROLLER" con el siguiente comando de configuración.

(Cisco Controller) > **config prompt WLC-UTN**

(WLC-UTN) >

Activar Telnet y HTTP para tener acceso al Wireless LAN Controller.

(WLC-UTN) > **config network telnet enable**

(WLC-UTN) > **config network webmode enable**

Guardar la configuración con el comando "save config", Ejecutar.

(WLC-UTN) > **save config**

Are you sure you want to save? (y/n) **y**

Configuration Saved!

4.1.4. Resumen de la Interfaz y WLAN

Para comprobar la configuración, puede emitir el resumen de la interfaz de programa y mostrar el resumen de la WLAN.

(WLC-UTN) >**show interface summary**

Interface Name Port Vlan Id IP Address Type Ap Mgr Guest

--- ---- --- --- --- --- ---

management LAG 2 172.16.2.10 Static Yes No

service-port N/A N/A 192.168.1.1 Static No No

virtual N/A N/A 1.1.1.1 Static No No

wireless.administrativos LAG 112 172.16.112.2 Dynamic No No

wireless.docentes LAG 96 172.16.96.2 Dynamic No No

wireless.estudiantes LAG 128 172.16.128.2 Dynamic No No

wireless.eventos LAG 160 172.16.160.2 Dynamic No No

(WLC-UTN) >**show wlan summary**

Number of WLANs..... 4

WLAN ID WLAN Profile Name / SSID Status Interface Name

--- --- --- ---

1 Docentes UTN / WUTN.Docentes Enabled wireless.docentes

2 Administrativos UTN / WUTN.Admin Enabled wireless.administrativos

3 Estudiantes UTN / WUTN.Estudiantes Enabled wireless.estudiantes

4 Eventos UTN / WUTN.Eventos Enabled wireless.eventos

4.1.5. Verificación de la versión del Software en el WLC

Compruebe la versión del software del controlador con el comando **show sysinfo** y **show boot**. En la parte inferior, vemos que el software funcionando para el WLC es el 7.0.116.0. Si el software no está actualizado, inicie sesión en Cisco.com y lea las instrucciones para actualizar el software en el WLC.

(WLC-UTN) >**show sysinfo**

Manufacturer's Name..... Cisco Systems Inc.

Product Name..... Cisco Controller

Product Version..... 7.0.116.0

Bootloader Version..... 1.0.1

Field Recovery Image Version..... 6.0.182.0

Firmware Version..... FPGA 1.3, Env 1.6, USB console 1.27

Build Type..... DATA + WPS

System Name..... WLC-UTN

System Location.....

System Contact.....

System ObjectID..... 1.3.6.1.4.1.9.1.1069

IP Address..... 172.16.2.10

Last Reset..... Software reset

System Up Time..... 2 days 12 hrs 20 mins 38 secs

System Timezone Location.....

Current Boot License Level..... base

Current Boot License Type..... Permanent

Next Boot License Level..... base

Next Boot License Type..... Permanent

Configured Country..... Multiple Countries:US,EC

Operating Environment..... Commercial (0 to 40 C)

Internal Temp Alarm Limits..... 0 to 65 C

Internal Temperature..... +36 C

External Temperature..... +22 C

Fan Status..... OK

State of 802.11b Network..... Enabled

State of 802.11a Network..... Enabled

Number of WLANs..... 6

Number of Active Clients..... 10

Burned-in MAC Address..... 50:3D:E5:19:AC:80

Power Supply 1..... Present, OK

Power Supply 2..... Absent

Maximum number of APs supported..... 50

(WLC-UTN) >**show boot**

Primary Boot Image..... 7.0.116.0 (default) (active)

Backup Boot Image..... 7.3.101.0

4.1.6. WLC Software Upgrade

Se puede utilizar cualquiera de estos dos métodos con el fin de actualizar el Cisco WLC:

- Graphical User Interface (GUI)
- Command Line interface (CLI)

Esta secuencia se recomienda para la actualización de software del WLC:

1. Cargar un backup de la configuración del controlador a un servidor TFTP.
2. Desactivar las redes 802.11a y 802.11b/g en el controlador.
3. Actualizar la imagen primaria en el controlador.
4. Actualizar la imagen boot en el controlador.
5. Vuelva habilitar las redes 802.11a y 802.11b/g en el controlador.

Es muy recomendable hacer una copia de seguridad (backup) de la configuración del Wireless LAN Controller antes de realizar la actualización.

4.1.6.1. Procedimiento de Actualización GUI

Cuando se actualiza el WLC con el uso de la interfaz gráfica de usuario, se pierde conectividad de capa 3 (IP) dentro de los períodos de tiempo cuando se reinicia el controlador. Por esta razón, se recomienda que utilice una conexión por el puerto de consola para comprobar el estado del controlador durante el proceso de actualización y así agilizar cualquier procedimiento de recuperación, si es necesario.

Cuando se actualiza el software del controlador, el software en los APs asociados al WLC también se actualiza automáticamente. Cuando un AP está cargando el software, cada uno de sus Leds parpadea en sucesión. Hasta 10 Access Points pueden ser al mismo tiempo actualizados desde el controlador. No apague el controlador o cualquier APs durante este proceso, de lo contrario, puede dañar la imagen del software. Cuando se actualiza el controlador a una versión de software intermedio, espere hasta que todos los APs se unan al controlador para actualizar a la versión intermedia antes de instalar la siguiente versión

del software. La actualización de un controlador con un gran número de APs puede llegar a tardar hasta 30 minutos, dependiendo del tamaño de la red. Sin embargo, con el aumento del número de actualizaciones simultáneas de los APs soportados en la versión de software, el tiempo de actualización debe ser reducido significativamente. Los APs deben permanecer encendidos, y el controlador no debe reiniciarse durante este tiempo.

Instrucciones paso a paso:

1. Complete estos pasos para acceder al controlador a través del navegador:

a. HTTP a la dirección IP de administración del controlador (por ejemplo, http://172.16.2.10). Se pedirán las credenciales de usuario.

b. Introduzca el nombre de usuario y la contraseña del controlador y haga clic en Aceptar.

c. La ventana Monitor aparece. La información resumida del controlador muestra la versión actual del software que se ejecuta en el WLC (FIGURA 101).

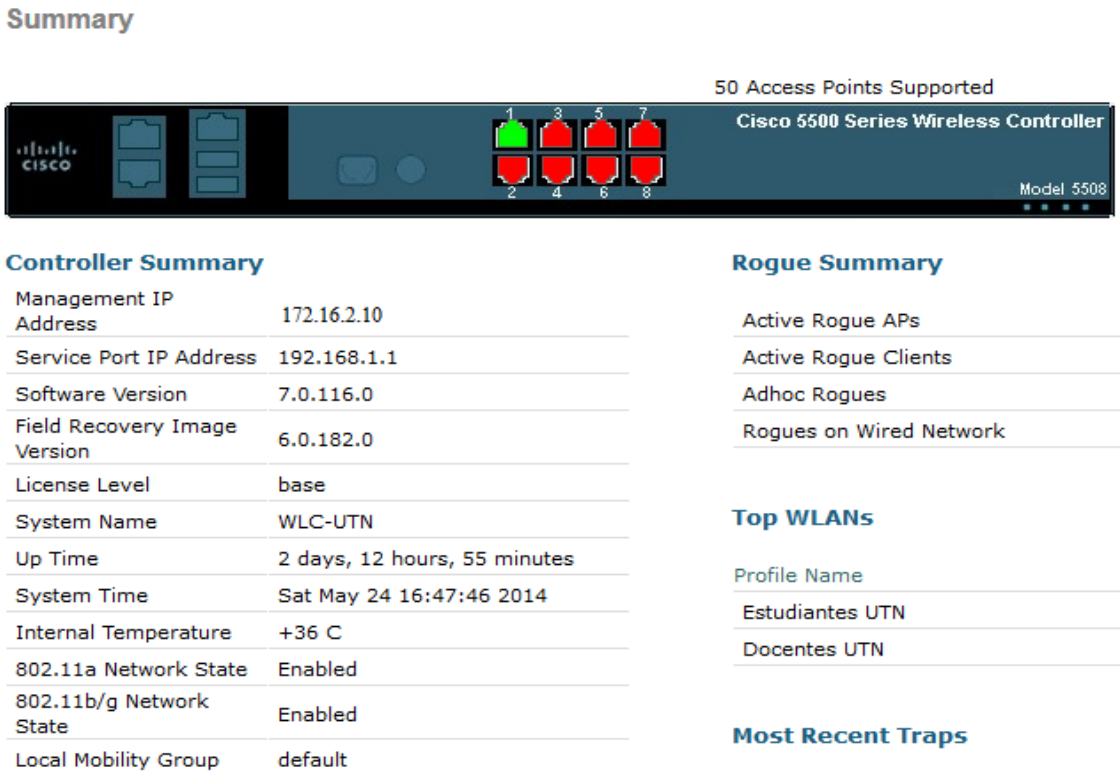


FIGURA 101 Software versión 7.0.116.0
Fuente: Cisco Wireless LAN Controller 5508

2. Siga estos pasos e orden a fin de definir los parámetros de descarga de la actualización de software:

a. Haga clic en el menú "**COMMANDS**" en la parte superior de la ventana.

El archivo de descarga del controlador aparece en la ventana.

b. Introduzca los parámetros de descarga.

Los parámetros a definir incluyen:

- TFTP server IP Address
- File Path
- Maximum retries
- Timeout
- File Name

Los parámetros usados en la actualización del software 7.0.116.0 del WLC son:

- TFTP server IP Address: 172.16.2.254 (PC)
- Maximum retries: 10
- Timeout: 6
- File Path: ./
- File Name: AIR-CT5500-K9-7-0-116-0.aes

c. Haga clic en Download para iniciar el proceso de actualización (FIGURA 102).

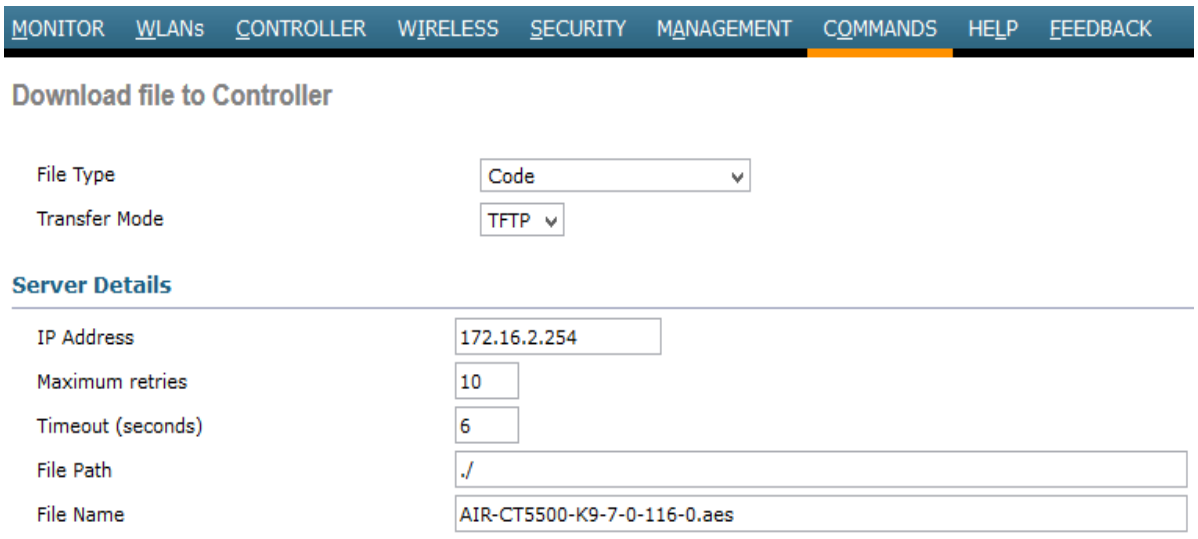


FIGURA 102 Download file to Controller

Fuente: Cisco Wireless LAN Controller 5508

Cuando se realiza la actualización de la interfaz gráfica de usuario (GUI), por File Path, se puede insertar un punto (.) siempre y cuando la imagen esté en el directorio root de su servidor TFTP. De esta manera, usted no tiene que introducir el path donde está la imagen guardada.

3. Reinicie el sistema después de la transferencia del archivo para que el nuevo software tenga efecto.

4. En la ventana System Reboot (FIGURA 103), haga clic en “Save and Reboot” en la parte superior derecha de la ventana.

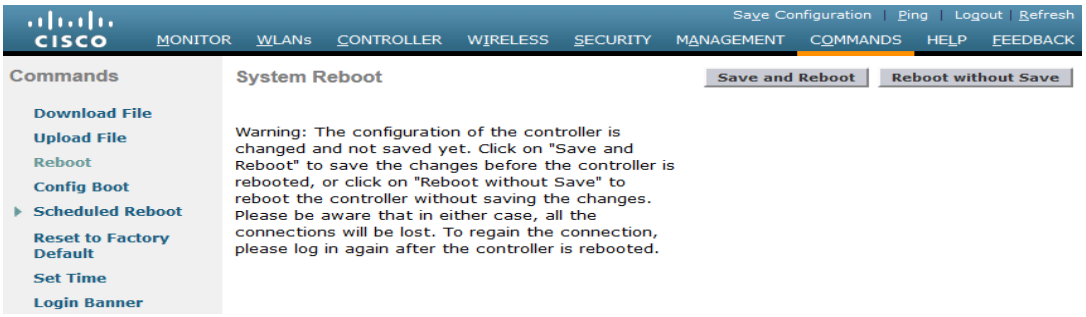


FIGURA 103 Save and Reboot del WLC
Fuente: Cisco Wireless LAN Controller 5508

5. Después del reinicio, se puede volver a iniciar sesión en el WLC y verificar que la nueva versión de software se ejecuta.

4.1.6.2. Procedimiento de Actualización CLI

Instrucciones pasó a paso:

1. Asegúrese de que al servidor TFTP se puede acceder desde el controlador y asegúrese de que el archivo de actualización se encuentra en el directorio root del servidor TFTP. Consulte en el Wireless Software Center (solo clientes registrados) con el fin de descargar las imágenes más recientes del software. Copie los archivos en el directorio por defecto en el servidor TFTP.

2. Es mejor completar este procedimiento a través del puerto de consola, pero se puede también por SSH o Telnet (si está habilitado) a la dirección IP de management del WLC con el fin de completar el procedimiento. El uso de SSH o Telnet resulta en la pérdida de conectividad con la controladora durante el siguiente proceso de reinicio de la

descarga de imagen. Por lo tanto, el acceso a la consola debe estar disponible a fin de acelerar el troubleshooting y recovery del controlador si la actualización falla. Acceder al controlador y ejecutar el comando "**show sysinfo**" con el fin de verificar el software actual que se ejecuta en el controlador. El resultado al desplegar el comando **show sysinfo**, nos muestra que el WLC ejecuta la versión 7.0.116.0

3. Completar estos pasos para definir los parámetros de descarga:

a. Ejecutar el comando **transfer download mode tftp** con el fin de definir el modo de transferencia del archivo.

b. Ejecutar el comando **transfer download serverip** TFTP_server_IP_address con el fin de definir la dirección IP del servidor TFTP.

c. Ejecutar el comando **transfer download path** TFTP_server_path con el fin de definir el path del directorio TFTP por defecto donde el software del sistema operativo del WLC se encuentra.

d. Ejecutar el comando **transfer download filename** filename con el fin de especificar el nombre de la imagen.

```
(WLC-UTN) >transfer download datatype code
(WLC-UTN) >transfer download mode tftp
(WLC-UTN) >transfer download serverip 172.16.2.254
(WLC-UTN) >transfer download path .
(WLC-UTN) >transfer download filename AIR-CT5500-K9-7-0-116-0.aes
```

4. Ejecutar el comando de **transfer download start** con el fin de iniciar el proceso de actualización.

```
(WLC-UTN) >transfer download start
Mode..... TFTP
Data Type..... Code
TFTP Server IP..... 172.16.2.254
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path..... ./
TFTP Filename..... AIR-CT5500-K9-7-0-116-0.aes
This may take some time.
Are you sure you want to start? (y/N) y
```

TFTP Code transfer starting.
TFTP receive complete... extracting components.
/mnt/application

Writing new RTOS to flash disk.

Executing install_rtos script.

Writing new Code to flash disk.

Executing install_code script.

Writing new APIB to flash disk.

Executing install_apib script.

Executing fini script.

TFTP File transfer is successful.
Reboot the controller for update to complete.
Optionally, pre-download the image to APs before rebooting to reduce network downtime.

5. Reinicie el WLC después de que se complete el proceso de actualización para que el nuevo código tenga efecto.
6. Ejecutar el comando **reset system**, e ingresar **y** o **yes** en respuesta a la pregunta “Would you like to save them now?”.

En el WLC Serie 5500, no se puede actualizar la versión del gestor de arranque (bootloader) debido a las limitaciones de hardware. Además, este modelo no requiere de una actualización del gestor de arranque al igual que los modelos más grandes de WLC. Se puede actualizar el boot image antes o después de la imagen principal.

4.1.7. Remover la imagen primaria o secundaria del WLC

El WLC, por defecto, mantiene dos imágenes. Estas son la imagen primaria y la imagen de backup. La imagen primaria es la imagen activa usada por el WLC mientras que la imagen de backup es utilizada como un respaldo de la imagen activa.

Cuando actualizas el WLC con una nueva imagen, el WLC automáticamente copia la nueva imagen sobre la imagen de backup.

Para ver la imagen activa que el WLC está ejecutando actualmente (la imagen primaria), se debe hacer clic en el menú Monitor de la interfaz gráfica de usuario (GUI) del WLC y mirar el campo Software Version debajo de Controller Summary. Desde la línea de comandos (CLI) se puede utilizar el comando “show boot” para ver la imagen primaria y de backup presentes en el WLC.

WLC-UTN) >**show boot**

Primary Boot Image..... 7.0.116.0 (default) (active)

Backup Boot Image..... 7.3.101.0

Con el fin de eliminar o sobrescribir una imagen en el WLC, arranca el WLC con la imagen que desea conservar y realizar una actualización. De esta manera, la nueva imagen reemplaza la imagen de backup.

También puede cambiar la imagen activa al arranque del WLC manualmente utilizando el comando config boot **<**primary/backup**>**.

(WLC-UTN) >config boot ?

primary Sets the primary image as active.

backup Sets the backup image as active.

El config boot image puede ser también configurado con la interfaz gráfica de usuario del WLC. Consulte “How to Use the Backup Image on Wireless LAN Controllers (WLCs)” para obtener más información sobre el procedimiento detallado (ANEXO 5).

Se necesita guardar y reiniciar la configuración del WLC para que la controladora utilice la nueva imagen activa.

4.1.8. Interfaces

En el WLC tenemos siete interfaces que se han configurado de la siguiente manera como se muestra en la

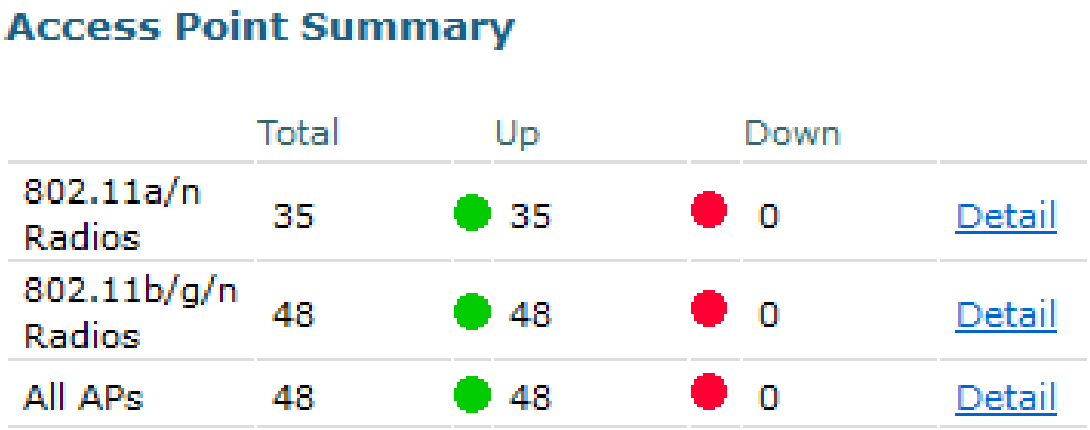
FIGURA 104 (Controller −> Interfaces):

FIGURA 104 Interfaces

Fuente: Cisco Wireless LAN Controller 5508

4.1.9. Gestión de Access Points

El WLC nos permite integrar por cuestiones de licenciamiento hasta un determinado número de Access Point, de los cuales se han instalado 50 APs y se encuentran funcionando 48 APs como se indica en la FIGURA 105.



Access Point Summary

	Total	Up	Down	
802.11a/n Radios	35	35	0	Detail
802.11b/g/n Radios	48	48	0	Detail
All APs	48	48	0	Detail

FIGURA 105 Access Point Summary
Fuente: Cisco Wireless LAN Controller 5508

La siguiente FIGURA 106 nos muestra el número de APs que se encuentran funcionando con el WLC con algunos parámetros importantes como el nombre, modelo, MAC, entre otros.

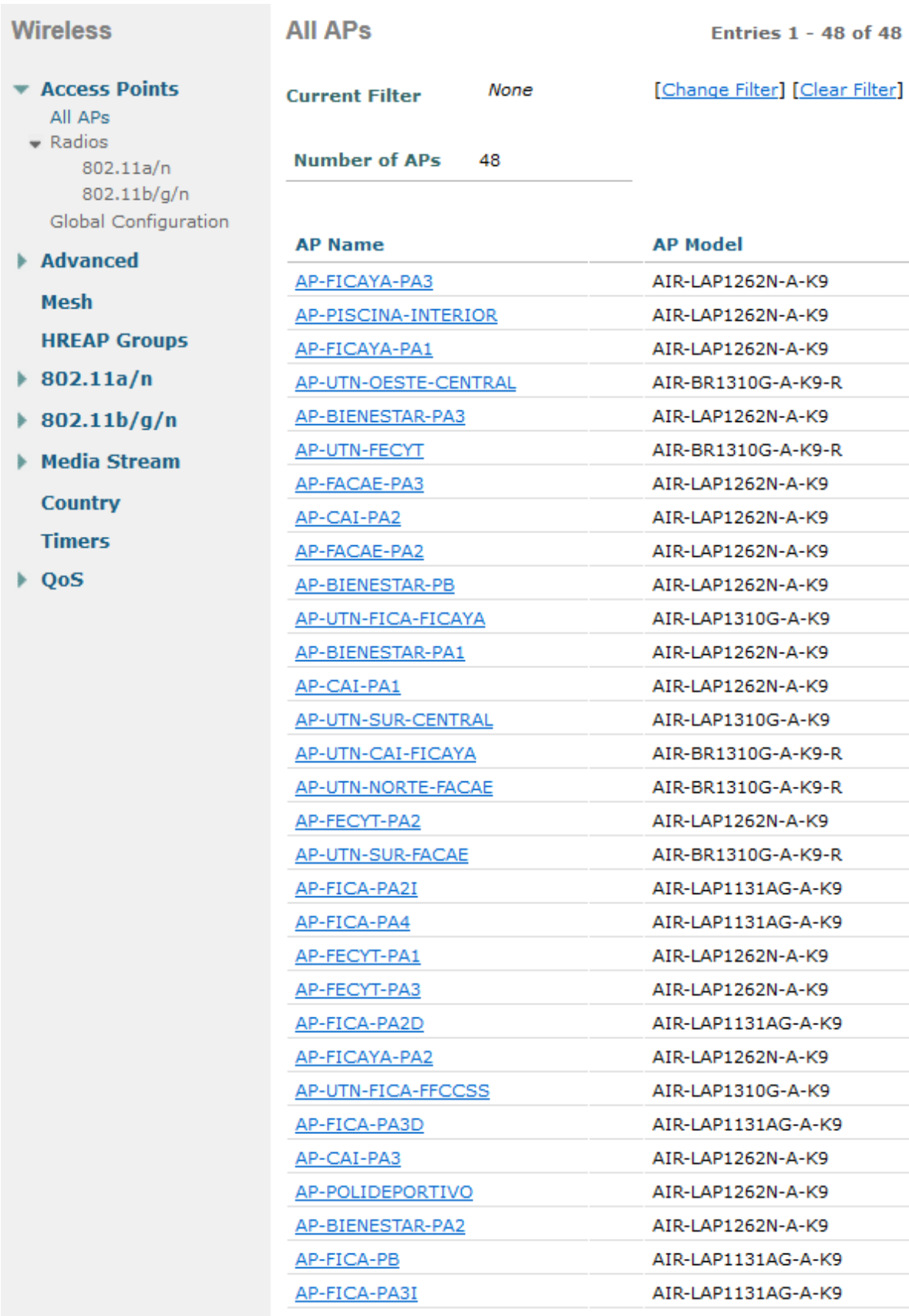


FIGURA 106 Parámetros de todos los APs

Fuente: Cisco Wireless LAN Controller 5508

4.1.9.1. Configuración del Access Point

Para la configuración de un AP que se integra por primera vez al WLC se debe configurar parámetros generales como el nombre del AP, ubicación, dirección IP, máscara, gateway y DNS (FIGURA 107 y FIGURA 108).

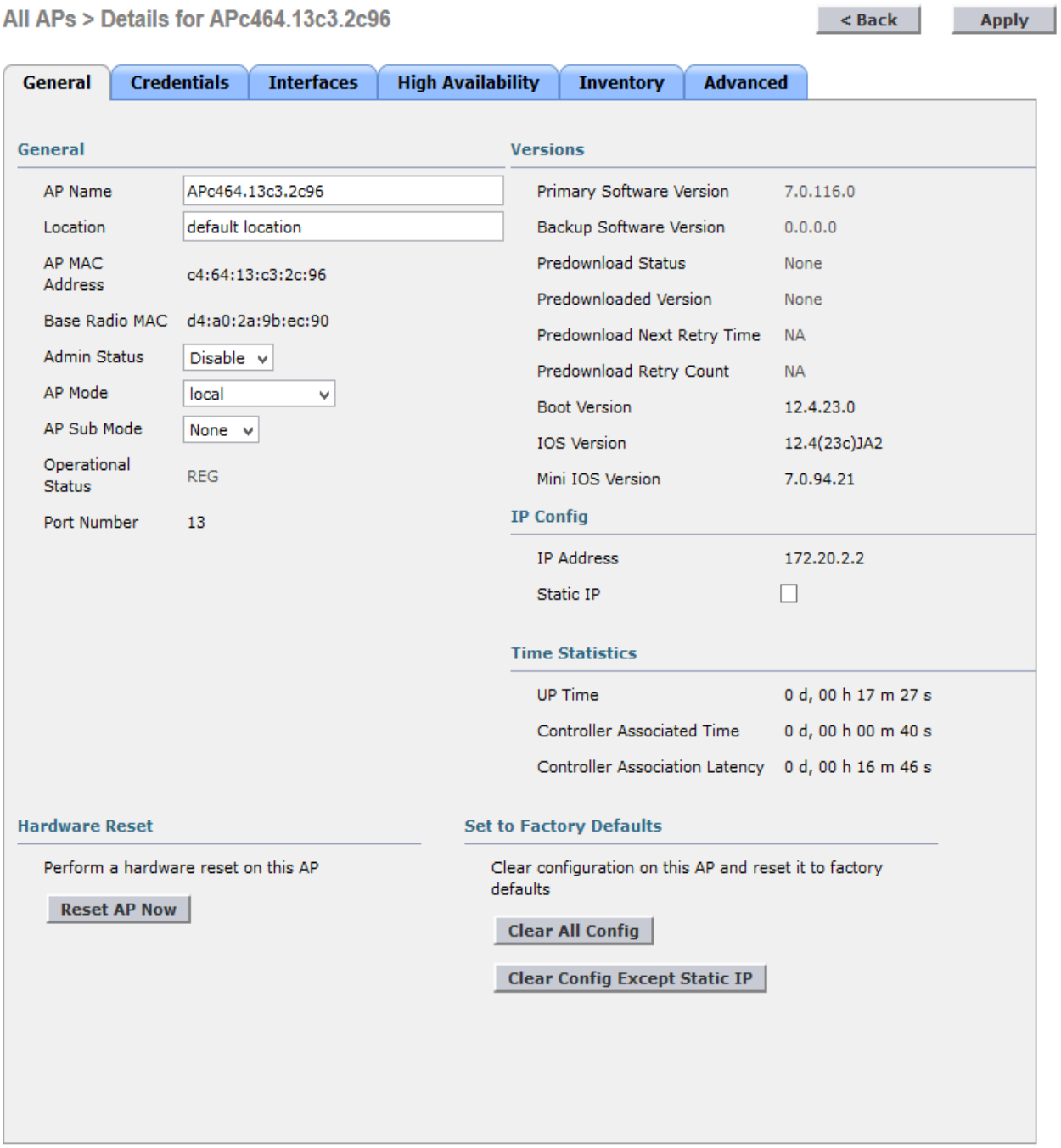


FIGURA 107 Configuración por defecto del AP

Fuente: Cisco Wireless LAN Controller 5508

FIGURA 108 Configuración del AP en una determinada VLAN

Fuente: Cisco Wireless LAN Controller 5508

4.1.10. Gestión de WLANs

Para la creación de una WLAN se configura el enlace a las interfaces virtuales generadas en el WLC como se indica en el subtema 4.1.8, para utilizar el segmento de red o VLAN determinado para el nuevo SSID (

FIGURA **109**).

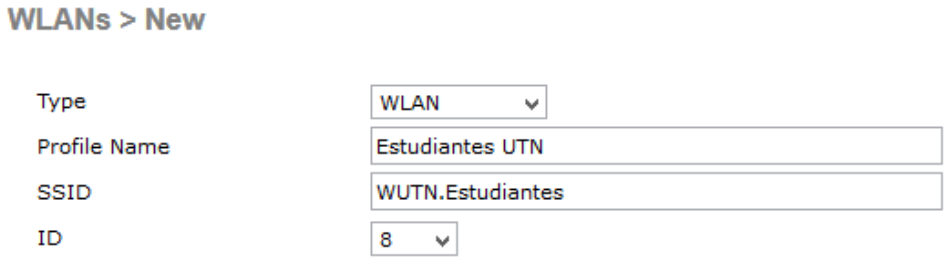


FIGURA 109 Creación de la WLAN

Fuente: Cisco Wireless LAN Controller 5508

Una vez creada la WLAN habilitamos en el parámetro “Status” la casilla de enabled, en el parámetro “Interface” escogemos la interfaz “wireless.estudiantes” y por último dejamos habilitado el “Broadcast SSID” para la visibilidad y propagación de la red inalámbrica (FIGURA 110).

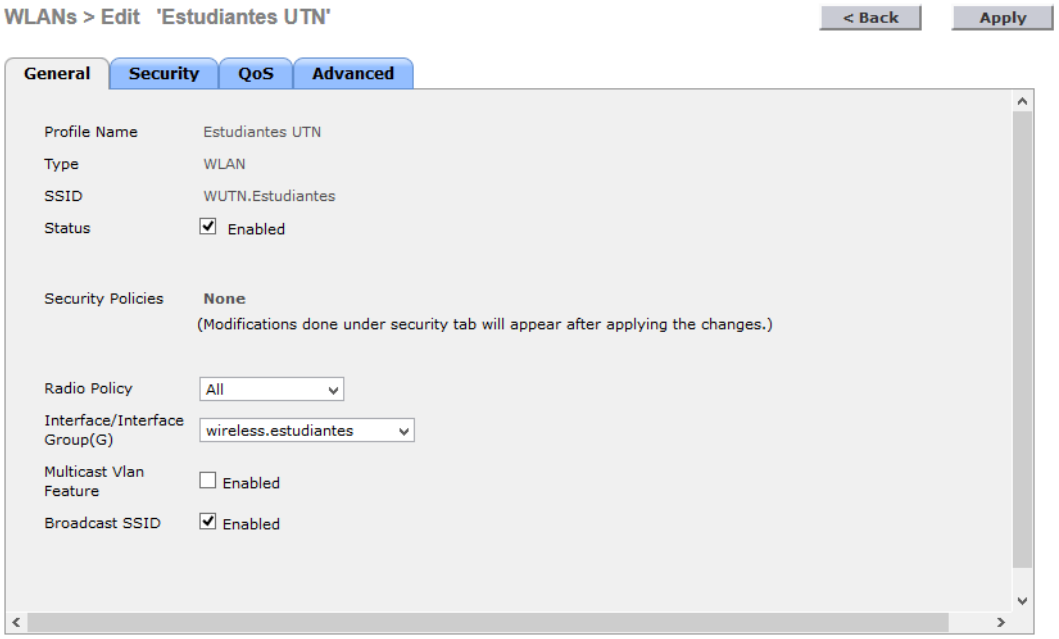


FIGURA 110 Configuración de aspectos generales

Fuente: Cisco Wireless LAN Controller 5508

En el menú de “Security” seleccionamos los parámetros de autenticación para cada una de las WLANs creadas (FIGURA 111).

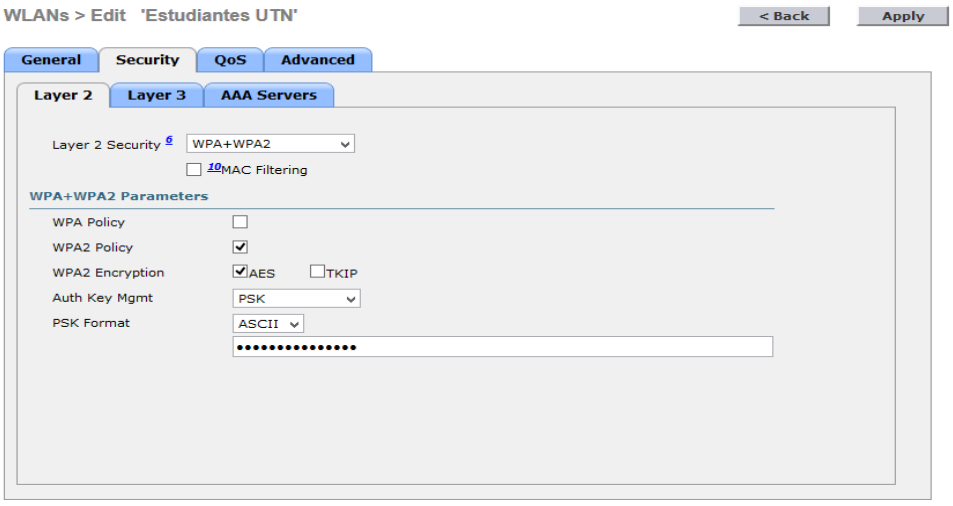


FIGURA 111 Configuración de Seguridad

Fuente: Cisco Wireless LAN Controller 5508

Por último en el menú de Advanced en el parámetro “DHCP Server” ingresamos la dirección IP de nuestro servidor DHCP (FIGURA 112).

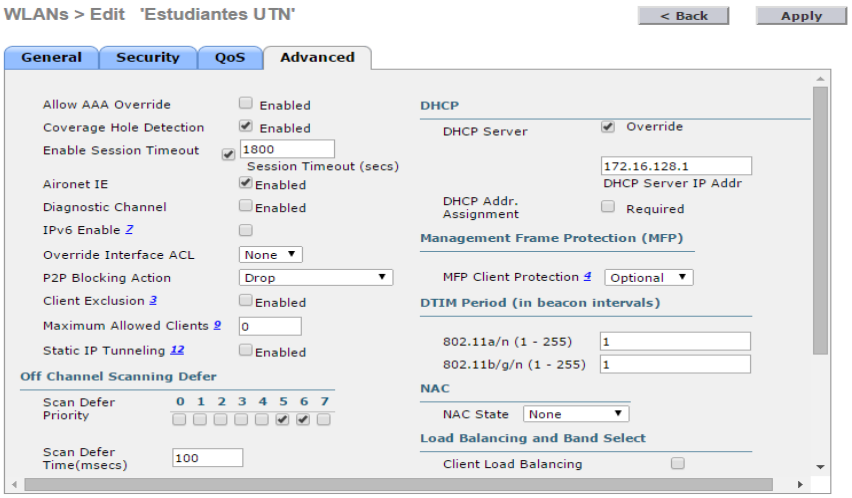


FIGURA 112 Configuración del menú Advanced

Fuente: Cisco Wireless LAN Controller 5508

4.1.11. Gestión de Grupos de AP

Es un parámetro avanzado que permite distribuir de mejor manera cada AP o conjunto de APs integrándoles a las WLANs creadas, lo que permite tener una mejor gestión y administración de acuerdo al requerimiento del administrador (FIGURA 113).

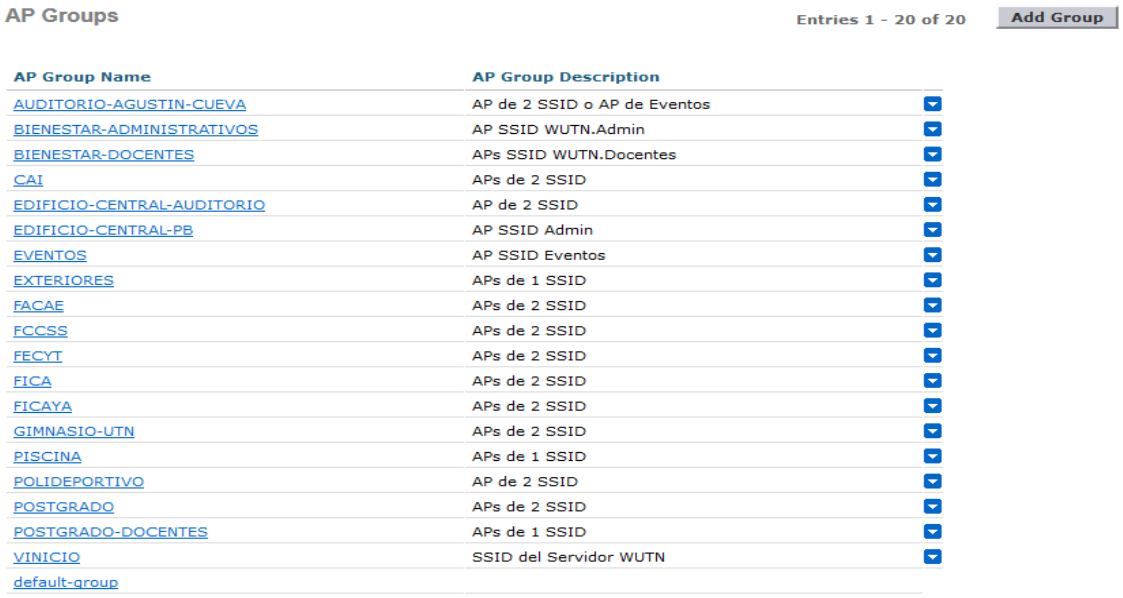


FIGURA 113 Configuración de los Grupos de AP

Fuente: Cisco Wireless LAN Controller 5508

4.1.12. Mapeo de Puertos de los Access Points

4.1.12.1. Mapeo de Puertos APs de Exteriores (OUTDOOR AP 1310G)

TABLA 57 Mapeo de Puertos APs de Exteriores WUTN

# AP	NOMBRE	MODELO AP	UBICACIÓN	TIPO DE SWITCH	PUERTO
AP1	AP-UTN-FICA-FICAYA	AIR-LAP1310G-A-K9	Rack Aso. Profesores FICA	2960-24TC-L	19
AP2	AP-UTN-CAI-FICAYA	AIR-BR1310G-A-K9-R	Rack Biblioteca	2960-24TC-L	18
AP3	AP-UTN-FICA-FFCCSS	AIR-LAP1310G-A-K9	Rack Aso. Profesores FICA	2960-24TC-L	20
AP4	AP-UTN-EDFISICA	AIR-BR1310G-A-K9-R	Rack Educación Física	2960-24TC-L	23
AP5	AP-UTN-ESTE-AUDITORIO	AIR-BR1310G-A-K9-R	Rack Agustín Cueva	3COM 4400SE	24
AP6	AP-UTN-NORTE-AUDITORIO	AIR-LAP1310G-A-K9	Rack Agustín Cueva	3COM 4400SE	9
AP7	AP-UTN-SUR-CENTRAL	AIR-LAP1310G-A-K9	Rack Terraza Edif. Central	3COM 4400SE	10
AP8	AP-UTN-NORTE-CENTRAL	AIR-BR1310G-A-K9-R	Rack Terraza Edif. Central	3COM 4400SE	9
AP9	AP-UTN-CAI-TERRAZA	AIR-LAP1310G-A-K9	Rack CAI PA2	3COM 4200	24
AP10	AP-UTN-SUR-FACAE	AIR-BR1310G-A-K9-R	Rack Principal FACAE	3COM 4400	8
AP11	AP-UTN-NORTE-FACAE	AIR-BR1310G-A-K9-R	Rack Principal FACAE	3COM 4400	9
AP12	AP-UTN-FECYT	AIR-BR1310G-A-K9-R	Rack Principal FECYT	2960-24TC-L	24
AP13	AP-UTN-OESTE-CENTRAL	AIR-BR1310G-A-K9-R	Rack Planta 1 Edif. Central	2960-24TC-L	11
AP14	AP-UTN-NORTE-ENTRADA	AIR-BR1310G-A-K9-R	Rack Garita	3COM 4400SE	24
AP15	AP-UTN-PISCINA	AIR-LAP1310G-A-K9	Rack Piscina	3COM 4400SE	24

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

4.1.12.2. Mapeo de Puertos APs de Interiores FACAE (INDOOR AP 1262N)

TABLA 58 Mapeo de Puertos APs de Interiores FACAE WUTN

# AP	NOMBRE	MODELO AP	UBICACIÓN	TIPO DE SWITCH	PUERTO
AP16	AP-FACAE-PA1	AIR-LAP1262N-A-K9	Rack Principal FACAE	3COM 4400	10
AP17	AP-FACAE-PA2	AIR-LAP1262N-A-K9	Rack Principal FACAE	3COM 4400	11
AP18	AP-FACAE-PA3	AIR-LAP1262N-A-K9	Rack Principal FACAE	3COM 4400	12

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

4.1.12.3. Mapeo de Puertos APs de Interiores FECYT (INDOOR AP 1262N)

TABLA 59 Mapeo de Puertos APs de Interiores FECYT WUTN

# AP	NOMBRE	MODELO AP	UBICACIÓN	TIPO DE SWITCH	PUERTO
AP19	AP-FECYT-PA1	AIR-LAP1262N-A-K9	Rack Principal FECYT	2960-24TC-L	21
AP20	AP-FECYT-PA2	AIR-LAP1262N-A-K9	Rack Principal FECYT	2960-24TC-L	22
AP21	AP-FECYT-PA3	AIR-LAP1262N-A-K9	Rack Principal FECYT	2960-24TC-L	23

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

4.1.12.4. Mapeo de Puertos APs de Interiores Agustín Cueva (INDOOR AP 1262N)

TABLA 60 Mapeo de Puertos APs de Interiores Agustín Cueva WUTN

# AP	NOMBRE	MODELO AP	UBICACIÓN	TIPO DE SWITCH	PUERTO
AP22	AP-AUDITORIO-INTERIOR	AIR-LAP1262N-A-K9	Rack Agustín Cueva	3COM 4400SE	23

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

4.1.12.5. Mapeo de Puertos APs de Interiores Edificio Central (INDOOR AP 1262N)

TABLA 61 Mapeo de Puertos APs de Interiores Edificio Central WUTN

# AP	NOMBRE	MODELO AP	UBICACIÓN	TIPO DE SWITCH	PUERTO
AP23	AP-CENTRAL-PB	AIR-LAP1262N-A-K9	Rack Derecho Edif. Central	2960-48TC-L	47
AP24	AP-CENTRAL-PA2	AIR-LAP1262N-A-K9	Rack Auditorio José Martí	2960-48TC-L	47

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

4.1.12.6. Mapeo de Puertos APs de Interiores Edificio Bienestar (INDOOR AP 1262N)

TABLA 62 Mapeo de Puertos APs de Interiores Edificio Bienestar WUTN

# AP	NOMBRE	MODELO AP	UBICACIÓN	TIPO DE SWITCH	PUERTO
AP25	AP-BIENESTAR-PB	AIR-LAP1262N-A-K9	BienestarRack0101	WS-C2960X-48TS-LL	37
AP26	AP-BIENESTAR-PA1	AIR-LAP1262N-A-K9	BienestarRack0102	WS-C2960X-48TS-LL	40
AP27	AP-BIENESTAR-PA2	AIR-LAP1262N-A-K9	BienestarRack0201	WS-C2960X-48TS-LL	37
AP28	AP-BIENESTAR-PA3	AIR-LAP1262N-A-K9	BienestarRack0202	WS-C2960X-48TS-LL	47

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

4.1.12.7. Mapeo de Puertos APs de Interiores FICAYA (INDOOR AP 1262N)

TABLA 63 Mapeo de Puertos APs de Interiores FICAYA WUTN

# AP	NOMBRE	MODELO AP	UBICACIÓN	TIPO DE SWITCH	PUERTO
AP29	AP-FICAYA-PA1	AIR-LAP1262N-A-K9	Rack Principal FICAYA	3COM 4400	22
AP30	AP-FICAYA-PA2	AIR-LAP1262N-A-K9	Rack Principal FICAYA	3COM 4400	23
AP31	AP-FICAYA-PA3	AIR-LAP1262N-A-K9	Rack Principal FICAYA	3COM 4400	24

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

4.1.12.8. Mapeo de Puertos APs de Interiores FICA (INDOOR AP 1131AG)

TABLA 64 Mapeo de Puertos APs de Interiores FICA WUTN

# AP	NOMBRE	MODELO AP	UBICACIÓN	TIPO DE SWITCH	PUERTO
AP32	AP-FICA-PB	AIR-LAP1131AG-A-K9	Rack Principal FICA	WS-C4506-E L3	23
AP33	AP-FICA-PA2D	AIR-LAP1131AG-A-K9	Rack Principal FICA	WS-C4506-E L3	10
AP34	AP-FICA-PA2I	AIR-LAP1131AG-A-K9	Rack Principal FICA	WS-C4506-E L3	14
AP35	AP-FICA-PA3D	AIR-LAP1131AG-A-K9	Rack Principal FICA	WS-C4506-E L3	40
AP36	AP-FICA-PA3I	AIR-LAP1131AG-A-K9	Rack Principal FICA	WS-C4506-E L3	39
AP37	AP-FICA-PA4	AIR-LAP1131AG-A-K9	Rack Principal FICA	WS-C4506-E L3	37

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

4.1.12.9. Mapeo de Puertos APs de Interiores FCCSS (INDOOR AP 1262N)

TABLA 65 Mapeo de Puertos APs de Interiores FCCSS WUTN

# AP	NOMBRE	MODELO AP	UBICACIÓN	TIPO DE SWITCH	PUERTO
AP38	AP-FCCSS-PA1	AIR-LAP1262N-A-K9	Rack Principal FCCSS	3COM 4400	21
AP39	AP-FCCSS-PA2	AIR-LAP1262N-A-K9	Rack Principal FCCSS	3COM 4400	22
AP40	AP-FCCSS-PA3	AIR-LAP1262N-A-K9	Rack Principal FCCSS	3COM 4400	23

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

4.1.12.10. Mapeo de Puertos APs de Interiores CAI (INDOOR AP 1262N)

TABLA 66 Mapeo de Puertos APs de Interiores CAI WUTN

# AP	NOMBRE	MODELO AP	UBICACIÓN	TIPO DE SWITCH	PUERTO
AP41	AP-CAI-PA1	AIR-LAP1262N-A-K9	Rack CAI PA2	3COM 4200	21
AP42	AP-CAI-PA2	AIR-LAP1262N-A-K9	Rack CAI PA2	3COM 4200	22
AP43	AP-CAI-PA3	AIR-LAP1262N-A-K9	Rack CAI PA2	3COM 4200	23

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

4.1.12.11. Mapeo de Puertos APs de Interiores POSTGRADO (INDOOR AP 1262N)

TABLA 67 Mapeo de Puertos APs de Interiores POSTGRADO WUTN

# AP	NOMBRE	MODELO AP	UBICACIÓN	TIPO DE SWITCH	PUERTO
AP44	AP-POSTGRADO-PB1	AIR-LAP1262N-A-K9	Rack Principal POSTGRADO	WS-C4503-E L3	45
AP45	AP-POSTGRADO-PB2	AIR-LAP1262N-A-K9	Rack Principal POSTGRADO	WS-C4503-E L3	46
AP46	AP-POSTGRADO-PB-AUDITORIO	AIR-LAP1262N-A-K9	Rack Principal POSTGRADO	WS-C4503-E L3	44
AP47	AP-POSTGRADO-PA1	AIR-LAP1262N-A-K9	Rack POSTGRADO PA1	WS-C2960S-24PS-S	1
AP48	AP-POSTGRADO-PA2	AIR-LAP1262N-A-K9	Rack POSTGRADO PA1	WS-C2960S-24PS-S	2

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

4.1.12.12. Mapeo de Puertos APs de Interiores Complejo Acuático (INDOOR AP 1262N)

TABLA 68 Mapeo de Puertos APs de Interiores Complejo Acuático WUTN

# AP	NOMBRE	MODELO AP	UBICACIÓN	TIPO DE SWITCH	PUERTO
AP49	AP-PISCINA-INTERIOR	AIR-LAP1262N-A-K9	Rack Piscina	3COM 4400SE	23

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

4.1.12.13. Mapeo de Puertos APs de Interiores POLIDEPORTIVO (INDOOR AP 1262N)

TABLA 69 Mapeo de Puertos APs de Interiores POLIDEPORTIVO WUTN

# AP	NOMBRE	MODELO AP	UBICACIÓN	TIPO DE SWITCH	PUERTO
AP50	AP-POLIDEPORTIVO	AIR-LAP1262N-A-K9	Rack Educación Física	2960-24TC-L	24

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

4.2. INSTALACIÓN Y CONFIGURACIÓN DEL PORTAL CAUTIVO WIFIDOG

4.2.1. Introducción

Muchas empresas, en especial aquellas que dependen del tráfico de público como: restaurantes, cafés, hoteles e instituciones de educación superior ofrecen acceso gratuito a sus Access Point a través de una contraseña que se entrega a los clientes, este método no siempre es el más apropiado ya que el hecho de que la contraseña no sea actualizada frecuentemente y que sea distribuida verbalmente abre la posibilidad de que esta sea usada potencialmente por personas que no usaran los servicios del establecimiento comercial.

Una forma alternativa de controlar el acceso es a través de portales cautivos, Wifidog es uno de los más completos (

FIGURA **114**), además de ser uno de los pocos que permiten la administración de múltiples nodos a través de un sólo panel de control.

FIGURA 114 Logo del Portal Cautivo Wifidog
Fuente: Instalación de Wifidog

Wifidog es un producto Open Source desarrollado por la comunidad de hotspots públicos de Quebec (Canadá) Île Sans Fil ("Isla inalámbrica"). Cómo todo portal cautivo tiene dos partes, el Servidor de Autenticación y el Gateway.

El servidor de autenticación está hecho en PHP y usa PostgreSQL como su motor de base datos, además de estar desarrollado en base a Smarty, con lo cual es muy sencillo cambiar el tema del sitio por defecto. El Gateway está programado totalmente en C y utiliza sólo llamadas estándar de Linux, con lo cual puede ser integrado en cualquier servidor que haga de Firewall o Routers compatibles con los proyectos DD-WRT, OpenWRT y Tomato.

Una de las características de Wifidog, es que permite que sea el propio usuario que registrándose con su dirección de correo electrónico gane acceso al HotSpot, además que nos permite definir cuantos usuarios concurrentemente deseamos soportar a través de cada nodo Wi-fi (por defecto son 10).

Ya que tenemos una dirección de correo electrónico podemos posteriormente enviarle ofertas y promociones a nuestros usuarios, además gracias a su muy detallado sistema de estadísticas podemos identificar los 10 usuarios más móviles, los 10 más frecuentes, los 10 que usan más ancho de banda, etc., con lo que la administración de múltiples HotSpot se vuelve bastante amigable e intuitiva.

En resumen Wifidog consiste en dos componentes:

- El "Local Gateway"
- El "Auth-Server"

El Gateway redirige tráfico de un usuario hacia la Internet solo si el Auth-Server a autenticado correctamente a dicho usuario.

4.2.2. Configuración e Instalación del Hardware

Aunque, en un principio, Wifidog fue diseñado para dispositivos “embedded” tales como Routers Linksys. Este software funciona en cualquier PC o servidor. Las características del hardware mínimo para el funcionamiento de dicho software son las siguientes:

Requerimientos básicos de PC:

- CDROM Drive
- Procesador 486 o más

- 32 MB RAM[153]
- 1 GB de Disco Duro (ROM[154])
- 2 Tarjetas Ethernet de 10/100 o 10/100/1000

Requerimientos Adicionales para la implementación:

- Wireless LAN Controller
- APs integrados a la controladora
- DVD de instalación Debian 7.4.0

4.2.3. Proceso de instalación

Para el proceso de instalación se utilizará un Servidor HP Proliant DL160 G6 donde se instalará el sistema operativo Debian 7.4.0 (ANEXO 6) el mismo que servirá tanto como Servidor de Autenticación y Gateway. Antes que nada tenemos que ver las características del equipo antes mencionado y la topología a utilizar que se muestra en la FIGURA 49.

4.2.4. Características del Equipo (servidor)

El equipo cumple con las siguientes características:

- Posee instalado Software LINUX con Sistema Operativo Debian 7.
- Procesador AMD FX(tm)-8320 Eight-Core 3.50 GHz.
- Memoria RAM 4 GB.
- Disco duro de 1 TB.

Este dispositivo cumple con las siguientes funciones:

- Trabajar como AUTH-Server.
- Gateway Wifidog.
- Servidor DHCP para la LAN.

4.2.5. Equipos de Prueba

Los Dispositivos cliente que se conectarán a la LAN a través del AP, deberán pasar a través del Portal Cautivo, una vez que este sea autenticado el cliente podrá acceder a la Internet.

---

[153] **RAM** Random Access Memory (Memoria de Acceso Aleatorio)
[154] **ROM** Read Only Memory (Memoria de Solo Lectura)

4.2.6. Descripción de la topología de prueba

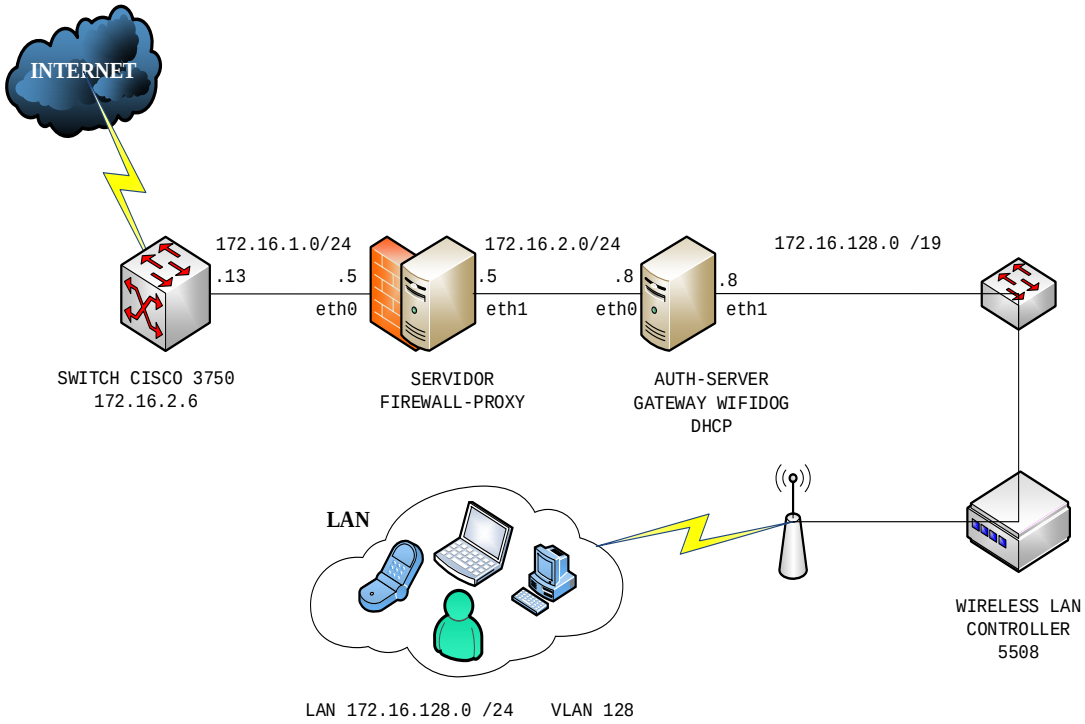


Figura 115 Diagrama Lógico de prueba para Wifidog

Fuente: Área de Redes y Comunicaciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN

4.2.7. Instalación de Wifidog

Wifidog consiste en dos componentes: El “Local Gateway” y el “Auth-Server”. El Gateway redirige el tráfico hacia internet dependiendo si el Auth-Server ha permitido el ingreso al usuario. En el ANEXO 7 se muestran los pasos que describen detalladamente la instalación en un ambiente de servidor Linux, utilizando un sistema operativo Debian versión 7.4.0.

4.3. INSTALACIÓN Y CONFIGURACIÓN DE WEBMIN

4.3.1. Instalación de Webmin en CentOS 6.5

Webmin es un administrador de sistema basado en Web para Unix/Linux. A través de una cómoda GUI y utilizando cualquier navegador se podrá configurar cualquier servidor Unix/Linux. Con Webmin se configura cuentas de usuario, archivos compartidos, servidores como; Firewall con shorewall, Proxy con squid, Apache, MySQL, DHCP o servicios DNS, etc. Es relativamente más sencillo que editar archivos de configuración por consola. (Boyano, 2014)

Existen dos formas de instalar Webmin en un servidor con CentOS 6.5 instalado (ANEXO 10), una mediante un archivo rpm y otra a través del repositorio para Yum. Personalmente prefiero la segunda opción.

4.3.2. Instalación mediante RPM

Lo primero si deseas realizar la instalación utilizando RPM es descargar el archivo desde la página de descargas de Webmin o ejecutar el comando:

wget http://sourceforge.net/projects/webadmin/files/webmin/1.670/webmin-1.670-1.noarch.rpm

Una vez descargado el archivo rpm ejecuta el comando:

rpm -U webmin-1.670-1.noarch.rpm

El resto de la instalación se realizará automáticamente en el directorio: /usr/libexec/webmin, el nombre de usuario de administración y la contraseña serán establecidos como la cuenta de root actual. Para conectarse a Webmin ingresamos en cualquier navegador la siguiente dirección “http://localhost:10000” o reemplazamos localhost por la dirección IP del servidor.

4.3.3. Instalación usando el repositorio Webmin para Yum

Si prefieres instalar y actualizar Webmin a través de RPM utilizando Yum, se debe crear el archivo: /etc/yum.repos.d/webmin.repo utilizando cualquier editor:

cd /etc/yum.repos.d

nano webmin.repo

El archivo debe contener las siguientes líneas:

[Webmin]

name=Webmin Distribution Neutral

#baseurl=http://download.webmin.com/download/yum

mirrorlist=http://download.webmin.com/download/yum/mirrorlist

enabled=1

Por último, también debes descargar e instalar la llave GPG de los paquetes firmados con los comandos:

wget http://www.webmin.com/jcameron-key.asc

rpm –-import jcameron-key.asc

Ahora ya estás listo para realizar la instalación de Webmin ejecutando el comando:

yum install webmin

Todas las dependencias se resolverán automáticamente.

Con esta forma de instalación usando el repositorio de Webmin para Yum nos garantizamos la actualización de los paquetes desde Yum simplemente ejecutando el comando:

yum update webmin

4.3.4. Distribuciones compatibles basadas en RPM

El RPM de Webmin puede ser instalado en Fedora, Red Hat Enterprise, las versiones anteriores de Red Hat, CentOS y todas las distribuciones derivadas de Fedora o Red Hat Enterprise Linux. Además, se puede instalar en sistemas que ejecutan Mandriva, Suse, TurboLinux y OpenLinux de Caldera.

Fuente: http://www.webmin.com/

4.3.5. Consideraciones de Interés

Si su sistema tiene un firewall instalado recuerde abrir el puerto 10000 para poder acceder a la interfaz gráfica de Webmin ingresando http://localhost:10000 en el navegador como se muestra en la FIGURA 116.

FIGURA 116 Login a Webmin como localhost

Fuente: Instalación de Webmin en el sistema operativo CentOS 6.5

“Es muy conveniente que una vez logueado por primera vez en Webmin se cambie el puerto de administración 10000 a otro distinto y que se utilice filtrado de IP para que sólo se permita el acceso a determinada dirección IP por razones de seguridad” (Boyano, 2014).

Después de haber ingresado como localhost vía WEB nos solicita que ingresemos un username y el password de administración para dirigirnos a la pantalla de bienvenida que podemos observar en la FIGURA 117.

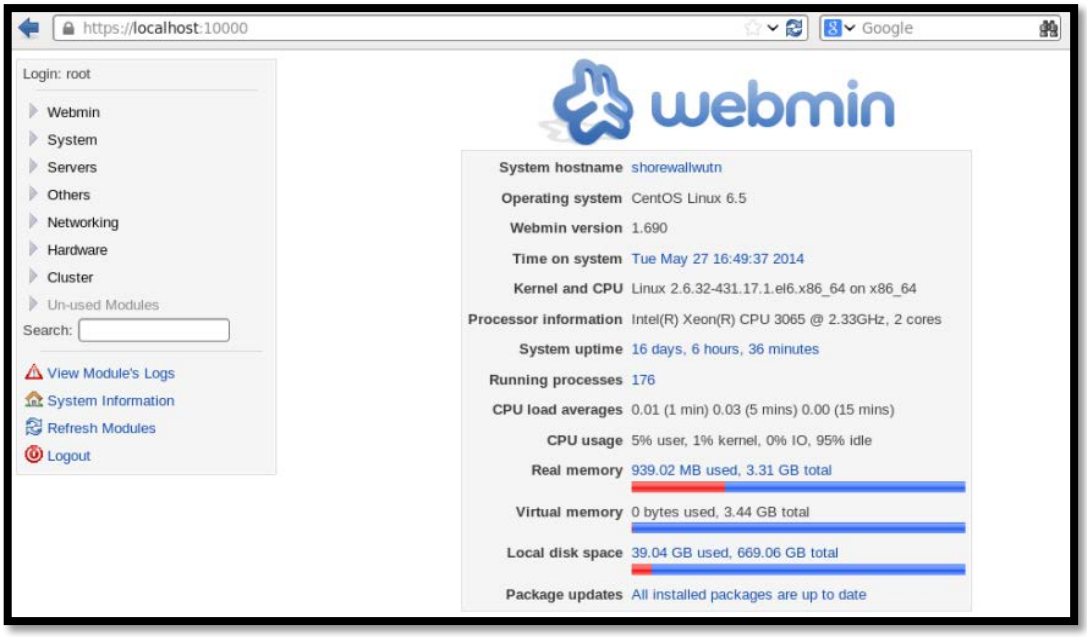


FIGURA 117 Pantalla de bienvenida a Webmin

Fuente: Instalación de Webmin en el sistema operativo CentOS 6.5

4.4. INSTALACIÓN Y CONFIGURACIÓN DE SHOREWALL

El Shoreline Firewall o más conocido como Shorewall es una herramienta de alto nivel para configuración de muros de cortafuegos. El administrador describe los requerimientos del firewall/gateway usando las entradas de un conjunto de archivos de configuración. Shorewall se puede utilizar en un sistema de servidor de seguridad, en un servidor multifuncional que cumpla las funciones de gateway/router o en un sistema GNU/Linux autónomo. Cabe señalar que Shorewall no es un demonio. (Eastep, 2014)

Un Firewall se puede describir como un dispositivo que funciona como cortafuegos entre dos o más redes, permitiendo o denegando acceso a los servicios que se encuentran asociados a protocolos y estos a su vez asociados a puertos; los cuales se transmiten de una red a otra. Tiene la gran responsabilidad de autorizar o bloquear las peticiones de acceso de los usuarios al servidor de autenticación RADIUS.

Shorewall puede descargarse en formato RPM desde “http://www.shorewall.net”. Si dispone de un servidor con CentOS 5 y 6 o Red Hat™ Enterprise Linux 5 o 6, puede utilizar el almacén YUM de Alcance Libre para servidores en producción, descargando el archivo “http://www.alcancelibre.org/al/server/AL-Server.repo” dentro del directorio “/etc/yum.repos.d/”:

cd /etc/yum.repos.d/

wget -N http://www.alcancelibre.org/al/server/AL-Server.repo

Este archivo, que se guarda como “/etc/yum.repos.d/AL-Server.repo”, debe tener el siguiente contenido:

[AL-Server]

name=AL Server para Enterprise Linux $releasever

mirrorlist=http://www.alcancelibre.org/al/el$releasever/al-server

gpgcheck=1

gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY

La instalación a través del mandato Yum requiere utilizar lo siguiente:

yum -y install shorewall

4.4.1. Archivos de configuración de shorewall

Las configuraciones realizadas para levantar el servicio de firewall se detalla a continuación:

4.4.1.1. Shorewall.conf (/etc/shorewall/shorewall.conf)

En éste se definen dos parámetros principales STARTUP_ENABLED e IP_FORWARDING. Para la siguiente configuración solo activaremos las siguientes opciones cambiando “No” por “Yes”:

STARTUP_ENABLED=Yes para activar el firewall

Y la opción:

IP_FORWARDING=On para habilitar el forwarding.

4.4.1.2. Network Zones (/etc/shorewall/zones)

FIGURA 118 Network Zones

Fuente: Instalación de Shorewall en el sistema operativo CentOS 6.5

Este fichero se utiliza para definir las zonas que se administrarán con Shorewall y el tipo de zona (firewall, ipv4 o ipsec). La zona “fw” está presente en el archivo “/etc/shorewall.conf” como configuración predeterminada. A continuación se muestra las zonas creadas: hacia la Internet (wan), hacia el firewall (Fw) y hacia la red local (lan).

4.4.1.3. Network Interfaces (/etc/shorewall/interfaces)

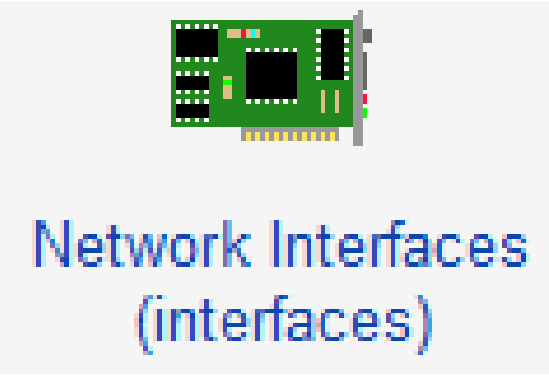


Figura 119 Network Interfaces

Fuente: Instalación de Shorewall en el sistema operativo CentOS 6.5

En éste fichero se establecen cuáles serán las interfaces para las diferentes zonas. Se asocian las interfaces que corresponden a la zona wan y lan. De acuerdo al diseño, la configuración es la siguiente: eth0 (zona wan) y eth1 (zona lan). Además se debe configurar de modo automático la dirección de Broadcast.

4.4.1.4. Default Policies (/etc/shorewall/policy)

FIGURA 120 Default Policies

Fuente: Instalación de Shorewall en el sistema operativo CentOS 6.5

En este fichero se establece como se accederá desde una zona hacia otra. Por seguridad todo el tráfico de zona a zona está bloqueado y en el fichero rules está definido sólo el tráfico que se permite entre zonas. Las opciones básicas de políticas son:

- ACCEPT – Aceptar la conexión.
- DROP – Ignorar la solicitud de conexión.
- REJECT – Retornar un error apropiado a la solicitud de conexión.

4.4.1.5. Firewall Rules (/etc/shorewall/rules)

Figura 121 Firewall Rules

Fuente: Instalación de Shorewall en el sistema operativo CentOS 6.5

Todos los puertos están cerrados de modo predefinido, y en este fichero es donde se habilitan los puertos necesarios. Por ejemplo la regla principal para permitir el acceso para el servidor de autenticación AAA es la siguiente:

```
ACCEPT  lan     Fw      udp     1812,1813
```

La siguiente regla se interpretaría de la siguiente manera: Aceptar las peticiones desde la zona lan hacia la zona Fw por el protocolo UDP a los puertos 1812 y 1813.

4.4.1.6. Masquerading (/etc/shorewall/masq)

FIGURA 122 Masquerading

Fuente: Instalación de Shorewall en el sistema operativo CentOS 6.5

"Si dispone de un único dispositivo de red, omita el siguiente paso. Si dispone de más de un dispositivo de red y se requiere habilitar el enmascaramiento de direcciones IP de un dispositivo hacia otro se debe editar el archivo" (Barrios Dueñas, 2014).

4.4.1.7. Static NAT (/etc/shorewall/nat)

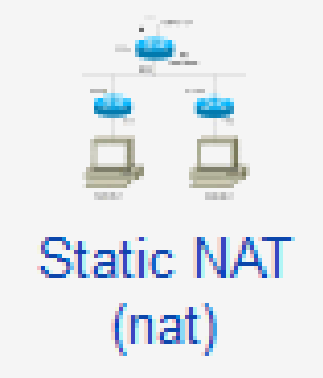


Figura 123 Static NAT

Fuente: Instalación de Shorewall en el sistema operativo CentOS 6.5

El NAT estático se utiliza a menudo para permitir conexiones hacia un servidor interno desde fuera de la red para lograr que el tráfico de datos sea bidireccional.

4.4.2. Activar y controlar Shorewall

Una vez configurados los archivos que son necesarios para que arranque el servicio de Firewall con Webmin, se tiene diferentes opciones para aplicar, refrescar, limpiar, detener la configuración del servicio de shorewall como se muestra en la FIGURA 124.

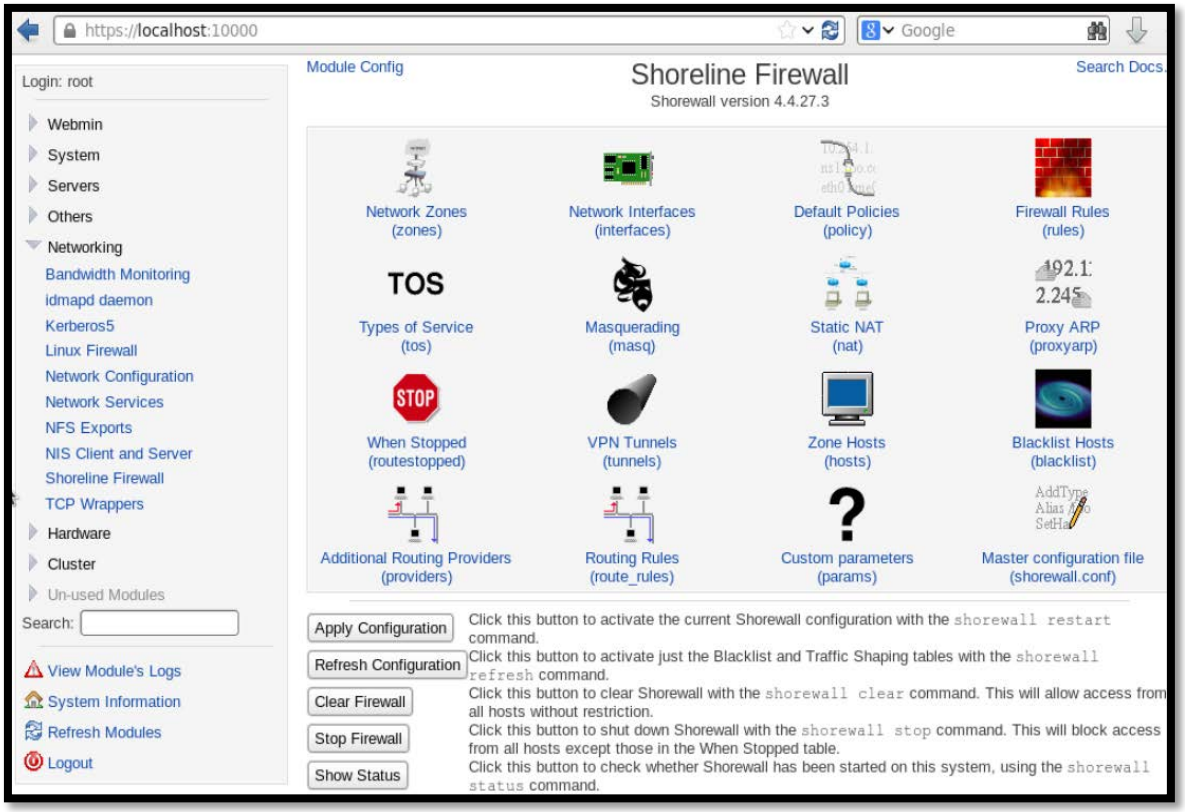


FIGURA 124 Página del Firewall Shorewall

Fuente: Instalación de Shorewall en el sistema operativo CentOS 6.5

4.5. INSTALACIÓN Y CONFIGURACIÓN DEL PROXY SQUID

“Un proxy es un programa o dispositivo que realiza una gestión de acceso a Internet en lugar de otro ordenador. Un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor que está accediendo. Cuando navegamos a través de un proxy, nosotros en realidad no estamos accediendo directamente al servidor, sino que realizamos una solicitud sobre el proxy y es éste quien se conecta con el servidor que queremos acceder y nos devuelve el resultado de la solicitud” (Cordoba Serna, 2014).

4.5.1. Instalación de Squid

La instalación de Squid se lo puede realizar desde un terminal como root o desde webmin.

yum –y install squid

Desde webmin buscamos el software disponible y buscamos squid e instalamos el software.

4.5.2. Configuración de Squid

Para la configuración de squid se debe realizar el proxy transparente para no tener que configurar en cada computador, para ello es necesario agregar en el archivo /etc/squid/squid.conf lo siguiente:

```
http_port 3128 transparent
cache_mem 100 MB
cache_dir ufs /var/spool/squid 150 16 256
acl red_local src 172.16.128.0/19
acl localhost src 127.0.0.1/32
acl all src all
```

Además de agregar una regla en el cortafuegos donde se redireccionan todas las entradas de la red local por el puerto 80 al puerto 3128 donde squid es el servicio de proxy.

Desde webmin ingresamos a squid:

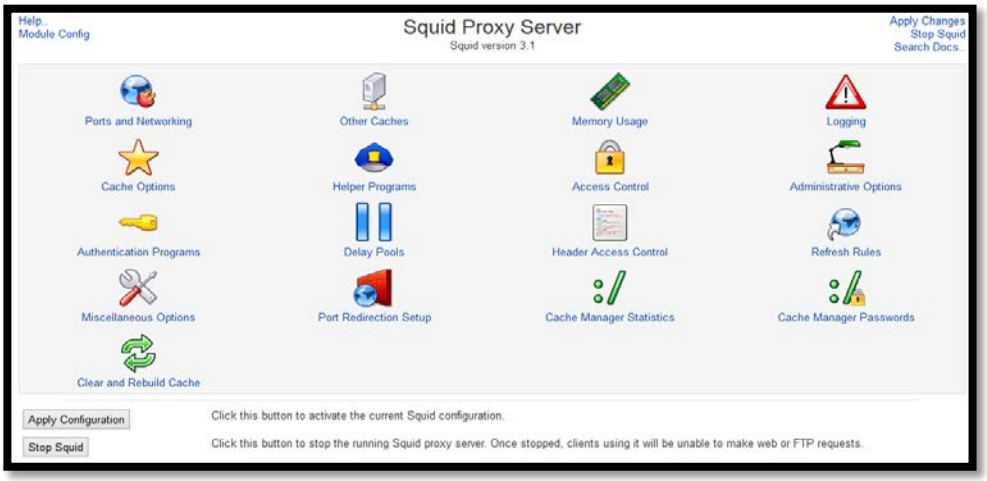


Figura 125 Página de configuración de Squid desde Webmin

Fuente: Instalación de Squid en el sistema operativo CentOS 6.5

Para la negación es necesario crear nuevas reglas de acceso en la interfaz gráfica Squid Proxy Server desde Webmin y agregar las palabras o sitios Web que serán negados, es importante basarnos en criterios que nos permitan mediante las políticas de acceso a la red censurar las páginas o palabras de contenido no académico.

Las páginas denegadas son:

- www.facebook.com
- facebook.com
- m.facebook.com
- api.facebook.com
- fbcdn-profile-a.akamaihd.net
- graph.facebook.com
- www.twitter.com
- www.youtube.com
- www.justin.tv
- www.teenteufel.com
- www.redtube.com
- www.zoosexhere.com
- mobile.youporn.com
- piecd.mobidick.tv
- www.tiava.com
- rubias19.com
- petardas.com
- penthouse.com
- www.xvideos.com
- multi.xnxx.com

Las palabras denegadas son:

- juegos
- sexo
- porno
- mp3
- xxx
- locas
- perr
- put
- babos
- culo
- desnud

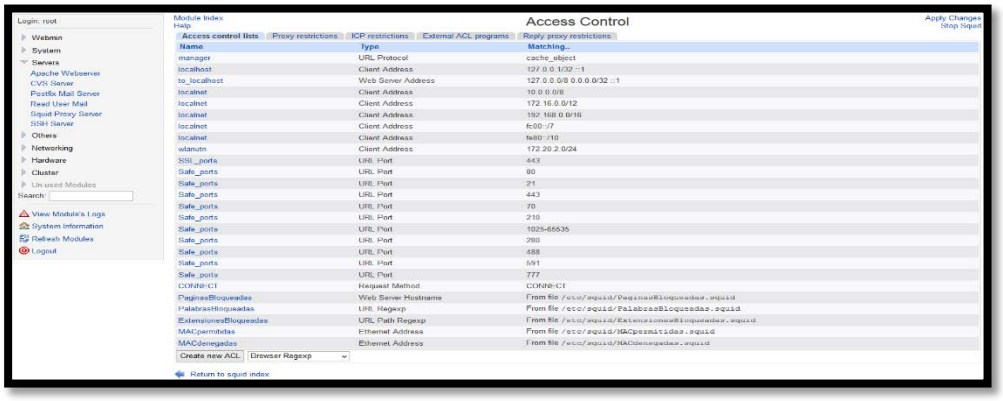


FIGURA 126 Reglas de Control de Acceso Squid

Fuente: Instalación de Squid en el sistema operativo CentOS 6.5

Dependiendo del tipo de parámetro que se necesite se agrega una nueva ACL, la cual se debe subir de posición para que funcione, caso contrario quedaría inhabilitada.

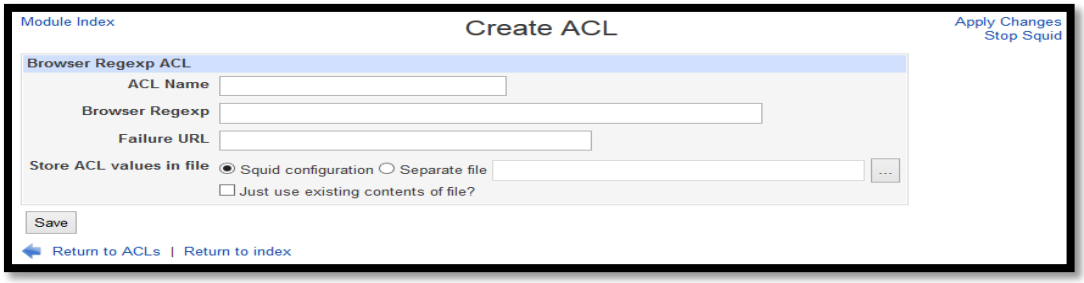


FIGURA 127 Creación de ACL

Fuente: Instalación de Squid en el sistema operativo CentOS 6.5

4.6. GESTIÓN DE USUARIOS LDAP

El Manual Técnico que se describe en el ANEXO 11, tiene como objetivo indicar detalladamente los pasos necesarios para la instalación y configuración del directorio LDAP en un servidor de la Universidad Técnica del Norte con sistema operativo Debian 6.0.7. LDAP permite el acceso a la información del directorio mediante un esquema cliente-servidor, donde uno o varios servidores mantienen la misma información de directorio y los clientes registrados en la Institución realizan consultas a cualquiera de ellos para acceder al servicio de Internet inalámbrico.

El manual se encuentra dirigido al personal que labora en el área de Gestión de Redes y Comunicaciones (GRC) de la Dirección de Desarrollo Tecnológico e Informático (DDTI), quienes serán los encargados de instalar y configurar los servicios si llegara a presentarse alguna anomalía. Cabe recalcar que es una guía de solución para personas que deseen implementarlo en cualquier otro ámbito.

Para la administración y gestión de la base de datos de usuarios LDAP se utiliza la herramienta “phpLDAPadmin”; la cual permite agregar, modificar y eliminar unidades organizativas, grupos, usuarios y atributos de manera más rápida y eficiente.

4.7. GESTIÓN DE USUARIOS POR FILTRADO MAC

El filtrado MAC es un método muy práctico para poder controlar el acceso a redes inalámbricas, lo que optimiza notablemente que solo los dispositivos que estén registrados podrán hacer uso de la red. La dirección MAC no es más que un identificativo único de cada dispositivo pero no tan seguro porque puede existir suplantación de direcciones MAC.

Se realizó la integración del direccionamiento MAC con el Proxy Squid, por medio del cual se deniega el acceso a páginas, palabras y formatos de extensión de descarga siempre y cuando no esté registrada la MAC del dispositivo final.

CAPITULO V

5. ANÁLISIS COSTO BENEFICIO

Se realizó el análisis costo beneficio considerando las herramientas de hardware y software utilizadas en la implementación de la red LAN Inalámbrica en la Universidad Técnica del Norte.

5.1. PRESUPUESTO DE INVERSIÓN

La inversión realizada se fundamenta en el análisis de todos los requerimientos necesarios para la implementación de la red Inalámbrica como servidores, APs, kit de montaje y servicios que a continuación se muestran en el presupuesto de conectividad, valores variables y total.

5.1.1. Presupuesto de Conectividad

Para determinar la conectividad e infraestructura física y lógica del proyecto se realizó una lista de todos los equipos necesarios que fueron utilizados en la implementación de la red Inalámbrica.

Tabla 70 Presupuesto de Inversión para la conectividad de la Red Inalámbrica de la UTN

CANTIDAD	DESCRIPCIÓN	COSTO UNITARIO	COSTO TOTAL
2	HP EliteBook 857Op, 17-3520M (3.6GHz/2.90GHz/4MB), 8GB 1600 2D, 750GB 7200 2.5", 15.6 LED HD AG, 1 GB Radeon 7570M. BD/DVD+Rw, Centrino a/b/g/n 2x2, BT 4.0 WWAN Upgradeable, no Modem. TPM + FS, 720p HD webcam, Win7 Pro 64 oS10, vPro, 6- Cell 62Wh, 1/1/0	$ 1.750,00	$ 3.500,00
	Upgrade para la WLC actual		
1	25 APs Adder License for the 5508 Controller	$ 10.452,88	$ 10.452,88

	Access Point Externos		
6	802.11g LWAPP AP Int. Antenna FCC Cnfg	$ 0,00	$ 0,00
6	AIR Line Cord North America	$ 8,50	$ 51,00
6	Cisco 1310 Series IOS Wireless LAN LWAPP Recovery	$ 1.146,00	$ 6.876,00
6	Aironet 1300 Roof Mount Kit	$ 201,40	$ 1.208,40
6	2.4 GHz, 8.5 dBi Patch Antenna w/ RP-TNC Connector	$ 202,40	$ 1.214,40
	Access Point Internos		
29	802.11a/g/n Ctrlr-based AP; Ext Ant; A Reg Domain	$ 0,00	$ 0,00
29	Radios Cisco 1260 Series IOS Wireless LAN Controller-based Recovery	$ 839,00	$ 24.331,00
87	2.4 GHz 2.2 dBi Straight Dipole Antenna Gray, RP-TNC	$ 16,00	$ 1.392,00
29	Kit de Montage 802.11n AP Low Profile Mounting Bracket (Default)	$ 4,37	$ 126,73
29	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	$ 4,37	$ 126,73
29	Service Provider Option 60 for Vendor Class Identifier	$ 0,00	$ 0,00
29	Power Injector - AP1140/1250/1260/3500 Series	$ 105,00	$ 3.045,00
		TOTAL	**$ 52.324,14**

Fuente: Cotización de la empresa de telecomunicaciones Sinfotecnia

5.1.2. Presupuesto de Gastos Variables

A parte del equipamiento tecnológico que se utilizó en la implementación es importante tomar en cuenta equipos y servicios adicionales que pueden ser variables y dependientes de acuerdo a los convenios o contratos del proyecto con las entidades involucradas.

TABLA 71 Presupuesto de Inversión de Valores Variables

CANTIDAD	DESCRIPCIÓN	COSTO UNITARIO	COSTO TOTAL
35	Se realizó la instalación y configuración de acoplamiento de los 35 APs a la Wireless LAN Controller en el campus universitario, y se instaló los 6 APs en exteriores y los 29 APs de interiores.	$ 93,00	$ 3.255,00
1	Adicionalmente se realizó la reubicación de 9 APs para mejorar el área de cobertura de la red Wireless.	$ 1.450,00	$ 1.450,00
1	Se realizó la instalación de los 35 puntos de cableado estructurado en categoría 6 incluido material (cable UTP, jack, patch cord, etc) necesarios para la interconexión de los APs a la red LAN de la Universidad.	$ 0,00	$ 0,00
		TOTAL	**$ 4.705,00**

Fuente: Cotización de CEDIA y de la empresa de telecomunicaciones Sinfotecnia

5.1.3. Presupuesto Total

El presupuesto total es el resultado de la conectividad Inalámbrica y los gastos variables que influyen en el servicio de la red propuesta:

$$\$\,52.324{,}14 + \$\,4.705{,}00 = \$\,57.029{,}14$$

Para el análisis Costo Beneficio se tendrá en cuenta solo el primer valor como gasto del proyecto debido a que el segundo valor puede variar hasta llegar a cero debido a que es un proyecto de contratación pública en el cual se pueden omitir estos gastos mediante convenios.

5.2. ANÁLISIS DE GASTOS DE INTERNET

Los gastos para el proyecto de diseño e implementación de la red Inalámbrica de la Universidad Técnica del Norte tienen mucha relación con el convenio de todos los servicios ofrecidos por CEDIA.

Como institución de educación superior se cree conveniente que el paquete por el que se debe optar es AVANZADO 2, el cual ofrece muchas ventajas y servicios en lo que respecta al Ancho de Banda de Internet Comercial y de Internet Avanzado.

TABLA 72 Costo de los Servicios de CEDIA

DESCRIPCIÓN	ANCHO DE BANDA	GASTOS INTERNET (MENSUAL)	GASTOS INTERNET (5 AÑOS - 60 MESES)
Costo de los Servicios de CEDIA (Internet Comercial, Conexión a Red Clara Nacional e internacional, membresía a CEDIA)	450 Mbps[155]	$ 14.754,92	$ 885.295,20
		SUBTOTAL (SIN IVA)	$ 885.295,20
		IVA 12 %	$ 106.235,42
		TOTAL	**$ 991.530,62**

Fuente: Costos proporcionados por el convenio con CEDIA

5.3. ANÁLISIS COSTO BENEFICIO

"El Análisis Costo Beneficio se formuló, en parte, con la finalidad de imprimir objetividad al análisis económico de la evaluación del sector público, lo cual reduce el efecto de los intereses políticos y particulares. Sin embargo, siempre hay discrepancias

[155] **450 Mbps** Ancho de Banda contratado a CEDIA para la Prestación de Servicios de Internet Comercial y de Internet Avanzado.

predecibles entre los ciudadanos (individuos y grupos) respecto de la evaluación y definición de los beneficios de una alternativa" (Blank & Tarquin, 2006, pág. 326).

El Análisis Costo Beneficio se emplea principalmente en la evaluación de proyectos y la selección de alternativas del sector público, de esta manera este método utiliza los siguientes pasos:

a) Llevar a cabo una lluvia de ideas o reunir datos provenientes de factores importantes relacionados con cada una de sus decisiones.

b) Determinar los costos relacionados con cada factor. Algunos costos, como la mano de obra serán exactos mientras que otros deberán ser estimados.

c) Sumar los costos totales para cada decisión propuesta.

d) Determinar los beneficios en dólares para cada decisión.

e) Poner las cifras de los costos y beneficios totales en la forma de una relación donde los beneficios son el numerador y los costos son el denominador.

f) Comparar las relaciones de Beneficios a Costos para las diferentes decisiones propuestas donde la mejor solución es aquella con la relación más alta.

5.3.1. Cálculo Costo Beneficio

El valor que indica la relación de costo beneficio genera los siguientes criterios que guían las decisiones de factibilidad del proyecto:

- Si el C/B > 1, el proyecto es rentable.
- Si el C/B ≤ 1, el proyecto no es viable.

Para determinar el costo beneficio se cuenta con los siguientes datos obtenidos de las tablas de presupuesto de conectividad (Tabla 70) y los gastos de Internet (TABLA 72):

$$CB = \frac{Beneficios - Contrabeneficios}{Costos}$$

$$CB = \frac{B - CB}{C}$$

Gasto de los Servicios de CEDIA: $ 991.530,62

Costo (Presupuesto de Inversión): $ 52.324,14

Beneficios: 991.530,62 – 52.324,14 = $ 939.206,48

Contrabeneficios: $ 0

$$CB = \frac{939.206{,}48 - 0}{52.324{,}14}$$

$$CB = \frac{939.206{,}48}{52.324{,}14}$$

$$CB = 17{,}95$$

Se pudo determinar una relación Costo Beneficio de 17,95 por lo que se puede afirmar que el proyecto seguirá siendo rentable en los próximos cinco años, gracias a que los beneficios que se obtendrán con la propuesta son mayores a los costos que representarían si se niega la implementación de la Red Inalámbrica en el campus de la Universidad Técnica del Norte.

5.4. BENEFICIARIOS

Los beneficiarios directos e indirectos del proyecto son más de 8000 usuarios entre docentes, administrativos, empleados y estudiantes de pregrado y postgrado de las diferentes carreras que ofrece la universidad a la región norte del país.

Sin duda alguna los índices de calidad académica incrementarán notablemente con la implementación de la red Inalámbrica alcanzando a cubrir puntos importantes de acreditación institucional y por cada una de las carreras pertenecientes a la universidad.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Se han cumplido los objetivos planteados en el presente trabajo de titulación: Diseñar una Red LAN Inalámbrica previo al análisis situacional que sirvió como base para su futura implementación.

- Para la realización de un diseño de infraestructura de red se debe tomar en cuenta ciertas consideraciones como disponibilidad, escalabilidad, confiabilidad, seguridad, interoperabilidad, número de usuarios, autenticación de usuarios, disponibilidad de ancho de banda, gestión y administración centralizada y movilidad para satisfacer las necesidades de los usuarios que pertenecen al campus universitario.

- Los cálculos de área de cobertura de los Access Points ayudan a respaldar y sustentar un buen diseño de infraestructura de Red Inalámbrica.

- Se considera configurar de forma manual los canales de trabajo 1, 6, 11 en base al diseño de distribución de los APs.

- RADIUS es un protocolo basado en estándares, y cualquier plataforma que pretende apoyar RADIUS debe ser compatible con el estándar.

- RADIUS es una posibilidad que las organizaciones pueden llevar a cabo con su infraestructura tecnológica actual, la misma que se adecuará sin mayores impactos económicos o funcionales.

- El sistema operativo Linux seleccionado para el Portal Cautivo WifiDog fue Debian por su flexibilidad en la instalación y configuración de cada uno de los ficheros, mientras que el sistema operativo utilizado para el Firewall – Proxy fue CentOS.

RECOMENDACIONES

- Se debe capacitar al personal encargado de la Gestión de Redes y Comunicaciones de la Universidad Técnica del Norte informando de todos los servicios generados y las implicaciones que tendría el uso indebido de la misma.

- Se recomienda tener un respaldo de todos los archivos de configuración del Portal Cautivo, Servidor de Autenticación y Firewall-Proxy.

- Previo al diseño e implementación de una red inalámbrica se deben realizar pruebas de campo para determinar el alcance de cobertura de la señal de los Access Points porque pueden existir factores que incidan en cambios sobre el diseño planteado.

- Los APs que se tienen en funcionamiento no abastecen a cubrir algunas zonas del campus universitario por lo que se recomienda aumentar más APs para realizar un balanceo de carga y no exceder el límite de conexiones por cada AP.

- Las falencias de la Red Inalámbrica se debe sin duda alguna al crecimiento de usuarios que utilizan sin ningún tipo de control y con dos o más dispositivos conectados concurrentemente por cada usuario.

- En el peor de los casos que el Wireless LAN Controller deje de funcionar por cualquier motivo se debería considerar tener un backup de otro WLC.

- Para evitar cualquier anomalía de los equipos se debe pensar seriamente en un sistema de respaldo de energía propio para el Datacenter, y de esta manera optimizar los recursos de red necesarios.

REFERENCIAS BIBLIOGRÁFICAS

Adeva Brito, D. (10 de Marzo de 2014). *Las Formas Geométricas.* Obtenido de Sitio Web La cata de queso: http://blogs.redalumnos.com/0d6316c3b982c903/FORMAS

Aguero Calvo, R. (28 de Octubre de 2011). *WLAN: Estándar IEEE 802.11.* Obtenido de Grupo de Ingeniería en Telemática: https://docs.google.com/viewer?a=v&q=cache:m4wK2ELXs38J:www.tlmat.unican.es/siteadmin/submaterials/518.pdf+ramon+aguero+calvo+redes+inalambricas&hl=en&gl=ec&pid=bl&srcid=ADGEESjpmnb4mZOAi8gJexd42U0cBcxb_u-FFSzUTZE5bv7E7_r2uouajsNHEPrID9poW6nIzkxbHNWFJO0LK

Anguera, J., & Pérez, A. (2011). *Teoría de Antenas.* Barcelona: Creative Commons Deed.

Ariganello, E., & Barrientos Sevilla, E. (2010). *Redes Cisco CCNP a Fondo.* Madrid: Alfaomega Ra-Ma.

Barrios Dueñas, J. (10 de Abril de 2014). *Configuración básica de Shorewall*. Obtenido de Sitio Web Alcance Libre: http://www.alcancelibre.org/staticpages/index.php/configuracion-basica-shorewall

Blank, L. T., & Tarquin, A. J. (2006). *Ingeniería Económica.* México: McGraw-Hill.

Boyano, J. J. (10 de Abril de 2014). *Instalación de Webmin en CentOS 6.3*. Obtenido de Sitio Web El Blog de Juan José Boyano: http://jjboyano.wordpress.com/2013/01/31/instalacion-de-webmin-en-centos-6-3/

Carlos. (10 de Febrero de 2010). *Cacharrero Puro y Duro*. Obtenido de Antenas Wireless: http://cacharreopuroyduro.blogspot.com/2010/02/antenas-wireless.html

Chillispot. (5 de 11 de 2013). *Chillispot Captive Portal*. Obtenido de Sitio Web Chillispot Captive Portal: http://www.chillispot.org/

Cisco. (5 de Diciembre de 2013). *Cisco Aironet 1130AG IEEE 802.11 A/B/G Access Point.* Obtenido de Sitio Web Cisco Aironet 1130AG: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1130-ag-series/product_data_sheet0900aecd801b9058.pdf

Cisco. (5 de Diciembre de 2013). *Cisco Aironet 1260 Series Access Point.* Obtenido de Sitio Web Cisco Aironet 1260:

http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1260-series/data_sheet_c78-593663.pdf

Cisco. (5 de Diciembre de 2013). *Cisco Aironet 1300 Series Outdoor Access Point or Bridge.* Obtenido de Sitio Web Cisco Aironet 1300: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1300-series/product_data_sheet09186a00802252e1.pdf

Cisco. (5 de Diciembre de 2013). *Cisco Aironet 1400 Series Wireless Bridge.* Obtenido de Sitio Web Cisco Aironet 1400: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1400-wireless-bridge/product_data_sheet09186a008018495c.pdf

Cisco. (5 de Marzo de 2014). *Cisco 5500 Series Wireless Controller.* Obtenido de Sitio Web Cisco 5500 Series Wireless Controller: http://www.cisco.com/c/en/us/products/collateral/wireless/5500-series-wireless-controllers/data_sheet_c78-521631.pdf

Cisco Networking Academy. (2008). *Conmutación y Conexión Inalámbrica de LAN.* San José, California: Cisco Systems, Inc.

Cobo, D. (8 de Octubre de 2012). *WordPress.com*. Obtenido de DANICOBOINFOR: http://danicoboinfor.wordpress.com/2012/10/08/wlan/

Cordoba Serna, R. (10 de Mayo de 2014). *Que es el servidor Proxy*. Obtenido de Sitio Web Técnico en Sistema: http://raicordoba.blogspot.com/2013/09/que-proxy-que-es-un-servidor-proxy-como.html

Delgado Ortiz, H. H. (2009). *Redes Inalámbricas.* Lima - Perú: Empresa Editora Macro E.I.R.L.

Diego. (3 de Marzo de 2014). *Como calcular el área de un sector circular.* Obtenido de Sitio Web Todos los Como: http://todosloscomo.com/2012/10/22/como-calcular-el-area-de-un-sector-circular/

Eastep, T. M. (10 de Abril de 2014). *Iptables made easy Shorewall*. Obtenido de Sitio Web Shorewall: http://shorewall.net/Introduction.html

Electric Sheep Fencing LLC. (5 de 11 de 2013). *PfSense*. Obtenido de Sitio Web PfSense: http://www.pfsense.org/

Espinoza, M. P., & Loayza, C. C. (15 de Abril de 2013). *Seguridad para la Red Inalámbrica de un Campus Universitario.* Obtenido de Seguridad para la Red Inalámbrica de un Campus Universitario: http://www.utpl.edu.ec/seguridad/wp-content/uploads/2008/10/seg_wifi.pdf

FACAE. (15 de Junio de 2013). *Universidad Técnica del Norte*. Obtenido de UniPortal Web UTN: http://www.utn.edu.ec/facae/

FCCSS. (15 de Junio de 2013). *Universidad Técnica del Norte*. Obtenido de UniPortal Web UTN: http://www.utn.edu.ec/fccss/

FECYT. (15 de Junio de 2013). *Universidad Técnica del Norte*. Obtenido de UniPortal Web UTN: http://www.utn.edu.ec/fecyt/

Fernández Hansen, Y., Ramos Varón, A. A., & García Moran, J. P. (2009). *RADIUS / AAA / 802.1x Sistemas basados en la Autenticación en en Windows y Linux/GNU Seguridad Máxima.* Madrid: Ra-Ma.

FICA. (15 de Junio de 2013). *Universidad Técnica del Norte*. Obtenido de UniPortal Web UTN: http://www.utn.edu.ec/fica/

FICAYA. (15 de Junio de 2013). *Universidad Técnica del Norte*. Obtenido de UniPortal Web UTN: http://www.utn.edu.ec/ficaya/

Fierro Fierro, M. M., & González Bonifaz, F. A. (3 de Febrero de 2012). *DSpace ESPOCH.* Obtenido de Tesis de Estudio Comparativo de Aplicaciones para la Implementación de Portales Cautivos Empleando Interconectividad entre los Locales de Bonny Restaurant.: http://dspace.espoch.edu.ec/bitstream/123456789/1492/1/18T00454.pdf

Fürman, J. (15 de Mayo de 2014). *Overlapping eduroam Networks Operated by Different Organizations*. Obtenido de Sitio Web CESNET: http://archiv.cesnet.cz/doc/techzpravy/2009/eduroam-overlap/

Grupo de Redes de Computadores. (30 de Mayo de 2013). *GRC*. Obtenido de Universidad Politécnica de Valencia: http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf

Herrera Ramírez, E., Días Ramírez, A., & Calafate, C. T. (2008). *Desarrollando el estándar IEEE 802.11n, un paso adelante en WLAN.* México: CiComp'07.

Hiertz et al. (Enero de 2010). The IEEE 802.11 Universe. *IEEE Communications, 48*(1), 62-70.

Holt, A., & Huang, C.-Y. (2010). *802.11 Wireless Networks Security and Analysis.* London: Springer.

IEEE Std 802.11™-2012: Revision of IEEE Std 802.11-2007. (2012). *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* New York, USA: IEEE Standards Association.

Île Sans Fil. (5 de 11 de 2013). *Wifidog a Captive Portal Suite*. Obtenido de Sitio Web Wifidog a Captive Portal Suite: http://dev.wifidog.org/

Kasper, M. (5 de 11 de 2013). *m0n0wall*. Obtenido de Sitio Web m0n0wall: http://m0n0.ch/wall/

Kassar, M., Kervella, B., & Pujolle, G. (Junio de 2008). An overview of vertical handover decision strategies in heterogeneous wireless networks. *Comput. Commun. 31, 31*. Recuperado el 26 de Agosto de 2013

Kioskea ES. (5 de Septiembre de 2013). *Propagación de las ondas de radio (802.11)*. Obtenido de kioskea.net: http://es.kioskea.net/contents/819-propagacion-de-las-ondas-de-radio-802-11

Linux-OS. (5 de 11 de 2013). *GNU/Linux, Software Libre, Tecnologías y algo mas…*. Obtenido de WiFiDOG - Captive Portal Suite: http://www.linux-os.com.ar/linuxos/wifidog-captive-portal-suite

Magaña, M. (25 de Abril de 2013). Obtenido de IEEE 802.11: http://tic-calidad-ieee.blogspot.com/

Magnetoxx24. (16 de Diciembre de 2012). *Zonas de Fresnel en Redes Inalámbricas*. Obtenido de Un Blog de Tecnología, Software Libre, Redes y Telecomunicaciones: http://magnetoxx24.wordpress.com/2012/12/16/zonas-de-fresnel-en-redes-inalambricas/

Monsalve, J. (24 de Junio de 2011). *Antenas una explicación de su funcionamiento (II)*. Obtenido de diarioelectronicohoy.com: http://www.diarioelectronicohoy.com/antenas-una-explicacion-de-su-funcionamiento-ii/

Ramírez Pérez, C. (2011). *Handoff vertical basado en procesos analíticos jerárquicos.* Universidad Autónoma Metropolitana Iztapalapa. México: Casa abierta al tiempo. Recuperado el 25 de Agosto de 2013

Ricciardi, F. (5 de 11 de 2013). *Zeroshell Net Services*. Obtenido de Sitio Web Zeroshell Net Services: http://www.zeroshell.org/

Solano Jiménez, J. M., & Oña Garcés, M. B. (24 de Marzo de 2010). *DSpace ESPOCH.* Obtenido de Tesis de Estudio de Portales Cautivos de gestión de acceso Inalámbrico a Internet de la ESPOCH: http://dspace.espoch.edu.ec/bitstream/123456789/103/1/18T00381.pdf

Soyinka, W. (2010). *Wireless Network Administration a Beginners Guide.* USA: McGraw-Hill.

Stallings, W. (2005). *Wireless Communication and Networks Second Edition.* New Jersey: Pearson Prentice Hall.

Vincent, S., & Vançon, T. (5 de 11 de 2013). *PepperSpot*. Obtenido de Sitio Web PepperSpot: http://pepperspot.sourceforge.net/

Wikipedia. (16 de Octubre de 2012). *Wikipedia The Free Encyclopedia*. Obtenido de Wikimedia Foundation, Inc: http://en.wikipedia.org/wiki/IEEE_802.11

wndw.net. (Septiembre de 2008). *wndw.net.* Recuperado el 2 de Agosto de 2013, de Redes Inalámbricas en los Países en Desarrollo: http://wndw.net/pdf/wndw3-es/wndw3-es-print.pdf

ANEXO 1

CISCO AIRONET 1300 SERIES OUTDOOR ACCESS POINT DATA SHEET

Data Sheet

Cisco Aironet 1300 Series Outdoor Access Point or Bridge

Product Overview

The Cisco® Aironet® 1300 Series Outdoor Access Point or Bridge (Figure 1) is an 802.11g access point and bridge that provides high-speed and cost-effective wireless connectivity between multiple fixed or mobile networks and clients. Building a metropolitan-area wireless infrastructure with the Cisco Aironet 1300 Series provides deployment personnel with a flexible, easy-to-use solution that meets the security requirements of wide-area networking professionals. The Cisco Aironet 1300 Series can be deployed as an autonomous access point or bridge, providing intelligent network services as a standalone device. Alternatively, the Cisco Aironet 1300 Series can be deployed as part of the Cisco Unified Wireless Network, managed centrally by a Cisco wireless LAN controller.

Figure 1. Cisco Aironet 1300 Series

The Cisco Aironet 1300 Series supports the 802.11g standard—providing 54-Mbps data rates with a proven, secure technology while maintaining full backward compatibility with legacy 802.11b devices. It is delivered in a compact, rugged enclosure for deployment in outdoor environments, and is available in two versions. The Cisco Aironet 1300 Series with integrated antenna can be quickly installed to provide a LAN bridge to a remote site or multiple sites. The 1300 Series with antenna connectors supports a variety of Cisco 2.4-GHz antennas, providing range and coverage versatility.

The Cisco Aironet 1300 Series is available either as part of the Cisco Unified Wireless Network or as an autonomous access point or bridge. The Cisco Unified Wireless Network is a comprehensive solution that delivers an integrated, end-to-end wired and wireless network. Using the radio and network management features of the Cisco Unified Wireless Network for simplified deployment, the Cisco Aironet 1300 Series extends the security, scalability, reliability, ease of deployment, and manageability available in wired networks to the wireless LAN. Unified access points operate with the Lightweight Access Point Protocol (LWAPP) and work in conjunction with Cisco wireless LAN controllers and the Wireless Control System (WCS). When configured with LWAPP, the Cisco Aironet 1300 Series can automatically detect the best-available Cisco wireless LAN controller and download appropriate policies and configuration information with no hands-on intervention.

Autonomous access points are based on Cisco IOS® Software and may optionally operate with the CiscoWorks Wireless LAN Solution Engine (WLSE). Autonomous access points, along with the WLSE, deliver a core set of features and may be field-upgraded to take advantage of the full benefits of the Cisco Unified Wireless Network as requirements evolve. As an autonomous access point or bridge, the Cisco Aironet 1300 Series may be configured to operate as a wireless access point, bridge, or a workgroup bridge.

Users and Applications

The Cisco Aironet 1300 Series can provide outdoor wireless access, an ongoing savings of leased-line expenses, a method to connect networks despite physical barriers such as lakes or highways, and rapid deployment of network connections—often while waiting on other facilities, such as fiber-optic installations. The types of organizations that will benefit from the advantages of the Cisco Aironet 1300 Series include education, enterprise, government, healthcare, military, public safety, transportation, and WLAN service providers. These organizations have a variety of possible applications, as shown in Figure 2 and described in the following paragraphs.

Campus Networks

Whether the deployment is in a typical college campus or corporate offices with multiple buildings, IT professionals are faced with interconnecting local area networks around and in between each of the buildings. These LANs require cost-effective, high-bandwidth connections with seamless mobility throughout the WLAN. They also require the flexibility and control that is unavailable through leased lines or that would otherwise require trenching for new cable installations. The Cisco Aironet 1300 Series can be used as an outdoor access point, either operating with the Cisco wireless LAN controller and WCS or autonomously as an intelligent access point. It can also be used as an autonomous wireless bridge to connect remote buildings to the LAN.

Nomadic Networks and Users

More and more, networks are "on the move." Vehicles such as buses, trains, ambulances, and patrol cars are being equipped with their own LAN-supported devices, including notebooks, personal digital assistants (PDAs), cameras, and scanners. These mobile networks provide new passenger services, improved public service, and operational efficiency but they need to be interconnected to enable information-sharing and more informed decision-making. The Cisco Aironet 1300 Series can operate in autonomous mode as a workgroup bridge connecting in-vehicle devices to Cisco Aironet access points and bridges that are fixed throughout the service area.

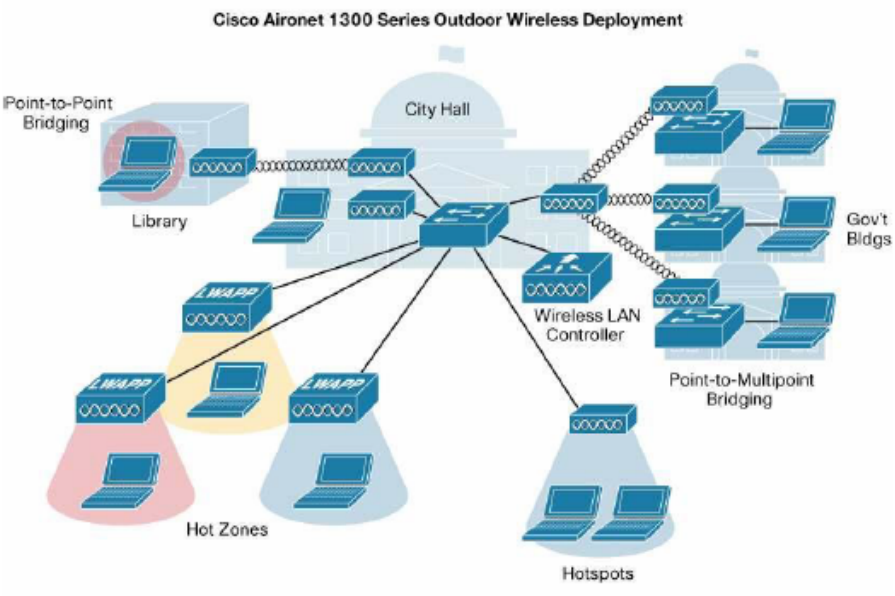
Outdoor Public Access

The proliferation of WLAN hotspots has allowed users to stay connected while in hotels, airports, and even coffee shops. As more users desire ubiquitous connectivity, outdoor hotspots are being added—and some include multiple city blocks or even town centers. These outdoor hotspots can be cost-effectively deployed with the Cisco Aironet 1300 Series unified or autonomous access points.

Temporary Networks

The variety of temporary solutions is limitless, with applications such as remote military campaigns, short-term office leases, temporary buildings such as trailers, or even parking lot tent sales. These deployments require a temporary network infrastructure that is rugged, portable, easy to install, and flexible. The Cisco Aironet 1300 Series can be quickly deployed, with complete functionality packaged in the integrated antenna version, or with a selection of easy-to-install remote antennas for the connectorized version.

Figure 2. Cisco Aironet 1300 Series Applications Example



Benefits

Industry-Leading Performance

- Data rates of 54 Mbps in the 2.4-GHz band
- Bridge range of 20 miles (32 kilometers [km]) at 11 Mbps
- Aggregate throughput approaching 28 Mbps
- Maximum transmit power of 100 milliwatts (mW) for 802.11b and 30 mW for 802.11g. Maximum power setting will vary according to individual country regulations.
- For vehicle-installed deployments, over 100 km per hour speeds at 12 and 24 Mbps with 128-byte packets at 1 percent packet error rate (PER) (workgroup bridge mode connected to a Cisco Aironet access point or bridge)
- Support for antenna diversity

Low Total Cost of Ownership

- Compelling return on investment (ROI) compared to cable installation or ongoing leased-line fees
- Low bridging-system cost
- Low outdoor access-point system cost
- Ability to reuse existing Cisco Aironet Series 350 Wireless Bridges for low upgrade costs
- Investment protection with future Cisco IOS Software upgrades

Flexible and Easy to Install

- The Cisco Unified Wireless Network simplifies wireless LAN deployment and management by providing clear visibility and dynamic control of the RF environment.
- Convenient LEDs provide bridge alignment feedback and diagnostics.

- Quick-hang mounting bracket allows for an easy installation process; roof and wall mounting kits offer more mounting options.
- Rapid deployment, redeployment, and recommissioning can be achieved with no reliance upon third-party service providers or a lengthy license or trenching process.
- Multiple, configurable radio network roles enable point-to-point and point-to-multipoint bridging.
- Wide DC power-input range allows a variety of power supply options such as solar power or vehicle power (+10 to +48 volts direct current [VDC]).
- Supports a wide operating-temperature range of –22°F to 131℉ (–30°to +55℃).
- Meets NEMA 4 and IP56 specifications for harsh environments.
- Supports captured antennas for easy mounting and support for external antennas, including existing Cisco Aironet 2.4-GHz antennas.

Award-Winning Security

The Cisco Aironet 1300 Series has achieved National Institute of Standards and Technology (NIST) FIPS 140-2 level 2 validation and is in process for Common Criteria validation under the National Information Assurance Partnership (NIAP) program.

The Cisco Aironet 1300 Series supports 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA, and numerous Extensible Authentication Protocol (EAP) types. WPA and WPA2 are the Wi-Fi Alliance certifications for interoperable, standards-based WLAN security. These certifications support IEEE 802.1X for user-based authentication, Temporal Key Integrity Protocol (TKIP) for WPA encryption, and Advanced Encryption Standard (AES) for WPA2 encryption. These certifications help to ensure interoperability between Wi-Fi-certified WLAN devices from different manufacturers.

The Cisco Aironet 1300 Series hardware-accelerated AES encryption supports enterprise-class, government-grade secure encryption over the WLAN without compromising performance. IEEE 802.1X authentication helps to ensure that only authorized users are allowed on the network. Backward compatibility and support for WPA client devices running TKIP, the RC4 encryption algorithm, is also supported by the Cisco Aironet 1300 Series.

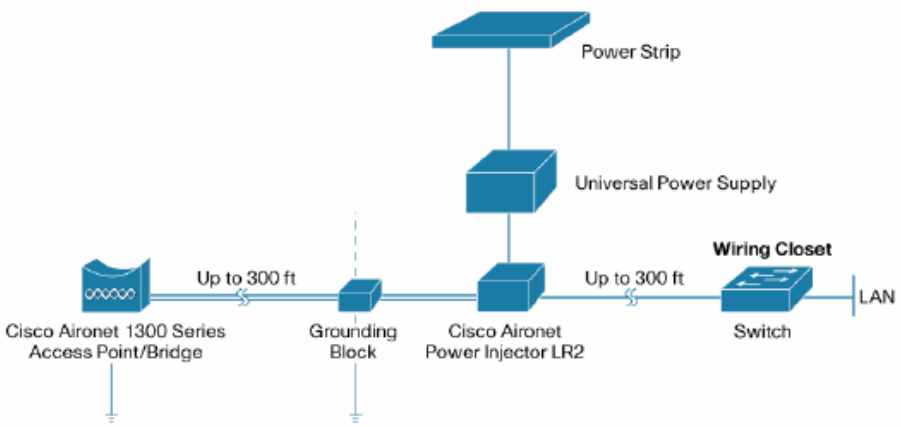
Cisco Aironet 1300 Series access points operating with LWAPP support Cisco Unified Intrusion Detection System or Intrusion Prevention System (IDS/IPS), which is part of the Cisco Self-Defending Network and is the industry's first integrated wired and wireless network security solution. The Cisco Unified IDS/IPS takes a comprehensive approach to security—at the wireless edge, wired edge, WAN edge, and through the data center. When a trusted client acts maliciously, the Cisco wired IDS detects the attack and sends shun requests to the Cisco wireless LAN controllers, which will then disassociate the client device. Cisco Unified IDS goes beyond simple fire walling. If a user is allowed to access a specific server, but is not allowed to access a particular directory on the server, the anomalous behavior is detected and mitigated.

Autonomous or unified Cisco Aironet 1300 Series Access Points support management frame protection for the authentication of 802.11 management frames by the wireless network infrastructure. This allows the network to detect spoofed frames from access points or malicious users impersonating infrastructure access points. If an access point detects a malicious attack, an incident will be generated by the access point and reports will be gathered on the controller, Cisco WCS, or CiscoWorks WLSE.

Product Architecture

A flexible outdoor wireless-bridge or access-point solution is provided through the combination of the Cisco Aironet 1300 Series, a power injector, and options for both antennas and mounting. Figure 3 shows how the units connect.

Figure 3. Network Diagram with Power Injector



Cisco Aironet 1300 Series

The Cisco Aironet 1300 Series provides the 802.11g interface for access-point capability or bridge connections. By placing the unit outdoors, close to the antenna, you can minimize the wireless cable losses—thereby maximizing the range of the network. The unit is available with either an integrated antenna, or with connectors for external antennas (Figure 4). The high-gain, integrated antenna is designed for easy installations of point-to-point links or non-root nodes of point-to-multipoint networks as an autonomous bridge. The nonintegrated antenna version provides professional installers with an RP-TNC connector that allows the deployment of omnidirectional, sector, or high-gain dish antennas for specific application requirements.

Figure 4. Cisco Aironet 1300 Series Connector Options

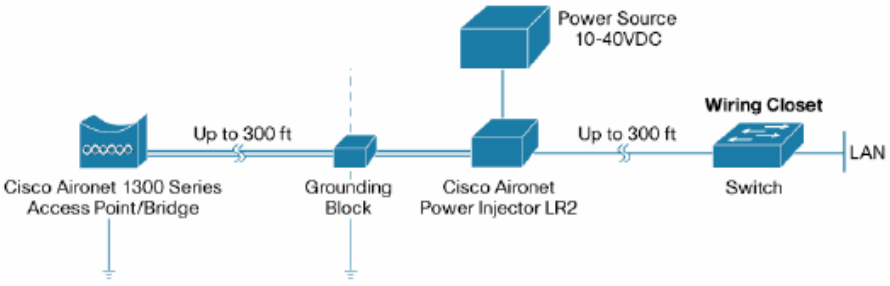
Power Injector

The Cisco Aironet Bridge Power Injector converts the standard 10/100BASE-T Ethernet interface that is suitable for weather-protected areas to a dual F-Type connector interface for coaxial cables that are more suitable for harsh outdoor environments. The power injector also provides power to the outdoor unit over the same cables with a power-discover feature and surge protection. To support longer cabling from your wired switch or router, the power injector enables total cable runs up to 200 meters (Category 5 [Cat5] and coaxial). The Cisco Aironet 1300 Series ships with the Cisco Aironet Power Injector LR2 (Figure 5) and an AC power supply.

Figure 5. Cisco Aironet Power Injector AIR-PWRINJ-BLR2/AIRPWRINJ-BLR2T

The optional Cisco Aironet Power Injector LR2T takes power from any +12 to +40 VDC source not supplied by Cisco. Typically, the DC source is a vehicle or solar-power source (Figure 6). This power injector provides the flexibility needed when an AC power source is not available.

Figure 6. Network Diagram with Optional Power Injector



Mounting Hardware and Antennas

In addition to having a variety of antennas available from Cisco, the Cisco 1300 Series also has different mounting options (Figure 7). These optional mounting kits are available for mounting to a roof, wall, or pole. The quick-hang mounting bracket enables a simple, one-person installation. For more information on available antennas, please refer to the Cisco Aironet Antennas and Accessories Data Sheet and Reference Guide:

- Data Sheet:
  http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008022b11b.html
- Reference Guide:
  http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html

Figure 7. Cisco Aironet 1300 Series Mounting Hardware and Antennas

Features

The Cisco Aironet 1300 Series access point or bridge provides the following features.

Antenna Alignment Assistance

The autonomous Cisco Aironet 1300 Series provides an autoconfiguration and installation mode for quick deployment of point-to-point links without the need for configuration through Telnet, FTP, or Simple Network Management Protocol (SNMP). This mode provides LEDs with signal-strength information used in the installation and alignment process. As a result, installers are free to perform their installation process and verify the link quality without knowledge of Cisco IOS Software or data networking.

Automatic RF Configuration

Under the Cisco Unified Wireless Network, radio resource management provides automatic configuration of RF parameters for access points such as the Cisco Aironet 1300 Series Access Points. The result is a coordinated RF plan for access points under the span of the Cisco wireless LAN controller, which also recognizes the presence of other RF emitting devices. This minimizes interference to and from neighboring access points, ensuring optimal network capacity.

Seamless Layer 2 and Layer 3 Roaming

The Cisco Aironet 1300 Series provides fast secure roaming of wireless clients and autonomous non-root bridges and workgroup bridges. In both the unified access point and the autonomous access point, the encryption keys for mobile devices are cached locally, allowing the mobile device to roam between access points while remaining authenticated to the network. This significantly reduces roaming time by eliminating the need to conduct the four-way handshake with each roam. Autonomous non-root bridges and workgroup bridges also scan in the background to search for alternative Cisco Aironet access points and bridges that mobile device may be roaming to, which also reduces roaming time.

Support for Port Aggregation Protocol and Cisco Fast EtherChannel Technology

Bandwidth can be increased between bridged networks through the aggregation of multiple autonomous bridges at each site via Cisco Fast EtherChannel® technology, Port Aggregation Protocol (PAgP), or routing protocols.

Wireless Link-Distance Adjustment

For an autonomous Cisco Aironet 1300 Series device, the link-distance parameter allows the user to tune the Carrier-Sense Multiple Access/Collision Avoidance (CSMA/CA) parameters for the particular range in use to maximize performance.

Wireless Packet Concatenation

The concatenation of smaller packets into larger ones allows autonomous Cisco Aironet 1300 Series access point or bridge to more efficiently use the wireless medium and provide higher overall data throughputs.

Wireless Programmable Clear-Channel Assessment

With a programmable clear-channel assessment, an autonomous Cisco Aironet 1300 Series access point or bridge can be configured to the particular background-interference level found in your environment. This provides reduced contention overhead with other wireless systems.

Summary

The Cisco Aironet 1300 Series is a flexible outdoor 802.11b and 802.11g access point or bridge that provides high-speed and cost-effective wireless connectivity between multiple fixed or mobile networks and clients.

Product Specifications

Link Roles and Product Compatibility

Table 1 outlines the link roles in which the Cisco Aironet 1300 Series can operate, and identifies the products that it is compatible with in the particular role.

Table 1. Link Role and Product Compatibility

Role	Applications	Unified or Autonomous Architecture	Compatibility
Access Point	Engineered specifically for harsh outdoor environments, yet also capable in indoor deployments, the Cisco Aironet 1300 Series is ideal for WLANs requiring outdoor coverage. The Cisco Aironet 1300 Series is Wi-Fi certified as an access point and also supports the innovative features available with Cisco Aironet and Cisco Compatible client devices.	Unified or Autonomous	• Compatible with any Wi-Fi certified WPA or WPA2 client device for basic capability • Compatible with Cisco Aironet clients and Cisco Compatible clients for extended capability
Bridge	The Cisco Aironet 1300 Series supports either point-to-point or point-to-multipoint configurations to cost-effectively interconnect remote, temporary, or mobile networks. It can serve as an upgrade or replacement to the Cisco Aironet 350 Wireless Bridge by providing over-the-air compatibility with existing Cisco Aironet 350 Series Wireless Bridges. While in bridge mode, client associations are also accepted—effectively providing simultaneous bridge and access-point capability.	Autonomous	Compatible with Cisco Aironet 1300 Series and 350 Series Wireless Bridges
Workgroup Bridge	There is no hard/soft limit on the number of devices you can have, however we only recommend up to a maximum of 20 devices.	Autonomous	Supports operation with Cisco Aironet access points and Cisco bridges

Protocols

Table 2 lists the protocols supported by the Cisco Aironet 1300 Series.

Table 2. Protocols

Protocols	Description
Air Interface Standard	IEEE 802.11b or IEEE 802.11g **Note:** Autonomous bridge mode has enhancements to the standard to allow longer-range bridging communications.
Frequency Band	• 2.412 to 2.462 GHz (FCC) • 2.412 to 2.472 GHz (ETSI) • 2.412 to 2.472 GHz (TELEC)
Wireless Modulation	802.11b • Direct Sequence Spread Spectrum (DSSS): ◦ Differential Binary Phase Shift Keying (DBPSK) at 1 Mbps ◦ Differential Quadrature Phase Shift Keying (DQPSK) at 2 Mbps ◦ Complementary Code Keying (CCK) at 5.5 and 11 Mbps 802.11g • Orthogonal Frequency Divisional Multiplexing (OFDM): ◦ BPSK at 6 and 9 Mbps ◦ QPSK at 12 and 18 Mbps ◦ 16-quadrature amplitude modulation (QAM) at 24 and 36 Mbps ◦ 64-QAM at 48 and 54 Mbps
Media Access Protocol	Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)
Lightweight Access Point Protocol	A network protocol for lightweight access points that also provides for centralized management.
Operating Channels	802.11b/g • ETSI: 13 • Americas: 11 • TELEC (Japan): 13

Protocols	Description
Nonoverlapping Channels	3
Security—Bridge Role*	Cisco Wireless Security Suite, including: **Authentication** 802.1X support including LEAP to yield mutual authentication and dynamic per-user, per session encryption keys **Encryption** • Cisco TKIP or WPA TKIP; key hashing (per-packet keying), Message Integrity Check (MIC) and broadcast key rotation • AES (802.11i)
Security—Access Point Role	Cisco Wireless Security Suite supporting WPA and WPA2, including: **Authentication** • Management frame protection provides for the authentication of 802.11 management frames by the wireless network infrastructure. This allows the network to detect spoofed frames from access points or malicious users impersonating infrastructure access points. If an access point detects a malicious attack, an incident will be generated by the access points and reports will be gathered on the Cisco wireless LAN controller, Cisco WCS, or CiscoWorks WLSE. • 802.1X support including Cisco LEAP, Protected EAP-Generic Token Card (PEAP-GTC), PEAP-Microsoft Challenge Authentication Protocol Version 2 (MSCHAPv2), EAP Message Digest 5 (EAP MD5), EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (EAP-TTLS), EAP-Subscriber Identity Module (EAP-SIM), and EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) to yield mutual authentication and dynamic per user, per-session encryption keys **Encryption** • WPA: Cisco TKIP or WPA TKIP; key hashing (per-packet keying), MIC and broadcast key rotation • WPA2: AES (802.11i)
Security—Workgroup Bridge Role*	Cisco Wireless Security Suite, including: **Authentication** • 802.1X support including Cisco LEAP to yield mutual authentication and dynamic per-user, per session encryption keys **Encryption** • Cisco TKIP or WPA TKIP; key hashing (per-packet keying), MIC and broadcast key rotation • AES (802.11i)
SNMP Compliance	Versions 1 and 2

* Cisco Aironet 1300 Series can operate as a workgroup bridge or wireless bridge when it is an autonomous device. When the Cisco Aironet 1300 Series is operating under the Cisco Unified Wireless Network architecture, it only operates as an access point.

Components

Table 3 lists the components available for the Cisco Aironet 1300 Series.

Table 3. Components

Components	Description
Power Injector LR2	The power injector converts the standard 10/100BASE-T Ethernet Cat5 RJ-45 interface that is suitable for weather-protected areas to a dual F-Type connector interface for dual coaxial cables that are more suitable for harsh outdoor environments. While providing a 100BASE-T interface to the Cisco Aironet 1300 Series, the power injector also provides power to the unit over the same cables with a power discovery feature that protects other appliances from damage should they accidentally be connected. As an added benefit to the installer, the automatic medium-dependent interface crossover (Auto-MDIX) feature is built in, allowing the dual cables to be swapped while maintaining the same capability. To support longer cable runs from your network switch or router, the power injector is designed to accommodate up to a 100 meter coaxial cable run plus 100 meters of indoor Cat5 cable—enabling total cable runs up to 200 meters. Lightning and surge protection is also included at the F-Type connector interface to provide added protection to your network devices. The power injector requires a 48V DC source supplied by Cisco.
Power Injector LR2T	The Power Injector LR2T supports all the capabilities of LR2. It is designed for use in transportation applications and operates with an input voltage range of +12 to +40V DC. The DC source is provided by the user. The LR2T can therefore be vehicle- or solar-powered.
Power Supply	• 48V DC supply for AIR-PWRINJ-BLR2= • User-supplied 12 to 40V DC source for AIR-PWRINJ_BLR2T=. Could require an external load-dump-module for automotive and bus installations.
AIR-BR1310G-x-K9 or AIR LAP1310G-x-K9 Integrated Antenna	• Vertical polarization • 13-dBi gain • 36°E-plane by 38°H-plane (3-dB beam width)

Interfaces

Table 4 lists the Cisco Aironet 1300 Series interfaces.

Table 4. Interfaces

	AIR-BR1310G-x-K9 AIR-BR1310G-x-K9-R AIR-LAP1310G-x-K9 AIR-LAP1310G-x-K9R	AIR-PWRINJ-BLR2 AIR-PWRINJ-BLR2T
Status LEDs	Four LEDs: Install, Radio, Status, and Ethernet	One bicolor LED showing power status
F-Type Connectors	Dual coaxial cable carries full-duplex Ethernet, DC power, and full-duplex console port (RS-232 connection)	Dual coaxial cable carries full-duplex Ethernet, DC power, and full-duplex console port (RS 232 connection)
Antenna Interface	• AIR-BR1310G-x-K9 or AIR-LAP1310G-x-K9: Air interface (integrated directional antenna) • AIR-BR1310G-x-K9-R or AIR-LAP1310G-x-K9R: Two RP-TNC type connectors for external antennas	—
DC Power	—	One two-pin Switchcraft connector (with threaded locking sleeve) and matching connector
RJ-45 Interface	—	One RJ-45 connector for console-port access (9600 bps only), a second RJ-45 connector for 10/100BASE-T LAN interface
Grounding Lugs	Two grounding lugs for lightening protection.	—

Memory Requirements

Table 5 lists the memory specifications for the Cisco Aironet 1300 Series.

Table 5. Memory Requirements

8 MB of Flash Memory	Memory space for future firmware upgrades to support new 802.11 standards and advanced features.

Performance

Table 6 lists the Cisco Aironet 1300 Series performance capabilities.

Table 6. Performance Capabilities

	AIR-BR1310G-A-K9 or AIR-LAP1310G-A-K9	AIR-BR1310G-A-K9-R or AIR-LAP1310G-A-K9R
Available Transmit Power Settings	802.11b: • 100 mW (20 dBm) • 50 mW (17 dBm) • 30 mW (15 dBm) • 20 mW (13 dBm) • 10 mW (10 dBm) • 5 mW (7 dBm) • 1 mW (0 dBm) 802.11g: • 30 mW (15 dBm) • 20 mW (13 dBm) • 10 mW (10 dBm) • 5 mW (7 dBm) • 1 mW (0 dBm)	802.11b: • 100 mW (20 dBm) • 50 mW (17 dBm) • 30 mW (15 dBm) • 20 mW (13 dBm) • 10 mW (10 dBm) • 5 mW (7 dBm) • 1 mW (0 dBm) 802.11g: • 30 mW (15 dBm) • 20 mW (13 dBm) • 10 mW (10 dBm) • 5 mW (7 dBm) • 1 mW (0 dBm)
	Note: Maximum power setting will vary according to individual country regulations.	
Maximum Operational Receive Level	–20 dBm	–20 dBm
Maximum Survivable Receive Level	10 dBm	10 dBm

	AIR-BR1310G-A-K9 or AIR-LAP1310G-A-K9	AIR-BR1310G-A-K9-R or AIR-LAP1310G-A-K9R
Receive Sensitivity (10 Percent with 3200 Byte Packets)	• 1 Mbps: –94 dBm • 2 Mbps: –91 dBm • 5.5 Mbps: –89 dBm • 11 Mbps: –85 dBm • 6 Mbps: –90 dBm • 9 Mbps: –89 dBm • 12 Mbps: –86 dBm • 18 Mbps: –84 dBm • 24 Mbps: –81 dBm • 36 Mbps: –77 dBm • 48 Mbps: –73 dBm • 54 Mbps: –72 dBm	• 1 Mbps: –94 dBm • 2 Mbps: –91 dBm • 5.5 Mbps: –89 dBm • 11 Mbps: –85 dBm • 6 Mbps: –90 dBm • 9 Mbps: –89 dBm • 12 Mbps: –86 dBm • 18 Mbps: –84 dBm • 24 Mbps: –81 dBm • 36 Mbps: –77 dBm • 48 Mbps: –73 dBm • 54 Mbps: –72 dBm
Maximum Bridge Relative Velocity (Autonomous-Mode Only)	Over 100 km per hour at 12 and 24 Mbps with 128-byte packets at 1 percent PER	
Access Point Role: Outdoor Range	Americas • 865 feet (260 meters) at 54 Mbps • 3465 feet (1055 meters) at 11 Mbps ETSI • 150 feet (45 meters) at 54 Mbps • 775 feet (235 meters) at 11 Mbps TELEC • 485 feet (145 meters) at 54 Mbps • 1095 feet (330 meters) at 11 Mbps **Note:** Access point with 13-dBi integrated antenna and Cisco clients	Americas • 350 feet (105 meters) at 54 Mbps • 1410 feet (430 meters) at 11 Mbps ETSI • 195 feet (60 meters) at 54 Mbps • 630 feet (190 meters) at 11 Mbps TELEC • 195 feet (60 meters) at 54 Mbps • 445 feet (135 meters) at 11 Mbps **Note:** Access point with 5.2-dBi patch antenna and Cisco clients
Bridge Role: Point to Point Range*	Americas • 1.3 miles (2 km) at 54 Mbps • 9 miles (15 km) at 11 Mbps EMEA • 0.2 miles (0.36 km) at 54 Mbps • 2.3 miles (3.5 km) at 11 Mbps TELEC • 0.7 miles (1.1 km) at 54 Mbps • 3.2 miles (5 km) at 11 Mbps **Note:** 13-dBi integrated antenna at root and non root bridge	Americas • 4.5 miles (7 km) at 54 Mbps • 14 miles (23 km) at 11 Mbps EMEA • 5.5 miles (9 km) at 11 Mbps TELEC • 4.5 miles (7 km) at 54 Mbps • 12 miles (20 km) at 11 Mbps **Note:** 21-dBi dish antenna at root and non root bridge
Bridge Role: Point to Multipoint Range*	Americas • 1.1 miles (1.8 km) at 54 Mbps • 8 miles (13 km) at 11 Mbps EMEA • 0.25 miles (0.4 km) at 54 Mbps • 1.1 miles (1.8 km) at 11 Mbps TELEC • 0.8 miles (1.3 km) at 54 Mbps • 3.6 miles (5.8 km) at 11 Mbps **Note:** 14-dBi sector antenna at root and 13-dBi integrated antenna at non-root	Americas • 2.0 miles (3.3 km) at 54 Mbps • 10 miles (16 km) at 11 Mbps EMEA • 2.5 miles (4 km) at 11 Mbps TELEC • 2.0 miles (3.3 km) at 54 Mbps • 9.0 miles (14 km) at 11 Mbps **Note:** 14-dBi sector at root and 21-dBi dish at non root

* Bridge role is only available for autonomous deployments. The distances referenced here are approximations and should be used for estimation purposes only.

Physical Specifications

Table 7 lists the physical specifications of the Cisco Aironet 1300 Series.

Table 7. Physical Specifications

	AIR-BR1310G-x-K9 AIR BR1310G x K9 R AIR-LAP1310G-x-K9 AIR-LAP1310G-x-K9R	AIR-PWRINJ-BLR2	AIR-PWRINJ-BLR2T
Dimensions	8 in. x 8.1 in. x 3.12 in. (20.3 cm x 20.57 cm x 7.87 cm)	4.62 in. x 4.76 in. x 1.07 in. (11.73 cm x 12.09 cm x 2.71 cm)	4.62 in. x 4.76 in. x 1.07 in. (11.73 cm x 12.09 cm x 2.71 cm)
Weight	2.5 lb (1.25 kg)	2 lb (1 kg)	2 lb (1 kg)
Operational Temperature	–22° to +131°F (–30° to +55°C)	–22° to +131°F (–30° to +55°C)	–22° to +131°F (–30° to +55°C)
Storage Temperature	–40° to +185°F (–40° to +85°C)	–40° to +185°F (-40° to +85°C)	–40° to +185°F (–40° to +85°C)
Operational Altitude	10,000 ft (3048m)	10,000 ft (3048m)	10,000 ft (3048m)
Storage Altitude	16,000 ft (4877 m)	16,000 ft (4877 m)	16,000 ft (4877 m)
Humidity	0 to 100% at 100°F (38°C) (condensing)	0 to 90% at 100°F (38°C) (noncondensing)	0 to 90% at 100°F (38°C) (noncondensing)
Vibration	SAEJ1455 section 4.9	SAEJ1455 section 4.9	SAEJ1455 section 4.9
Enclosure	NEMA 4; IP56; UL2083; environmentally sealed	UL2083; metal case	UL2083; metal case

Power Requirements

Table 8 lists Cisco Aironet 1300 Series power requirements.

Table 8. Power Requirements

	AIR-BR1310G-x-K9 AIR BR1310G x-K9-R AIR-LAP1310G-x-K9 AIR-LAP1310G-x-K9R	AIR-PWRINJ-BLR2	AIR-PWRINJ-BLR2T
AC Power	Not required—uses DC voltage from power injector	100 to 240V AC, ±10% (power supply provided by Cisco)	Not required
DC Power	—	• +48V DC, ±10% • Up to 9 W	• +12 to +40V DC, ±10% • Up to 11 W

Approvals and Compliance

The Cisco Aironet 1300 Series meets the following approvals and compliance standards (Table 9).

Table 9. Approvals and Compliance

	AIR-BR1310G-x-K9 AIR-BR1310G-x-K9-R AIR-LAP1310G-x-K9 AIR-LAP1310G-x-K9R	AIR-PWRINJ-BLR2 AIR-PWRINJ-BLR2T
Country Compliance	Customers are responsible for verifying approval for use in their country. Please visit http://www.cisco.com/go/aironet/compliance to verify approval and to identify the regulatory domain that corresponds to a particular country. Not all regulatory domains have been approved. As they are approved, the part numbers will be available on the Global Price List.	
Wi-Fi Certification	Wi Fi CERTIFIED	—

	AIR-BR1310G-x-K9 AIR-BR1310G-x-K9-R AIR-LAP1310G-x-K9 AIR-LAP1310G-x-K9R	AIR-PWRINJ-BLR2 AIR-PWRINJ-BLR2T
Safety	• UL 60950 third edition • CSA C22.2 No. 60950-00 • IEC 60950 Sec Ed, amendments 1-4 • EN 60950; 1992, amendments 1-4 • CSA 94/UL50—NEMA rated	• UL 60950 third edition • CSA C22.2 No. 60950-00 • IEC 60950 Sec Ed, amendments 1-4 • EN 60950; 1992, amendments 1-4 • UL2043 • FIPS 140-2 prevalidation list
Radio Approvals	• FCC Part 15.247 • RSS—139-1, RSS-210 (Canada) • EN 300.328 (Europe) • Telec 33B (Japan) • ARIB-STD-T66 v2.1 • FCC Bulletin OET-65CRSS-102 • Designed to EN60945	—
EMI and Susceptibility (Class B)	• FCC Part 15.107 and 15.109 Class B • ICES-003 Class B (Canada) • EN 55022 Class B • EN 55024 • AS/NZS 3548 Class B • VCCI Class B • EN 301.489-1 and 17 (Europe) • Designed to CISPR 25, ISO 11452-24, EN50121, EN60571 and SAEJ1113	• FCC Part 15.107 and 15.109 • Class B • ICES-003 Class B (Canada) • EN 55022 Class B • EN 55024 • AS/NZS 3548 Class B • VCCI Class B • EN 301.489-1 and 17 (Europe)

Additional Specifications

Warranty: One year

Ordering Information

To place an order, visit the Cisco Ordering Home Page. For assistance in determining the correct wireless bridge to order, as well as appropriate accessories, please read the Cisco Aironet 1300 Series Ordering Guide.

To Download the Software

Cisco Aironet software can be downloaded at the Cisco Software Center.

Service and Support

Cisco Systems offers a wide range of service programs to accelerate customer success. These innovative programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, see Cisco Technical Support Services.

For More Information

For more information about the Cisco Aironet 1300 Series, visit http://www.cisco.com/go/aironet or contact your local account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA

C78-340315-07 08/09

ANEXO 2

CISCO AIRONET 1130AG SERIES ACCESS POINT DATA SHEET

Data Sheet

Cisco Aironet 1130AG Series IEEE 802.11A/B/G Access Point

Low-profile enterprise-class access point with integrated antennas for easy deployment in offices and similar RF environments.

Product Overview

Cisco® Aironet® 1130AG Series IEEE 802.11a/b/g access points provide high-capacity, high-security, enterprise-class features in an unobtrusive, office-class design, delivering WLAN access with the lowest total cost of ownership. With high-performing dual IEEE 802.11a and 802.11g radios, the Cisco Aironet 1130AG Series provides a combined capacity of up to 108 Mbps to meet the needs of growing WLANs. Hardware-assisted Advanced Encryption Standard (AES) or temporal key integrity protocol (TKIP) encryption provides uncompromised support for interoperable IEEE 802.11i, Wi-Fi Protected Access 2 (WPA2) or WPA security. The Cisco Aironet 1130AG Series uses radio and network management features for simplified deployment, along with built-in omnidirectional antennas that provide robust and predictable WLAN coverage for offices and similar RF environments. The competitively priced Cisco Aironet 1130AG Series is ready to install and easy to manage, reducing the cost of deployment and ongoing maintenance.

The Cisco Aironet 1130AG Series is available in two versions: unified or autonomous. Unified access points operate with the Lightweight Access Point Protocol (LWAPP) and work in conjunction with Cisco wireless LAN controllers and the Cisco Wireless Control System (WCS). When configured with LWAPP, the Cisco Aironet 1130AG Series can automatically detect the best-available Cisco wireless LAN controller and download appropriate policies and configuration information with no manual intervention. Autonomous access points are based on Cisco IOS® Software and may optionally operate with the CiscoWorks Wireless LAN Solution Engine (WLSE). Autonomous access points, along with the CiscoWorks WLSE, deliver a core set of features and may be field-upgraded to take advantage of the full benefits of the Cisco Unified Wireless Network as requirements evolve.

The Cisco Aironet 1130AG Series delivers optimal value for offices and similar environments. Built-in antennas provide omnidirectional coverage specifically designed for today's open workspaces. A multipurpose mounting bracket easily secures Cisco Aironet 1130AG Series access points to ceilings and walls. With an unobtrusive design, Cisco Aironet 1130AG Series access points are aesthetically pleasing and blend into their environments. For maximum concealment, the access point may be placed above ceilings or suspended ceilings. The UL 2043 rating of the Cisco Aironet 1130AG Series allows the access point to be placed above ceilings in plenum areas regulated by municipal fire codes. Offered at a competitive price, and optimized for easy installation and operation, the Cisco Aironet 1130AG Series helps organizations attain a lower total cost of ownership.

Applications

In offices and similarly open environments, Cisco Aironet 1130AG Series access points may be installed on the ceiling to provide users with continuous coverage as they roam throughout a facility. In school buildings and similar facilities, the access points may be installed on the ceiling of each room and hallway to provide users with full coverage and high network availability. In areas where a ceiling installation may not be practical such as retail hotspots or similar small facilities, the access points can be mounted simply and securely on walls for complete coverage with minimal installation cost.

Award-Winning Security

The Cisco Aironet 1130AG Series has achieved National Institute of Standards and Technology (NIST) FIPS 140-2 level 2 validation and is in process for Information Assurance validation under the National Information Assurance Partnership (NIAP) Common Criteria program. The Cisco Aironet 1130AG Series supports 802.11i, Wi-Fi Protected Access (WPA), WPA2, and numerous Extensible Authentication Protocol (EAP) types. WPA and WPA2 are the Wi-Fi Alliance certifications for interoperable, standards-based WLAN security. These certifications support IEEE 802.1X for user-based authentication, Temporal Key Integrity Protocol (TKIP) for WPA encryption, and Advanced Encryption Standard (AES) for WPA2 encryption. These certifications help to ensure interoperability between Wi-Fi-certified WLAN devices from different manufacturers.

The Cisco Aironet 1130AG Series hardware-accelerated AES encryption supports enterprise-class, government-grade secure encryption over the WLAN without compromising performance. IEEE 802.1X authentication helps to ensure that only authorized users are allowed on the network. Backward compatibility and support for WPA client devices running TKIP, the RC4 encryption algorithm, is also supported by the Cisco Aironet 1130AG Series.

Cisco Aironet 1130AG Series Access Points operating with LWAPP support Cisco Unified Intrusion Detection System/Intrusion Prevention System (IDS/IPS), a software feature that is part of the Cisco Self-Defending Network and is the industry's first integrated wired and wireless security solution. Cisco Unified IDS/IPS takes a comprehensive approach to security—at the wireless edge, wired edge, WAN edge, and through the data center. When an associated client sends malicious traffic through the Cisco Unified Wireless Network, a Cisco wired IDS device detects the attack and sends shun requests to Cisco wireless LAN controllers, which will then disassociate the client device.

Autonomous or unified Cisco Aironet 1130AG Series Access Points support management frame protection for the authentication of 802.11 management frames by the wireless network infrastructure. This allows the network to detect spoofed frames from access points or malicious

users impersonating infrastructure access points. If an access point detects a malicious attack, an incident will be generated by the access point and reports will be gathered on the Cisco wireless LAN controller, Cisco WCS, or CiscoWorks WLSE.

Features and Benefits

Table 1 lists features and benefits of Cisco Aironet 1130AG Series access points.

Table 1. Features and Benefits of Cisco Aironet 1130AG Series Access Points

Feature	Benefit
Dual 802.11a and 802.11g Radios	• Provides up to 108 Mbps of capacity in a single device for industry-leading capacity and backward compatibility with legacy 802.11b clients.
Supports 15 Nonoverlapping Channels	• Lower potential interference with neighboring access points simplifies deployment • Fewer transmission errors deliver greater throughput
Industry-Leading Radio Design	• Provides robust signals to long distances • Mitigates the effects of multipath signal propagation for more consistent coverage
Variable Transmit Power Settings	• Allows access point coverage to be tuned for differing requirements • Low—dBm setting supports closer spacing of access points in high-density deployments
Integrated Antennas	• Complete system is deployable out of the box without external antennas • Specifically designed to provide omnidirectional coverage for offices and similar radio frequency environments
Hardware-Assisted AES Encryption	• Provides high security without performance degradation
Cisco Unified IDS/IPS	• This integrated software feature is part of the Cisco Self-Defending Network and is the industry's first integrated wired and wireless security solution. When a trusted client acts maliciously, the wired IDS detects the attack and sends shun requests to Cisco WLAN controllers, which will then disassociate the client device.
Management Frame Protection	• This feature provides for the authentication of 802.11 management frames by the wireless network infrastructure. This allows the network to detect spoofed frames from access points or malicious users impersonating infrastructure access points. If an access point detects a malicious attack, an incident will be generated by the access points and reports will be gathered on the Cisco wireless LAN controller, Cisco WCS, or CiscoWorks WLSE.
IEEE 802.11i-Compliant; WPA2-Certified and WPA-Certified	• Helps to ensure interoperable security with wireless LAN client devices from other manufacturers
Low-Profile Design	• Unobtrusive design blends in to environment • "Quiet" LED does not draw attention to it when operating normally and no action is required
Multipurpose and Lockable Mounting Bracket	• Installs easily to walls, ceilings, and suspended ceiling railways • Accommodates standard padlock to prevent theft
Inline Power Support (IEEE 802.3af and Cisco Inline Power)	• Provides an interoperable alternative to AC power • Simplifies deployment by allowing power to be supplied over the Ethernet cable • Compatible with 802.3af-compliant power sources
Cisco Green Bulk Packaging	To reduce product packaging and preserve the environment, the Cisco Aironet 1130 Series may be ordered in a bulk package that includes 10 access points and 10 mounting kits.

Summary/Conclusion

The Cisco Aironet 1130AG Series provides the ideal enterprise access point for offices and similar environments. With two high-performance radios, these access points provide simultaneous support for the 802.11a and 802.11g standards, offering 108 Mbps of capacity for your growing WLAN. Incorporating AES encryption in hardware, the Cisco Aironet 1130AG Series complies with the 802.11i security standard and is WPA2-certified, helping to assure that your network employs the strongest security available while maintaining interoperability with products from other manufacturers. Additional design features, including diversity antennas with omnidirectional

coverage and an unobtrusive form factor, along with an attractive price, provide low total cost of ownership.

For office environments, the Cisco Aironet 1130AG Series is a cost-compelling solution for a high-capacity, high-security, enterprise-class WLAN.

Product Specifications

Table 2 lists the product specifications for Cisco Aironet 1130AG access points.

Table 2. Product Specifications for Cisco Aironet 1130AG Access Points

Item	Specification
Part Number for Individual Access Points	• AIR-AP1131AG-x-K9 (Cisco IOS Software) • AIR-LAP1131AG-x-K9 (Cisco Unified Wireless Network Software) **Note**: The Cisco Aironet 1130AG Series may be ordered with Cisco IOS Software to operate as an autonomous AP with Cisco Unified Wireless Network Software using LWAPP. When the 1130AG is operating as a lightweight AP a WLAN controller is required. • Regulatory Domains: (x = Regulatory Domain) • A = FCC • C = China • E = ETSI • I = Israel • J = TELEC (Japan) • K = Korea • N = North America (Excluding FCC) • P = Japan2 • S = Singapore • T = Taiwan Customers are responsible for verifying approval for use in their individual countries. To verify approval and to identify the regulatory domain that corresponds to a particular country please visit: http://www.cisco.com/go/aironet/compliance Not all regulatory domains have been approved. As they are approved, the part numbers will be available on the Global Price List.
Part Number for Cisco Green Bulk Packaging	• AIR-AP1131-x-K9-10 (Cisco IOS Software) • AIR-LAP1131-xK9-10 (Cisco Unified Wireless Network Software) **Note**: The Cisco Aironet 1130AG Series may be ordered with Cisco IOS Software to operate as an autonomous AP with Cisco Unified Wireless Network Software using LWAPP. When the 1130AG is operating as a lightweight AP a WLAN controller is required. • Regulatory Domains: (x = Regulatory Domain) • A = FCC • E = ETSI • Customers are responsible for verifying approval for use in their individual countries. To verify approval and to identify the regulatory domain that corresponds to a particular country please visit: http://www.cisco.com/go/aironet/compliance
Software	• Cisco IOS Software Release 12.3(8)JA or later (autonomous). • Cisco IOS Software Release 12.3(11)JX or later (Lightweight Mode). • Cisco Unified Wireless Network Software Release 4.0 or later.
Data Rates Supported	• 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps • 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
Network Standard	IEEE 802.11a, 802.11b, and 802.11g
Uplink	Autosensing 802.3 10/100BASE-T Ethernet

Item	Specification
Frequency Band and Operating Channels	**Americas (FCC)** • 2.412 to 2.462 GHz; 11 channels • 5.15 to 5.35, 5.725 to 5.825 GHz; 12 channels **China** • 2.412 to 2.472 GHz; 13 channels • 5.725 to 5.825 GHz; 4 channels **ETSI** • 2.412 to 2.472 GHz; 13 channels • 5.15 to 5.725 GHz; 19 channels **Israel** • 2.432 to 2.472 GHz; 9 channels • 5.15 to 5.35 GHz, 8 channels **Japan (TELEC)** • 2.412 to 2.472 GHz; 13 channels Orthogonal Frequency Division Multiplexing (OFDM) • 2.412 to 2.484 GHz; 14 channels Complementary Code Keying (CCK) • 5.15 to 5.25 GHz; 4 channels **Japan–P (TELEC 2 (Japan2) Cnfg)** • 2.412 to 2.472 GHz; 13 channels Orthogonal Frequency Division Multiplexing (OFDM) • 5.15 to 5.35 GHz, 8 channels **Korea** • 2.412 to 2.472 GHz; 13 channels • 5.15 to 5.35, 5.46 to 5.72, 5.725 to 5.825, 19 channels **North America** • 2.412 to 2.462 GHz; 11 channels • 5.15 to 5.35, 5.725 to 5.825 GHz; 12 channels **Singapore** • 2.412 to 2.472 GHz, 13 channels • 5.15 to 5.35 GHz, 8 channels and 5.725 to 5.825 GHz, 12 channels **Taiwan** • 2.412 to 2.462 GHz, 11 channels • 5.25-5.35 GHz, 5.725 to 5.825, 7 channels
Nonoverlapping Channels	802.11a: Up to 19	802.11b/g: 3
Receive Sensitivity (Typical)	**802.11a:** 6 Mbps: -87 dBm 9 Mbps: -86 dBm 12 Mbps: -85 dBm 18 Mbps: -84 dBm 24 Mbps: -80 dBm 36 Mbps: -78 dBm 48 Mbps: -73 dBm 54 Mbps: -71 dBm	**802.11g:** 1 Mbps: -93 dBm 2 Mbps: -91 dBm 5.5 Mbps: -88 dBm 6 Mbps: -86 dBm 9 Mbps: -85 dBm 11 Mbps: -85 dBm 12 Mbps: -84 dBm 18 Mbps: -83 dBm 24 Mbps: -79 dBm 36 Mbps: -77 dBm 48 Mbps: -72 dBm 54 Mbps: -70 dBm

Available Transmit Power Settings (Maximum Power Setting Will Vary by Channel and According to Individual Country Regulations)	**802.11a:** OFDM: 17 dBm (50 mW) 15 dBm (30 mW) 14 dBm (25 mW) 11 dBm (12 mW) 8 dBm (6 mW) 5 dBm (3 mW) 2 mW (2 dBm) -1 dBm (1 mW)	**802.11b:** CCK: 20 dBm (100 mW) 17 dBm (50 mW) 14 dBm (25 mW) 11 dBm (12 mW) 8 dBm (6 mW) 5 dBm (3 mW) 2 dBm (2 mW) -1 dBm (1 mW)	**802.11g:** OFDM: 17 dBm (50 mW) 14 dBm (25 mW) 11 dBm (12 mW) 8 dBm (6 mW) 5 dBm (3 mW) 2 dBm (2 mW) -1 dBm (1 mW)
Range	**Indoor (Distance Across Open Office Environment):**		**Outdoor:**

Item	Specification			
	802.11a: 80 ft (24 m) @ 54 Mbps 150 ft (45 m) @ 48 Mbps 200 ft (60 m) @ 36 Mbps 225 ft (69 m) @ 24 Mbps 250 ft (76 m) @ 18 Mbps 275 ft (84 m) @ 12 Mbps 300 ft (91 m) @ 9 Mbps 325 ft (100 m) @ 6 Mbps	**802.11g:** 100 ft (30 m) @ 54 Mbps 175 ft (53 m) @ 48 Mbps 250 ft (76 m) @ 36 Mbps 275 ft (84 m) @ 24 Mbps 325 ft (100 m) @ 18 Mbps 350 ft (107 m) @ 12 Mbps 360 ft (110 m) @ 11 Mbps 375 ft (114 m) @ 9 Mbps 400 ft (122 m) @ 6 Mbps 420 ft (128 m) @ 5.5 Mbps 440 ft (134 m) @ 2 Mbps 450 ft (137 m) @ 1 Mbps	**802.11a:** 100 ft (30 m) @ 54 Mbps 300 ft (91 m) @ 48 Mbps 425 ft (130 m) @ 36 Mbps 500 ft (152 m) @ 24 Mbps 550 ft (168 m) @ 18 Mbps 600 ft (183 m) @ 12 Mbps 625 ft (190 m) @ 9 Mbps 650 ft (198 m) @ 6 Mbps	**802.11g:** 120 ft (37 m) @ 54 Mbps 350 ft (107 m) @ 48 Mbps 550 ft (168 m) @ 36 Mbps 650 ft (198 m) @ 24 Mbps 750 ft (229 m) @ 18 Mbps 800 ft (244 m) @ 12 Mbps 820 ft (250 m) @ 11 Mbps 875 ft (267 m) @ 9 Mbps 900 ft (274 m) @ 6 Mbps 910 ft (277 m) @ 5.5 Mbps 940 ft (287 m) @ 2 Mbps 950 ft (290 m) @ 1 Mbps
	Ranges and actual throughput vary based upon numerous environmental factors so individual performance may differ.			
Compliance	**Standards** Safety • UL 60950-1 • CAN/CSA-C22.2 No. 60950-1 • UL 2043 • IEC 60950-1 • EN 60950-1 • NIST FIPS 140-2 level 2 validation Radio Approvals • FCC Part 15.247, 15.407 • RSS-210 (Canada) • EN 300.328, EN 301.893 (Europe) • ARIB-STD 33 (Japan) • ARIB-STD 66 (Japan) • ARIB-STD T71 (Japan) • AS/NZS 4268.2003 (Australia and New Zealand) EMI and Susceptibility (Class B) • FCC Part 15.107 and 15.109 • ICES-003 (Canada) • VCCI (Japan) • EN 301.489-1 and -17 (Europe) Security • 802.11i, WPA2, WPA • 802.1X • AES, TKIP • FIPS 140-2 Pre-Validation List • Common Criteria (when running Cisco IOS software) Other • IEEE 802.11g and IEEE 802.11a • FCC Bulletin OET-65C • RSS-102			

Item	Specification
Antennas	• 2.4 GHz ◦ Gain 3.0 dBi ◦ Horizontal Beamwidth 360° • 5 GHz ◦ Gain 4.5 dBi ◦ Horizontal Beamwidth 360°
Security	**Authentication** Security Standards • WPA • WPA2 (802.11i) • Cisco TKIP • Cisco message integrity check (MIC) • IEEE 802.11 WEP keys of 40 bits and 128 bits **802.1X EAP types:** • EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) • Protected EAP-Generic Token Card (PEAP-GTC) • PEAP-Microsoft Challenge Authentication Protocol Version 2 (PEAP-MSCHAP) • EAP-Transport Layer Security (EAP-TLS) • EAP-Tunneled TLS (EAP-TTLS) • EAP-Subscriber Identity Module (EAP-SIM) • Cisco LEAP **Encryption** • AES-CCMP encryption (WPA2) • TKIP (WPA) • Cisco TKIP • WPA TKIP • IEEE 802.11 WEP keys of 40 bits and 128 bits
Status LEDs	**External:** • Status LED indicates operating state, association status, error/warning condition, boot sequence, and maintenance status **Internal:** • Ethernet LED indicates activity over the Ethernet, status • Radio LED indicates activity over the radios, status
Dimensions (H x W x D)	7.5 in. x 7.5 in. x 1.3 in. (19.1 x 19.1 x 3.3 cm)
Weight	1.5 lb (0.67 kg)
Environmental	• 32-104°F (0-40°C) • 10-90 percent humidity (noncondensing)
System Memory	• 32 MB RAM • 16 MB FLASH
Input Power Requirements	• 100-240 VAC; 50-60Hz (power supply) • 36-57 VDC (device)
Power Draw	12.2W maximum
Warranty	One year
Wi-Fi Certification	

System Requirements

Table 3 lists the system requirements for Cisco Aironet 1130AG access points.

Table 3. System Requirements for Cisco Aironet 1130AG Access Points

Access Utilizing	Description
Browser	Using the Web browser management GUI, requires a computer running Internet Explorer Version 6.0 or newer, or Netscape Navigator Version 7.0 or newer.

Power over Ethernet (PoE)	Power sourcing equipment (PSE) compliant with Cisco Inline Power or IEEE 802.3af, and providing at least 12.2W at 48 VDC.

Service and Support

Cisco Systems® offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, visit Cisco Technical Support Services or Cisco Advanced Services.

For More Information

For more information about the Cisco Aironet 1130AG Series, visit http://www.cisco.com/go/wireless or contact your local account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-338069-05 06/08

ANEXO 3

CISCO AIRONET 1260 SERIES ACCESS POINT DATA SHEET

Data Sheet

Cisco Aironet 1130AG Series IEEE 802.11A/B/G Access Point

Low-profile enterprise-class access point with integrated antennas for easy deployment in offices and similar RF environments.

Product Overview

Cisco® Aironet® 1130AG Series IEEE 802.11a/b/g access points provide high-capacity, high-security, enterprise-class features in an unobtrusive, office-class design, delivering WLAN access with the lowest total cost of ownership. With high-performing dual IEEE 802.11a and 802.11g radios, the Cisco Aironet 1130AG Series provides a combined capacity of up to 108 Mbps to meet the needs of growing WLANs. Hardware-assisted Advanced Encryption Standard (AES) or temporal key integrity protocol (TKIP) encryption provides uncompromised support for interoperable IEEE 802.11i, Wi-Fi Protected Access 2 (WPA2) or WPA security. The Cisco Aironet 1130AG Series uses radio and network management features for simplified deployment, along with built-in omnidirectional antennas that provide robust and predictable WLAN coverage for offices and similar RF environments. The competitively priced Cisco Aironet 1130AG Series is ready to install and easy to manage, reducing the cost of deployment and ongoing maintenance.

The Cisco Aironet 1130AG Series is available in two versions: unified or autonomous. Unified access points operate with the Lightweight Access Point Protocol (LWAPP) and work in conjunction with Cisco wireless LAN controllers and the Cisco Wireless Control System (WCS). When configured with LWAPP, the Cisco Aironet 1130AG Series can automatically detect the best-available Cisco wireless LAN controller and download appropriate policies and configuration information with no manual intervention. Autonomous access points are based on Cisco IOS® Software and may optionally operate with the CiscoWorks Wireless LAN Solution Engine (WLSE). Autonomous access points, along with the CiscoWorks WLSE, deliver a core set of features and may be field-upgraded to take advantage of the full benefits of the Cisco Unified Wireless Network as requirements evolve.

Data Sheet

Cisco Aironet 1260 Series Access Point

Performance and Flexibility for Challenging RF Environments
- Nine times faster than 802.11a/g networks
- ClientLink improves reliability and coverage for legacy clients
- BandSelect improves 5-GHz client connections in mixed client environments
- VideoStream uses multicast to improve rich-media applications

Rugged Metal Housing and Extended Operating Temperature
- Ideal for factories, warehouses, and other industrial environments
- Supports external antennas for a variety of RF environments and deployment scenarios
- UL 2043 plenum-rated for above ceiling installation options or suspended from drop ceilings

Easy Installation and Power Efficient
- 802.11n performance with existing PoE switches
- Sleek design blends into a variety of indoor environments

Easy-to-Install, Multipurpose Mounting Bracket
- Designed for easy replacement of existing access points
- Locks for theft protection

Simplified Network Management
- Controller-based or standalone deployment options

Secure Connections
- Supports rogue access point detection and denial-of-service attacks
- Management frame protection detects malicious users and alerts network administrators

Greater Network Capacity
- Dynamic frequency selection 2 (DFS-2) compliant

Cisco® Aironet® 1260 Series wireless access points provide reliable and predictable 802.11n wireless coverage for indoor environments. These enterprise-class access points deliver up to nine times the throughput of 802.11a/g networks for rich-media applications. Designed specifically for challenging environments, the 1260 Series supports external antennas and a broad operating-temperature range.

RF Excellence

Building on the Cisco Aironet heritage of RF excellence, the 1260 Series delivers industry-leading performance for secure and reliable wireless connections. Enterprise-class silicon and optimized radios deliver a robust mobility experience using Cisco M-Drive technology, which includes:

- ClientLink improves reliability and coverage for legacy clients
- BandSelect improves 5-GHz client connections in mixed client environments
- VideoStream uses multicast to improve rich-media applications

All of these features ensure the best possible end-user experience on the wireless network.

Cisco also offers the industry's broadest selection of 802.11n antennas, delivering optimal coverage for a variety of deployment scenarios.

The Cisco Aironet 1260 Series is a component of the Cisco Unified Wireless Network, which can scale up to 18,000 access points with full Layer 3 mobility across central or remote locations on the enterprise campus, in branch offices, and at remote sites. The Cisco Unified Wireless Network is the industry's most flexible, resilient, and scalable architecture, delivering secure access to mobility services and applications and offering the lowest total cost of ownership and investment protection by integrating seamlessly with the existing wired network.

Product Specifications

Table 1 lists the product specifications for Cisco Aironet 1260 Series Access Points.

Table 1. Product Specifications for Cisco Aironet 1260 Series Access Points

Item	Specification
Part Numbers	**Cisco Aironet 1260 Series Access Point** **Controller-based access point** **Indoor, challenging environments, with external antennas** • AIR-LAP1262N-x-K9 - Dual-band Controller-based 802.11 a/g/n • AIR-LAP1261N-x-K9 - Single-band Controller-based 802.11 g/n • AIR-AP1262N-x-K9 - Dual-band Standalone 802.11 a/g/n • AIR-AP1261N-x-K9 - Single-band Standalone 802.11 g/n • AIR-LAP1262N-xK910 - Eco-pack (dual-band 802.11a/g/n) 10 quantity Controller-based access points • AIR-AP1262N-xK9-5 - Eco-pack (dual-band 802.11a/g/n) 5 quantity Standalone access points **SMARTnet Services** • CON-SNT-LAP1262x - SMARTnet 8x5xNBD 1260 Series access point (dual-band 802.11 a/g/n) • CON-SNT-LAP1261x - SMARTnet 8x5xNBD 1260 Series access point (single-band 802.11 g/n) • CON-SNT-LAP1262x - SMARTnet 8x5xNBD 10 quantity eco-pack 1260 Series access point (dual-band 802.11a/g/n) **Cisco Wireless LAN Services** • AS-WLAN-CNSLT - Cisco Wireless LAN Network Planning and Design Service • AS-WLAN-CNSLT - Cisco Wireless LAN 802.11n Migration Service • AS-WLAN-CNSLT - Cisco Wireless LAN Performance and Security Assessment Service **Regulatory domains: (x = regulatory domain)** Customers are responsible for verifying approval for use in their individual countries. To verify approval and to identify the regulatory domain that corresponds to a particular country, please visit: http://www.cisco.com/go/aironet/compliance Not all regulatory domains have been approved. As they are approved, the part numbers will be available on the Global Price List.
Software	• Cisco Unified Wireless Network Software Release 7.0 or later • Cisco IOS® Software Release 12.4(25d)JA
802.11n Version 2.0 (and Related) Capabilities	• 2x3 multiple-input multiple-output (MIMO) with two spatial streams • Maximal ratio combining (MRC) • Legacy beamforming • 20- and 40-MHz channels • PHY data rates up to 300 Mbps • Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx) • 802.11 dynamic frequency selection (DFS) • Cyclic shift diversity (CSD) support
Data Rates Supported	**802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps** **802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps** **802.11n data rates (2.4 GHz and 5 GHz):**

MCS Index[1]	GI[2] = 800 ns		GI = 400 ns	
	20-MHz Rate (Mbps)	40-MHz Rate (Mbps)	20-MHz Rate (Mbps)	40-MHz Rate (Mbps)
0	6.5	13.5	7.2	15
1	13	27	14.4	30
2	19.5	40.5	21.7	45
3	26	54	28.9	60
4	39	81	43.3	90

[1] MCS Index: The Modulation and Coding Scheme (MCS) index determines the number of spatial streams, the modulation, the coding rate, and data rate values.
[2] GI: A guard interval (GI) between symbols helps receivers overcome the effects of multipath delays.

Item	Specification				
	5	52	108	57.8	120
	6	58.5	121.5	65	135
	7	65	135	72.2	150
	8	13	27	14.4	30
	9	26	54	28.9	60
	10	39	81	43.3	90
	11	52	108	57.8	120
	12	78	162	86.7	180
	13	104	216	115.6	240
	14	117	243	130	270
	15	130	270	144.4	300

Frequency Band and 20-MHz Operating Channels	**A (A Regulatory Domain):** • 2.412 to 2.462 GHz; 11 channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.700 GHz, 8 channels (excludes 5.600 to 5.640 GHz) • 5.745 to 5.825 GHz; 5 channels **C (C Regulatory Domain):** • 2.412 to 2.472 GHz; 13 channels • 5.745 to 5.825 GHz; 5 channels **E (E Reg Domain):** • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.700 GHz, 8 channels (excludes 5.600 to 5.640 GHz) **I (I Regulatory Domain):** • 2.412 to 2.472 GHz, 13 channels • 5.180 to 5.320 GHz; 8 channels **K (K Regulatory Domain):** • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.620 GHz, 7 channels • 5.745 to 5.805 GHz, 4 channels	**N (N Regulatory Domain):** • 2.412 to 2.462 GHz; 11 channels • 5.180 to 5.320 GHz; 8 channels • 5.745 to 5.825 GHz; 5 channels **Q (Q Regulatory Domain):** • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.700 GHz; 11 channels **S (S Regulatory Domain):** • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels • 5.745 to 5.825 GHz; 5 channels **T (T Regulatory Domain):** • 2.412 to 2.462 GHz; 11 channels • 5.280 to 5.320 GHz; 3 channels • 5.500 to 5.700 GHz, 11 channels • 5.745 to 5.825 GHz; 5 channels
Note: Customers are responsible for verifying approval for use in their individual countries. To verify approval and to identify the regulatory domain that corresponds to a particular country, please visit: http://www.cisco.com/go/aironet/compliance.		
Maximum Number of Nonoverlapping Channels	**2.4 GHz** • 802.11b/g: ◦ 20 MHz: 3 • 802.11n: ◦ 20 MHz: 3	**5 GHz** • 802.11a: ◦ 20 MHz: 21 • 802.11n: ◦ 20 MHz: 21 ◦ 40 MHz: 9
Note: This varies by regulatory domain. Refer to the product documentation for specific details for each regulatory domain.		

Item	Specification			
Receive Sensitivity	**802.11b (Complementary Code Keying [CCK])** -101 dBm @ 1 Mb/s -98 dBm @ 2 Mb/s -92 dBm @ 5.5 Mb/s -89 dBm @ 11 Mb/s	**802.11g (non HT20)** -92 dBm @ 6 Mb/s -92 dBm @ 9 Mb/s -92 dBm @ 12 Mb/s -90 dBm @ 18 Mb/s -86 dBm @ 24 Mb/s -84 dBm @ 36 Mb/s -79 dBm @ 48 Mb/s -78 dBm @ 54 Mb/s	**802.11a (non HT20)** -93 dBm @ 6 Mb/s -93 dBm @ 9 Mb/s -92 dBm @ 12 Mb/s -90 dBm @ 18 Mb/s -87 dBm @ 24 Mb/s -84 dBm @ 36 Mb/s -79 dBm @ 48 Mb/s -79 dBm @ 54 Mb/s	
	2.4-GHz **802.11n (HT20)** -92 dBm @ MCS0 -90 dBm @ MCS1 -88 dBm @ MCS2 -85 dBm @ MCS3 -82 dBm @ MCS4 -77 dBm @ MCS5 -76 dBm @ MCS6 -74 dBm @ MCS7 -92 dBm @ MCS8 -90 dBm @ MCS9 -87 dBm @ MCS10 -85 dBm @ MCS11 -82 dBm @ MCS12 -77 dBm @ MCS13 -75 dBm @ MCS14 -74 dBm @ MCS15		**5-GHz** **802.11n (HT20)** -93 dBm @ MCS0 -91 dBm @ MCS1 -89 dBm @ MCS2 -86 dBm @ MCS3 -83 dBm @ MCS4 -78 dBm @ MCS5 -77 dBm @ MCS6 -75 dBm @ MCS7 -87 dBm @ MCS8 -87 dBm @ MCS9 -85 dBm @ MCS10 -83 dBm @ MCS11 -79 dBm @ MCS12 -75 dBm @ MCS13 -73 dBm @ MCS14 -72 dBm @ MCS15	**5-GHz** **802.11n (HT40)** -91 dBm @ MCS0 -89 dBm @ MCS1 -87 dBm @ MCS2 -83 dBm @ MCS3 -80 dBm @ MCS4 -75 dBm @ MCS5 -74 dBm @ MCS6 -72 dBm @ MCS7 -86 dBm @ MCS8 -85 dBm @ MCS9 -84 dBm @ MCS10 -80 dBm @ MCS11 -77 dBm @ MCS12 -72 dBm @ MCS13 -71 dBm @ MCS14 -70 dBm @ MCS15
Maximum Transmit Power	**2.4 GHz** • 802.11b ◦ 23 dBm with 2 antennas • 802.11g ◦ 20 dBm with 2 antennas • 802.11n (non-HT duplicate mode) ◦ 20 dBm with 2 antennas • 802.11n (HT20) ◦ 20 dBm with 2 antennas		**5 GHz** • 802.11a ◦ 20 dBm with 2 antennas • 802.11n non-HT duplicate mode ◦ 20 dBm with 2 antennas • 802.11n (HT20) ◦ 20 dBm with 2 antennas • 802.11n (HT40) ◦ 20 dBm with 2 antennas	
Note: The maximum power setting will vary by channel and according to individual country regulations. Refer to the product documentation for specific details.				
Available Transmit Power Settings	**2.4 GHz** 23 dBm (200 mW) CCK Only 20 dBm (100 mW) 17 dBm (50 mW) 14 dBm (25 mW) 11 dBm (12.5 mW) 8 dBm (6.25 mW) 5 dBm (3.13 mW) 2 dBm (1.56 mW) -1 dBm (0.78 mW)		**5 GHz** 20 dBm (100 mW) 17 dBm (50 mW) 14 dBm (25 mW) 11 dBm (12.5 mW) 8 dBm (6.25 mW) 5 dBm (3.13 mW) 2 dBm (1.56 mW) -1 dBm (0.78 mW)	
Note: The maximum power setting will vary by channel and according to individual country regulations. Refer to the product documentation for specific details.				

Item	Specification
External Antenna (sold separately)	Cisco offers the industry's broadest selection of 802.11n antennas delivering optimal coverage for a variety of deployment scenarios.
Interfaces	• 10/100/1000BASE-T autosensing (RJ-45) • Management console port (RJ-45)
Indicators	• Status LED indicates boot loader status, association status, operating status, boot loader warnings, and boot loader errors
Dimensions (W x L x H)	• Access point (without mounting bracket): 8.7 x 8.7 x 1.84 in. (22.1 x 22.1 x 4.7 cm)
Weight	• 2.3 lbs (1.04 kg)
Environmental	• Nonoperating (storage) temperature: -40 to 185°F (-4 0 to 85°C) • Operating temperature: -4 to +131°F (-20 to +55°C) • Operating humidity: 10 to 90 percent (noncondensing)
System Memory	• 128 MB DRAM • 32 MB flash
Input Power Requirements	• AP1260: 44 to 57 VDC • Power Supply and Power Injector: 100 to 240 VAC; 50 to 60 Hz
Powering Options	• 802.3af Ethernet Switch • Cisco AP1260 Power Injectors (AIR-PWRINJ4=) • Cisco AP1260 Local Power Supply (AIR-PWR-B=)
Power Draw	• AP1260: 12.95 W **Note:** When deployed using Power over Ethernet (PoE), the power drawn from the power sourcing equipment will be higher by some amount dependent on the length of the interconnecting cable. This additional power may be as high as 2.45W, bringing the total system power draw (access point + cabling) to 15.4W.
Warranty	• Limited Lifetime Hardware Warranty
Compliance Standards	• Safety: ◦ UL 60950-1 ◦ CAN/CSA-C22.2 No. 60950-1 ◦ UL 2043 ◦ IEC 60950-1 ◦ EN 60950-1 • Radio approvals: ◦ FCC Part 15.247, 15.407 ◦ RSS-210 (Canada) ◦ EN 300.328, EN 301.893 (Europe) ◦ ARIB-STD 33 (Japan) ◦ ARIB-STD 66 (Japan) ◦ ARIB-STD T71 (Japan) ◦ AS/NZS 4268.2003 (Australia and New Zealand) ◦ EMI and susceptibility (Class B) ◦ FCC Part 15.107 and 15.109 ◦ ICES-003 (Canada) ◦ VCCI (Japan) ◦ EN 301.489-1 and -17 (Europe) ◦ EN 60601-1-2 EMC requirements for the Medical Directive 93/42/EEC • IEEE Standard: ◦ IEEE 802.11a/b/g, IEEE 802.11n 2.0, IEEE 802.11h, IEEE 802.11d • Security: ◦ 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA ◦ 802.1X ◦ Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP) • EAP Type(s): ◦ Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) ◦ EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) ◦ Protected EAP (PEAP) v0 or EAP-MSCHAPv2

Item	Specification
	◦ Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) ◦ PEAPv1 or EAP-Generic Token Card (GTC) ◦ EAP-Subscriber Identity Module (SIM) • Multimedia: ◦ Wi-Fi Multimedia (WMM™) • Other: ◦ FCC Bulletin OET-65C ◦ RSS-102

Limited Lifetime Hardware Warranty

This Cisco Aironet 1260 Series Access Point comes with a Limited Lifetime Warranty that provides full warranty coverage of the hardware for as long as the original end user continues to own or use the product. The warranty includes 10-day advance hardware replacement and ensures that software media is defect-free for 90 days. For more details, visit: http://www.cisco.com/go/warranty.

Service and Support

Cisco and Cisco Wireless LAN Specialized Partners offer a broad portfolio of end-to-end services based on proven methodologies for planning, designing, implementing, operating, and optimizing the performance of a variety of secure voice and data wireless network solutions, technologies, and strategies. Cisco Wireless LAN Specialized Partners bring application expertise to help deliver a secure enterprise mobility solution with a low total cost of ownership. For more information about Cisco 802.11n planning and deployment services, visit: http://www.cisco.com/go/wirelesslanservices.

For More Information

For more information about the Cisco Aironet 1260 Series, visit http://www.cisco.com/go/wireless or contact your local account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-593663-04 07/12

ANEXO 4

CISCO 5500 SERIES WIRELESS CONTROLLERS DATA SHEET

Data Sheet

Cisco 5500 Series Wireless Controllers

Maximum Performance and Scalability
- Support for up to 500 access points and 7000 clients
- 802.11n optimized for up to nine times the performance of 802.11a/g networks
- Enhanced uptime with the ability to simultaneously configure and manage 500 access points per controller

Improved Mobility and Services
- Larger mobility domain for more simultaneous client associations
- Faster radio resource management (RRM) updates for uninterrupted network access when roaming
- Intelligent RF control plane for self-configuration, self-healing, and self-optimization
- Efficient roaming improves application performance such as toll quality, voice, and consistent streaming of video and data backup

Licensing Flexibility and Investment Protection
- Additional access point capacity licenses may be added over time

Cisco OfficeExtend Solution
- Secure, simple, cost-effective mobile teleworker solution
- Up to 500 remote access points per controller
- Supports Cisco® Unified IP Phones for reduced cell phone charges

Comprehensive Wired/Wireless Security
- Full Control and Provisioning of Wireless Access Points (CAPWAP) access-point-to-controller encryption
- Supports rogue access point detection and denial-of-service attacks
- Management frame protection detects malicious users and alerts network administrators

Enterprise Wireless Mesh
- Dynamic wireless mesh networks support indoor and outdoor connectivity for areas that are difficult to wire

Environmentally Responsible
- Support for adaptive power management to turn off access point radios during off-peak hours to reduce power consumption
- OfficeExtend solution reduces costs and supports green best practices by reducing commuting time and saving on gas, vehicle mileage, and insurance costs

The Cisco® 5500 Series Wireless Controller, shown in Figure 1, is a highly scalable and flexible platform that enables systemwide services for mission-critical wireless networking in medium-sized to large enterprises and campus environments. Designed for 802.11n performance and maximum scalability, the 5500 Series offers enhanced uptime with:

- RF visibility and protection
- The ability to simultaneously manage up to 500 access points
- Superior performance for reliable streaming video and toll quality voice
- Sub-second stateful failover of all Access Points from Primary to Standby controller

Figure 1. Cisco 5500 Series Wireless LAN Controller

Features

Optimized for high-performance wireless networking, the 5500 Series offers improved mobility and prepares the business for the next wave of mobile devices and applications. The 5500 Series supports a higher density of clients and delivers more efficient roaming, with at least nine times the throughput of existing 802.11a/g networks.

The 5500 Series automates wireless configuration and management functions and allows network managers to have the visibility and control needed to cost-effectively manage, secure, and optimize the performance of their wireless networks. With integrated Cisco CleanAir™ technology, the 5500 Series protects 802.11n performance by providing cross-network access to real-time and historic RF interference information for quick, troubleshooting and resolution. As a component of the Cisco Unified Wireless Network, this controller provides real-time communications between Cisco Aironet® access points, the Cisco Wireless Control System (WCS), and the Cisco Mobility Services Engine to deliver centralized security policies, wireless intrusion prevention system (IPS) capabilities, award-winning RF management, and quality of service (QoS).

Software Licensing Flexibility

Base access point licensing offers flexibility to add up to 500 additional access points as business needs grow. The licensing structure supports a variety of business mobility needs as part of the basic feature set, including the Cisco OfficeExtend solution for secure, mobile teleworking and Cisco Enterprise Wireless Mesh, which allows access points to dynamically establish wireless connections in locations where it may be difficult or impossible to physically connect to the wired network.

Table 1 lists the features of the Cisco 5500 Series Wireless LAN Controllers.

Table 1. Cisco 5500 Series Wireless LAN Controller Features

Feature	Benefits
Scalability	• Supports 12, 25, 50,100, 250, or 500 access points for business-critical wireless services at locations of all sizes
High Performance	• Wired speed, nonblocking performance for 802.11n networks
RF Management	• Provides both real-time and historical information about RF interference impacting network performance across controllers, via systemwide Cisco CleanAir technology integration
OfficeExtend	• Supports corporate wireless service for mobile and remote workers with secure wired tunnels to the Cisco Aironet® 1130 or 1140 Series Access Points • Extends the corporate network to remote locations with minimal setup and maintenance requirements (zero-touch deployment) • Improves productivity and collaboration at remote site locations • Separate SSID tunnels allow both corporate and personal Internet access • Reduced CO2 emissions from decrease in commuting • Higher employee job satisfaction from ability to work at home • Improves business resiliency by providing continuous, secure connectivity in the event of disasters, pandemics, or inclement weather
Comprehensive End-to-End Security	• Offers Control and Provisioning of Wireless Access Points (CAPWAP) compliant DTLS encryption to ensure full-line-rate encryption between access points and controllers across remote WAN/LAN links
Enterprise Wireless Mesh	• Allows access points to dynamically establish wireless connections without the need for a physical connection to the wired network • Available on select Cisco Aironet access points, Enterprise Wireless Mesh is ideal for warehouses, manufacturing floors, shopping centers and any other location where extending a wired connection may prove difficult or aesthetically unappealing
High Performance Video	• Integrates Cisco VideoStream technology as part of the medianet framework to optimize the delivery of video applications across the WLAN
End-to-end Voice	• Supports Unified Communications for improved collaboration through messaging, presence, and conferencing • Supports all Cisco Unified Communications Wireless IP Phones for cost-effective, real-time voice services
High Availability	• An optional redundant power supply that helps to ensure maximum availability
Environmentally Responsible	• Organizations may choose to turn off access point radios to reduce power consumption during off peak hours
Mobility, security and management for IPv6 & dual-stack clients	• Secure, reliable wireless connectivity and consistent end-user experience • Increased network availability through proactive blocking of known threats • Equips administrators for IPv6 troubleshooting, planning, and client traceability from a common wired and wireless management system

Table 2 lists the product specifications for Cisco 5500 Series Wireless Controllers.

Table 2. Product Specifications for Cisco 5500 Series Wireless Controllers

Item	Specifications
Wireless	IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11n, 802.11u
Wired/Switching/Routing	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, 1000BASE-T. 1000BASE-SX, 1000-BASE-LH, IEEE 802.1Q Vtagging, and IEEE 802.1AX Link Aggregation.
Data Request For Comments (RFC)	• RFC 768 UDP • RFC 791 IP • RFC 2460 IPv6 (pass through Bridging mode only) • RFC 792 ICMP • RFC 793 TCP • RFC 826 ARP • RFC 1122 Requirements for Internet Hosts • RFC 1519 CIDR • RFC 1542 BOOTP • RFC 2131 DHCP • RFC 5415 CAPWAP Protocol Specification • RFC 5416 CAPWAP Binding for 802.11
Security Standards	• WPA • IEEE 802.11i (WPA2, RSN) • RFC 1321 MD5 Message-Digest Algorithm • RFC 1851 The ESP Triple DES Transform • RFC 2104 HMAC: Keyed Hashing for Message Authentication • RFC 2246 TLS Protocol Version 1.0 • RFC 2401 Security Architecture for the Internet Protocol • RFC 2403 HMAC-MD5-96 within ESP and AH • RFC 2404 HMAC-SHA-1-96 within ESP and AH • RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV • RFC 2406 IPsec • RFC 2407 Interpretation for ISAKMP • RFC 2408 ISAKMP • RFC 2409 IKE • RFC 2451 ESP CBC-Mode Cipher Algorithms • RFC 3280 Internet X.509 PKI Certificate and CRL Profile • RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec • RFC 3686 Using AES Counter Mode with IPsec ESP • RFC 4347 Datagram Transport Layer Security • RFC 4346 TLS Protocol Version 1.1
Encryption	• WEP and TKIP-MIC: RC4 40, 104 and 128 bits (both static and shared keys) • AES: CBC, CCM, CCMP • DES: DES-CBC, 3DES • SSL and TLS: RC4 128-bit and RSA 1024- and 2048-bit • DTLS: AES-CBC • IPSec: DES-CBC, 3DES, AES-CBC
Authentication, Authorization, and Accounting (AAA)	• IEEE 802.1X • RFC 2548 Microsoft Vendor-Specific RADIUS Attributes • RFC 2716 PPP EAP-TLS • RFC 2865 RADIUS Authentication • RFC 2866 RADIUS Accounting • RFC 2867 RADIUS Tunnel Accounting • RFC 2869 RADIUS Extensions • RFC 3576 Dynamic Authorization Extensions to RADIUS • RFC 3579 RADIUS Support for EAP

Item	Specifications
	• RFC 3580 IEEE 802.1X RADIUS Guidelines • RFC 3748 Extensible Authentication Protocol • Web-based authentication • TACACS support for management users
Management	• SNMP v1, v2c, v3 • RFC 854 Telnet • RFC 1155 Management Information for TCP/IP-Based Internets • RFC 1156 MIB • RFC 1157 SNMP • RFC 1213 SNMP MIB II • RFC 1350 TFTP • RFC 1643 Ethernet MIB • RFC 2030 SNTP • RFC 2616 HTTP • RFC 2665 Ethernet-Like Interface types MIB • RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions • RFC 2819 RMON MIB • RFC 2863 Interfaces Group MIB • RFC 3164 Syslog • RFC 3414 User-Based Security Model (USM) for SNMPv3 • RFC 3418 MIB for SNMP • RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs • Cisco private MIBs
Management Interfaces	• Web-based: HTTP/HTTPS • Command-line interface: Telnet, Secure Shell (SSH) Protocol, serial port • Cisco Wireless Control System (WCS)
Interfaces and Indicators	• Uplink: 8 (5508) 1000BaseT, 1000Base-SX and 1000Base-LH transceiver slots • Small Form-Factor Pluggable (SFP) options (only Cisco SFPs supported): GLC-T, GLC-SX-MM, GLC-LH-SM • LED indicators: link • Service Port: 10/100/1000 Mbps Ethernet (RJ45). • Service Port: 10/100/1000 Mbps Ethernet (RJ45) For High Availability for future use • LED indicators: link, • Utility Port: 10/100/1000 Mbps Ethernet (RJ45) • LED indicators: link • Expansion Slots: 1 (5508) • Console Port: RS232 (DB-9 male/RJ-45 connector included), mini-USB • Other Indicators: Sys, ACT, Power Supply 1, Power Supply 2
Physical and Environmental	• Dimensions (WxDxH): 17.30 x 21.20 x 1.75 in. (440 x 539 x 44.5 mm) • Weight: 20 lbs (9.1 kg) with 2 power supplies • Temperature: Operating temperature: 32 to 104°F (0 to 40°C); Storage temperature: –13 to 158°F (–25 to 70°C) • Humidity: Operating humidity: 10 95%, noncondensing. Storage humidity: up to 95% • Input power: 100 to 240 VAC; 50/60 Hz; 1.05 A at 110 VAC, 115 W Maximum; 0.523 A at 220 VAC, 115 W Maximum; Test Conditions: Redundant Power Supplies, 40C, Full Traffic. • Heat Dissipation: 392 BTU/hour at 110/220 VAC Maximum
Regulatory Compliance	CE Mark Safety: • UL 60950-1:2003 • EN 60950:2000 • EMI and susceptibility (Class A): • U.S.: FCC Part 15.107 and 15.109 • Canada: ICES-003 • Japan: VCCI • Europe: EN 55022, EN 55024

Tables 3 and Table 4 list the ordering and accessories information for Cisco 5500 Series Wireless Controllers.

Table 3. Ordering Information for Cisco 5500 Series Wireless Controllers

Part Number	Product Name	Cisco SMARTnet® Service 8x5xNBD
AIR-CT5508-12-K9	5500 Series Wireless Controller for up to 12 Cisco access points	CON-SNT-CT0812
AIR-CT5508-25-K9	5500 Series Wireless Controller for up to 25 Cisco access points	CON-SNT-CT0825
AIR-CT5508-50-K9	5500 Series Wireless Controller for up to 50 Cisco access points	CON-SNT-CT0850
AIR-CT5508-100-K9	5500 Series Wireless Controller for up to 100 Cisco access points	CON-SNT-CT08100
AIR-CT5508-250-K9	5500 Series Wireless Controller for up to 250 Cisco access points	CON-SNT-CT08250
AIR-CT5508-500-K9	5500 Series Wireless Controller for up to 500 Cisco access points	CON-SNT-CT08500
AIR-CT5508-500-2PK	2 Pack 5500 Series Wireless Controller for up to 500 Cisco access points each (1000 access points total)	CON-SNT-AIRC552P
AIR-CT5508-HA-K9	Cisco 5508 Series Wireless Controller for High Availability	CON-SNT-CT5508HA

Table 4. Accessories for Cisco 5500 Series Wireless Controllers

Part Number	Product Name
AIR-PWR-5500-AC=	5500 Series Wireless Controller Redundant AC Power Supply
AIR-FAN-5500=	5500 Series Wireless Controller Fan Tray
AIR-CT5500-RK-MNT	5500 Series Wireless Controller Spare mounting kit

Additive Capacity Upgrade Licenses

Tables 5 and 6 list additive capacity upgrade licenses for the Cisco 5500 Series.

Table 5. Ordering Information for Cisco 5500 Series Wireless Controllers Additive Capacity Licenses (e-Delivery Product Authorization Keys [PAKs])

	Part Number	Product Description	Cisco SMARTnet Service 8x5xNBD
e-License	L-LIC-CT5508-UPG	Primary upgrade SKU: Pick any number or combination of the following options under this SKU to upgrade one or many controllers under one product authorization key	CON-SNT-LCTUPG
	L-LIC-CT5508-25A	25 AP Adder License for the 5508 Controller (eDelivery)	CON-SNT-LCT25A
	L-LIC-CT5508-50A	50 AP Adder License for the 5508 Controller (eDelivery)	CON-SNT-LCT50A
	L-LIC-CT5508-100A	100 AP Adder License for the 5508 Controller (eDelivery)	CON-SNT-LCT100A
	L-LIC-CT5508-250A	250 AP Adder License for the 5508 Controller (eDelivery)	CON-SNT-LCT250A

Table 6. Ordering Information for Cisco 5500 Series Wireless Controllers Additive Capacity Licenses (Paper PAKs)

	Part Number	Product Description	Cisco SMARTnet Service 8x5xNBD
Paper License	LIC-CT5508-UPG	Primary upgrade SKU: Pick any number or combination of the following options under this SKU, to upgrade one or many controllers under one product authorization key.	CON-SNT-LCTUPG
	LIC-CT5508-25A	25 AP Adder License for the 5508 Controller	CON-SNT-LCT25A
	LIC-CT5508-50A	50 AP Adder License for the 5508 Controller	CON-SNT-LCT50A
	LIC-CT5508-100A	100 AP Adder License for the 5508 Controller	CON-SNT-LCT100A
	LIC-CT5508-250A	250 AP Adder License for the 5508 Controller	CON-SNT-LCT250A

The additive capacity licenses allow for the increase in access point capacity supported by the controller up to a maximum of 500 access points. As an example, if a controller was initially ordered with the 250 access point support, that capacity could be later increased to up to 500 access points by purchasing a 250 access point additive capacity license (1x-LIC-CT5508-250A).

A certificate with a PAK is required to add additional access point capacity on the Cisco 5500 Series Wireless Controller.

The certificate may be expedited via email. If a paper certificate is required for customs, it should be ordered to ship via U.S. mail. Each additive capacity license and PAK must be registered prior to installation.

Ordering and installing the Cisco 5500 Series Wireless Controller additive capacity licenses is a three-step process:

1. Select the correct SKU for email or paper delivery.
2. Register the PAK certificate (see Registering PAK Certificate).
3. Install the license on the Cisco 5500 Series Wireless Controller (see Installing License).

Please review the Cisco Wireless LAN Controller Configuration Guide, Release 6.0, for detailed ordering, registration, and installation information for the 5500 Series additive capacity licenses.

Electronic delivery of the same PAKs is available by ordering the e-License SKUs as listed in Table 4. If a paper certificate is required, please use the SKUs listed in Table 5.

PAK Certificate Registration

Customers are required to register a PAK certificate for all upgrade licenses for the Cisco 5500 Series Wireless Controllers. Customer email address and host name are required to register the PAK certificate at: http://www.cisco.com/go/license.

Installing License on Cisco WCS Server

Follow these steps to install a license file. If you need additional help, contact Cisco Technical Assistance Center (TAC) at 800 553-2447 or tac@cisco.com.

1. Install Cisco WCS software if not already completed.
2. Save the license file (.lic) to a temporary directory on your hard drive. (You will receive an email from Cisco with an attached license file.)
3. Open a supported version of the Internet Explorer browser.
4. In the location or address field, enter the following URL, replacing IP address with the IP address or host name of the Cisco WCS server: **https: // <IP address>**.
5. Log in to the Cisco WCS server as system administrator. (Be aware that usernames and passwords are case-sensitive.)
6. From the Help menu, select **Licensing**.
7. On the Licensing page, from the Command menu, select **Add License**.
8. On the Add License page, click **Browse** to navigate to the location where you saved the .lic file.
9. Click **Download**. The Cisco WCS server imports the license.

Table 7 shows the optional DTLS license for Cisco 5500 Series Wireless Controllers.

Datagram Transport Layer Security (DTLS) is required for all OfficeExtend deployments to encrypt the Data Plane traffic. **Customers planning to install this device physically in Russia must order the controller with DTLS disabled and then obtain a physical PAK in order to enable a DTLS license and should not download the license from Cisco.com.** Please consult your local government regulations to ensure that Data DTLS encryption is permitted.

If a customer chooses SWC5500K9-60, SWC5500K9-70 or SWC5500K9-72, DTLS Data Encryption is enabled by default. When a customer orders the 5500 and chooses either SWC5500LPE-K9-70 or SWC5500LPE-K9-72 in the Optional Licenses TAB, data DTLS Encryption is disabled.

The DTLS Paper PAK license is designated for customers who purchase a controller with DTLS disabled due to import restrictions but get permission to add DTLS support after initial purchase. This optional DTLS license is required for Cisco OfficeExtend deployment.

Table 7. Optional Licensing for Cisco 5500 Series Wireless Controllers (PAKs)

Part Number	Description
LIC-CT5508-LPE-K9	5508 Wireless Controller DTLS License (Paper PAK)
L-LIC-CT5508-LPE-K9	Cisco 5508 Controller DTLS License (electronic Certificate – must not be ordered by Russian Customers)

Other customers can simply use the procedure outlined below in order to download the DTLS license from CCO.

To Obtain a Data DTLS License:

Step 1. Browse to http://cisco.com/go/license

Step 2. On the Product License Registration page, choose **Licenses Not Requiring a PAK**.

Step 3. Choose **Cisco Wireless Controllers DTLS License** under Wireless.

Step 4. Complete the remaining steps to generate the license file. The license will be provided online or via email.

Step 5. Copy the license file to your TFTP server.

Step 6. Install the license by browsing to the WLC Web Administration Page:

Management --> Software Activation –> Commands --> Action: Install License

Step 7. Browse to: Cisco 5508 Wireless Controller Software Download Page

http://www.cisco.com/cisco/software/release.html?mdfid=282600534&release=7.0.230.0&relind=AVAILABLE&softwareid=280926587&rellifecycle=ED&reltype=latest

Step 8. Choose the release that corresponds to the SW running on your WLC

Step 9. Choose the **NON LDPE** software release: AIR-CT5500-K9-X-X-XX.aes

Step 10. Complete the remaining steps to download the software

Service and Support

Realize the full business value of your wireless network and mobility services investments faster with intelligent, customized services from Cisco and our partners. Backed by deep networking expertise and a broad ecosystem of partners, Cisco professional and technical services enable you to successfully plan, build, and run your network as a powerful business platform. Our services can help you successfully deploy the Cisco 6500 Series Wireless Services Module 2 Controller and integrate mobility solutions effectively to lower the total cost of ownership and secure your wireless network.

To learn more about Cisco wireless LAN service offers, visit: http://www.cisco.com/go/wirelesslanservices.

Summary

The Cisco 5500 Series Wireless Controller is designed for 802.11n performance and offers maximum scalability for enterprise and service provider wireless deployments. It simplifies deployment and operation of wireless networks, helping to ensure smooth performance, enhance security, and maximize network availability. The Cisco 5500 Series Wireless Controller manages all the Cisco access points within campus environments and branch locations, eliminating complexity and providing network administrators with visibility and control of their wireless LANs.

For More Information

For more information about Cisco wireless controllers, contact your local account representative or visit: http://www.cisco.com/en/US/products/ps6366/index.html.

For more information about the Cisco Unified Wireless Network framework, visit: http://www.cisco.com/go/unifiedwireless.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-521631-11 08/12

ANEXO 5

HOW TO USE THE BACKUP IMAGE ON WIRELESS LAN CONTROLLERS (WLCS)

How to Use the Backup Image on Wireless LAN Controllers (WLCs)

Document ID: 107530

Contents

Introduction

This document explains how to use the backup image on a Wireless LAN Controller (WLC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of how to configure the WLC and Lightweight Access Point (LAP) for basic operation
- Basic knowledge of Lightweight Access Point Protocol (LWAPP)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 2000 / 2100 / 4400 Series WLC that runs firmware 5.0
- LWAPP−based access points, Series 1230, 1240, 1130, 1250, 1140 and 1500

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Primary and Backup Images on WLCs

The WLC, by default, maintains two images. These images are the primary image and the backup image. The primary image is the active image used by the WLC while the backup image is used as a backup for the active image.

The controller bootloader (ppcboot) stores a copy of the active primary image and the backup image. If the primary image becomes corrupted, you can use the bootloader to boot with the backup image.

You can change the active image in two ways.

Assuming that the WLC has a valid backup image, reboot the controller. During the boot process on the WLC, press the **Esc** key in order to see the additional options.

This output shows an example:

```
Initializing memory.  Please wait.  256 MB SDRAM detected
BIOS Version: SM 02.00
BIOS Build date: 09/17/02
System Now Booting ...

Booting from disk..., please wait.

Cisco Bootloader Loading stage2...

    Cisco Bootloader (Version 3.2.116.21)


                     .o88b. d888888b .d8888.  .o88b.  .d88b.
                    d8P  Y8   `88'   88'  YP d8P  Y8 .8P  Y8.
                    8P         88    `8bo.   8P      88    88
                    8b         88      `Y8b. 8b      88    88
                    Y8b  d8   .88.   db   8D Y8b  d8 `8b  d8'
                     `Y88P' Y888888P `8888Y'  `Y88P'  `Y88P'


Booting Primary Image...
Press <ESC> now for additional boot options...

    Boot Options

Please choose an option from below:

 1. Run primary image (Version 3.2.116.21) (active)
 2. Run backup image  (Version 3.2.116.21)
 3. Manually upgrade primary image
 4. Change active boot image
 5. Clear Configuration
```

Choose Option 4: **Change Active Boot Image** from the boot menu to set the backup image as the active boot image. Now, when the controller resets, it boots with the new active image.

You can also change the active booting image of the WLC manually with the **config boot** *<primary/backup>* command.

Syntax Description

config boot	Configure boot option.
{**primary** | **backup**}	Set the primary image or backup image as active.

Each Cisco WLC can boot off the primary, last−loaded OS image or boot off the backup, earlier−loaded OS image. In order to change a Cisco WLC boot option, issue the **config boot** command. By default, the primary image on the controller will be chosen as the active image.

Examples

```
> config boot primary
> config boot backup
```

In order to configure the boot order using the WLC GUI, complete these steps:

1. From the WLC GUI, navigate to the **Commands** page.
2. From the Commands on the left, click **Config Boot**.

   The Config Boot Image page appears.

   This page displays the Primary and Backup images presently available on the controller, and also indicates the Active image.
3. In order to change the Active image, select the desired image from the image drop−down menu and click **Apply**.

   In this example, **Backup** is selected.
4. Save the configuration and reboot.

When the WLC reboots and comes back up, it will boot with the backup image.

When you upgrade the WLC with a new image, the WLC automatically writes the new image as the primary image and the previously existing primary image is written over the backup image.

Note: The previously existing backup image will be lost.

In order to see the active image that your controller is currently running, click on **Monitor** from the WLC GUI and look at the Software Version field under Controller Summary on the controller GUI. From the CLI, you can issue the **show boot** command to view the primary and backup image present on the WLC. Here is an example:

```
(Cisco Controller) >show boot
Primary Boot Image.............................. 4.0.179.8
Backup Boot Image............................... 4.0.206.0 (active)
```

In order to remove or overwrite an image on the WLC, boot up the WLC with the image that you want to keep and perform an upgrade. This way, the new image replaces the primary image.

Related Information

- **Password Recovery Procedure for the Wireless LAN Controller Module (WLCM) and Wireless Services Module (WiSM)**
- **Cisco Wireless LAN Controller Configuration Guide, Release 5.2**
- **Wireless LAN Controller and Lightweight Access Point Basic Configuration Example**
- **Wireless Support Page**
- **Technical Support & Documentation – Cisco Systems**

Updated: Nov 17, 2011 Document ID: 107530

ANEXO 6

INSTALACIÓN DEL SISTEMA OPERATIVO DEBIAN 7.4.0

ROCEDIMIENTO DE INSTALACIÓN DEL SISTEMA OPERATIVO DEBIAN 7.4.0

Descargue la imagen ISO del DVD de Debian 7.4.0 para arquitectura i386 o bien arquitectura amd64 (sólo es necesario el DVD 1 el cual encontrará en el siguiente URL:

- https://www.debian.org/CD/

Inserte el disco DVD de instalación de Debian 7.4.0 (recuerde que para ejecutar el DVD hay que configurar el BIOS) y espere 60 segundos para el inicio automático o bien pulse la tecla “ENTER” para iniciar de manera inmediata o la tecla “TAB” e ingrese a las opciones de instalación deseadas. Seleccionamos “Install” para instalar o actualizar el sistema operativo Linux Debian.

FIGURA 128 Opciones de instalación del sistema operativo
Fuente: Instalación del sistema operativo Debian 7.4.0

Luego de algunos segundos, debe seleccionar el idioma de instalación, que será también el idioma utilizado por el sistema. Para efectos de compatibilidad, se recomienda seleccionar el idioma en inglés (English).

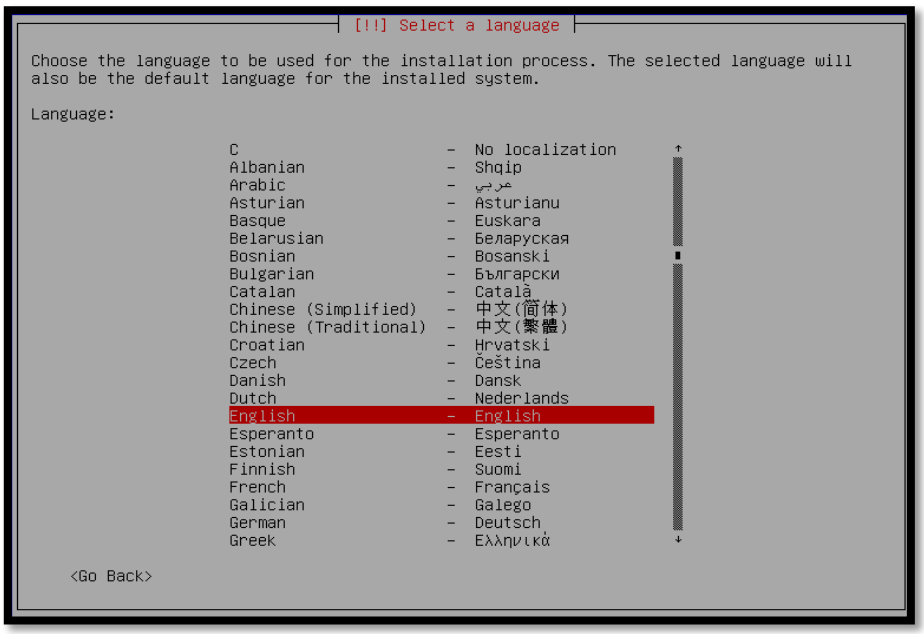


FIGURA 129 Selección del idioma de instalación y del sistema base

Fuente: Instalación del sistema operativo Debian 7.4.0

Después, deberá indicar la localización geográfica del servidor. Basado en el idioma seleccionado, aparecerá una lista con diversos países. Si no encuentra un país, puede seleccionar “other”.

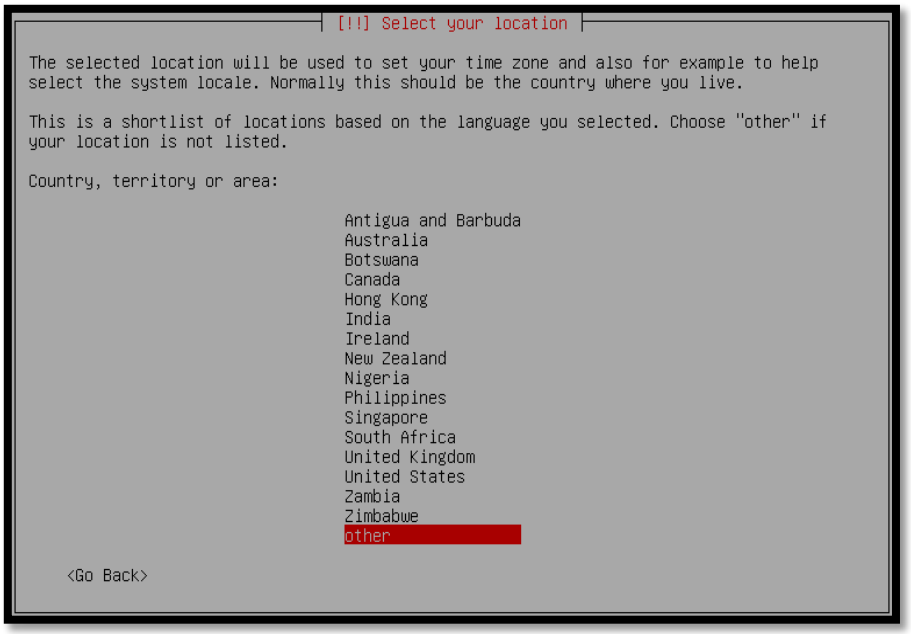


FIGURA 130 Localización geográfica del servidor

Fuente: Instalación del sistema operativo Debian 7.4.0

Si ha seleccionado “other”, después debe indicar la región.

FIGURA 131 Selección del continente o región

Fuente: Instalación del sistema operativo Debian 7.4.0

Después de haber seleccionado la región procedemos a escoger el país.

FIGURA 132 Selección del país de acuerdo a la región escogida

Fuente: Instalación del sistema operativo Debian 7.4.0

En el siguiente paso, vamos a escoger otra vez el idioma Inglés para evitar conflictos de compatibilidad.

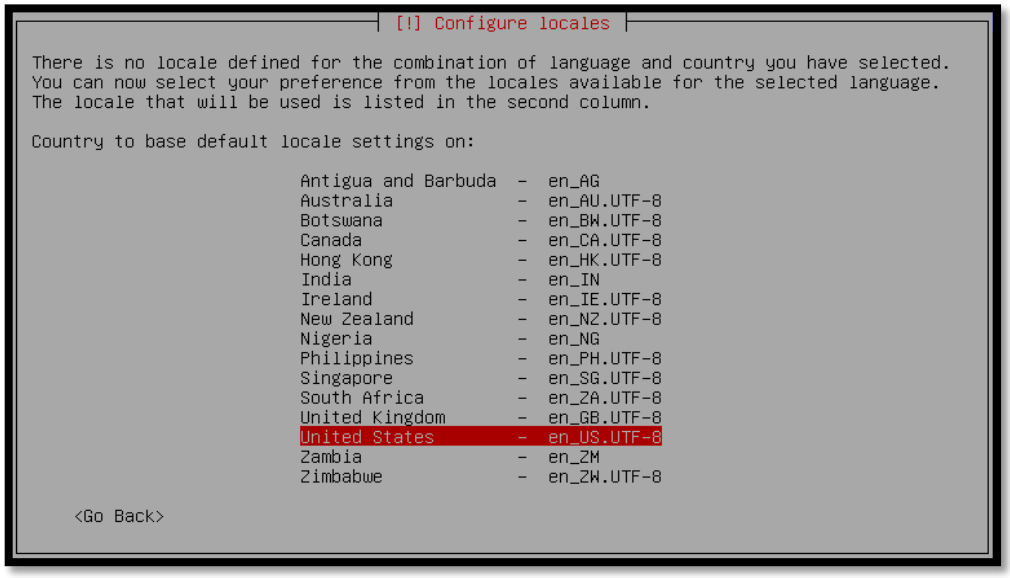


FIGURA 133 Definimos las configure locales

Fuente: Instalación del sistema operativo Debian 7.4.0

Después puede escoger el mapa de teclado. Si usted necesita escribir en español, puede seleccionar “Spanish” o “Latin American”.

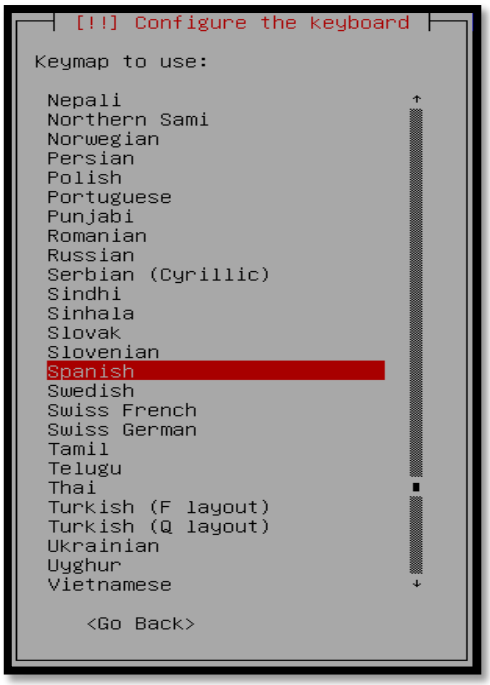


FIGURA 134 Configuración del idioma del teclado

Fuente: Instalación del sistema operativo Debian 7.4.0

Luego el instalador cargará algunos componentes antes de pasar a la configuración de red. Para conectarse a Internet se requiere básicamente la configuración de una dirección IP y de un nombre al sistema. La dirección IP y los demás parámetros de la red pueden obtenerse de forma automática, a partir de un servidor DHCP o configurarse manualmente.

Si el instalador no puede obtener de forma automática la dirección IP o si el proceso se interrumpe, será necesario configurar la conexión a Internet manualmente.

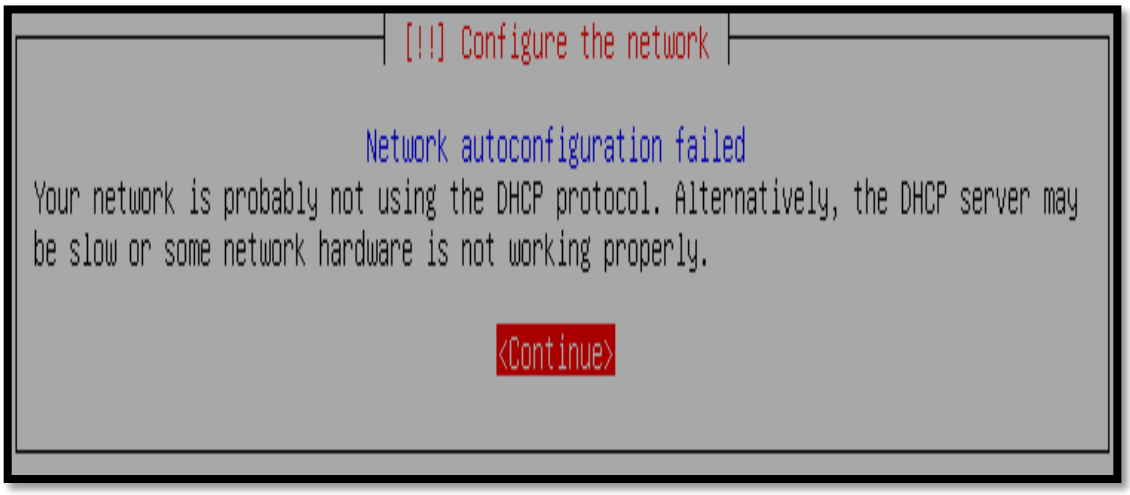


FIGURA 135 Fallo de autoconfiguración de la red

Fuente: Instalación del sistema operativo Debian 7.4.0

En este caso, seleccione la opción de no configurar la red en este tiempo “Do not configure the network at this time”.

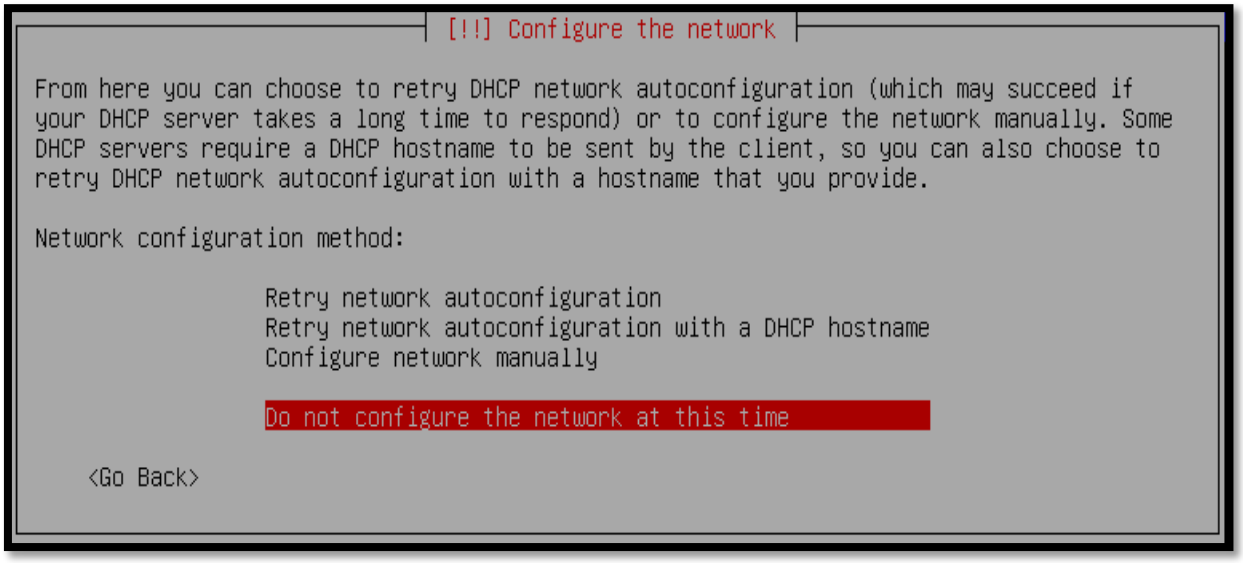


FIGURA 136 Opciones de configuración de la red

Fuente: Instalación del sistema operativo Debian 7.4.0

Indique el nombre por el cual el sistema será reconocido en la red. Tal como la dirección IP, este nombre debe ser único en la red local.

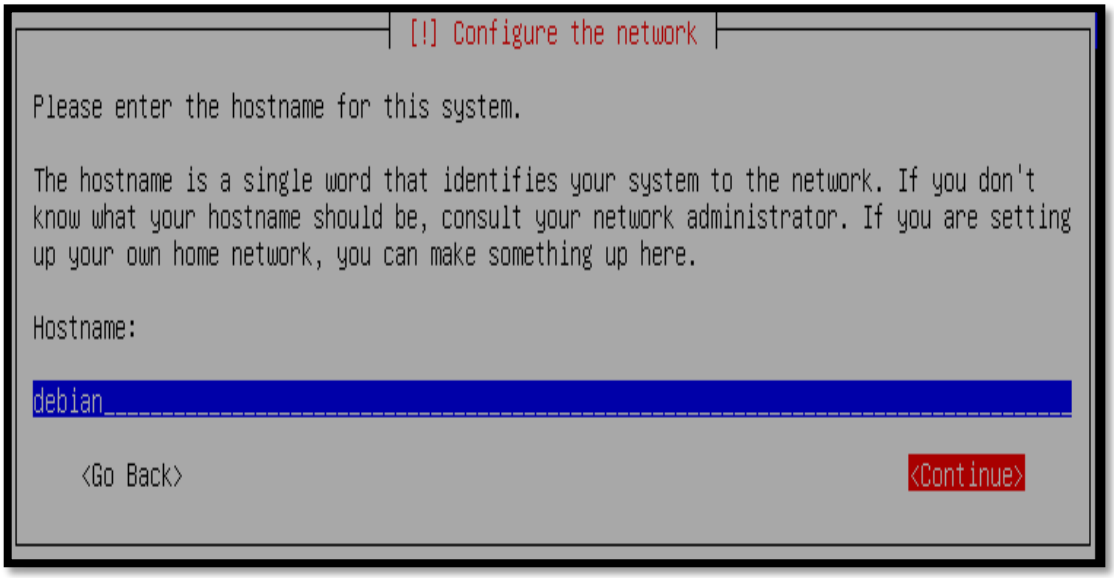


FIGURA 137 Configuración del Hostname del sistema

Fuente: Instalación del sistema operativo Debian 7.4.0

El instalador requiere la configuración de dos cuentas de sistema. La primera es el root que se trata de una cuenta especial con privilegios de administrador y con plenos poderes de acción sobre el sistema. La segunda es la de un usuario normal, con privilegios limitados por seguridad.

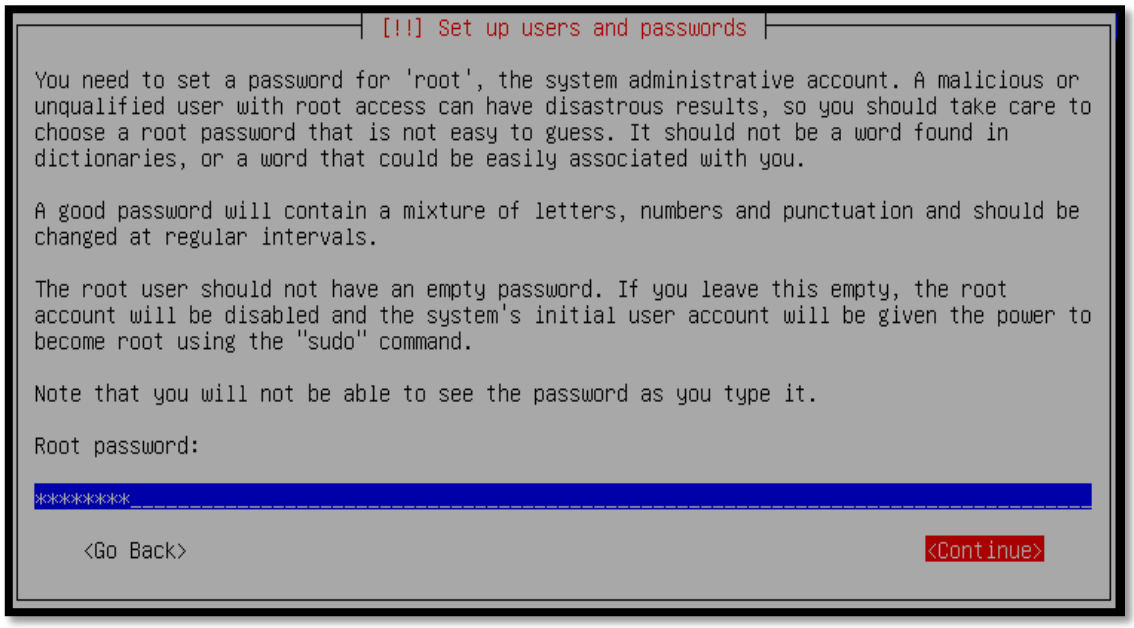


FIGURA 138 Configuración de la contraseña de root

Fuente: Instalación del sistema operativo Debian 7.4.0

Para la cuenta del súper usuario o root se necesita una contraseña o password. Recuerde que el nombre predefinido de esta cuenta es root. También es clave repetir que el root tiene el privilegio de modificar el sistema, por lo tanto, siempre es buena idea escoger una contraseña que sea difícil de adivinar o romper.

A continuación confirmaremos la contraseña de la cuenta de root. Es necesario escribir dos veces la misma contraseña para verificar que no tenga errores.

FIGURA 139 Verificación de la contraseña de root

Fuente: Instalación del sistema operativo Debian 7.4.0

Un usuario normal sin privilegios también debe ser creado. Para completar este paso, debe indicar el nombre completo de este usuario.

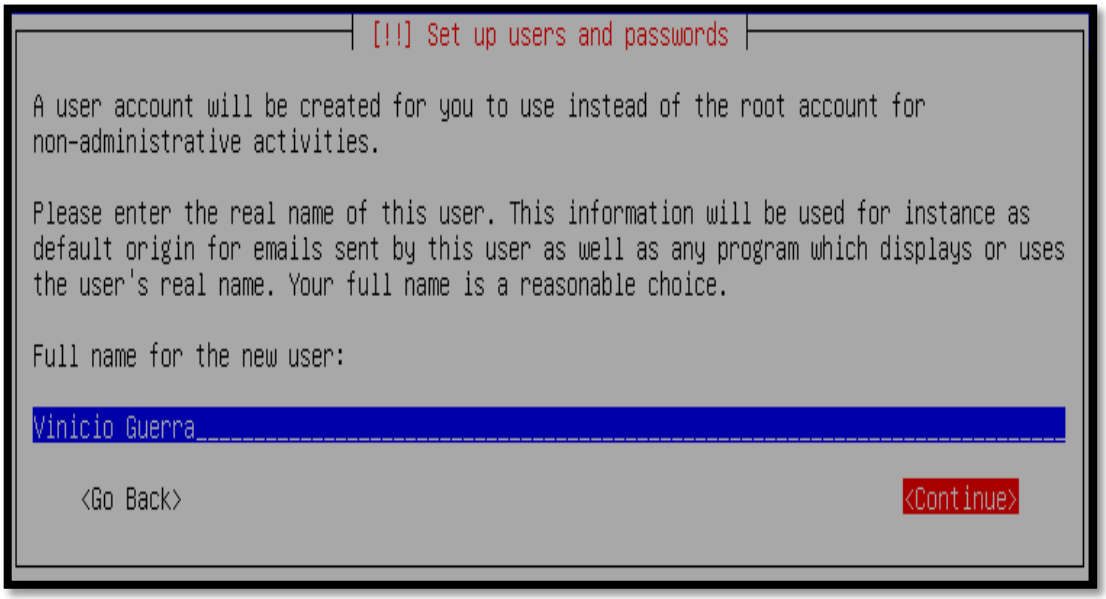


FIGURA 140 Configuración del nombre completo del usuario

Fuente: Instalación del sistema operativo Debian 7.4.0

Luego indicar el login del usuario, el cual se trata del nombre con que se identificará la cuenta del usuario.

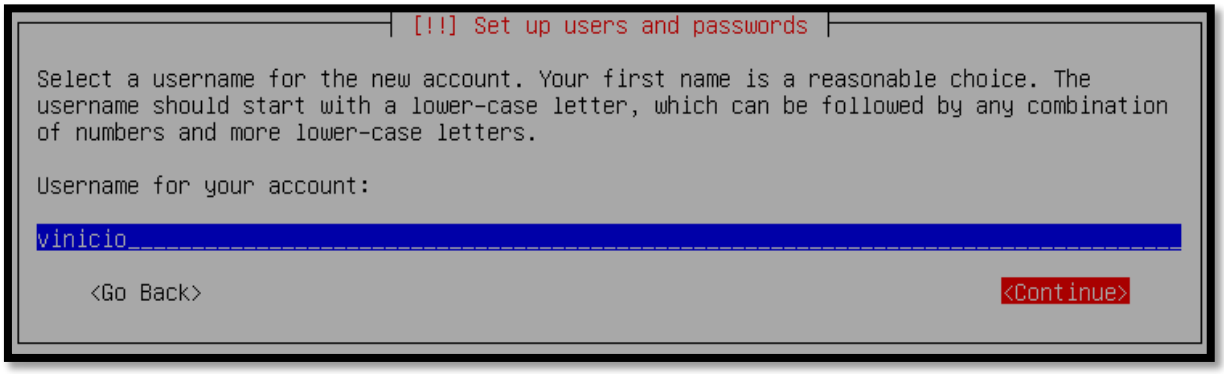


FIGURA 141 Configuración de la cuenta de usuario

Fuente: Instalación del sistema operativo Debian 7.4.0

Una vez creado el usuario debemos escoger una contraseña.

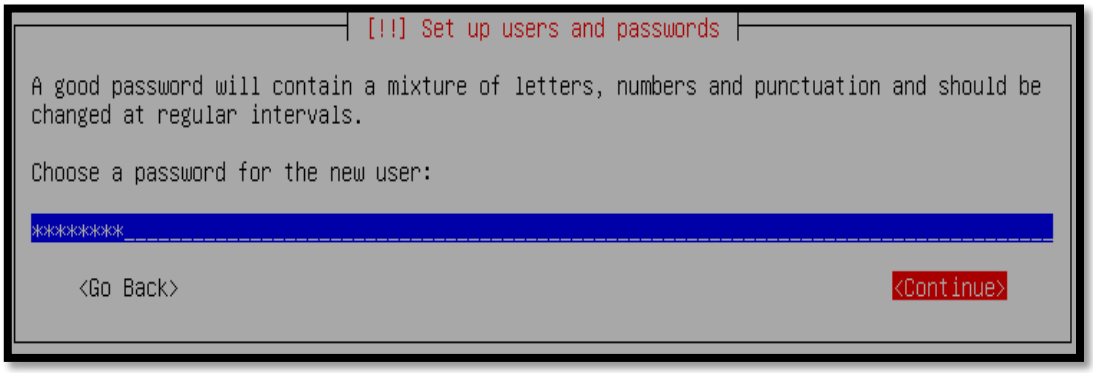


FIGURA 142 Configuración de la contraseña del usuario

Fuente: Instalación del sistema operativo Debian 7.4.0

Ingresamos nuevamente la contraseña para verificar que no tenga errores.

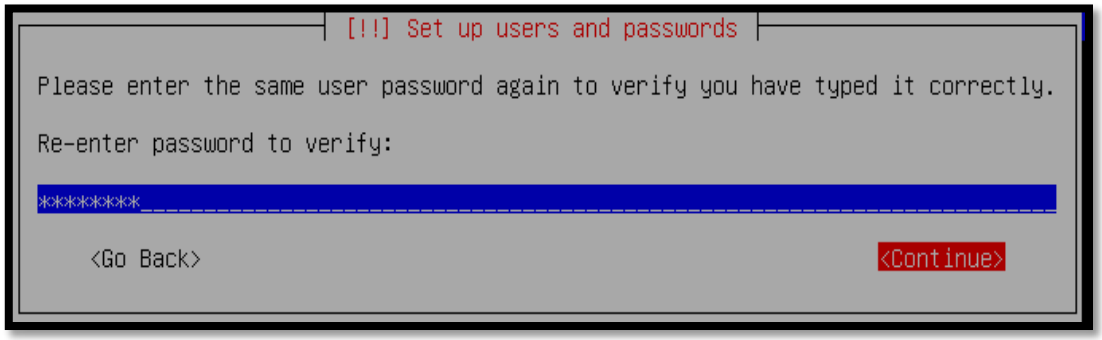


Figura 143 Verificación de la contraseña del usuario

Fuente: Instalación del sistema operativo Debian 7.4.0

Para seleccionar de manera adecuada el reloj del sistema, aparecerá una lista con husos horarios o zonas de tiempo válido para el país que se escogió previamente.

FIGURA 144 Configuración de la zona de tiempo

Fuente: Instalación del sistema operativo Debian 7.4.0

El particionamiento consiste en organizar el disco en varias áreas o particiones, cada una con un objetivo o un tipo de archivos específicos. El instalador Debian ofrece diversas opciones y estrategias de particionamiento del disco duro.

En este caso optamos por dividir el disco en tres partes, una para la instalación del sistema (“/” o “root”), otra para almacenar los datos (“/home”) y una tercera partición de memoria virtual (“swap”) también será creada.

La opción “Particionamiento manual” nos permite crear de una manera sencilla y rápida las particiones de acuerdo a nuestros requerimientos.

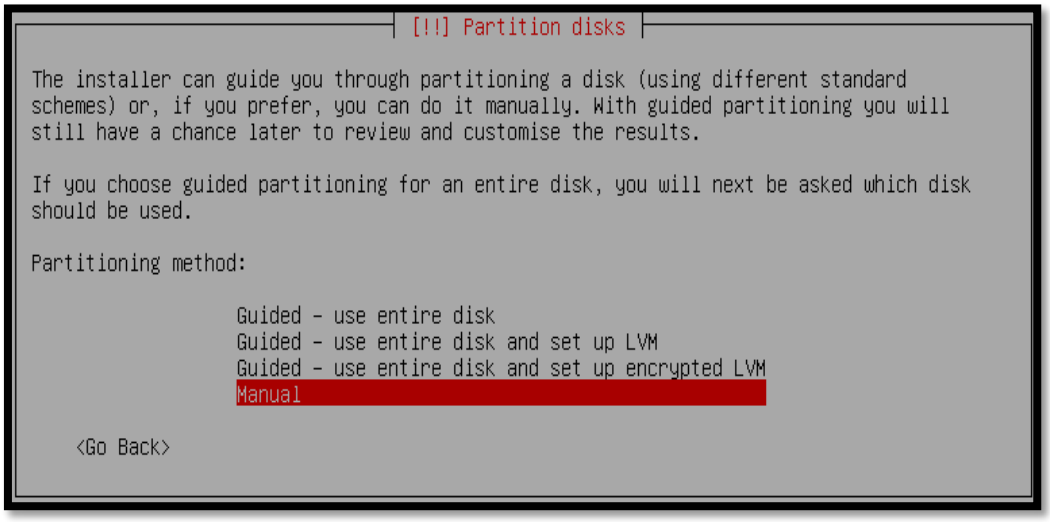


FIGURA 145 Elección del método de Particionamiento Manual

Fuente: Instalación del sistema operativo Debian 7.4.0

En este paso, debe escoger el disco donde se crearán las particiones. En Linux, los discos con interfaz SCSI o SATA son nombrados sda, sdb, etc., mientras que los discos con interfaz IDE o PATA son nombrados como hda, hdb, etc.

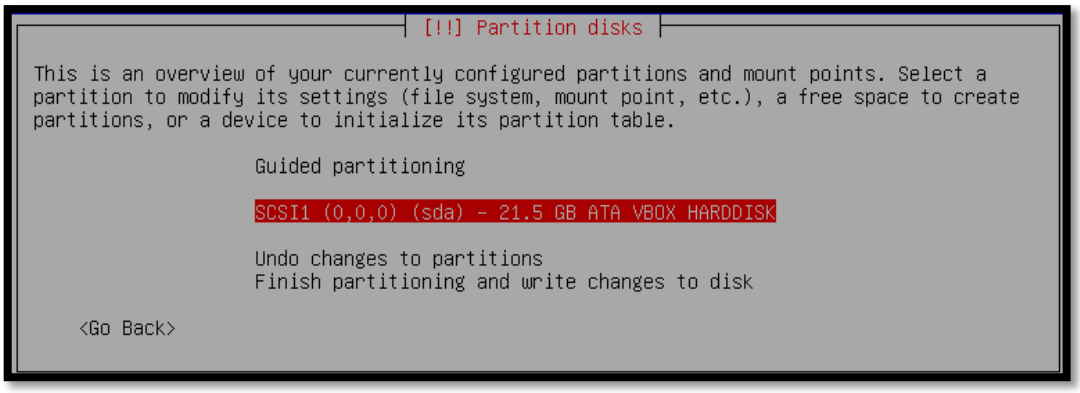


FIGURA 146 Selección del disco a particionar

Fuente: Instalación del sistema operativo Debian 7.4.0

Confirmación de que deseamos crear una tabla de particiones en este dispositivo.

Figura 147 Pregunta de confirmación para crear una nueva partición

Fuente: Instalación del sistema operativo Debian 7.4.0

Se selecciona el espacio libre de la primera partición que se va a modificar con las opciones de formato del sistema de archivos y el punto de montaje.

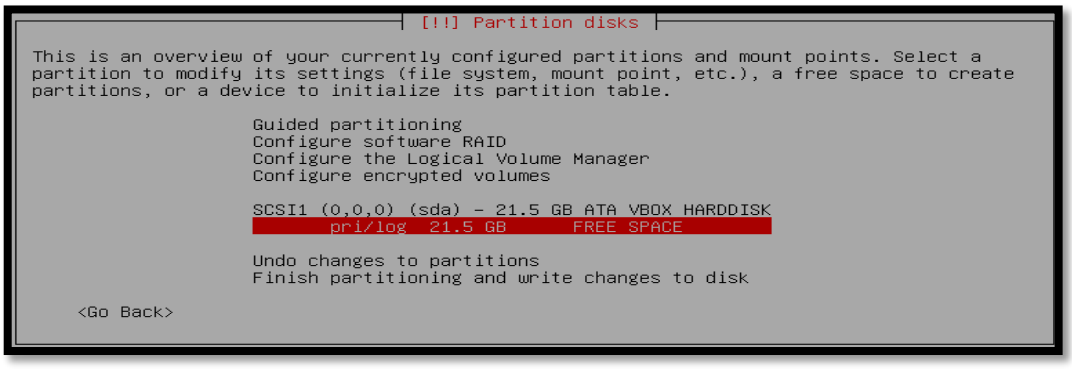


FIGURA 148 Selección del espacio libre de la primera partición a modificar

Fuente: Instalación del sistema operativo Debian 7.4.0

De qué manera utilizaremos el espacio libre de la nueva partición.

FIGURA 149 Pregunta de cómo utilizaremos el espacio libre

Fuente: Instalación del sistema operativo Debian 7.4.0

El tamaño máximo de la partición en este caso es de 21.5 GB, por ello se ha considerado asignarle a la primera partición 12 GB.

Figura 150 Tamaño de asignación a la primera partición

Fuente: Instalación del sistema operativo Debian 7.4.0

Selección del tipo de la primera partición.

FIGURA 151 Tipo de la primera partición

Fuente: Instalación del sistema operativo Debian 7.4.0

La ubicación de la primera partición será creada al inicio.

FIGURA 152 Ubicación de la primera partición

Fuente: Instalación del sistema operativo Debian 7.4.0

La primera partición sera utilizada como punto de montaje “/” con sistema de archivos “Ext4”. Para finalizar la creación de la primera partición nos dirigimos a la opción “Done setting up the partition”.

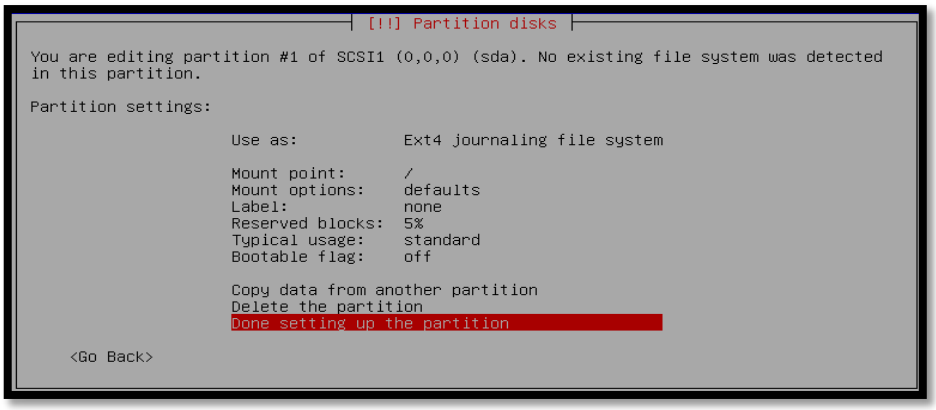


FIGURA 153 Finalización de la primera partición /

Fuente: Instalación del sistema operativo Debian 7.4.0

Se selecciona el espacio libre de la segunda partición que se va a modificar con las opciones de formato del sistema de archivos y el punto de montaje.

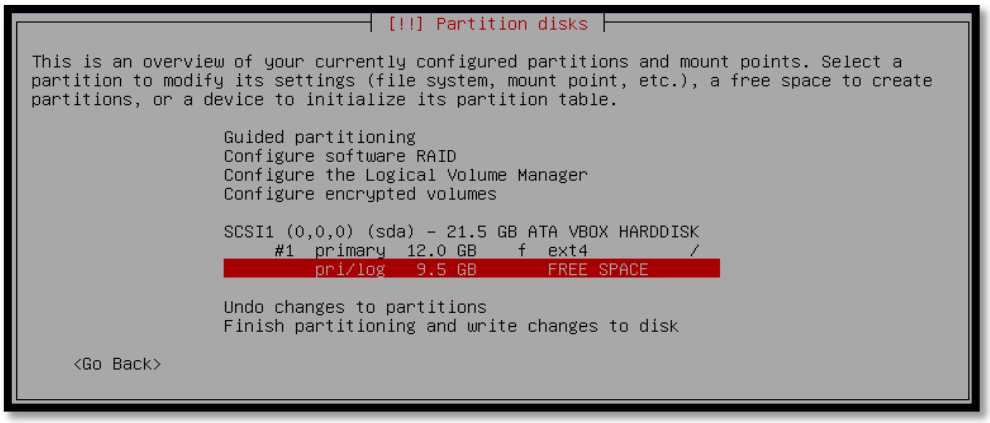


FIGURA 154 Selección del espacio libre de la segunda partición a modificar

Fuente: Instalación del sistema operativo Debian 7.4.0

De qué manera utilizaremos el espacio libre de la nueva partición.

FIGURA 155 Pregunta de cómo utilizaremos el espacio libre

Fuente: Instalación del sistema operativo Debian 7.4.0

El tamaño máximo de la partición en este caso es de 9.5 GB, por ello se ha considerado asignarle a la segunda partición 5.5 GB.

FIGURA 156 Tamaño de asignación a la segunda partición

Fuente: Instalación del sistema operativo Debian 7.4.0

Selección del tipo de la segunda partición.

FIGURA 157 Tipo de la segunda partición

Fuente: Instalación del sistema operativo Debian 7.4.0

La ubicación de la segunda partición será creada al final.

FIGURA 158 Ubicación de la segunda partición

Fuente: Instalación del sistema operativo Debian 7.4.0

La segunda partición sera utilizada como punto de montaje “/home” con sistema de archivos “Ext4”. Para finalizar la creación de la segunda partición nos dirigimos a la opción “Done setting up the partition”.

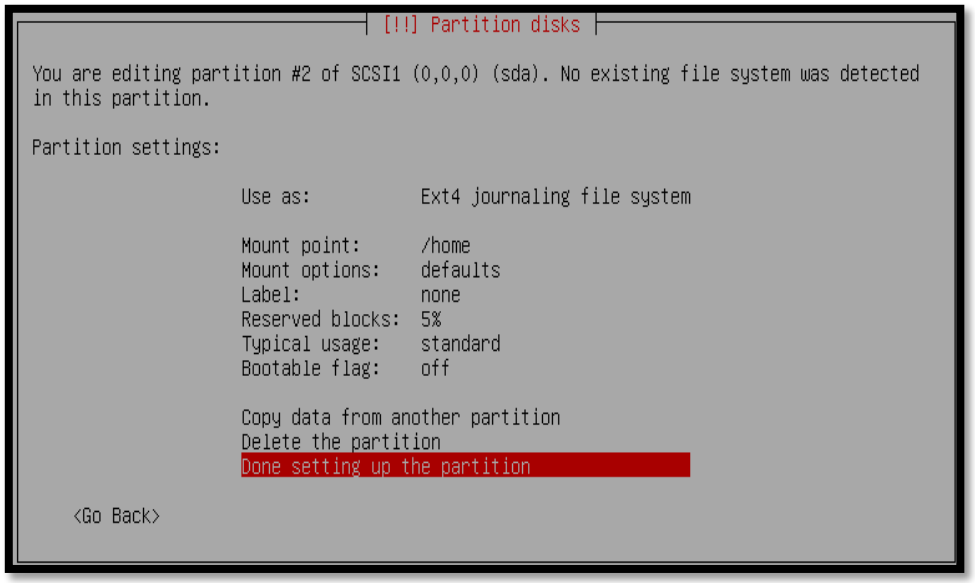


FIGURA 159 Finalización de la segunda partición /home

Fuente: Instalación del sistema operativo Debian 7.4.0

Se selecciona el espacio libre de la tercera partición que se va a modificar con las opciones de formato del sistema de archivos que para esta partición no será necesario y el punto de montaje.

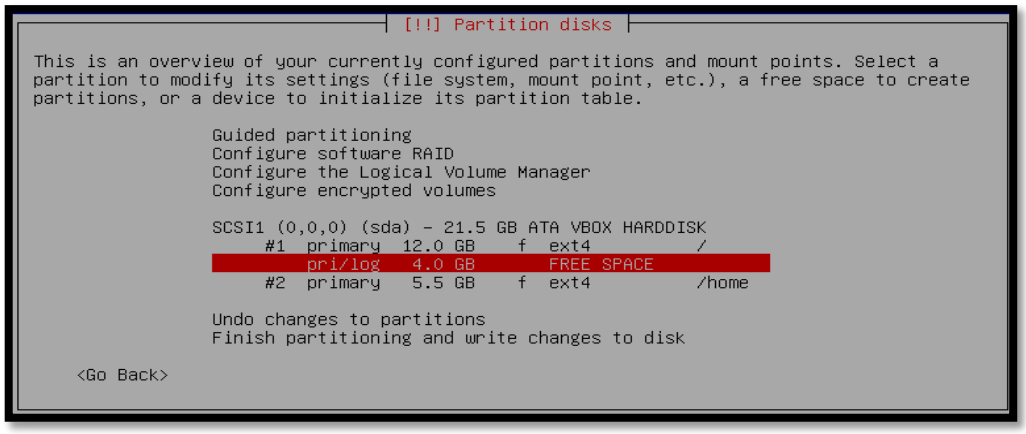


FIGURA 160 Selección del espacio libre de la tercera partición a modificar

Fuente: Instalación del sistema operativo Debian 7.4.0

De qué manera utilizaremos el espacio libre de la nueva partición.

FIGURA 161 Pregunta de cómo utilizaremos el espacio libre

Fuente: Instalación del sistema operativo Debian 7.4.0

El tamaño máximo de la partición en este caso es de 4 GB, por ello se ha considerado asignarle a la tecera partición todo el tamaño restante que sería de 4 GB.

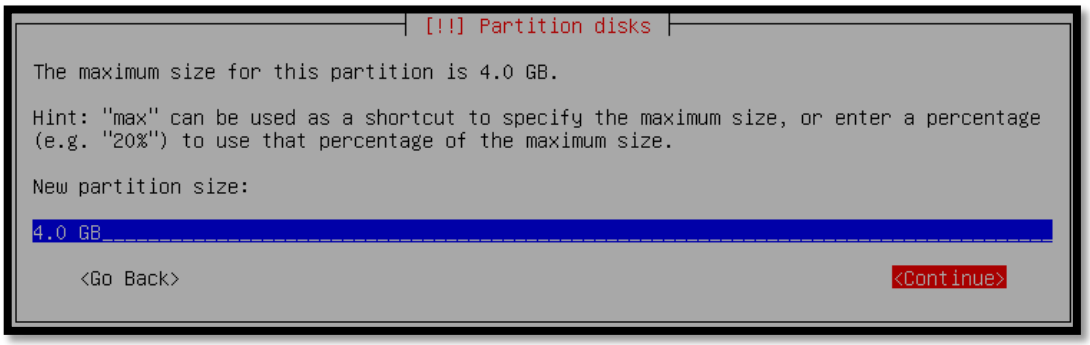


FIGURA 162 Tamaño de asignación a la tercera partición

Fuente: Instalación del sistema operativo Debian 7.4.0

Selección del tipo de la tercera partición.

FIGURA 163 Tipo de la tercera partición

Fuente: Instalación del sistema operativo Debian 7.4.0

La tercera partición será utilizada como área de intercambio o “swap area”. Para finalizar la creación de la tercera y ultima partición nos dirigimos a la opción “Done setting up the partition”.

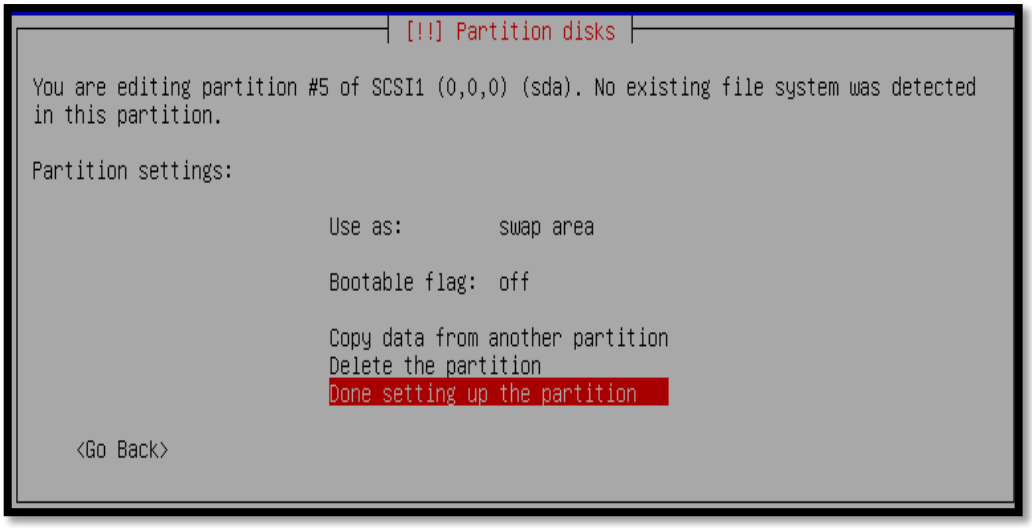


FIGURA 164 Finalización de la tercera partición swap area

Fuente: Instalación del sistema operativo Debian 7.4.0

La siguiente pantalla resume nuestra configuración, donde serán creadas 3 particiones:

PARTICIÓN	CONTENIDO
/ ó root	Aquí se instalarán los archivos del sistema.
swap area	Se trata de la memoria virtual.
/home	Aquí serán almacenados los archivos de los usuarios.

Para finalizar el particionamiento y las configuraciones seleccionamos la opción “Finish partitioning and write changes to disk”.

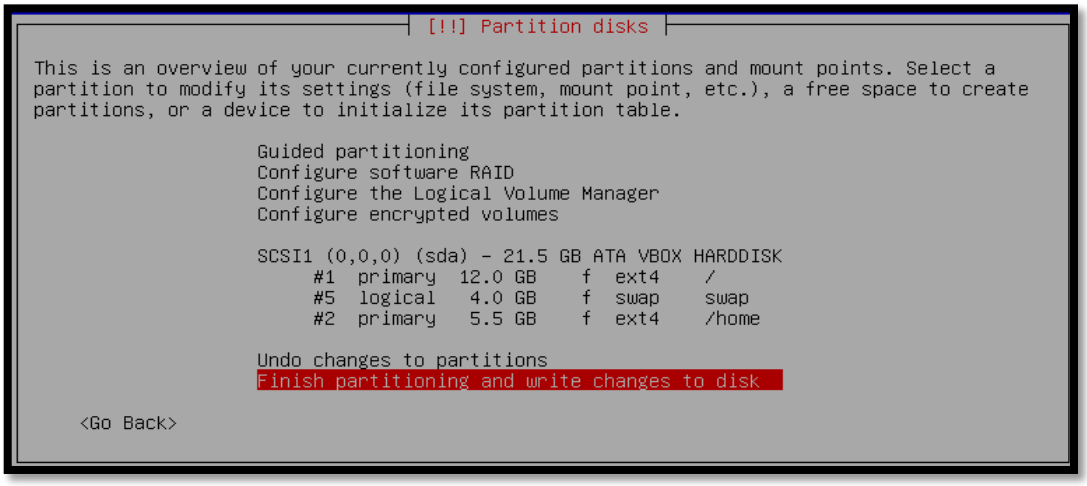


FIGURA 165 Finalización de la tabla de particionamiento del disco

Fuente: Instalación del sistema operativo Debian 7.4.0

Las particiones serán formateadas, por tanto todos los datos existentes en el disco serán eliminados.

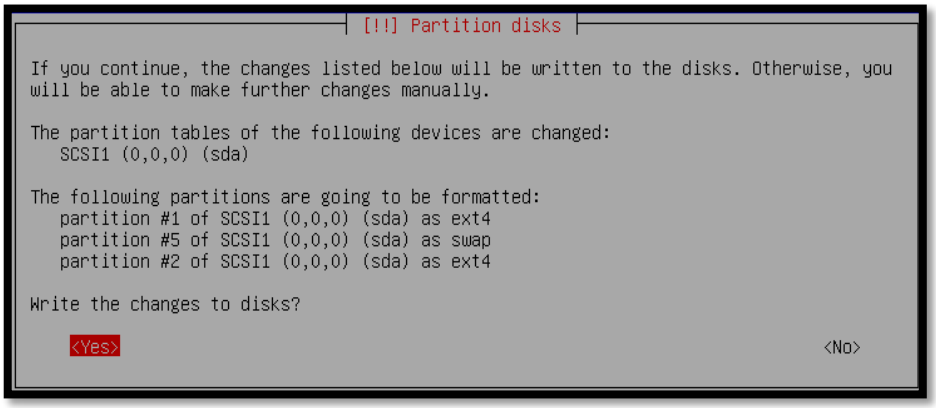


FIGURA 166 Escribir cambios en el disco

Fuente: Instalación del sistema operativo Debian 7.4.0

Formatear las particiones puede requerir un poco de tiempo dependiendo del tamaño del disco y del tipo de hardware.

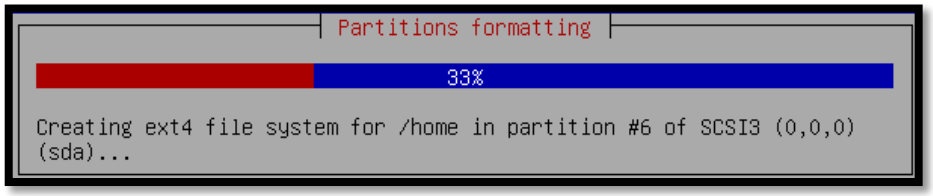


FIGURA 167 Las particiones serán formateadas

Fuente: Instalación del sistema operativo Debian 7.4.0

En este paso, el instalador comenzará la instalación de los paquetes necesarios para crear un sistema base. Este proceso puede demorar algún tiempo.

En la primera fase, serán descargados los paquetes necesarios.

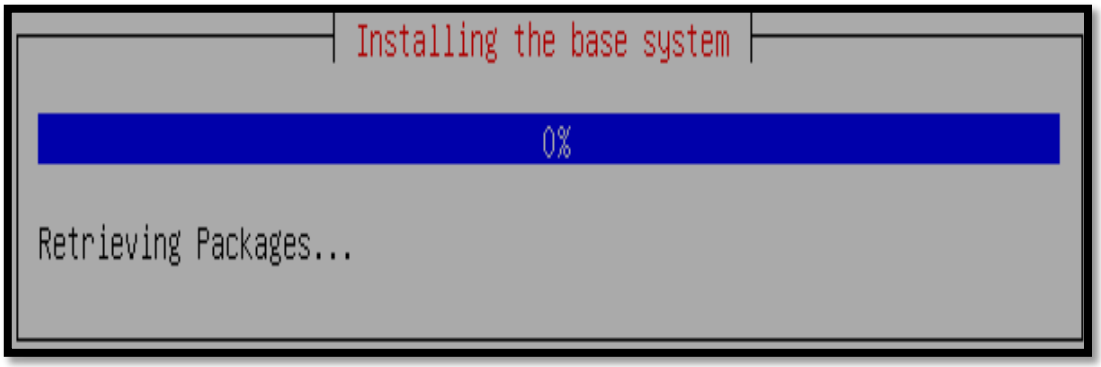


FIGURA 168 Descarga de paquetes del sistema base

Fuente: Instalación del sistema operativo Debian 7.4.0

En la segunda fase, los paquetes del sistema base serán instalados.

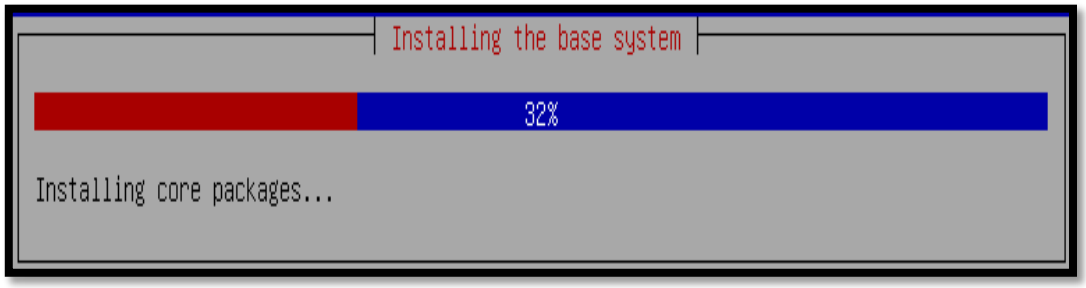


FIGURA 169 Instalación de paquetes del sistema base

Fuente: Instalación del sistema operativo Debian 7.4.0

Finalmente se instalará el kernel de Linux.

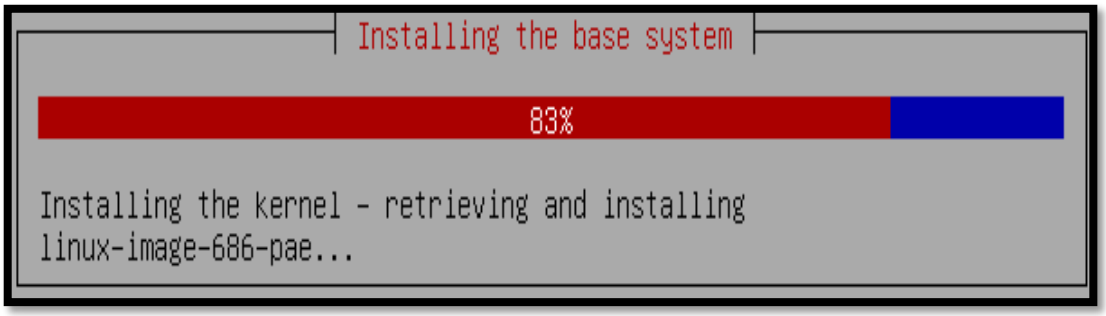


FIGURA 170 Instalación del kernel

Fuente: Instalación del sistema operativo Debian 7.4.0

En el caso que tengamos CDs o DVDs adicionales, en este paso de la instalación deberíamos insertarlos para que relice el sistema un scaneo de los paquetes. Si no desea scanear nada tan solo podemos saltar este paso escogiendo la opción “No”.

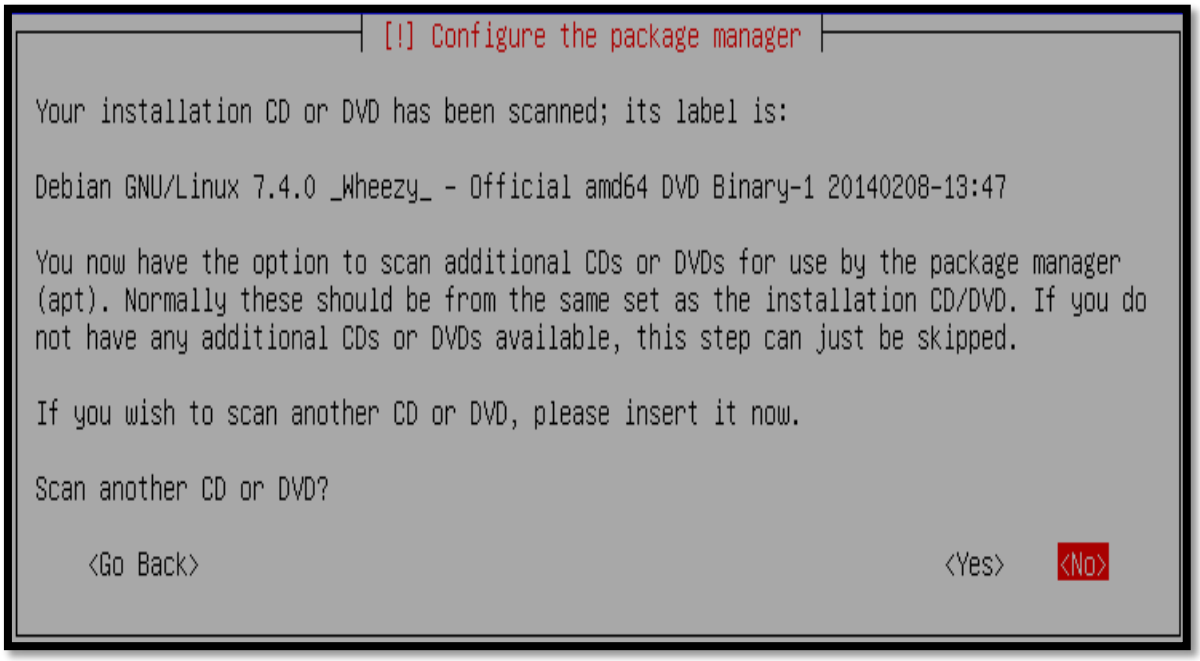


FIGURA 171 Configuración de administrador de paquetes con CDs o DVDs adicionales

Fuente: Instalación del sistema operativo Debian 7.4.0

No queremos utilizar ninguna réplica de red por lo tanto seleccionamos “No”.

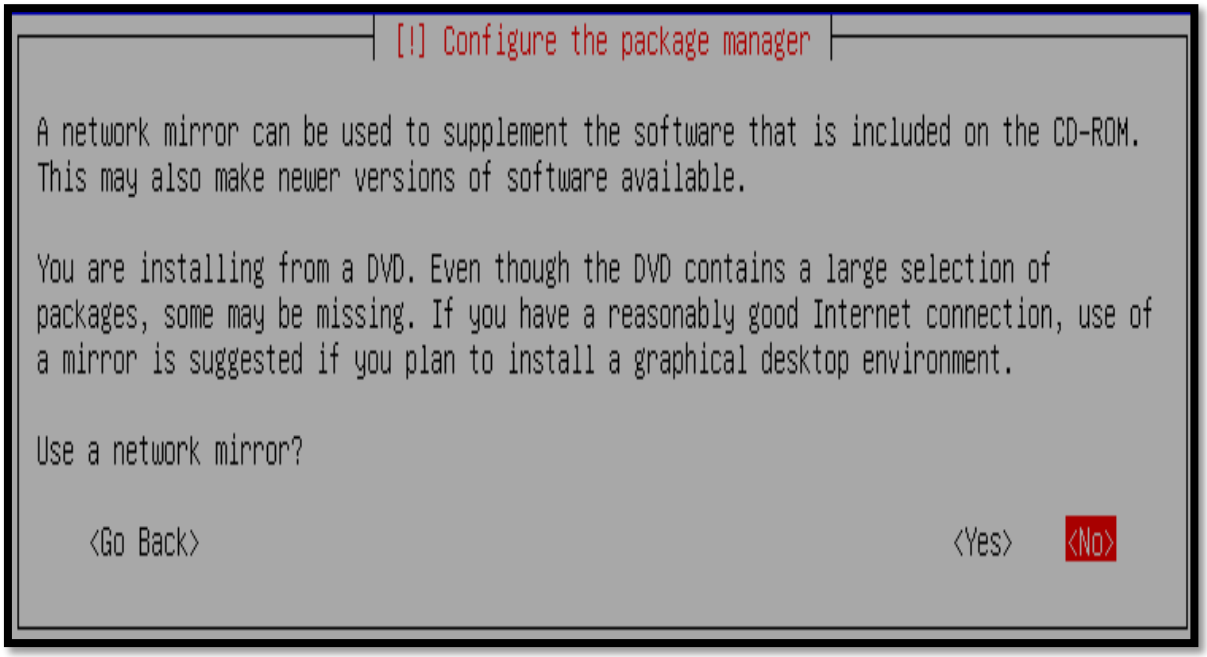


FIGURA 172 Configuración de réplica de red

Fuente: Instalación del sistema operativo Debian 7.4.0

La comunidad *Debian* mantiene un concurso de popularidad interno, con el fin de obtener estadísticas sobre los sistemas instalados. Por lo tanto, la instalación de este paquete depende de la instalación de otros paquetes.

Esta situación no es recomendable por lo que se sugiere seleccionar “No”

:

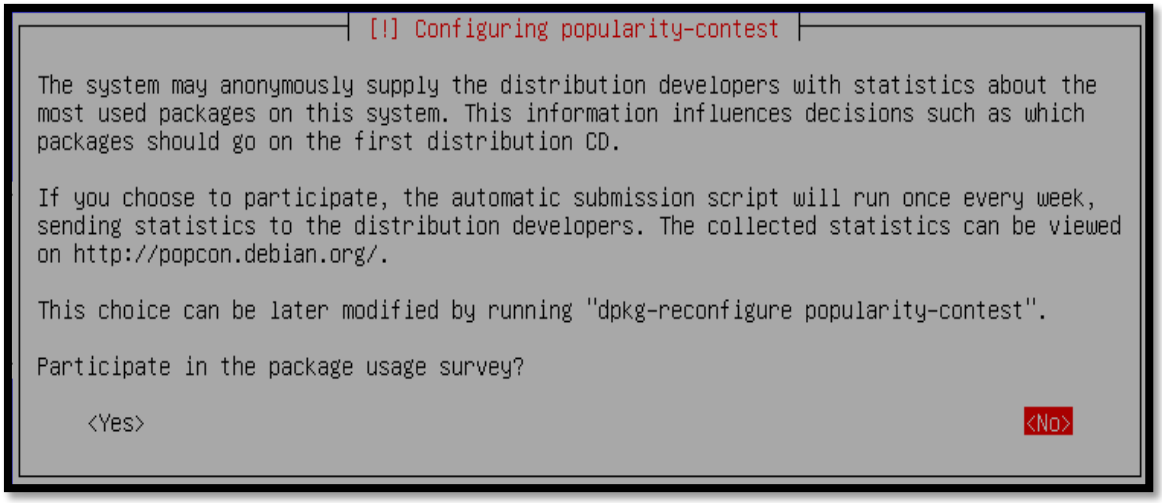


FIGURA 173 Configuración de concurso de popularidad

Fuente: Instalación del sistema operativo Debian 7.4.0

El instalador permite la instalación automática de diversas configuraciones del sistema. Como queremos personalizar totalmente nuestro sistema, escogeremos dos software para instalación existente: “Debian desktop environment” y “SSH server”. Con esto se instalará un sistema con las funcionalidades necesarias.

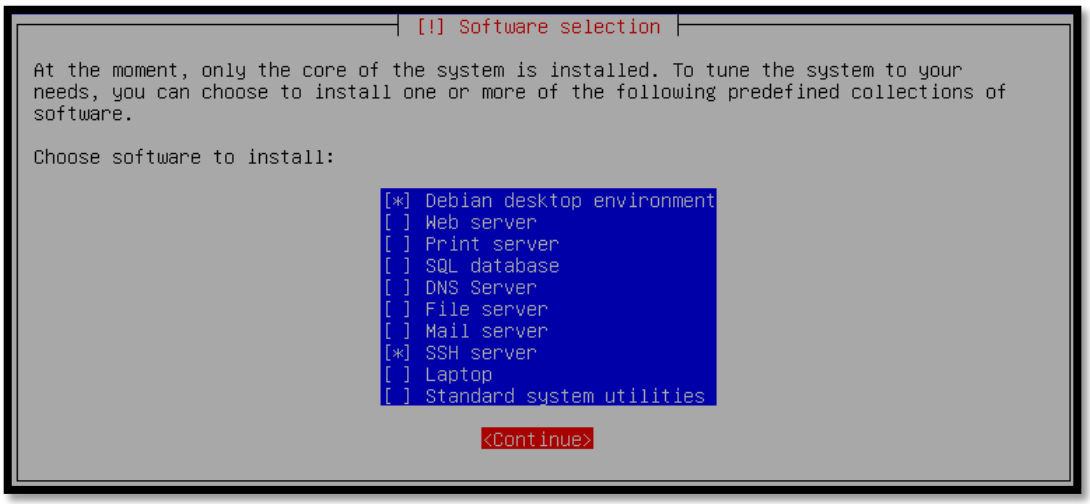


FIGURA 174 Selección del software de instalación

Fuente: Instalación del sistema operativo Debian 7.4.0

Al llegar a este paso, el sistema se encuentra prácticamente instalado. Sin embargo, para que éste pueda arrancar debe instalarse el gestor de arranque *"GRUB"* en el master boot record (mbr) del disco.

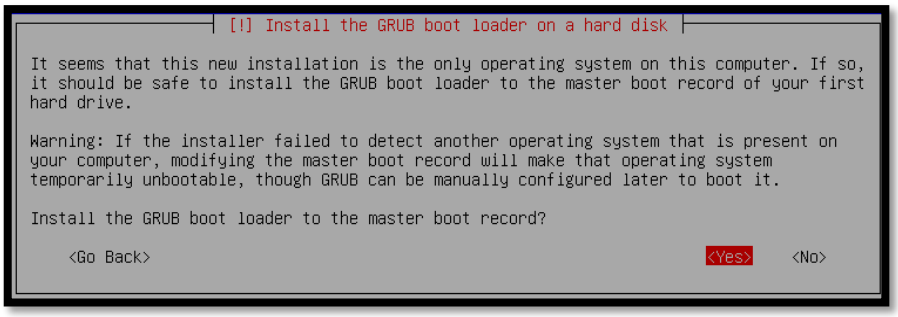


FIGURA 175 Instalación del gestor de arranque GRUB

Fuente: Instalación del sistema operativo Debian 7.4.0

La instalación está terminada. Debe retirar el CD o DVD de instalación de la unidad y seleccionar "Continue". Con esto finaliza la instalación y arranca el nuevo sistema.

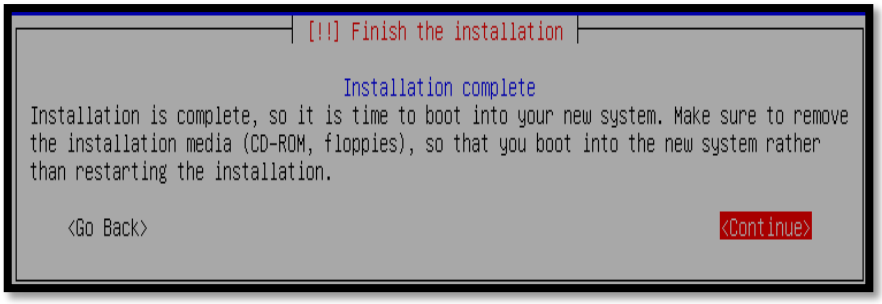


FIGURA 176 Finalización de la instalación

Fuente: Instalación del sistema operativo Debian 7.4.0

Si usted puede ver la siguiente pantalla, esto indica que la instalación terminó muy bien.

FIGURA 177 Arranque del GRUB con el sistema Linux Debian instalado

Fuente: Instalación del sistema operativo Debian 7.4.0

Una vez que hemos iniciado el sistema operativo nos desplegará la siguiente pantalla de login, donde ingresaremos la contraseña del usuario que fue creada en el momento de la instalación.

FIGURA 178 Ingreso de login y password del usuario
Fuente: Instalación del sistema operativo Debian 7.4.0

ANEXO 7

INSTALACIÓN DEL PORTAL CAUTIVO WIFIDOG EN DEBIAN 7.4.0

Wifidog Auth-Server bajo Debian

Comenzamos la instalación abriendo la consola de Linux en la siguiente ubicación Aplicaciones/Accesorios/Terminal. Ingrese su nombre de usuario y contraseña en el GUI[156].

La sesión se iniciará como usuario estándar (permisos de configuración restringidos), así que tenemos que añadir "sudo" frente a cada comando que requiera privilegios de administrador (root), o simplemente pasarnos al modo root con el siguiente comando:

sudo su (luego solicitará usuario y contraseña)

A continuación detallamos los pasos de la instalación:

Actualización de los paquetes del sistema operativo

Antes de instalar cualquier aplicación se debe asegurar tener acceso a Internet y actualizar los repositorios de Debian. El "Software Manager" de Debian es aptitude o apt, el cual permite redactar esta guía de instalación:

```
sudo apt-get update
sudo apt-get upgrade
```

Instalación de apache2 y php5

El servidor de autenticación Wifidog Auth-Server requiere que se instale un servidor WEB y PHP (apache2 y php5), a continuación el comando el cual se muestra en la FIGURA 179.

```
sudo apt-get install apache2 php5
```

[156] **GUI** Graphical User Interface (Interfaz Gráfica de Usuario)

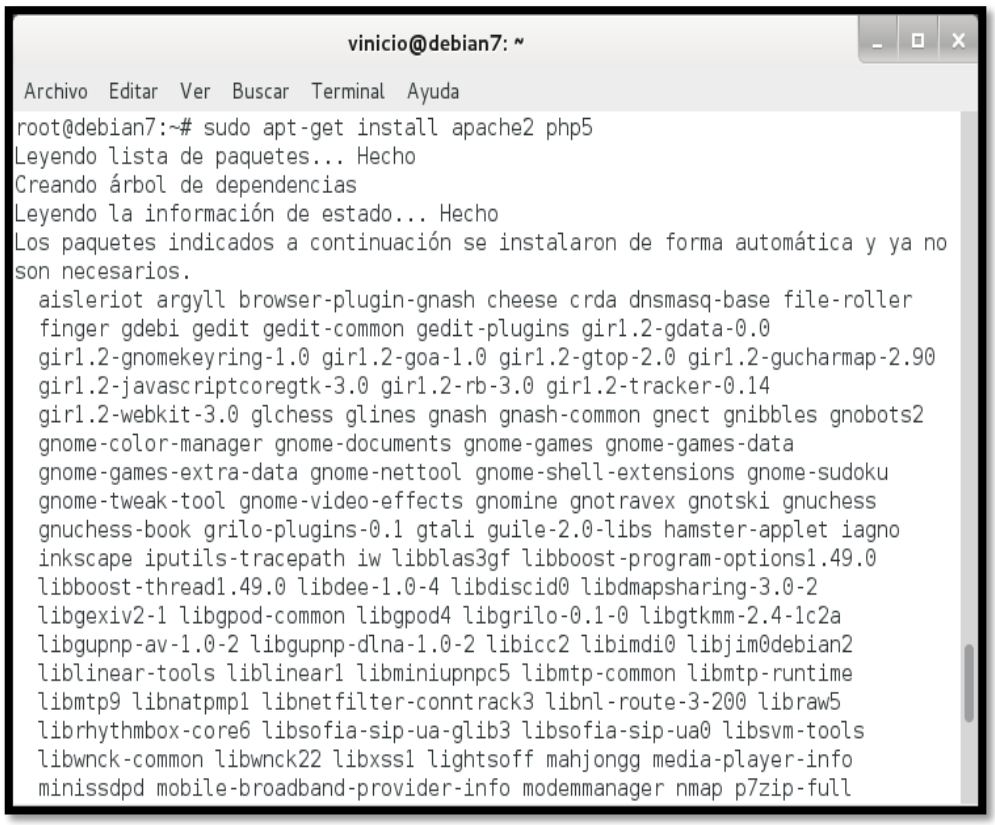


FIGURA 179 Instalación del servidor WEP y PHP

Fuente: Sistema Operativo Debian 7.4.0

Instalación de PostgresSQL

Se necesita de un servidor de Base de Datos, así que instalaremos PostgreSQL. Este ya viene configurado y lo activaremos con los siguientes comandos agregando el repositorio para poder instalar la versión de PostgreSQL 8.4:

Ingresamos al directorio “/etc/apt/sources.list” y añadimos el siguiente repositorio:

deb http://apt.postgresql.org/pub/repos/apt/ wheezy-pgdg main

Ejecutamos estos comandos para la instalación de PostgreSQL (FIGURA 180):

wget --quiet –O - http://apt.postgresql.org/pub/repos/apt/ACCC4CF8.asc | sudo apt-key add –

FIGURA 180 Comando de preinstalación de PostgreSQL

Fuente: Sistema Operativo Debian 7.4.0

sudo apt-get update

sudo apt-get install postgresql-8.4 postgresql-doc-8.4 postgresql-client-8.4 postgresql-client-common postgresql-contrib-8.4

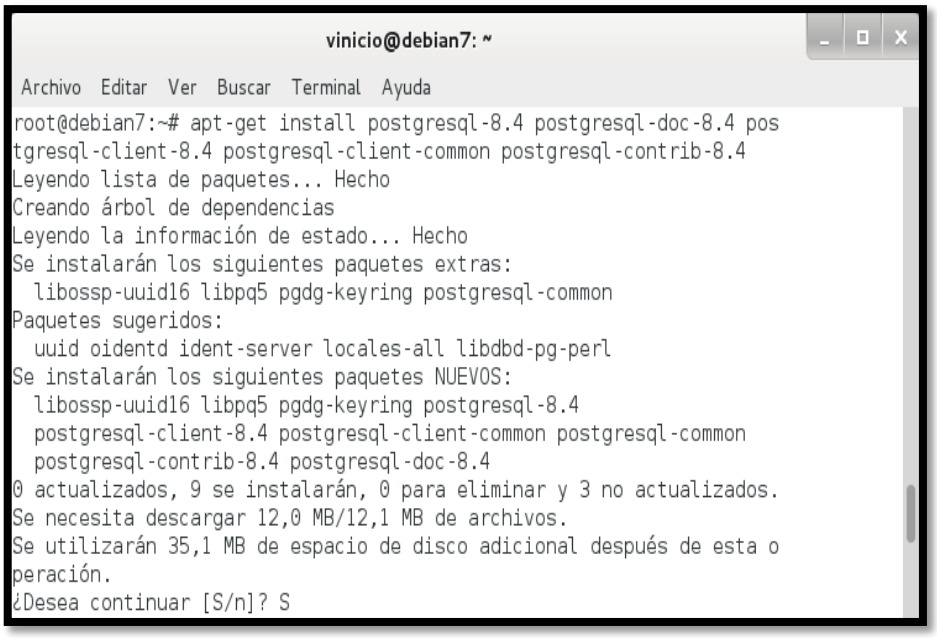


FIGURA 181 Instalación del servidor de Base de Datos PostgreSQL

Fuente: Sistema Operativo Debian 7.4.0

Ahora vamos a editar el siguiente archivo:

nano /etc/postgresql/8.4/main/pg_hba.conf

Y agregaremos una dirección o un rango de direcciones que tendrán acceso al servidor de base de datos desde otros equipos y reemplazaremos el método de autenticación ident por md5.

```
# Database administrative Login by Unix domain socket
local       all             postgres                                md5

# TYPE    DATABASE    USER  CIDR-ADDRESS       METHOD

# “local” is for Unix domain socket connections only
local       all             all                                     ident
# IPv4 local connections:
host        all             all     127.0.0.1/32    md5
host        all             all     0.0.0.0/0               md5  #(Todas las conexiones)
# IPv6 local connections:
host        all             all     ::1/128         md5
```

ó

```
# Database administrative Login by Unix domain socket
local      all             postgres                        md5

# TYPE    DATABASE    USER  CIDR-ADDRESS       METHOD

# “local” is for Unix domain socket connections only
local      all             all                             ident
# IPv4 local connections:
host       all             all       127.0.0.1/32    md5
host       all             all       172.16.1.0/24 md5  #(Rango permitido)
# IPv6 local connections:
host       all             all       ::1/128         md5
```

Si queremos permitir que puedan acceder remotamente al servicio tenemos que realizar una configuración para que el motor atienda las peticiones de todas las interfaces de red del servidor o solo algunas de ellas. Para ello editamos el archivo:

```
nano /etc/postgresql/8.4/main/postgresql.conf
```

En el cual buscamos la directiva (#listen_addresses = ‘localhost’), descomentamos y modificamos su valor dentro del archivo:

```
listen_addresses = ‘*’
```

En el mismo fichero postgresql.conf en la sección “Error Reporting and Logging”, debemos asegurarnos que los mensajes de error o los logs se visualicen donde se pueda ubicarlos.

```
log_destination = ‘syslog’
```

Ahora iniciamos el servicio de postgresql:

```
/etc/init.d/postgresql start
```

Instalación de Librerías Importantes

También necesitaremos algunas librerías específicas (FIGURA 182 y FIGURA 183): sudo apt-get install xml-core gettext libapache2-mod-php5 php5-cgi

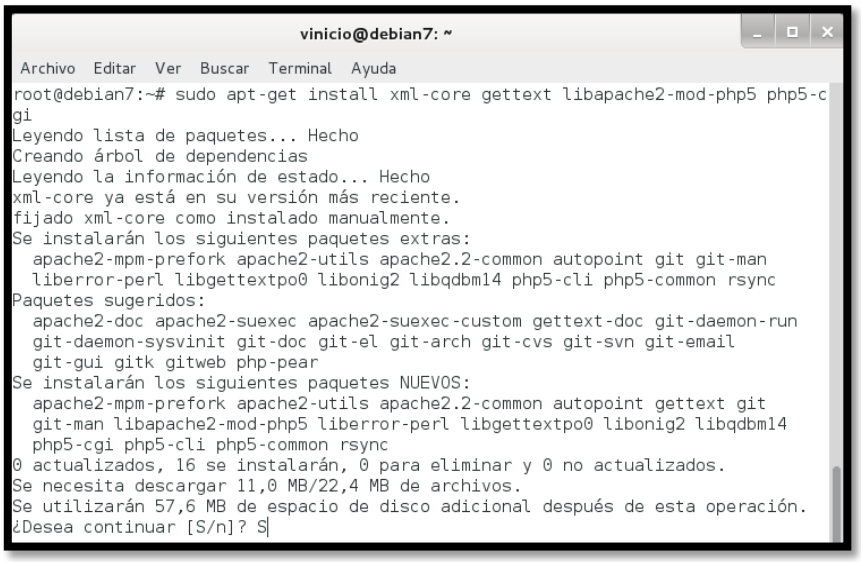


FIGURA 182 Instalación de Librerías

Fuente: Sistema Operativo Debian 7.4.0

sudo apt-get install php5-mcrypt php5-mhash php5-pgsql php-pear php5-xmlrpc php5-curl php5-gd

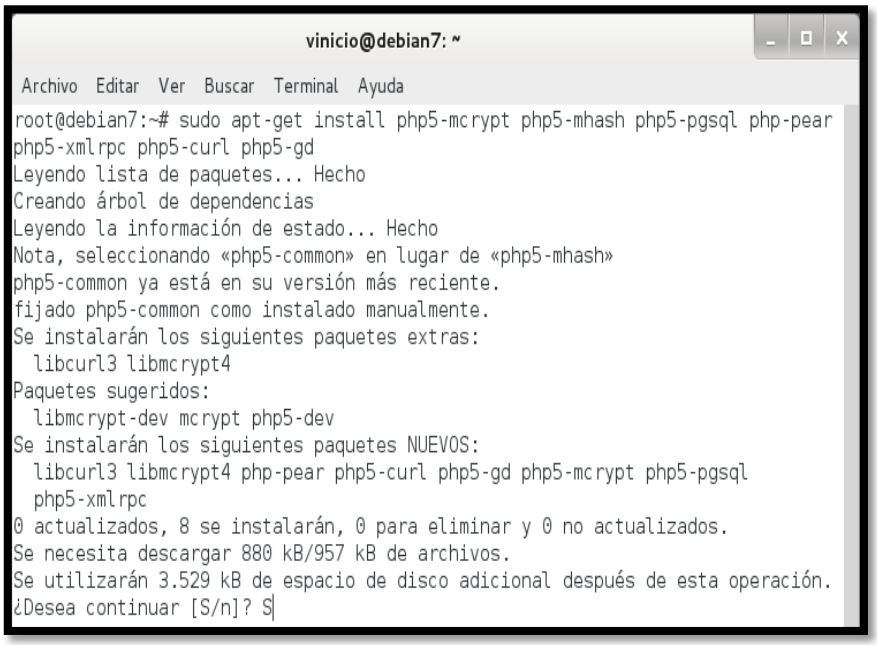


FIGURA 183 Instalación de Librerías

Fuente: Sistema Operativo Debian 7.4.0

Instalación del soporte de Idiomas

Si se desea soporte multi idiomas (multi-locales), se tendrá que instalar el siguiente paquete o configurar cada uno de ellos FIGURA 184.

sudo apt-get install locales-all

ó

sudo dpkg-reconfigure locales

FIGURA 184 Instalación de locales-all

Fuente: Sistema Operativo Debian 7.4.0

Instalación de Subversion

Para obtener la última versión de Wifidog-auth vamos a necesitar el paquete de subversion (FIGURA 185):

sudo apt-get install subversion

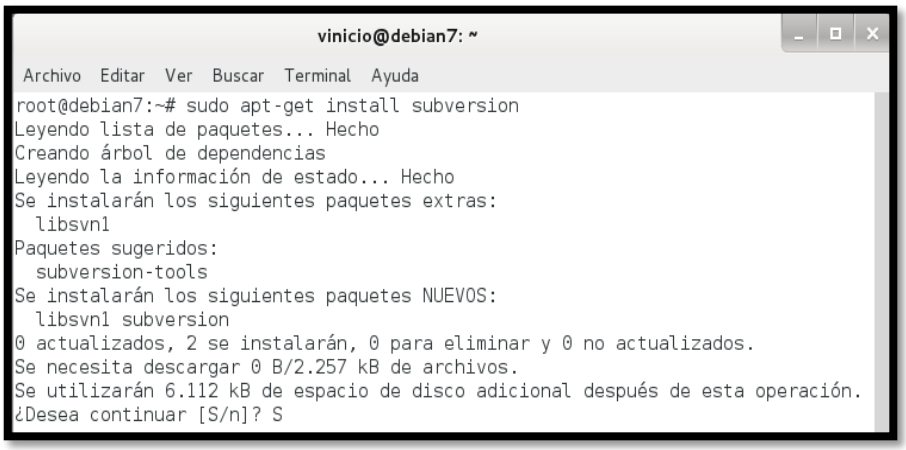


FIGURA 185 Instalación de Subversion

Fuente: Sistema Operativo Debian 7.4.0

Instalación del paquete Phlickr-0.2.5.tgz

Para instalar estas librerías debemos escribir los siguientes comandos:

sudo pear install XML_RPC

```
root@debian7:~# sudo pear install XML_RPC
WARNING: "pear/XML_RPC" is deprecated in favor of "pear/XML_RPC2"
downloading XML_RPC-1.5.5.tgz ...
Starting to download XML_RPC-1.5.5.tgz (31,862 bytes)
.........done: 31,862 bytes
install ok: channel://pear.php.net/XML_RPC-1.5.5
```

FIGURA 186 Resultado de Instalación de XML_RPC

Fuente: Sistema Operativo Debian 7.4.0

cd /tmp

wget http://sourceforge.net/projects/phlickr/files/Phlickr/0.2.5/Phlickr-0.2.5.tgz

```
root@debian7:~# cd /tmp
root@debian7:/tmp# wget http://sourceforge.net/projects/phlickr/files/Phlickr/0.
2.5/Phlickr-0.2.5.tgz
```

FIGURA 187 Descarga del paquete Phlickr

Fuente: Sistema Operativo Debian 7.4.0

sudo pear install Phlickr-0.2.5.tgz

```
root@debian7:/tmp# sudo pear install Phlickr-0.2.5.tgz
WARNING: "pear/PHPUnit2" is deprecated in favor of "channel://pear.phpunit.de/PH
PUnit"
Did not download optional dependencies: pear/PHPUnit2, use --alldeps to download
 automatically
pear/Phlickr can optionally use package "pear/PHPUnit2" (version >= 2.2.0)
install ok: channel://pear.php.net/Phlickr-0.2.5
```

FIGURA 188 Instalación del paquete Phlickr-0.2.5.tgz

Fuente: Sistema Operativo Debian 7.4.0

Por último removemos:

rm Phlickr-0.2.5.tgz

Instalación del servidor de autenticación Wifidog Auth-Server

svn checkout https://dev.wifidog.org/svn/trunk/wifidog-auth

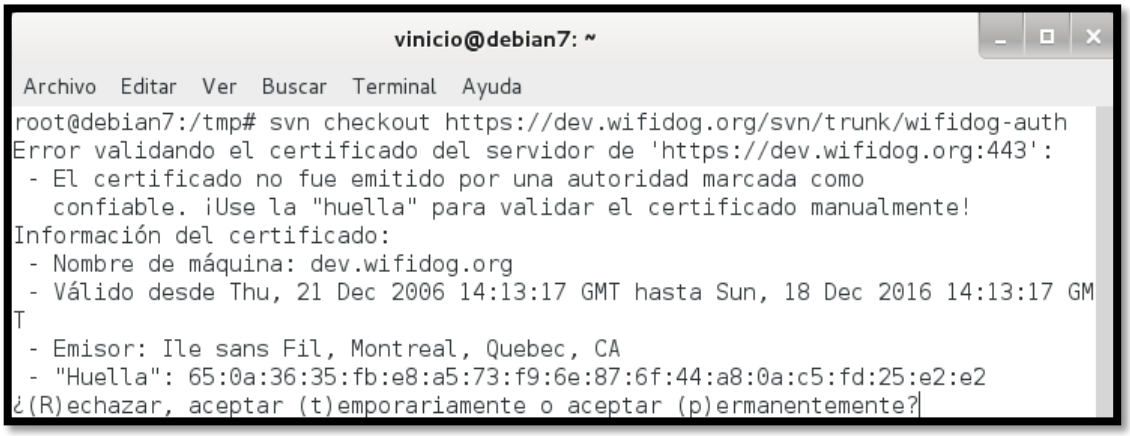


FIGURA 189 Validación del certificado Wifidog Auth-Server

Fuente: Sistema Operativo Debian 7.4.0

Si después de haber aceptado permanentemente escribiendo la letra “p” nos genera lo siguiente:

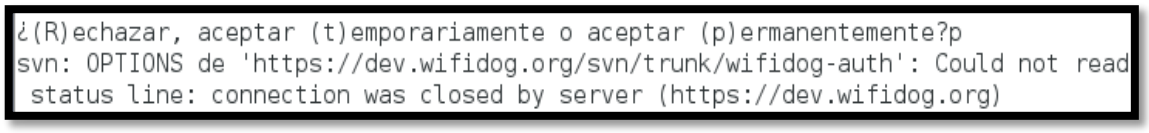


FIGURA 190 Error de validación del certificado

Fuente: Sistema Operativo Debian 7.4.0

Se debe teclear nuevamente el comando de instalación que se indica a continuación:

svn checkout https://dev.wifidog.org/svn/trunk/wifidog-auth

FIGURA 191 Instalación de Wifidog Auth-Server

Fuente: Sistema Operativo Debian 7.4.0

Y luego movemos al directorio:

sudo mv wifidog-auth/ /var/www/

Configuración del Servidor Apache2

Como este servidor no brindara otro uso “WEB” necesitamos cambiar la raíz del documento (caso contrario se debería de considerar instruirse en Apache2) para ello se ejecuta el siguiente comando:

sudo nano /etc/apache2/sites-available/default

Y cambiamos:

DocumentRoot "/var/www/html"

Por:

DocumentRoot "/var/www/wifidog-auth/wifidog"

Como se observa en la FIGURA 192:

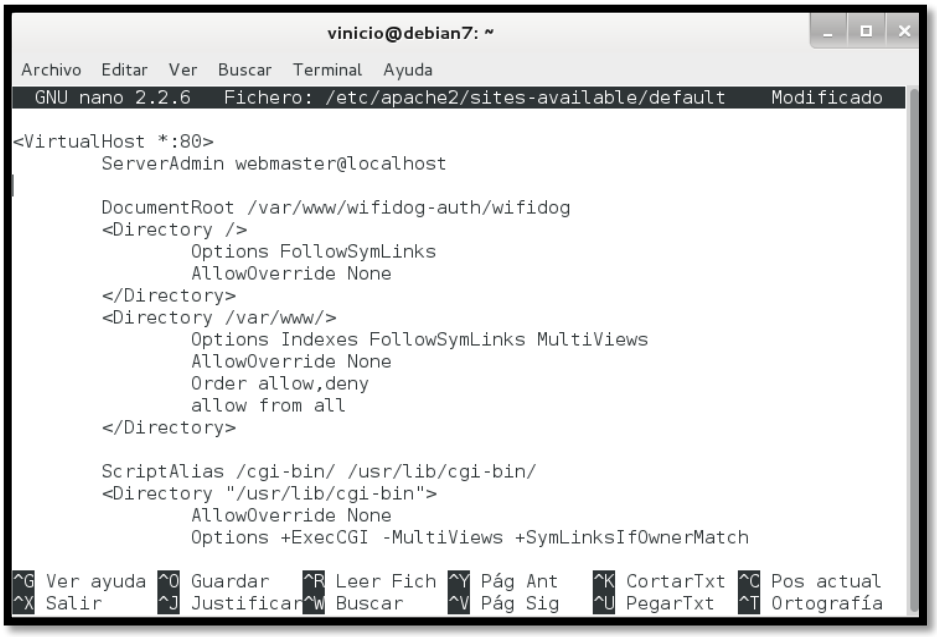


FIGURA 192 Configuración del servidor Apache2

Fuente: Sistema Operativo Debian 7.4.0

Se tiene que reiniciar o iniciar el servicio de apache con los comandos:

sudo /etc/init.d/apache2 restart

sudo /etc/init.d/apache2 start

Configuración del Timezone y el Lenguaje

Cambie el Timezone y el lenguaje para la página del portal en el archivo config.php.

sudo nano /var/www/wifidog-auth/wifidog/config.php

define('DATE_TIMEZONE', 'Canada/Eastern');

por

define('DATE_TIMEZONE', 'America/Guayaquil');

define('DEFAULT_LANG','fr_CA');

por

define('DEFAULT_LANG','es_EC');

Configuración del DNS

Cuando se cuenta con un servidor DNS local en Windows o Linux no debemos instalar nuevamente un servidor DNS. Es por ello que deberían solicitar al administrador o al encargado de la resolución de nombres la creación de las zonas directa e inversa junto con su dominio hacia la dirección IP de su equipo o servidor.

a) Para comprobar que el dominio está creado debemos ejecutar en el terminal "nslookup" e ingresar la dirección IP o el dominio, de esta manera verificaremos que esté funcionando el DNS (FIGURA 193).

b)

FIGURA 193 Resolución del dominio y la dirección IP

Fuente: Terminal de Windows

c) Editar el archivo /etc/resolv.conf para que nuestro servidor resuelva las peticiones DNS.

nano /etc/resolv.conf

Cambiar el nombre del servidor DNS por la IP del equipo:

FIGURA 194 Contenido del fichero resolv.conf
Fuente: Sistema Operativo Debian 7.4.0

Instalación y Configuración del Servidor de Correo Electrónico Postfix

Wifidog utiliza un sistema de registro para los nuevos usuarios, el cual envía un correo electrónico solicitando la confirmación de la cuenta de correo, para lo cual es necesaria la instalación de un servidor de Correo Electrónico. Para este proyecto se ha seleccionado como servidor de Correo Electrónico al Agente de Transporte de Correo (MTA) Postfix.

Postfix es un Servidor de Correos Electrónicos de software libre el cual en los últimos años se ha convertido en una alternativa más rápida, fácil de administrar y segura en comparación al ampliamente utilizado Sendmail.
Para instalar ciertos paquetes que necesitamos debemos añadir el siguiente repositorio a "/etc/apt/sources.list".

deb http://ftp.de.debian.org/debian wheezy main

Actualizamos los repositorios con un:

sudo apt-get update

Para ello vamos a instalar los servicios a utilizar ejecutando el siguiente comando:sudo apt-get install postfix libsasl2-modules mailutils

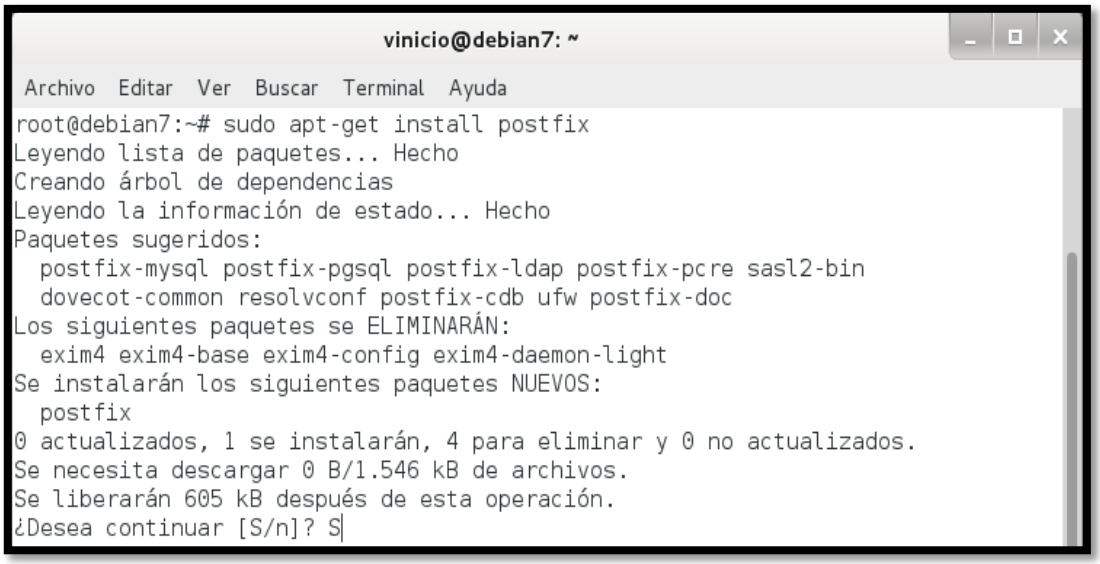


FIGURA 195 Instalación de Postfix y paquetes adicionales

Fuente: Sistema Operativo Debian 7.4.0

Aparecerán cuadros de dialogo, seleccione la opción de “Internet con smarthost” y deje las configuraciones por defecto de las próximas preguntas que se muestran a continuación:

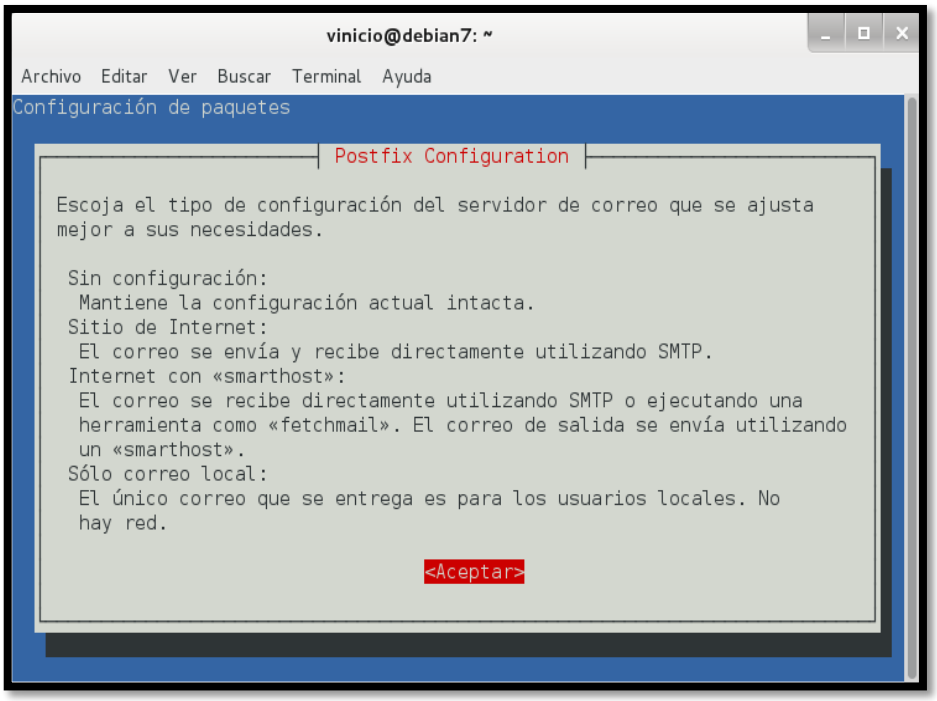


FIGURA 196 Explicación de los tipos de configuración del servidor de correo

Fuente: Sistema Operativo Debian 7.4.0

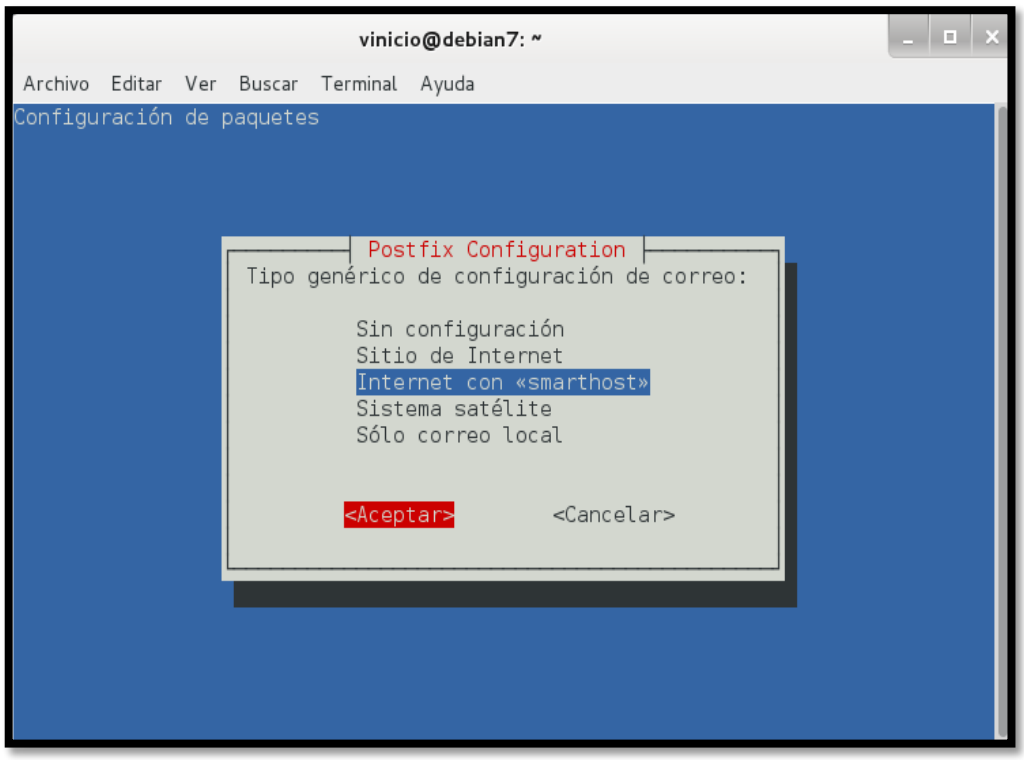


FIGURA 197 Seleccionamos Internet con smarthost

Fuente: Sistema Operativo Debian 7.4.0

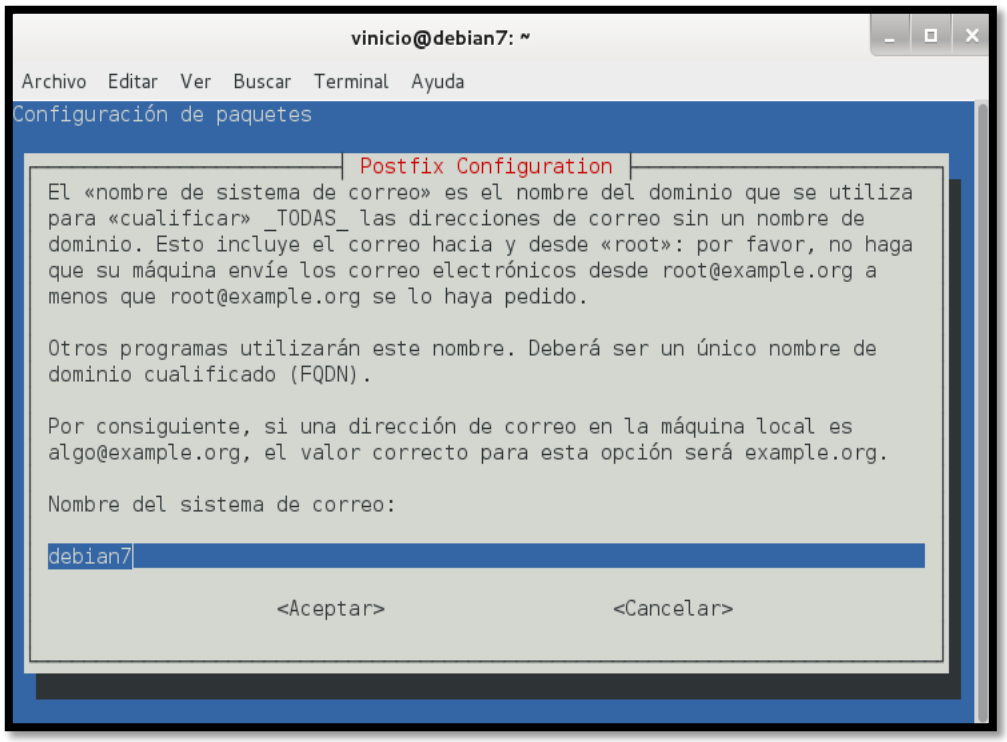


FIGURA 198 Parámetro por defecto (Nombre del sistema de correo)

Fuente: Sistema Operativo Debian 7.4.0

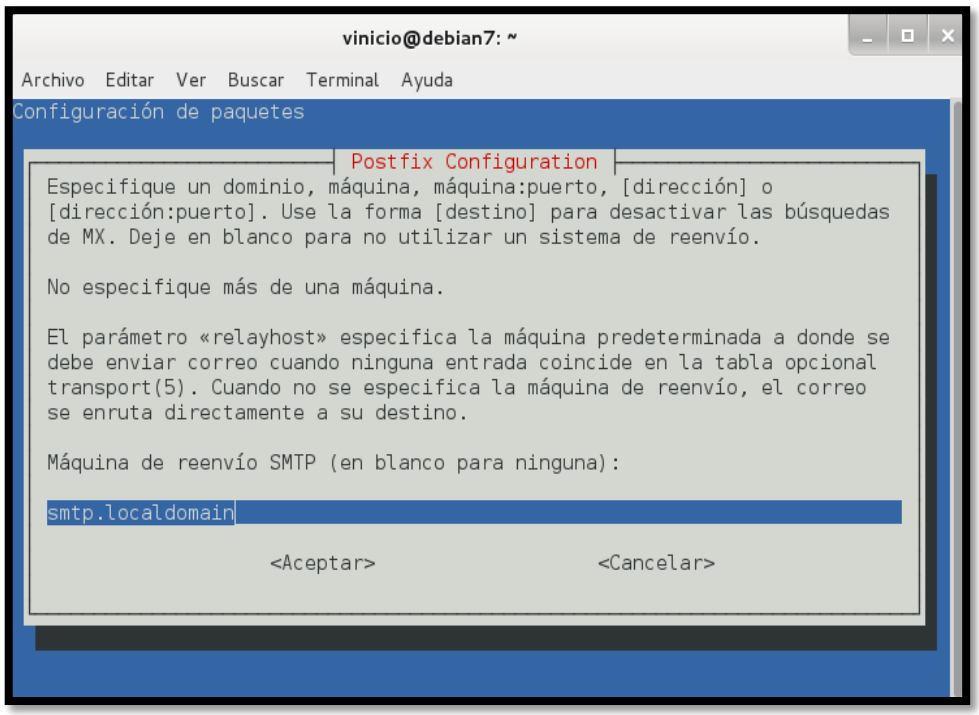


FIGURA 199 Parámetro por defecto (Máquina de reenvío SMTP)

Fuente: Sistema Operativo Debian 7.4.0

Y ahora si, se procede a instalar “sasl2-bin” de la siguiente manera:

sudo apt-get install sasl2-bin

Nos dirigimos a editar al siguiente fichero “/etc/default/saslauthd”:

START=no

Por

START=yes

Por último se reinicia el servicio:

/etc/init.d/saslauthd restart

En los últimos años la publicidad y el correo no deseado en internet se han convertido en un gran problema para las compañías Proveedoras de Servicios de Internet (ISP), por lo cual en la mayoría de servidores de correo las políticas de seguridad impiden establecer conexiones sin autentificación. Una alternativa para esto es el reenvió SMTP, con lo cual se puede establecer una conexión entre dos servidores que reenvíen correos. Para lo cual se configurara una cuenta de correo gratuito para que acepte conexiones de reenvió de SMTP.

El servicio de correo electrónico gratuito GMAIL, es una alternativa viable para reenvió de SMTP, debido a que GMAIL admite conexiones SMTP seguras. En esta ocasión utilizaremos la plataforma de correo de Office365 para reenvío de SMTP, el funcionamiento de esta configuración se explica en la siguiente ilustración (FIGURA 200).

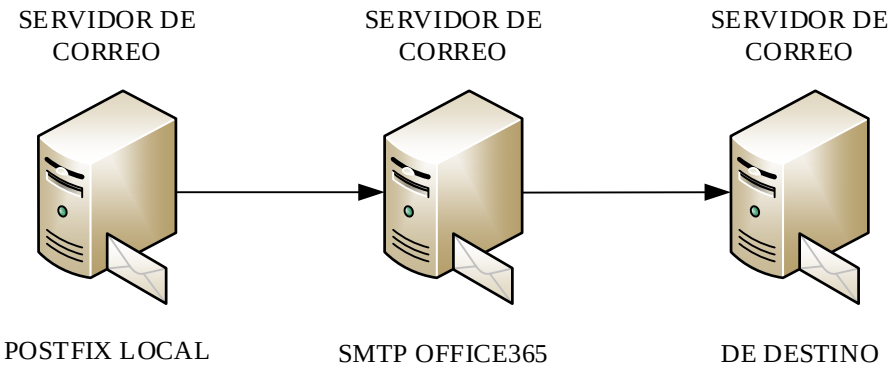


FIGURA 200 Reenvió SMTP del servidor de correo GMAIL

Fuente: E. Vinicio Guerra Morales

Para la configuración del reenvió de SMTP es necesario contar con una cuenta del correo electrónico de Office365, en este caso “wifidog@utn.edu.”. Esta cuenta será la que enviara el correo electrónico a todos los destinatarios para validar su cuenta de acceso a Internet.

El primer paso de la configuración de reenvío de SMTP es modificar el archivo “/etc/postfix/main.cf” en el servidor local Postfix y agregar las siguientes líneas de configuración:

```
    sudo nano /etc/postfix/main.cf
############################
## PARÁMETROS POR DEFECTO
############################
biff = no
append_dot_mydomain = no
readme_directory = no

####################
## PARÁMETROS TLS
####################
smtpd_tls_cert_file = /etc/ssl/certs/ssl-cert-snakeoil.pem
```

```
smtpd_tls_key_file = /etc/ssl/private/ssl-cert-snakeoil.key
smtp_use_tls = yes
smtpd_use_tls = yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
smtp_tls_note_starttls_offer = yes
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl/passwd
smtp_sasl_security_options = noanonymous
smtp_sasl_tls_security_options = noanonymous
smtp_send_dummy_mail_auth = yes
smtp_always_send_ehlo = yes
smtp_tls_security_level = may
smtp_tls_loglevel = 1
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt

##########################################
## PARÁMETROS DE CONFIGURACIÓN DE SMTP
##########################################
myhostname = debian7
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = autenticacion.utn.edu.ec, autenticacion, debian7.utn.edu.ec, debian7,
localhost.localdomain, localhost
relayhost = [utn-edu-ec.mail.protection.outlook.com]:25
mynetworks = 172.16.0.0/16 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
```

Se ingresa al siguiente fichero “/etc/hostname”, del cual nos basamos para indicar nuestro nombre de host que se establecerá en el parámetro “myhostname” del archivo de configuración de postfix “/etc/postfix/main.cf”:

```
myhostname = debian7
```

Si se quiere utilizar el servidor como relay de otros dispositivos, se tiene que declarar las redes donde están dichos equipos en el parámetro “mynetworks” como se indica a continuación:

mynetworks = 172.16.0.0/16 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128

Ahora hay que ingresar al siguiente fichero “/etc/hosts” a configurar el dominio de nuestro host:

172.16.2.8 debian7.utn.edu.ec debian7
172.16.2.8 autenticacion.utn.edu.ec autenticacion

El mismo que se establecerá en el parámetro “mydestination” como se indica a continuación:

mydestination = autenticacion.utn.edu.ec, autenticacion, debian7.utn.edu.ec,
debian7, localhost.localdomain, localhost

A continuación generaremos el fichero “passwd”:

nano /etc/postfix/sasl/passwd

Con nuestra configuración de seguridad:

[utn-edu-ec.mail.protection.outlook.com]:25 wifidog@utn.edu.ec:contraseña

Se asignan los permisos adecuados:

chmod 600 /etc/postfix/sasl/passwd

Se transforma el fichero “passwd” a un fichero indexado hash:

postmap /etc/postfix/sasl/passwd

Haciendo esto se tiene un nuevo fichero llamado “passwd.db”.

Se instala los certificados:

sudo apt-get install ca-certificates

Se añade la autoridad certificadora:

cat /etc/ssl/certs/Equifax_Secure_CA.pem >> /etc/postfix/cacert.pem

Luego se reinicia o inicia el servicio de postfix con los comandos:

sudo /etc/init.d/postfix restart

sudo /etc/init.d/postfix start

Se verifica que esté funcionando el envío de correo:

echo “Texto del mensaje de correo” | mail -s “Asunto” Correo de Destino

echo “Prueba de envío de correo” | mail -s “Prueba” wifidog@utn.edu.ec

Finalmente, si se quiere analizar los logs del correo para ver si ha existido algún error se lo hace de la siguiente manera:

tail –f /var/log/mail.log

tail –f /var/log/mail.err

Configuración del Auth-Server

Abra su browser y vaya a “http://sudominio.com/install.php” y siga las instrucciones que se le desplegaran. Si no ha configurado la redirección de DNS, puede obtener su dirección de IP con el comando “ifconfig”. También puede conectarse desde el servidor a instalar el software con:

http://localhost/install.php

Antes de empezar con la instalación vía web:

a) Primero es necesario crear un usuario wifidog en postgres, para ello los siguientes comandos:

sudo su – postgres

createuser wifidog --pwprompt

b) En PostgreSQL: Ingresamos el password que en este caso es “wifidogtest” y respondemos “No” a las siguientes 3 preguntas:

c) Cree una base de datos para este nuevo usuario.

createdb wifidog --encoding=UTF-8 --owner=wifidog

La pantalla a continuación muestra el proceso descrito anteriormente:

```
root@debian7:~# sudo su - postgres
postgres@debian7:~$ createuser wifidog --pwprompt
Enter password for new role:
Enter it again:
Shall the new role be a superuser? (y/n) n
Shall the new role be allowed to create databases? (y/n) n
Shall the new role be allowed to create more new roles? (y/n) n
postgres@debian7:~$
postgres@debian7:~$ createdb wifidog --encoding=UTF-8 --owner=wifidog
postgres@debian7:~$
```

FIGURA 201 Creación de usuario y la Base de datos de Wifidog

Fuente: Sistema Operativo Debian 7.4.0

d) Para Ingresar a la instalación vía web tecleamos en el navegador lo siguiente

Entonces, para obtener la clave que solicita al ingresar a: http://localhost/install.php, se utiliza el siguiente comando:

cat /tmp/dog_cookie.txt

```
postgres@debian7:~$ cat /tmp/dog_cookie.txt
3YCWIp9G
```

FIGURA 202 Solicitud de clave de ingreso

Fuente: Sistema Operativo Debian 7.4.0

e) Pantalla de inicio

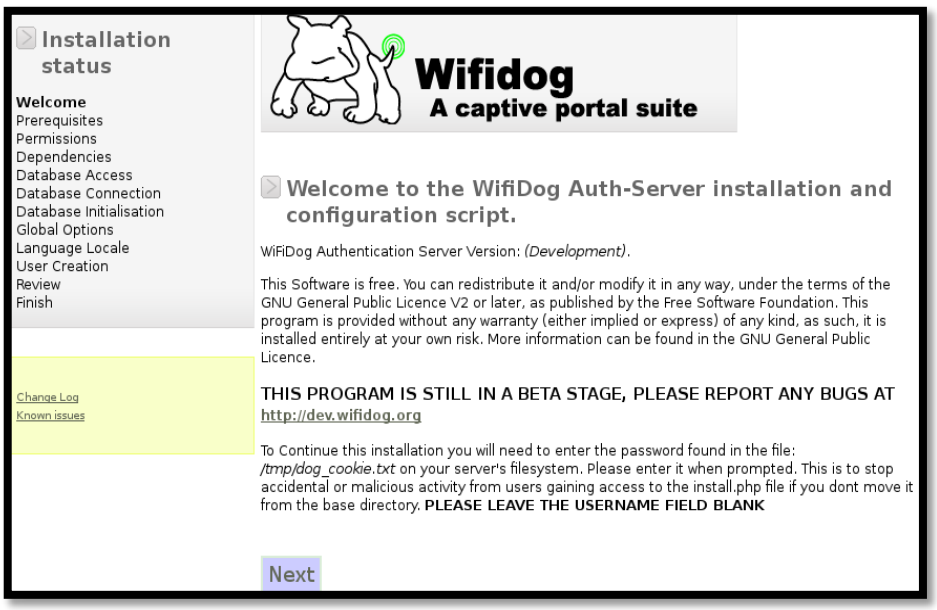


FIGURA 203 Inicio de instalación de Wifidog

Fuente: Sistema Operativo Debian 7.4.0

f) Clic en “next” en su navegador (se le preguntara por la contraseña de dog_cookie.txt)

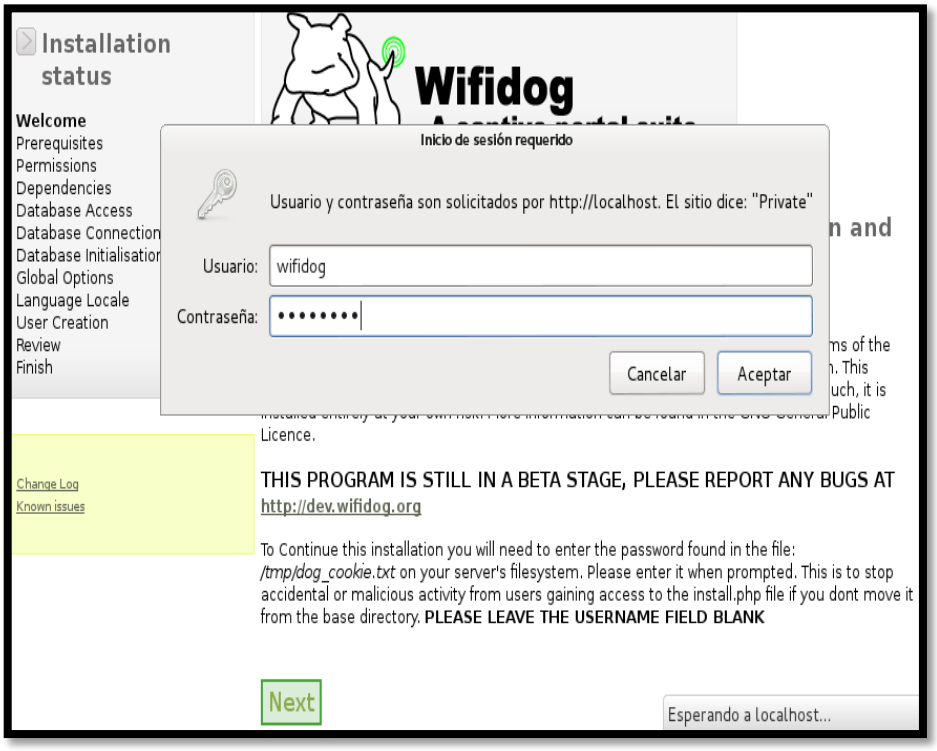


FIGURA 204 Ingreso de usuario y contraseña

Fuente: Sistema Operativo Debian 7.4.0

g) Una vez ingresado la contraseña obtenida de dog_cookie.txt se nos despliega la pantalla siguiente y hacemos clic en “next”:

FIGURA 205 Anuncio de seguridad de que ciertos comandos han sido completados

Fuente: Sistema Operativo Debian 7.4.0

h) A continuación se despliega la siguiente pantalla en la que se muestran los prerrequisitos para completar la instalación. Para ello es necesario realizar un "Copy & Paste" de la línea de comandos (indicados en ROJO), copie la serie de comandos y ejecute en la ventana terminal. Posteriormente en el navegador clic en "refresh" y luego en "next".

FIGURA 206 Prerrequisitos de Instalación

Fuente: Sistema Operativo Debian 7.4.0

```
root@debian7:~# mkdir /var/www/wifidog-auth/wifidog/tmp/simplepie_cache /var/www
/wifidog-auth/wifidog/tmp/openidserver /var/www/wifidog-auth/wifidog/lib/simplep
ie /var/www/wifidog-auth/wifidog/lib/feedpressreview
root@debian7:~# chgrp -R www-data /var/www/wifidog-auth/wifidog/ /var/www/wifido
g-auth/wifidog/tmp /var/www/wifidog-auth/wifidog/tmp/simplepie_cache /var/www/wi
fidog-auth/wifidog/lib/ /var/www/wifidog-auth/wifidog/tmp/smarty/templates_c /va
r/www/wifidog-auth/wifidog/tmp/smarty/cache /var/www/wifidog-auth/wifidog/tmp/op
enidserver /var/www/wifidog-auth/wifidog/lib/simplepie /var/www/wifidog-auth/wif
idog/lib/feedpressreview /var/www/wifidog-auth/wifidog/config.php ;
root@debian7:~# chmod g+wx /var/www/wifidog-auth/wifidog/ /var/www/wifidog-auth/
wifidog/tmp /var/www/wifidog-auth/wifidog/tmp/simplepie_cache /var/www/wifidog-a
uth/wifidog/lib/ /var/www/wifidog-auth/wifidog/tmp/smarty/templates_c /var/www/w
ifidog-auth/wifidog/tmp/smarty/cache /var/www/wifidog-auth/wifidog/tmp/openidser
ver /var/www/wifidog-auth/wifidog/lib/simplepie /var/www/wifidog-auth/wifidog/li
b/feedpressreview /var/www/wifidog-auth/wifidog/config.php ;
root@debian7:~#
```

FIGURA 207 Solución de errores de prerrequisitos de instalación

Fuente: Sistema Operativo Debian 7.4.0

i) Luego de actualizar los directorios hacer clic en “Refresh”, y enseguida se despliega la siguiente pantalla.

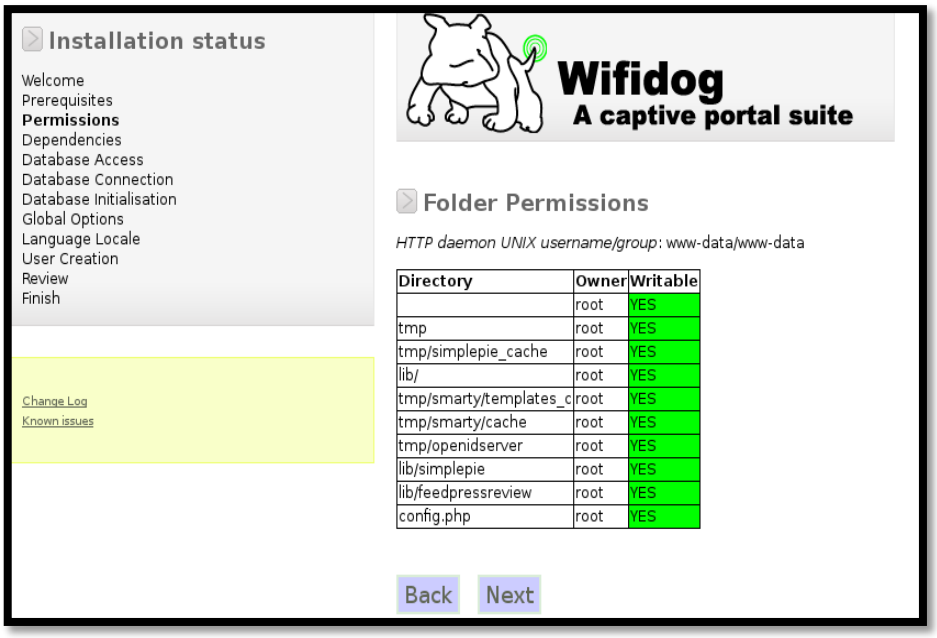


FIGURA 208 Actualización de directorios

Fuente: Sistema Operativo Debian 7.4.0

j) Haciendo clic en “next” de la pantalla anterior nos permite obtener la verificación del software instalado (Si ha seguido esta guía paso a paso, debe tener los requisitos básicos para la instalación).

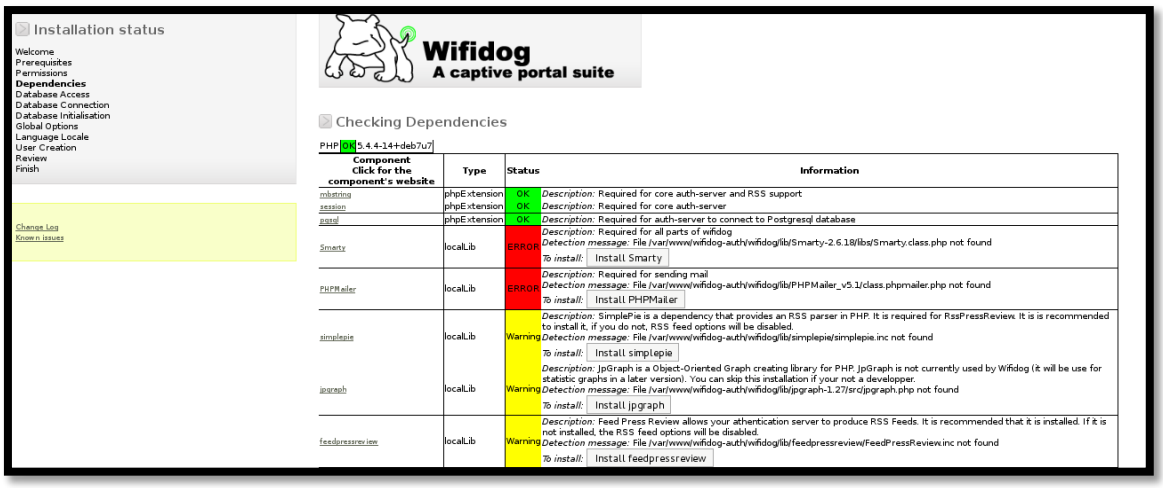


FIGURA 209 Información de dependencias por instalar

Fuente: Sistema Operativo Debian 7.4.0

Es necesario solucionar todos los errores que se presentan (los mensajes de warning no es obligatorio solucionarlos) para que se nos permita acceder a la siguiente etapa de instalación.

k) Clic para instalar “simplepie”, luego “next”. Clic para instalar “feedpressreview”, luego “next”. Clic para instalar “Phlickr” (aunque está instalado pero el sistema no lo detecta).

l) Descargar el paquete “Smarty-2.6.18.tar.gz” y moverlo al siguiente directorio:
/var/www/wifidog-auth/wifidog/tmp

m) Editar el fichero “Dependency.php” localizado en el directorio:
nano /var/www/wifidog-auth/wifidog/clases/Dependency.php

Esta parte es muy importante para poder instalar “Smarty-2.6.18.tar.gz” vía web debido a que lo que hacemos es cambiar el nombre de la descarga tal como se muestra a continuación de:

“http://smarty.net/do_download.php?download_file=Smarty-2.6.18.tar.gz",

```
"Smarty" => array (
'mandatory' => true,
"type" => "localLib",
"detectFiles" => "lib/Smarty-2.6.18/libs/Smarty.class.php",
'description' => "Required for all parts of wifidog",
'website' => "http://smarty.net/",
'installSourceUrl' => "http://smarty.net/do_download.php?download_file=Smarty-2.6.18.tar.gz",
'installMethod' => "tarball",
'installDestination' => "/"
),
```

FIGURA 210 Configuración por defecto de Smarty en el fichero Dependency.php
Fuente: Sistema Operativo Debian 7.4.0

Por:

"http://smarty.net/Smarty-2.6.18.tar.gz",

```
"Smarty" => array (
'mandatory' => true,
"type" => "localLib",
"detectFiles" => "lib/Smarty-2.6.18/libs/Smarty.class.php",
'description' => "Required for all parts of wifidog",
'website' => "http://smarty.net/",
'installSourceUrl' => "http://smarty.net/Smarty-2.6.18.tar.gz",
'installMethod' => "tarball",
'installDestination' => "/"
),
```

FIGURA 211 Configuración de instalación de Smarty en el fichero Dependency.php
Fuente: Sistema Operativo Debian 7.4.0

n) Con las dependencias editadas instalamos desde el navegador “Smarty” y “PHPMailer”, para luego hacer clic en “next”:

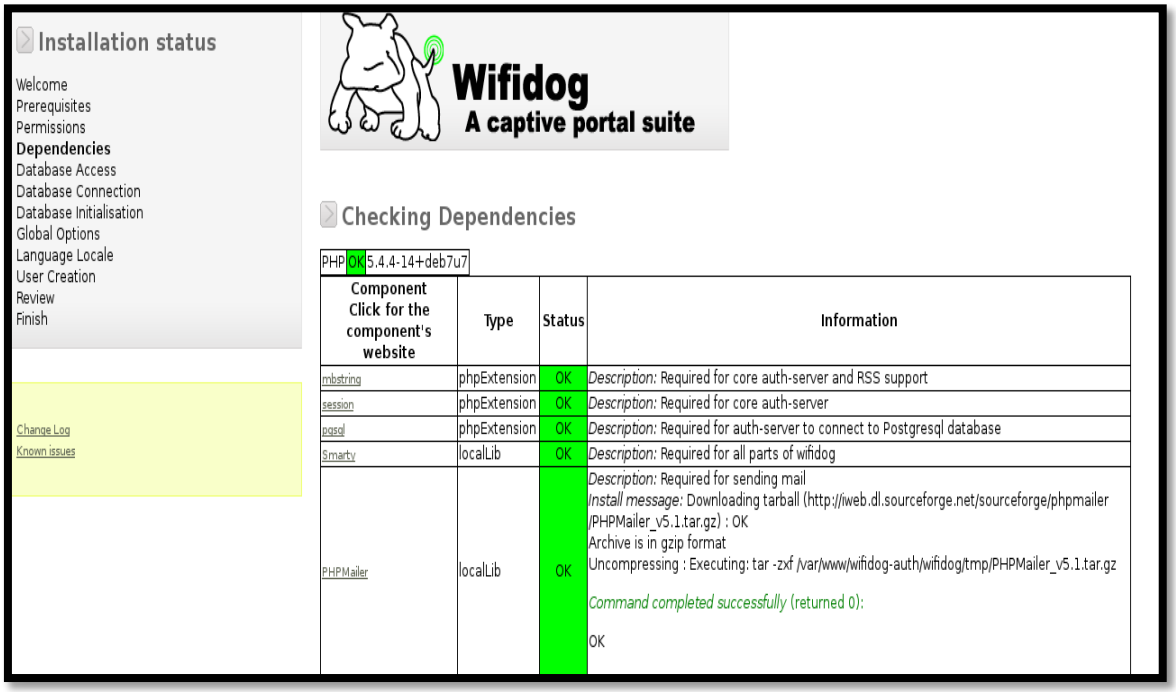


FIGURA 212 Información de dependencias instaladas

Fuente: Sistema Operativo Debian 7.4.0

o) Luego de corregir los errores accedemos a la siguiente pantalla

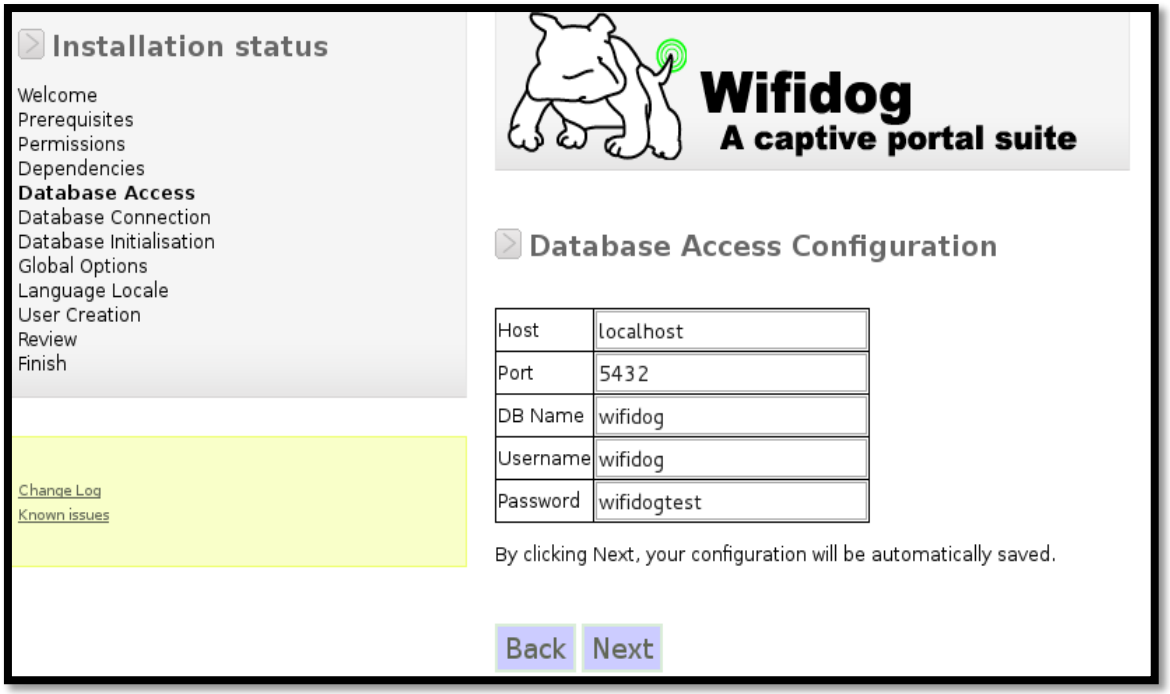


FIGURA 213 Configuración de Acceso a la Base de Datos

Fuente: Sistema Operativo Debian 7.4.0

p) Se ingresa a la información de la Conexión de su Base de datos y también en la inicialización de la misma, como se indica en las figuras mostradas a continuación:

La versión del servidor PostgreSQL es de vital importancia a la hora de crear la cuenta de administrador, de acuerdo a las pruebas realizadas con la versión 9 no fueron satisfactorias, por ello se recomienda trabajar en las versiones de 8.4.

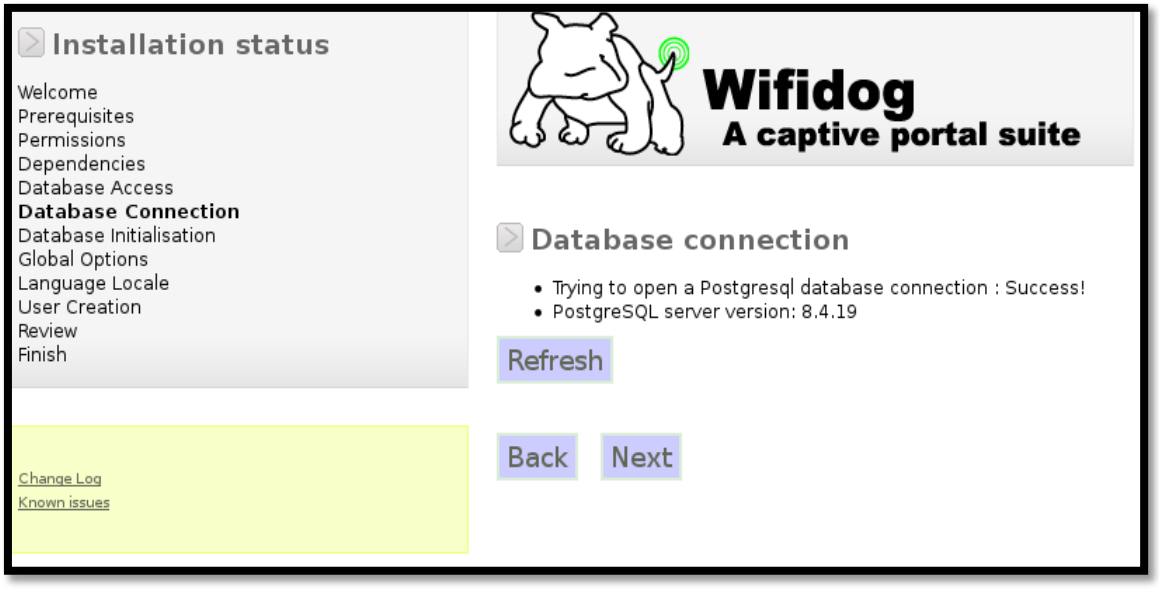


FIGURA 214 Conexión de la Base de Datos

Fuente: Sistema Operativo Debian 7.4.0

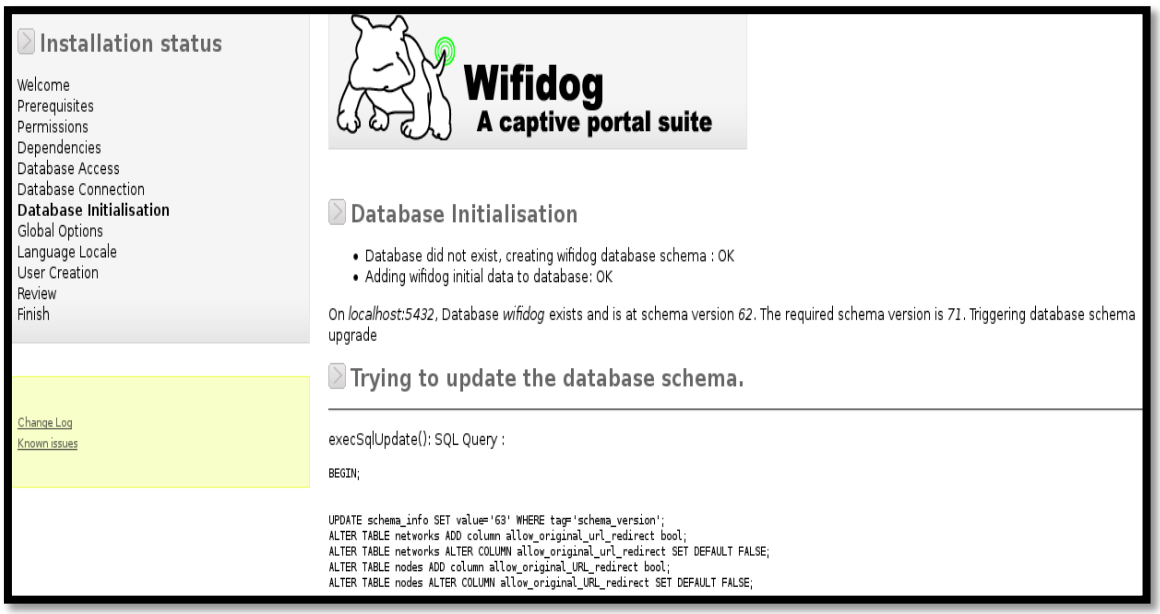


FIGURA 215 Inicialización de la Base de Datos

Fuente: Sistema Operativo Debian 7.4.0

q) Parámetros de Opciones Globales, se deja por defecto.

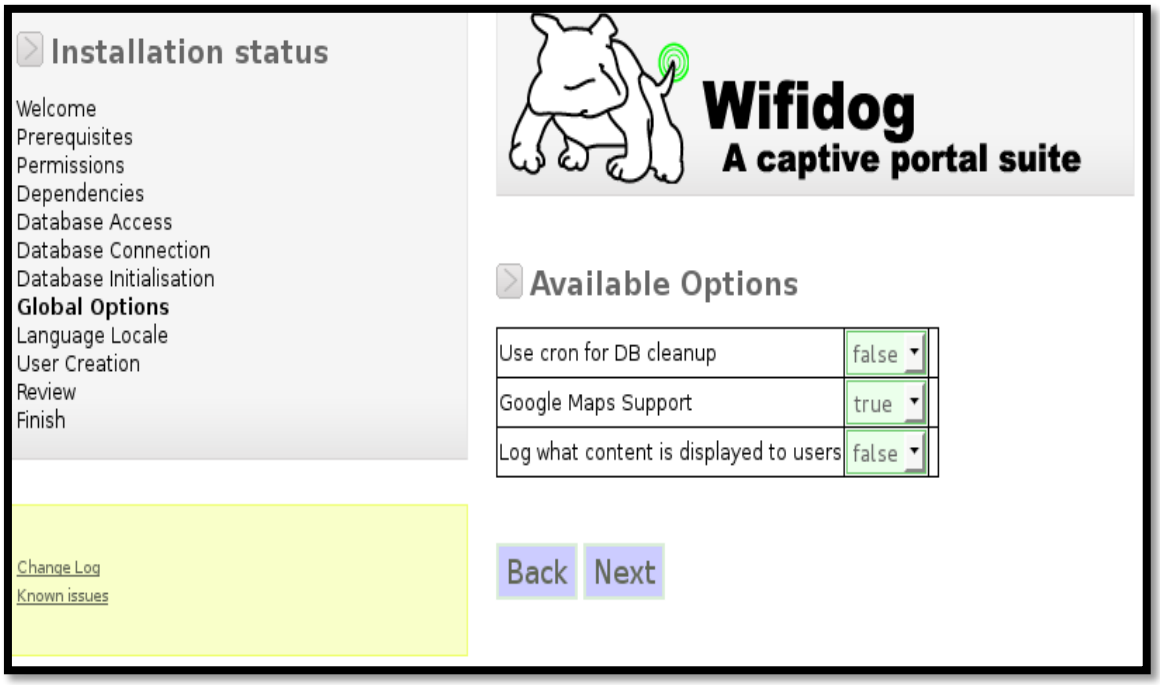


FIGURA 216 Parámetros de opciones globales

Fuente: Sistema Operativo Debian 7.4.0

r) Elección del lenguaje local.

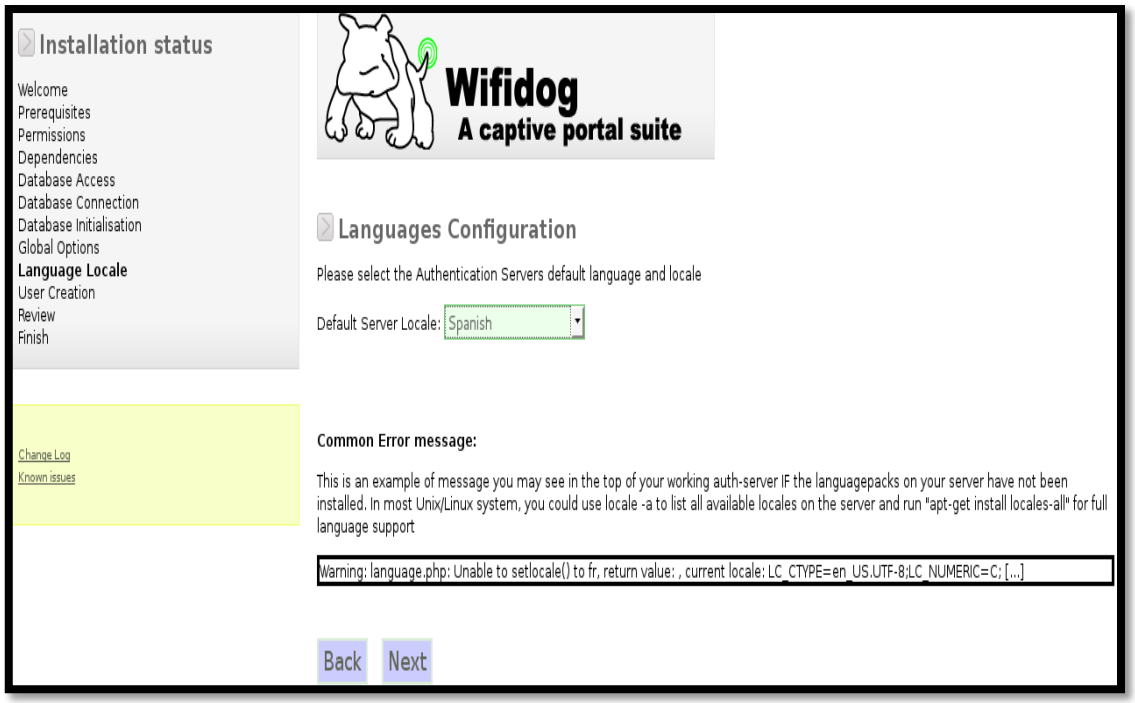


FIGURA 217 Configuración de Lenguajes

Fuente: Sistema Operativo Debian 7.4.0

FIGURA 218 Selección del Lenguaje

Fuente: Sistema Operativo Debian 7.4.0

s) Creación de la cuenta de administrador del portal cautivo.

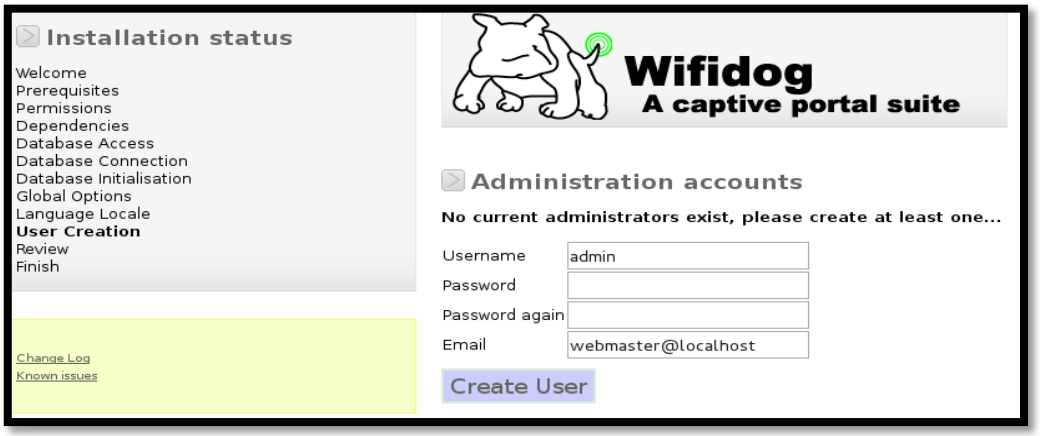


FIGURA 219 Parámetros por defecto para crear la cuenta de Administrador

Fuente: Sistema Operativo Debian 7.4.0

FIGURA 220 Ingreso de username, password y correo de la cuenta de Administrador

Fuente: Sistema Operativo Debian 7.4.0

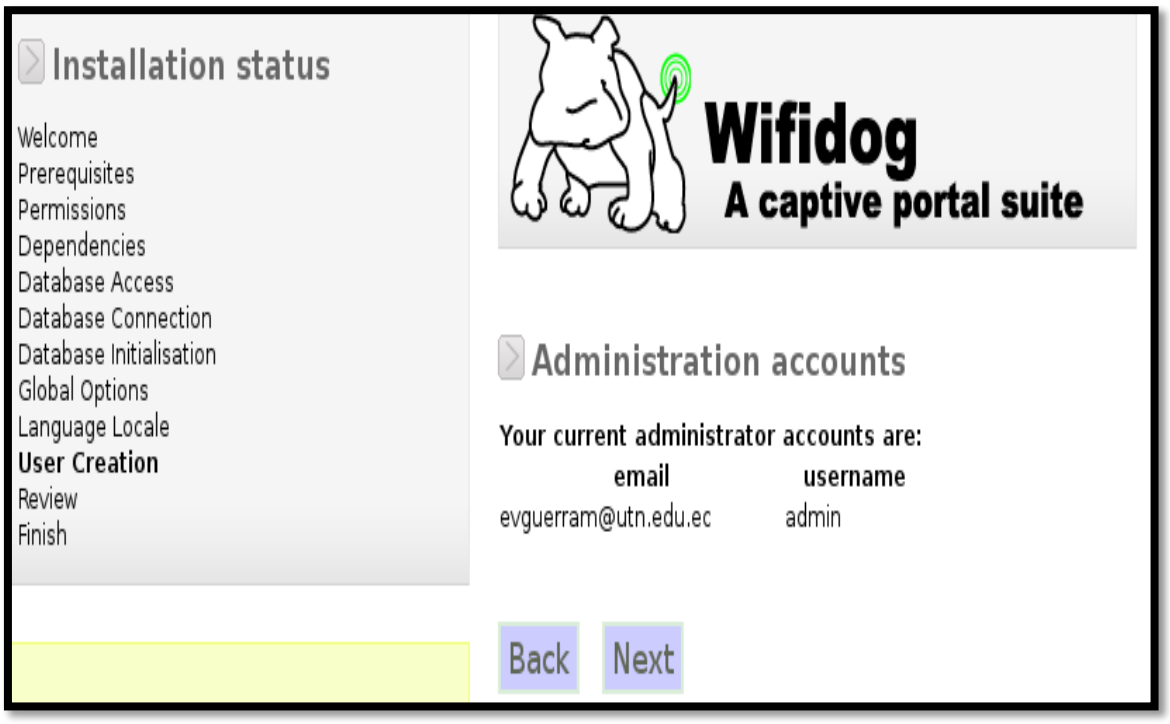


FIGURA 221 Cuenta de Administrador creada

Fuente: Sistema Operativo Debian 7.4.0

t) Finalización de la instalación

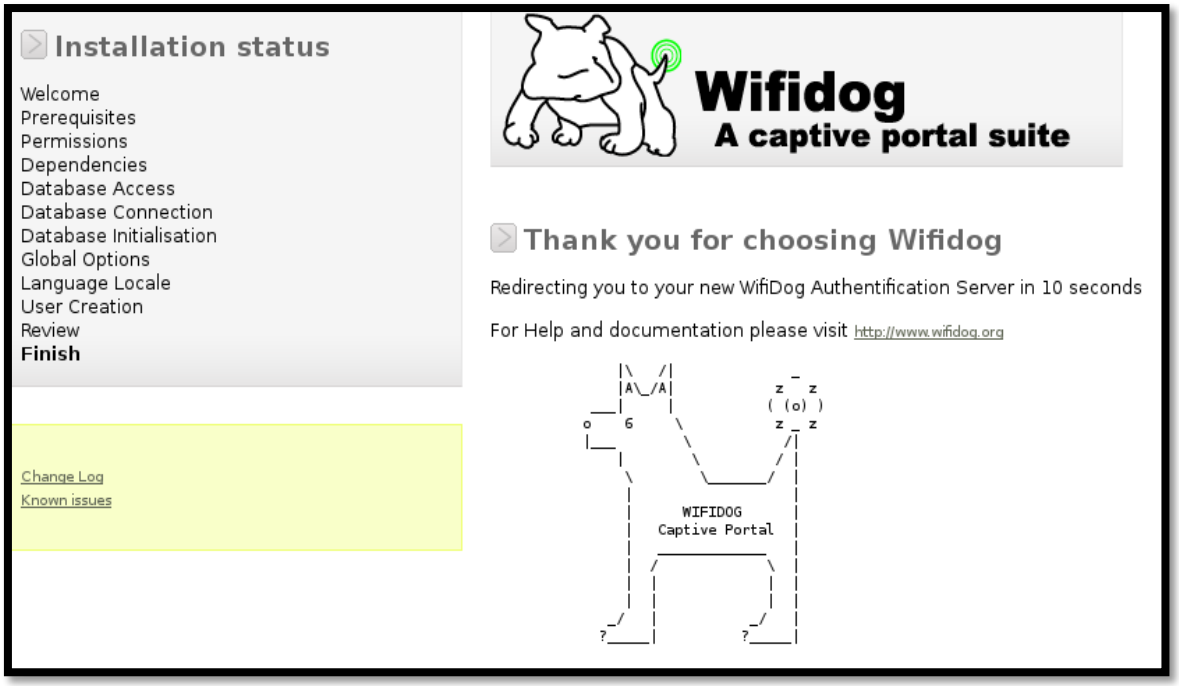


FIGURA 222 Verificación y finalización de Wifidog

Fuente: Sistema Operativo Debian 7.4.0

Remover archivos de instalación

El único que debe tener acceso al archivo “install.php” es usted. Necesitará mover este archivo fuera del lugar público, como se indica:

a) Ingresar al directorio de WifiDog (/var/www/wifidog-auth/wifidog).
cd /var/www/wifidog-auth/wifidog

b) Mover “install.php” al parent directory el cual no está visible al público:
mv install.php ../install.php
ó
sudo mv /var/www/wifidog-auth/wifidog/install.php /var/www/wifidog-auth

Configuración de las Tarjetas de Red

Cuando el sistema operativo Debian 7 fue instalado, automáticamente se configuró para tener conexión a Internet, entonces ahora se configura las dos tarjetas de red tanto para la WAN (Acceso a Internet) como para la LAN (conexión de clientes). Mientras se necesita realizar un “bridge” entre las dos tarjetas de red para pasar a los clientes de una red a otra y que de esta manera puedan salir a Internet.

- Abrir el archivo “/etc/network/interfaces”
- Editar las opciones en el archivo de las interfaces ubicadas en el path:
  nano /etc/network/interfaces

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 172.16.2.8
netmask 255.255.255.0
gateway 172.16.2.5
network 172.16.2.0
broadcast 172.16.2.255
dns-nameservers 172.16.1.158

auto eth1
```

iface eth1 inet static
address 172.16.128.8
netmask 255.255.224.0
gateway 172.16.2.8
network 172.16.128.0
broadcast 172.16.159.255

- Reiniciar la tarjetas de red con “/etc/init.d/networking restart”
- Escribir “ifconfig” para ver si ambas tarjetas están incluidas.

Deberá tener eth0 (red externa, conectada a Internet) y eth1 (red interna, conectada hacia el Access Point), ahora necesitamos hacer que las tarjetas se comuniquen entre sí. Esto es para que el tráfico de los clientes en la LAN (WLC y APs) pase hacia Internet. Esto se logra creando un “Proxy”.

- Copiar el archivo que se encuentra en el ANEXO 8.
- Copiar a “/etc/init.d”
- Asegurarse de nombrarlo “proxy.sh”
- Hacer ejecutable con el comando “chmod a+x proxy.sh”
- Editarlo a su gusto, dirigirse a la SECTION B y cambiar el EXTIP por la IP del servidor.
- Guardar el Archivo
- Realizar un enlace simbólico a rc2.d para asegurarnos que las reglas del proxy comiencen automáticamente cuando se reinicie la PC. Para ello digite el siguiente comando:

ln -s /etc/init.d/proxy.sh /etc/rc2.d/S95proxy

Instalación y Configuración de DHCP

A los usuarios de la LAN (del lado Wireless si se trata de una red en producción) se les está asignando la configuración IP y DNS cuando se conecten, el servidor Linux necesitara un Servidor DHCP corriendo en eth1 para asignarles IPs automáticamente a los clientes del Access Point.

a) Instalar DHCP server “sudo apt-get install isc-dhcp-server”

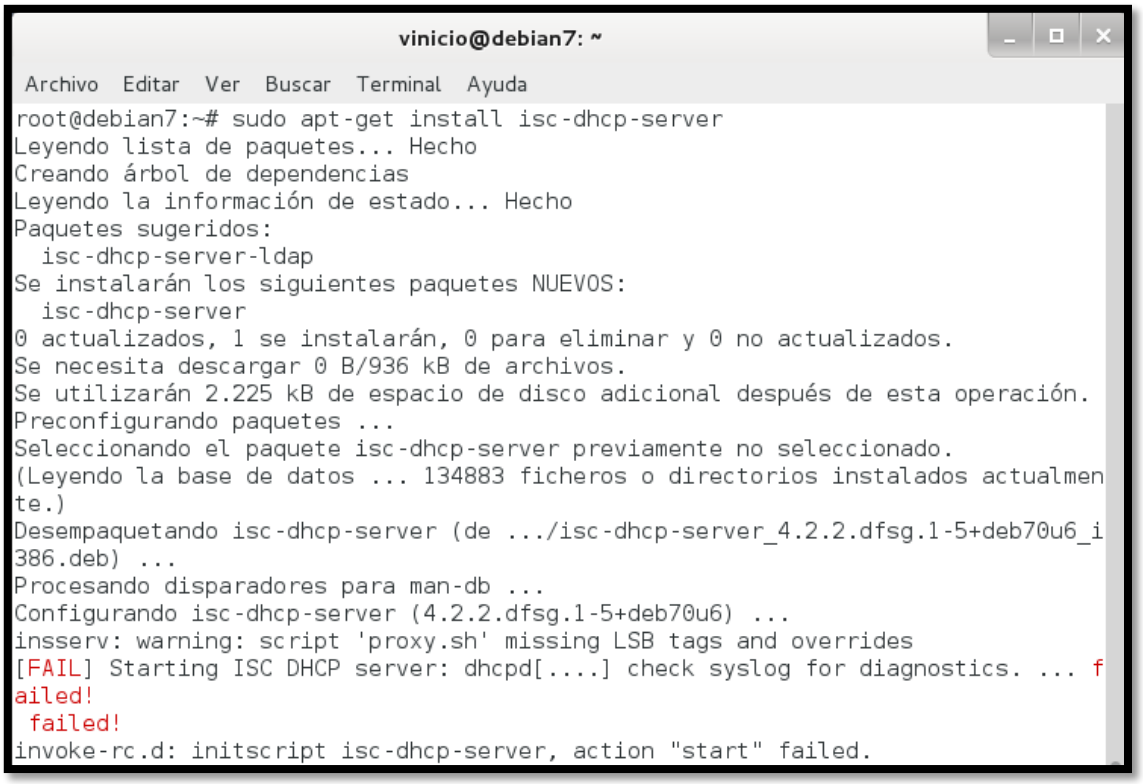


FIGURA 223 Instalación del Servidor DHCP

Fuente: Sistema Operativo Debian 7.4.0

b) Que el servidor DHCP falle en iniciar el servicio, eso está bien. Dicho error se debe a la no asignación de la interfaz que usará el servicio DHCP por defecto.

c) Escribir “/etc/init.d/isc-dhcp-server stop” para detener el servidor DHCP mientras se configura.

d) Obtener un respaldo del archivo “dhcpd.conf” y guárdelo en el mismo fichero:
cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf-respaldo

e) Editar los valores en “dhcpd.conf” con las IPs que se le asignarán a los clientes:
nano /etc/dhcp/dhcpd.conf

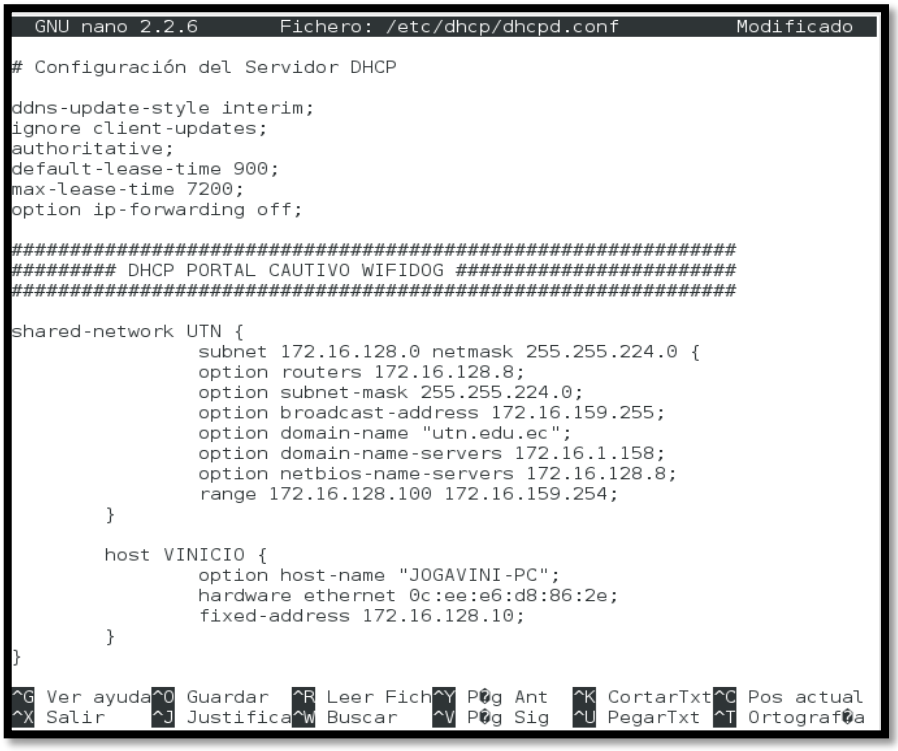


FIGURA 224 Configuración del fichero dhcpd.conf

Fuente: Sistema Operativo Debian 7.4.0

DHCP Server Configuration file

ddns-update-style interim;
ignore client-updates;
authoritative;
default-lease-time 900;
max-lease-time 7200;
option ip-forwarding off;

###
######### DHPC PORTAL CAUTIVO WIFIDOG ########################
###

shared-network UTN {
subnet 172.16.128.0 netmask 255.255.224.0 {
option routers 172.16.128.8;
option subnet-mask 255.255.224.0;
option broadcast-address 172.16.159.255;

```
        option domain-name “utn.edu.ec”;
        option domain-name-servers 172.16.1.158;
        option netbios-name-servers 172.16.128.8;
        range 172.16.128.100 172.16.159.254;
    }

    host VINICIO {
        option host-name "JOGAVINI-PC";
        hardware ethernet 0c:ee:e6:d8:86:2e;
        fixed-address 172.16.128.10;
    }
}
```

f) Reiniciar el servicio “/etc/init.d/isc-dhcp-server restart”

```
root@debian7:~# /etc/init.d/isc-dhcp-server restart
[FAIL] Stopping ISC DHCP server: dhcpd failed!
[ ok ] Starting ISC DHCP server: dhcpd.
```

FIGURA 225 Reinicio del servidor DHCP

Fuente: Sistema Operativo Debian 7.4.0

g) Para cambiar la tarjeta donde se quiere que arranque el DHCP se necesita editar “/etc/default/isc-dhcp-server” e ingresar su nueva designación (wlan0, eth0, eth1, etc).

nano /etc/default/isc-dhcp-server

INTERFACES=”eth1”

En este momento la tarjeta de red para nuestra LAN (un Access Point para una red en producción) está configurada para asignar IPs e información de DNS a los clientes.

En esta etapa debería de probar que el Servidor Linux está operando propiamente. Reinicie el servidor y cuando suba asegúrese que está asignando direcciones IP y que el “bridge” entre las dos tarjetas de red esté funcionando.

Asumiendo que todo esté trabajando estamos listos para configurar el router o una PC con el Gateway de Wifidog.

Instalación del Portal Cautivo de Wifidog en PC Linux

El Gateway puede ser instalado en un router común y corriente. Tenga en cuenta que el modificar un dispositivo electrónico con cualquiera de estos firmwares anulara la garantía del equipo. Debe de estar atento al fabricante del equipo y el firmware a instalar ya que son específicos por cada fabricante y modelo: DD-WRT, Coova, OpenWRT. En nuestro caso hemos decidido instalarlo en el mismo servidor donde está el Auth-server.

El Gateway de Wifidog es la base del "Portal Cautivo", es el componente que captura la página WEB del usuario inalámbrico, y lo redirecciona a la página de registro. Esta es la última pieza del rompecabezas que requiere la instalación para crear un servidor router. Para ello debemos seguir el siguiente procedimiento:

a) Dirigirse a la carpeta a "/usr/src"

b) Buscar en internet y descargarse el archivo "wifidog-20090925.tar.gz" y guardarlo en "usr/src"

c) Escribir "gunzip wifidog-20090925.tar.gz" para descomprimir el archivo.

d) Y ejecutar "tar -xvf wifidog-20090925.tar"

e) Ahora cambiarse de directorio con "cd wifidog-20090925" para moverse hacia la carpeta donde residen los archivos de Wifidog.

Antes de instalar los componentes de Wifidog debemos instalar los siguientes paquetes "gcc" y "make" con el siguiente comando "apt-get install gcc make".

Al completar este proceso hemos descomprimido los archivos de Wifidog en una carpeta separada localizada en "/usr/src/wifidog-20090925/". Ahora necesitamos instalar los componentes de Wifidog para hacerlo trabajar:

- Escribir "./configure"
- Ejecutar "make"
- Escribir "make install"

Se podrá observar algún texto en su pantalla mientras realiza los pasos para instalar. Ahora se necesita añadir el archivo de configuración.

- Tome el archivo "wifidog.conf" de este directorio "/usr/src/wifidog-20090925/" que también se encuentra en el ANEXO 9 y copiar el archivo a la carpeta "/usr/local/etc/".
- Cambiar el nombre del Gateway dentro del archivo al nombre que se le asignara. (default).

GatewayID default

- Editar la sección del Auth-Server para apuntar al servidor correcto.

AuthServer {
Hostname 172.16.2.8
SSLAvailable no

```
    Path /
}
```

ó,

```
AuthServer {
    Hostname autenticacion.utn.edu.ec
    SSLAvailable no
    Path /
}
```

Nodo de Pruebas del Gateway

Finalmente se necesita estar seguros que Wifidog funcione automáticamente cuando el servidor inicie, así que tenemos que añadir un archivo:

- Tomar el archivo nombrado wifidog que se encuentra en "/usr/local/bin/wifidog" y muévalo a la carpeta "/etc/init.d/"; este es un archivo tipo binario que ejecutará el Gateway.

- Escribir "ln -s /etc/init.d/wifidog /etc/rc2.d/S96wifidog" para decirle al sistema que comience Wifidog automáticamente.

- Si se recibe el siguiente error:

wifidog: error while loading shared libraries: libhttpd.so.0:
cannot open shared object file: No such file or directory

Debemos ejecutar el siguiente comando: ldconfig

- Crear una carpeta de nombre "wifidog" en el directorio siguiente:

```
cd /usr/local/
mkdir wifidog
```

- Copiar el archivo "wifidog-msg.html" a la carpeta "/usr/local/wifidog/"

```
cp /usr/src/wifidog-20090925/wifidog-msg.html /usr/local/wifidog/
```

- Escribir "ln -s /usr/src/wifidog-20090925/wifidog-msg.html" para decirle al sistema que comience "wifidog-msg.html" automáticamente y reiniciamos.

- Ejecutar el demonio de Wifidog de la siguiente manera:

```
/etc/init.d/wifidog –f –d 7
```

✓ -fpara ejecutar en primer plano y no se convierta en un demonio de segundo plano.

✓ -d 7 aumenta el nivel de salida de depuración (debug) al máximo.

◈ Cuando se ejecuta el demonio de Wifidog y se realizan pruebas en muchas ocasiones se queda inicializado el demonio, para ello se necesitan matar los procesos en lugar de reiniciar la PC. Esto se logra con dos comandos:

netstat -anutp	Información de las conexiones activas
kill -9 PID	Matar los procesos

Ahora configuramos en la interfaz del WLC la puerta de enlace hacia la tarjeta de red interna (eth1), apagamos el DHCP del WLC o Switch de Core que el servidor DHCP de nuestro servidor se encargará de ello. Luego de reiniciar el servidor podrá observar la página del “Portal Cautivo” cuando se conecte por medio de un AP.

Pruebas locales del Auth Server

Una vez realizada la instalación, configuración y ejecución del demonio de Wifidog se ingresa a cualquier navegador y se escribe la dirección IP de la tarjeta de red que se encuentra conectada a Internet o el dominio si se tiene.

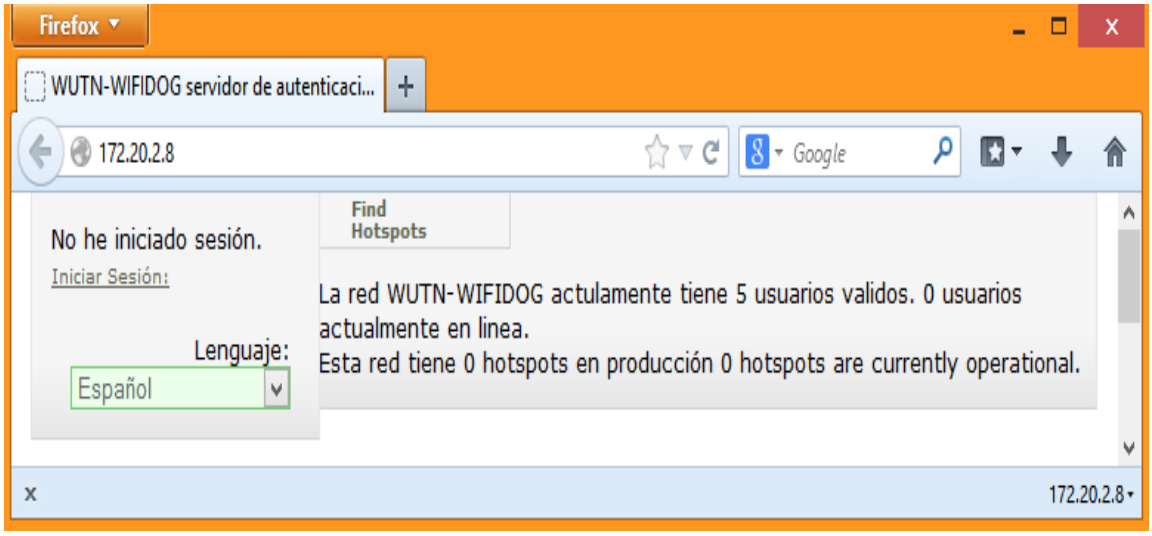


FIGURA 226 Pantalla de inicio del Auth-server

Fuente: Menú de opciones de configuración de Wifidog

El tema de fondo se puede cambiar una vez logueado con la cuenta de administrador creada previamente. Para ello haciendo click en “Iniciar Sesión” nos desplegará otra ventana para poder ingresar el usuario y password de administrador, de esa manera

podremos acceder a las opciones de administración de Wifidog.

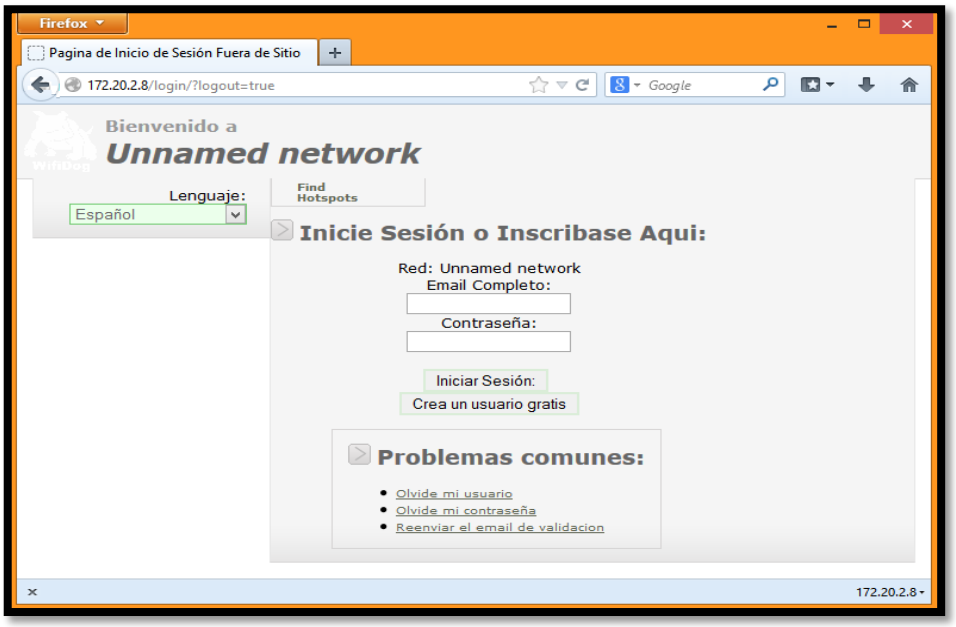


FIGURA 227 Pantalla para ingresar como usuario registrado o para crear nueva cuenta

Fuente: Menú de opciones de configuración de Wifidog

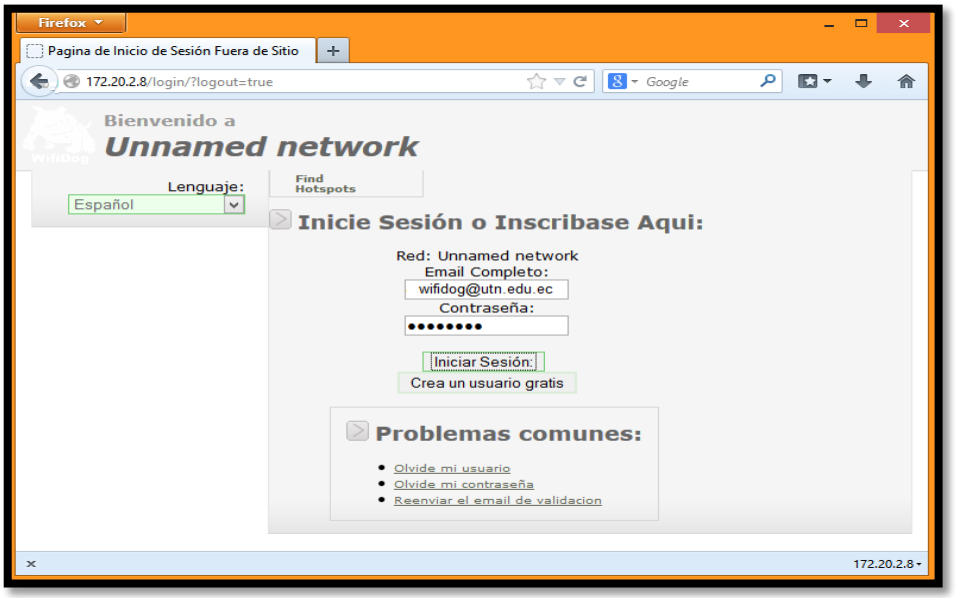


FIGURA 228 Ingreso de email y contraseña de administrador

Fuente: Menú de opciones de configuración de Wifidog

Ingresando como administrador nos permite editar las distintas opciones de configuraciones que brinda Wifidog, como son el tema de fondo del portal cautivo, el tiempo que se le permite a un usuario no registrado salir a internet sin necesidad de registrar la cuenta creada, la página por defecto a la cual se le quiere redireccionar una vez que tenga salida a internet.

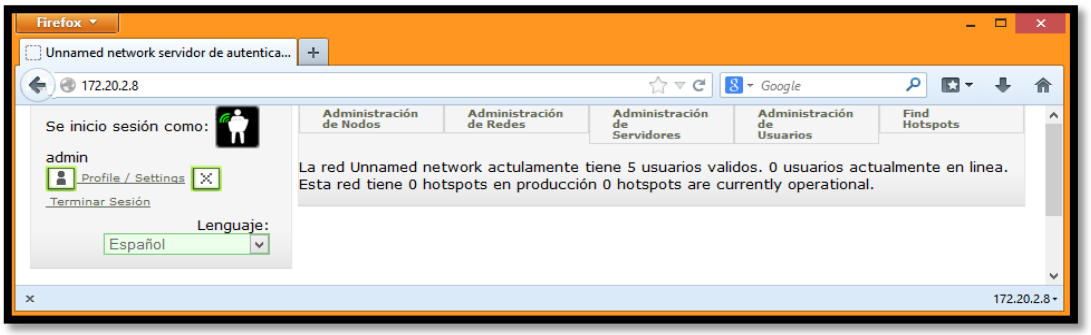


FIGURA 229 Opciones de Configuración de Administrador

Fuente: Menú de opciones de configuración de Wifidog

Una vez que se ha iniciado sesión como Administrador se puede editar las opciones de perfil admin (Profile/Settings) o ir configurando ciertos parámetros importantes para nuestro portal cautivo, los mismos que se despliegan en el menú de opciones y son los siguientes (Tabla 73).

Tabla 73 Menú de configuración de Wifidog

MENÚ PRINCIPAL	MENÚ SECUNDARIO	DESCRIPCIÓN
Administración de Nodos	Add a new node group. Agregar un nuevo Nodo. Edit node groups. Edit Nodes.	Agrega y edita los nodos de una red específica. Agrega y edita los grupos de nodos.
Administración de Redes	Add a new network on this server. Edit network.	Agrega y edita las redes del servidor y sus configuraciones personalizadas.
Administración de Servidores	Content type filters. Dependencies. Profile templates. Reusable content library. Server configuration. User roles. Virtual hosts.	Edita las configuraciones del servidor, como sus tipos de contenido, las dependencias necesarias, las plantillas para redes que pueden ser reusadas, el contenido de las redes que puede ser reusado, los roles de usuarios y los host virtuales que manejan los nombres de los dominios, en caso de que el servidor sea compartido con diferentes nombres de dominio.

Administración de Usuarios	Estadísticas. Importar base de datos de NoCat. User manager. Usuarios en línea.	Control de usuarios, estadísticas de acceso y además puede importar usuarios desde el software del portal cautivo NoCat.
Find Hotspots	Estado técnico completo del Nodo (incluye nodos no desplegados). List in HTML format. List in JiWireCSV format. List in KML format. List in RSS format. List in XML format. Mapas de HotSpots Activos	Busca los nodos activos de todas las redes configuradas en el servidor.

Fuente: Menú de opciones de configuración de Wifidog

Se selecciona el menú de “Administración de Nodos” y se hace clic en “Edit nodes”.

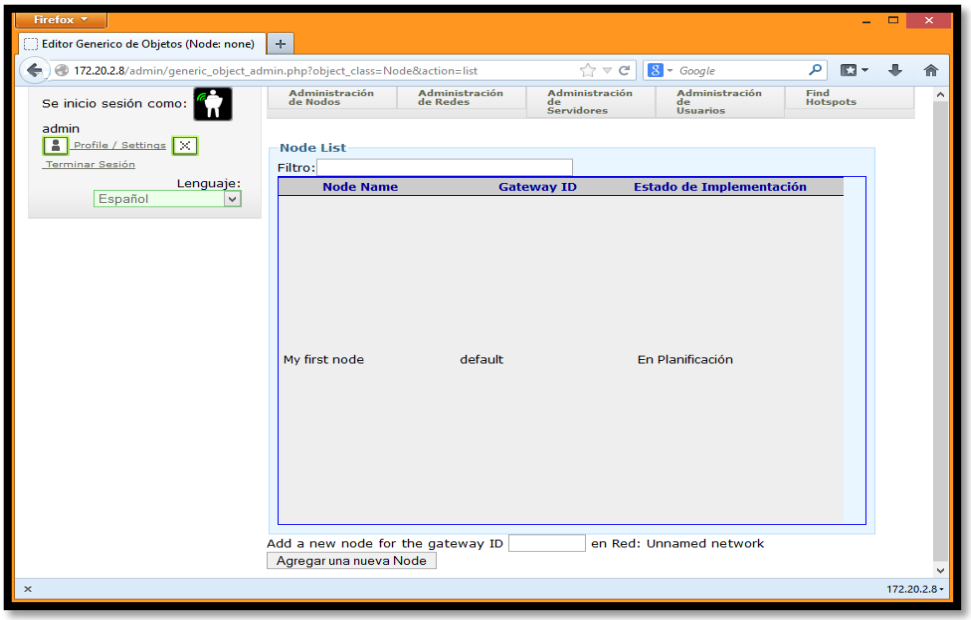


Figura 230 Creación de My first node

Fuente: Menú de opciones de configuración de Wifidog

Se hace clic en “My first node” y luego se rellena el formulario. El Gateway ID debe coincidir con el ID configurado en el archivo “/usr/local/etc/wifidog.conf”. Una vez que hemos llenado los parámetros importantes nos vamos a la parte inferior y hacemos clic en “Guardar Node”. Dentro de este parámetro tenemos los siguientes campos:

- Estadísticas
- Contenido del Nodo
- Información acerca del nodo
- Data de GIS
- Configuración del nodo
- Derechos de acceso

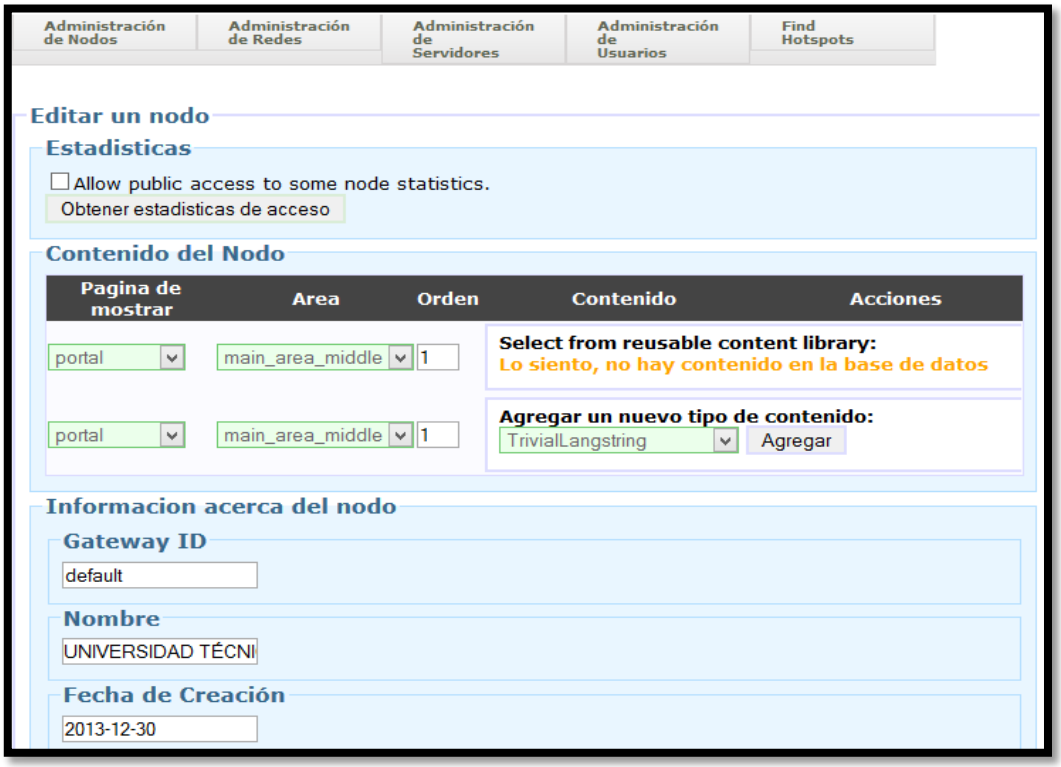


Figura 231 Editar un nodo parte 1

Fuente: Menú de opciones de configuración de Wifidog

Figura 232 Editar un nodo parte 2

Fuente: Menú de opciones de configuración de Wifidog

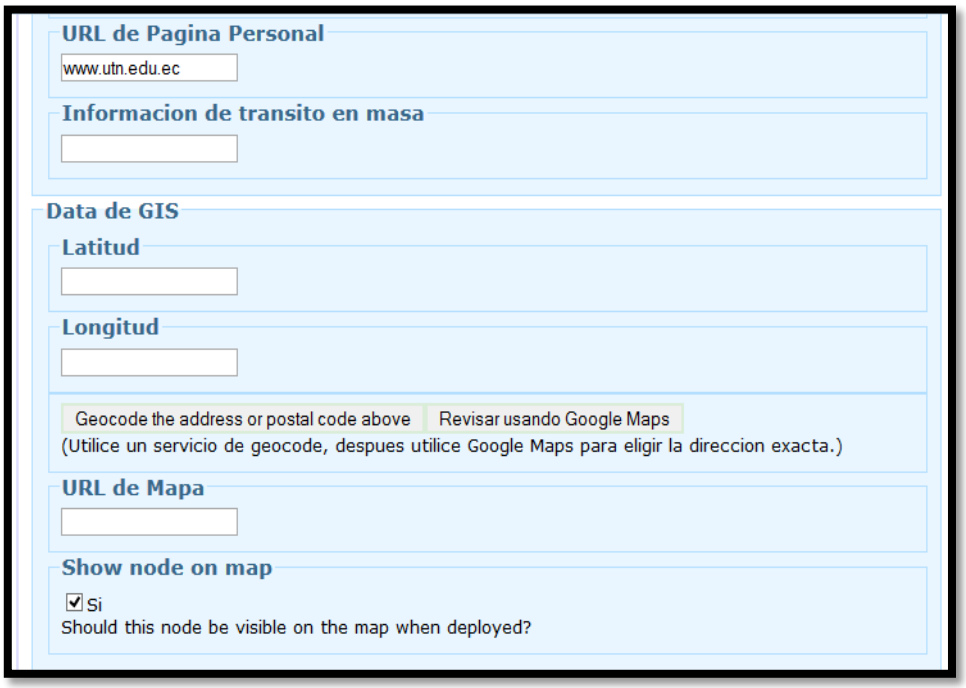


Figura 233 Editar un nodo parte 3

Fuente: Menú de opciones de configuración de Wifidog

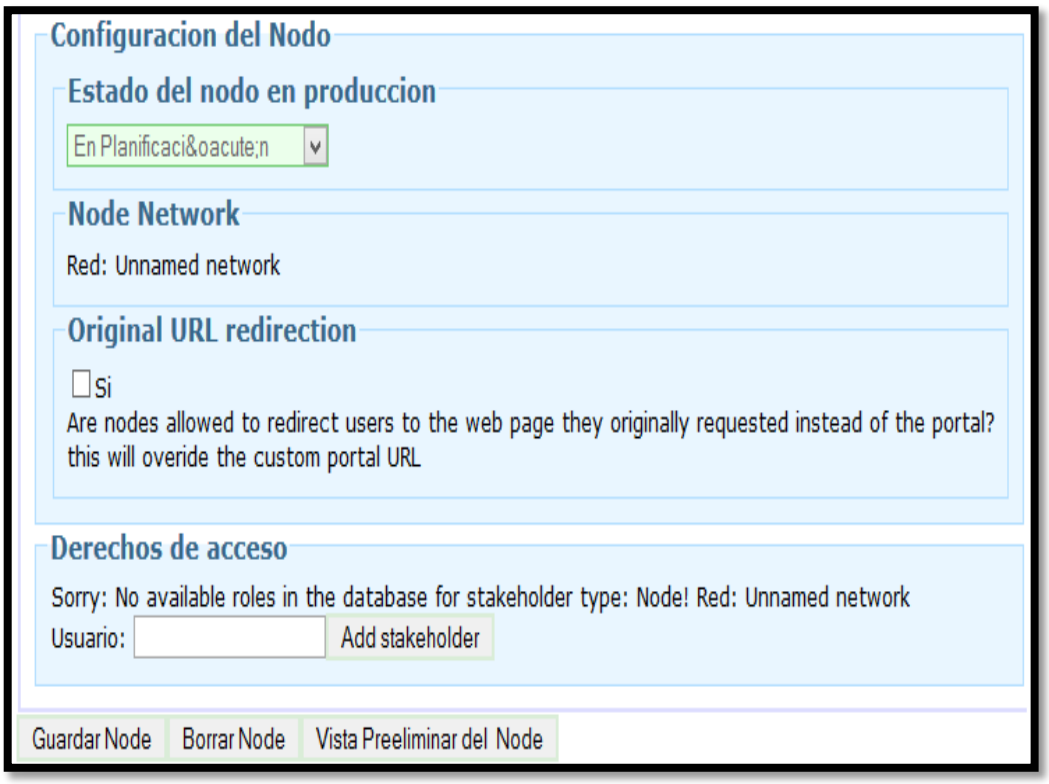


Figura 234 Editar un nodo parte 4

Fuente: Menú de opciones de configuración de Wifidog

Ahora se selecciona del menú de opciones “Administración de redes” y luego se hace clic en “Editar Unnamed network”. Dentro de este parámetro se tiene los siguientes campos:

- Contenido del Nodo
- Información acerca de la red
- Propiedades de red (Tema seleccionado para esta red)
- Autenticación de red
- Propiedades de nodo de la red
- Verificación de usuario de red
- Dynamic Abuse Control
- Derechos de Acceso
- Data de GIS

Figura 235 Editar una red parte 1

Fuente: Menú de opciones de configuración de Wifidog

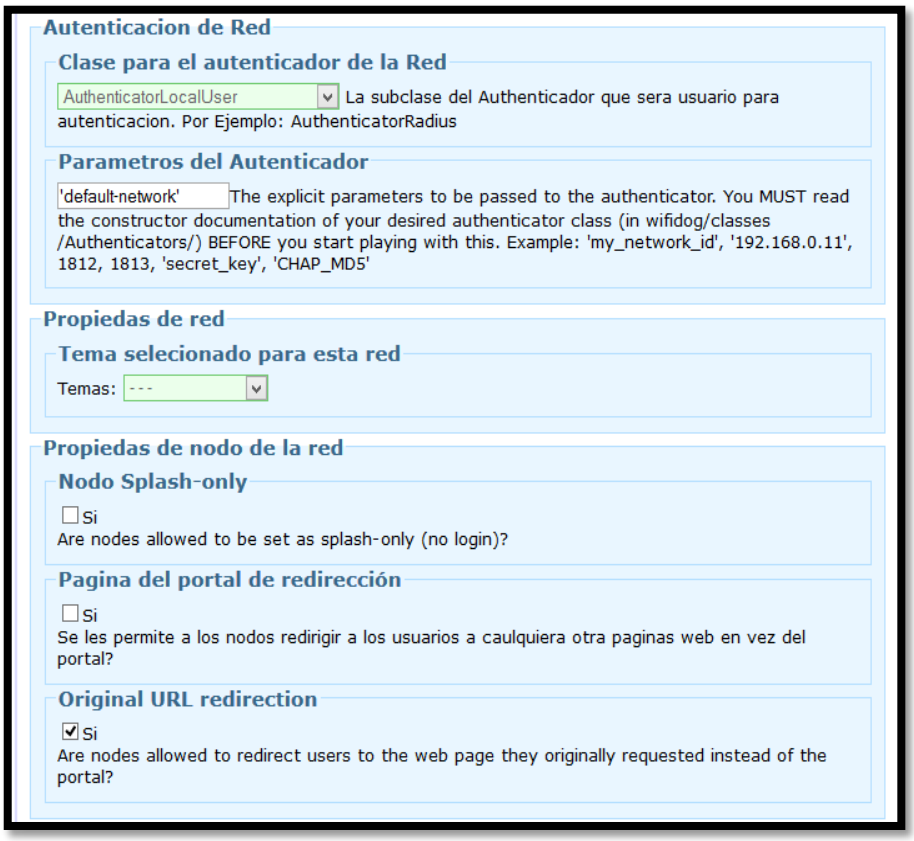


Figura 236 Editar una red parte 2

Fuente: Menú de opciones de configuración de Wifidog

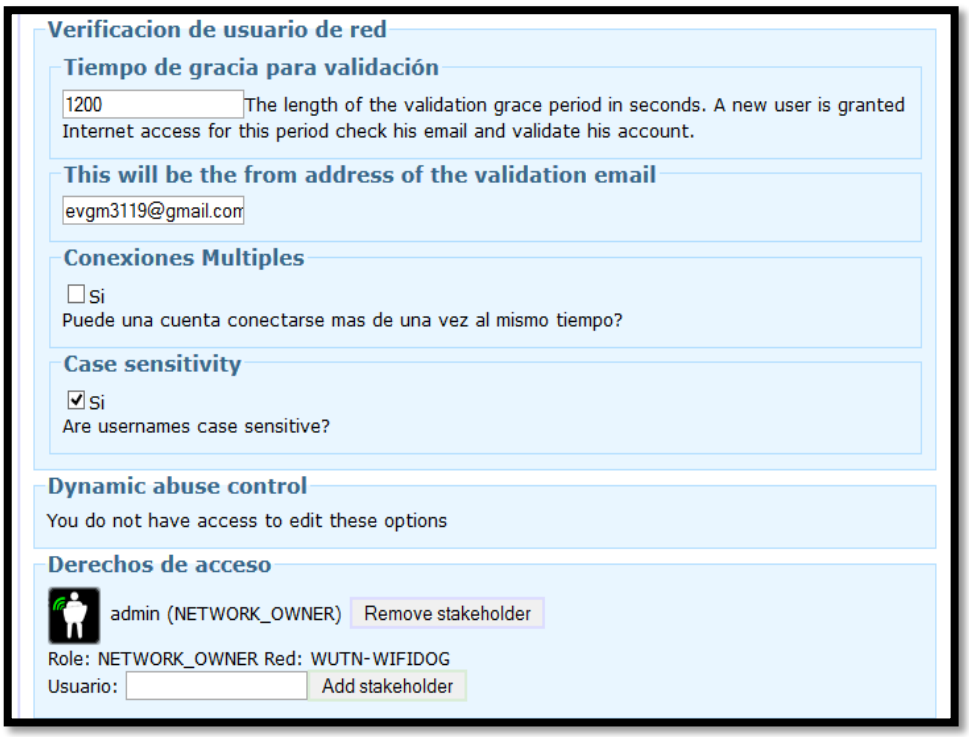


Figura 237 Editar una red parte 3

Fuente: Menú de opciones de configuración de Wifidog

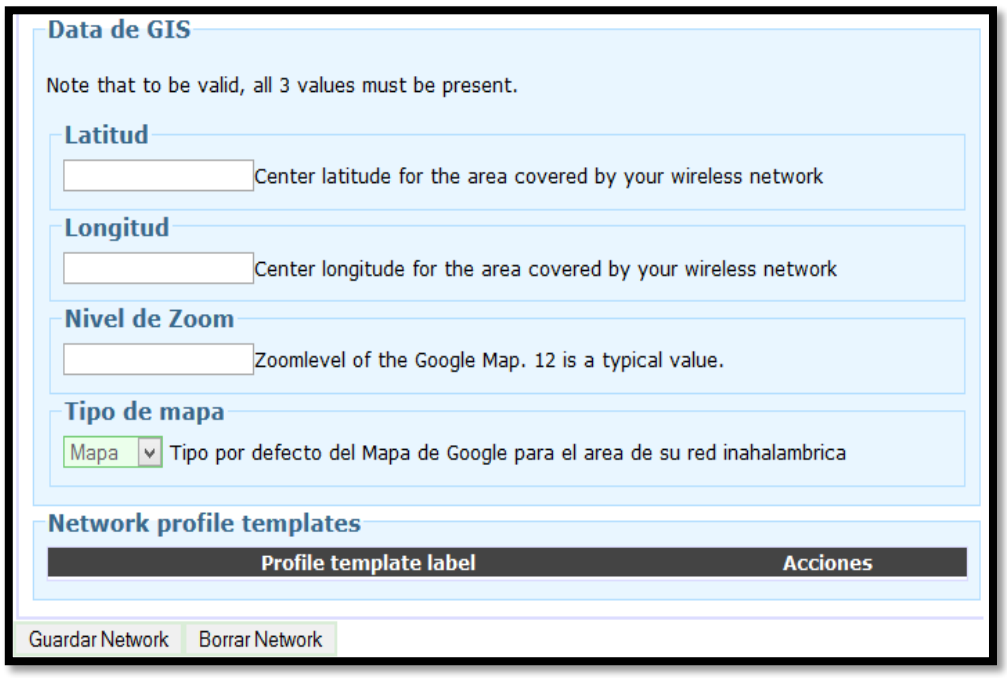


Figura 238 Editar una red parte 4

Fuente: Menú de opciones de configuración de Wifidog

En el campo “Propiedades de red” podemos seleccionar un tema para esta red de dos opciones:

- Île Sans Fil
- NetworkFusion (Tema seleccionado que se muestra en la siguiente Figura 239).

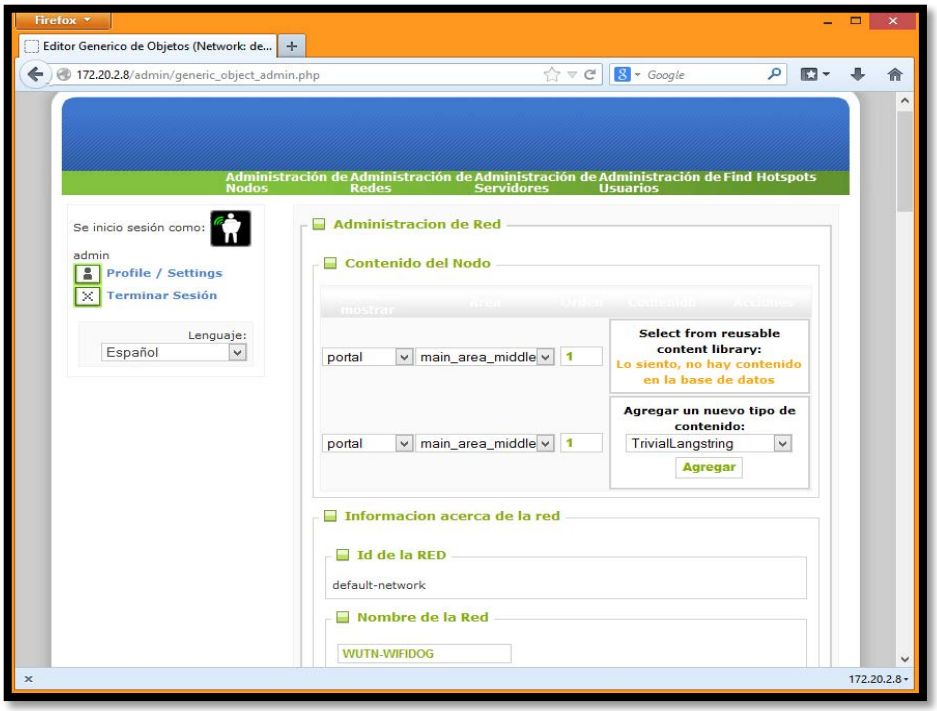


Figura 239 Tema seleccionado NetworkFusion

Fuente: Menú de opciones de configuración de Wifidog

Configuración de un Cliente

En la máquina que hemos establecido como cliente, podremos notar que el servidor DHCP está funcionando y que nos ha dado una IP para trabajar en la red, como se muestra en la Figura 240 y Figura 241.

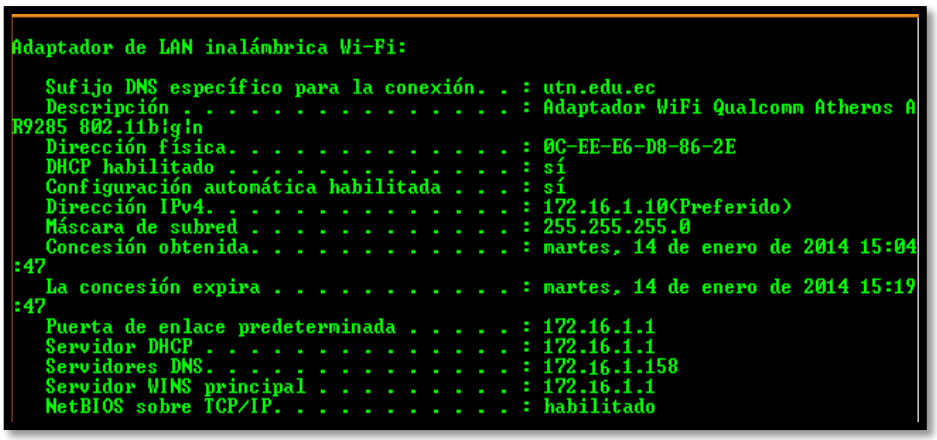


Figura 240 Información de Red

Fuente: Terminal de Windows del Cliente

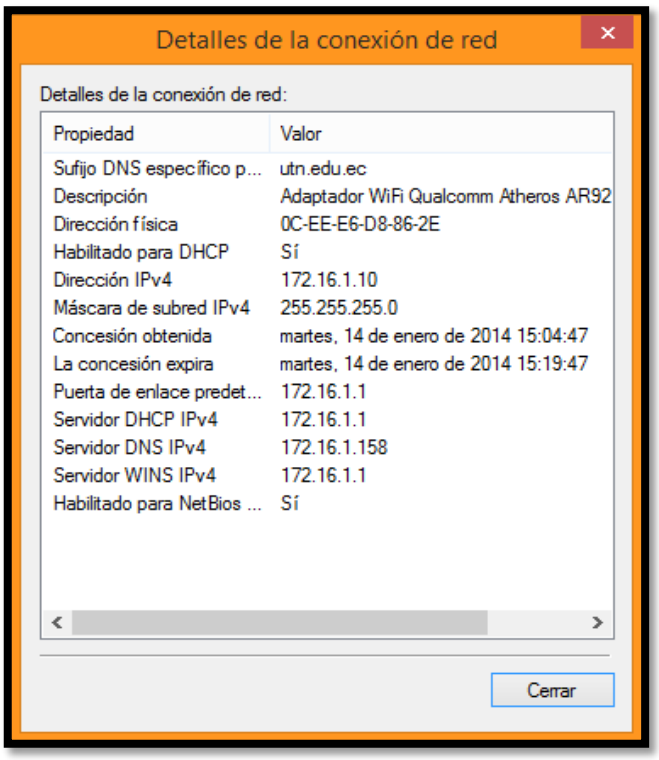


Figura 241 Detalles de la conexión de red

Fuente: Estado de la Tarjeta de red del Cliente

Una vez que tenemos direccionamiento IP, abrimos un navegador como Internet Explorer, Mozilla, Opera o Chrome e ingresamos a cualquier página web, como por ejemplo “www.google.com”. Una vez hecho esto se nos desplegara la página del portal cautivo Wifidog, como se indica en la Figura 242

.

Figura 242 Proceso de autenticación ofrecido por el servidor para el cliente

Fuente: Navegador web del cliente

En las opciones del portal cautivo nos permite ingresar nuestro nombre de usuario ó cuenta de email y la contraseña (Figura 243), en caso de ser clientes ya registrados. Caso contrario el portal cautivo nos brinda la oportunidad de crear una nueva cuenta para los usuarios nuevos. Debemos tener en cuenta algo importante que mientras no se ingrese usuario y contraseña no permitirá navegar a Internet.

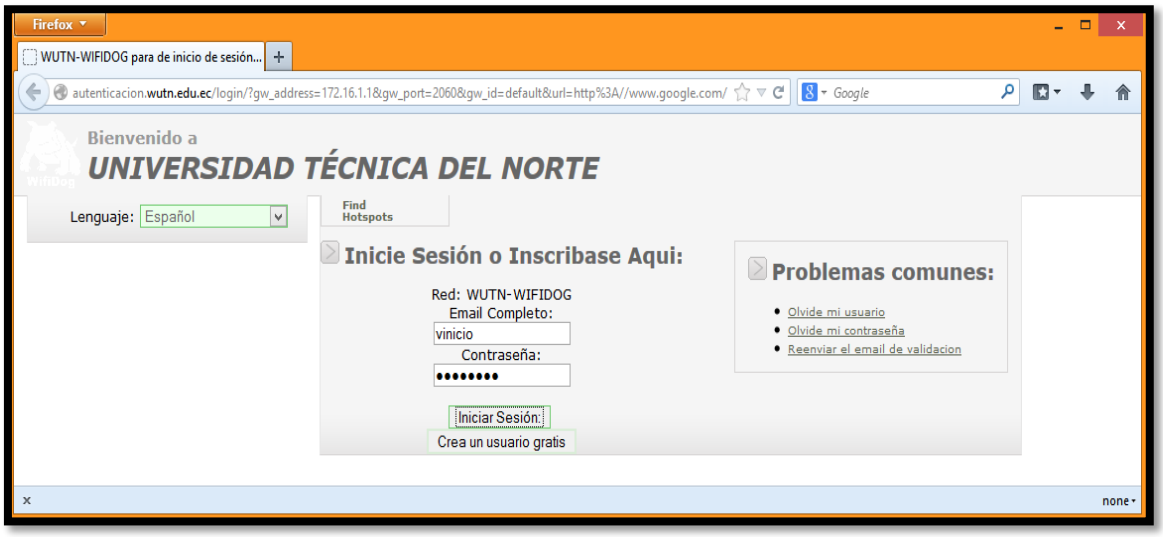


Figura 243 Proceso de Autenticación del Portal Cautivo

Fuente: Navegador web del cliente

Una vez ingresado correctamente el nombre y contraseña podemos navegar normalmente. Si es un nuevo usuario hacemos clic en “Crea un usuario gratis” e ingresamos los datos que nos solicita el portal cautivo, como se indica en la Figura 244.

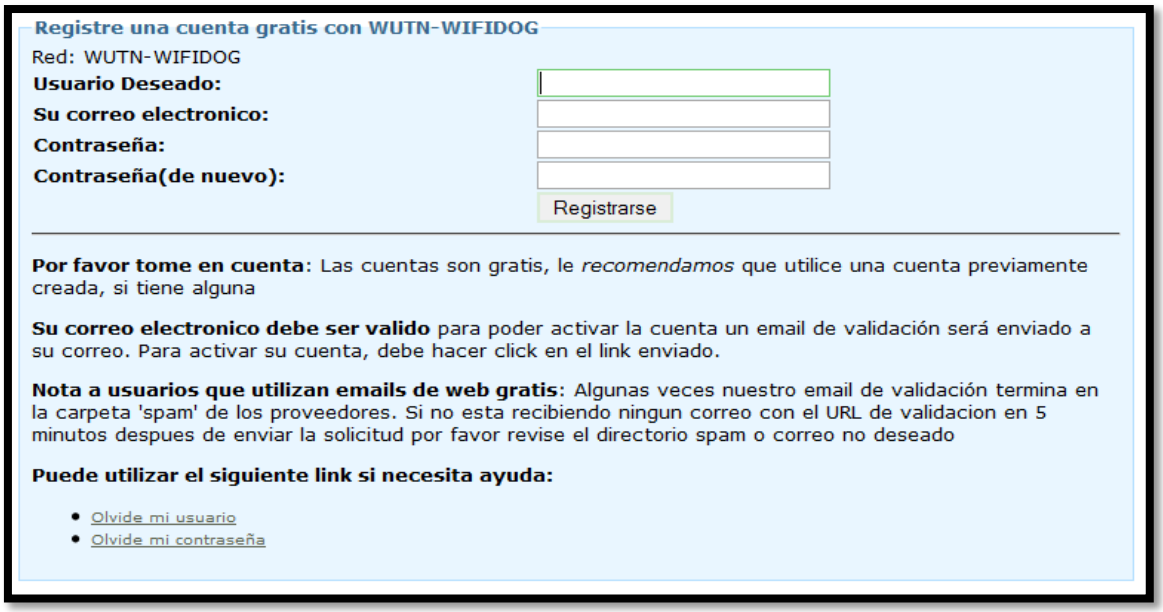


Figura 244 Creación de nueva cuenta

Fuente: Navegador web del cliente

Haciendo clic en “Registrarse”, nos indica que se tiene que validar la cuenta para un acceso permanente, mientras tanto la red le concede 20 minutos de navegación gratis.

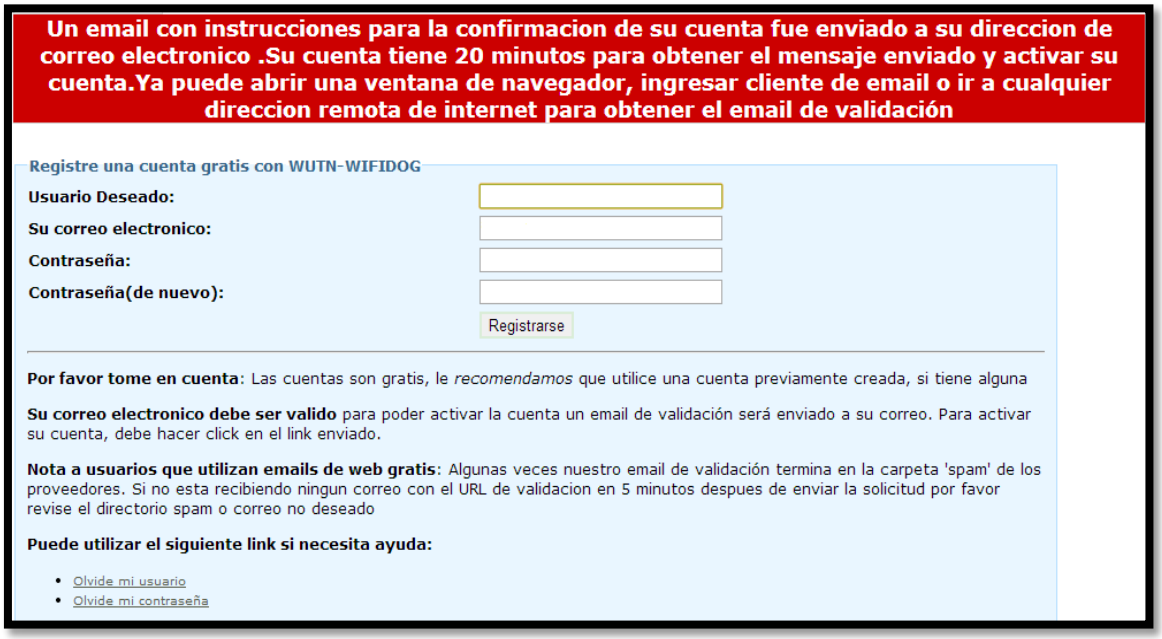


Figura 245 Aviso de validación y periodo de gracia

Fuente: Navegador web del cliente

Validación de una Cuenta como Administrador

Para poder validar una cuenta de usuario debemos ingresar con la cuenta de administrador que se configuró en la instalación. Posterior a ello nos dirigimos al menú de “Administración de usuarios” y damos clic en “User manager”. Claramente la Figura 246 nos indica que el estado de la cuenta del usuario “vinicio” que pertenece a la red “default-network” está por ser validado por el administrador.

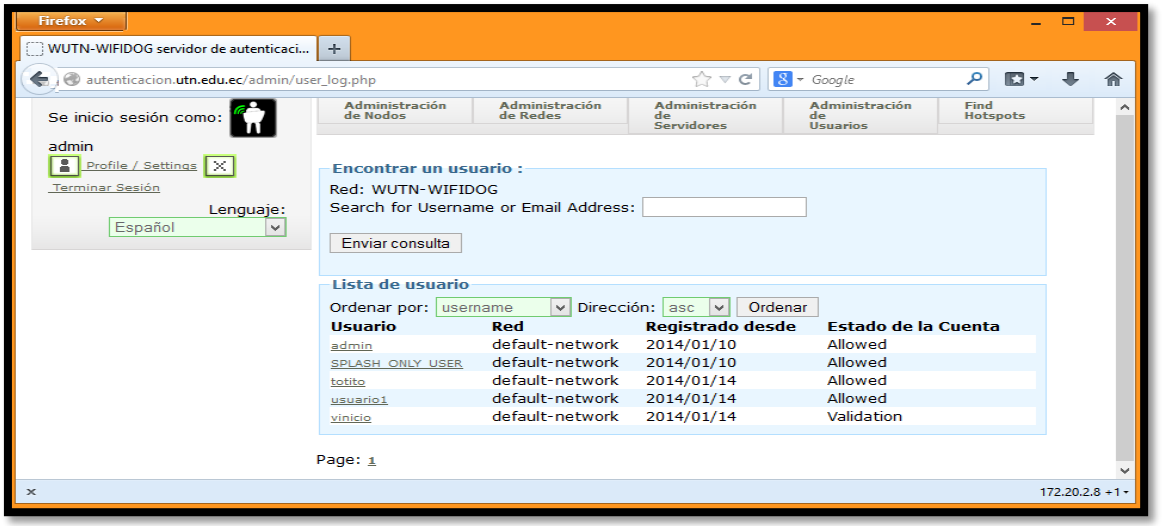


Figura 246 Administración de usuarios

Fuente: Menú de opciones de configuración de Wifidog

Haciendo clic en la cuenta de usuario que queremos validar nos despliega una ventana con varias opciones para el Estado de la cuenta, de todas ellas, que se indican a continuación seleccionaremos “Allowed” y “Guardar user”.

- Error
- Denied
- Allowed
- Validation
- Validation Failed
- Locked

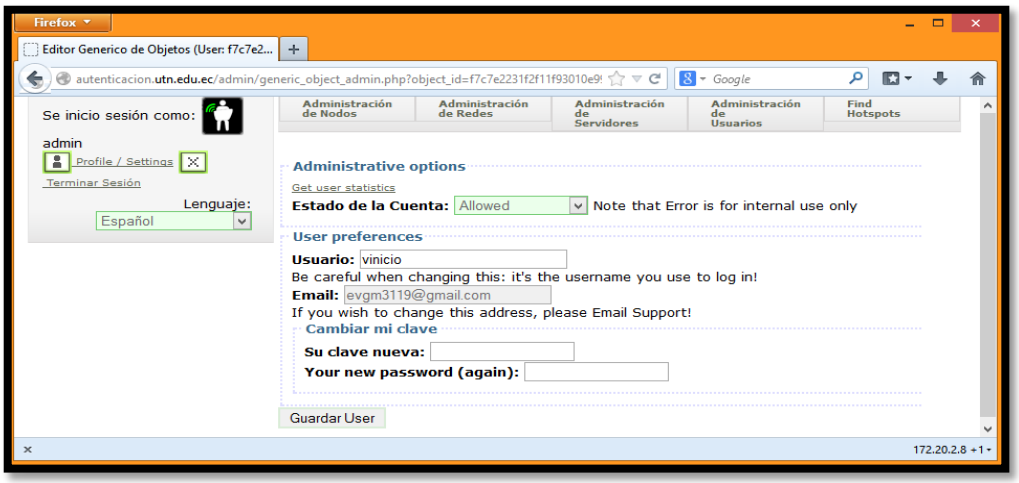


Figura 247 Validación de la cuenta al cliente vinicio

Fuente: Menú de opciones de configuración de Wifidog

La Figura 248 a continuación muestra la conectividad con el Gateway, lo que permite acceder a Internet.

- ping 192.168.1.1

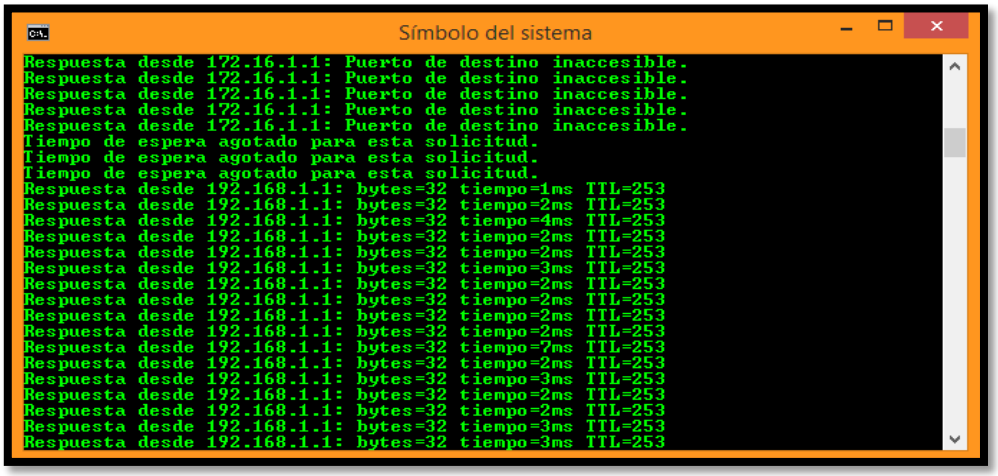


Figura 248 Conectividad a la Dirección IP del Gateway

Fuente: Terminal de Windows del Cliente

Validación de una Cuenta por Correo Electrónico

Una vez que se ha llenado los datos de la Figura 244 y se ha hecho clic en “Registrarse” automáticamente nuestro relay del servidor de correo Postfix enviará a la dirección de correo del cliente un enlace de confirmación de la cuenta tal como se indica en la Figura 249.

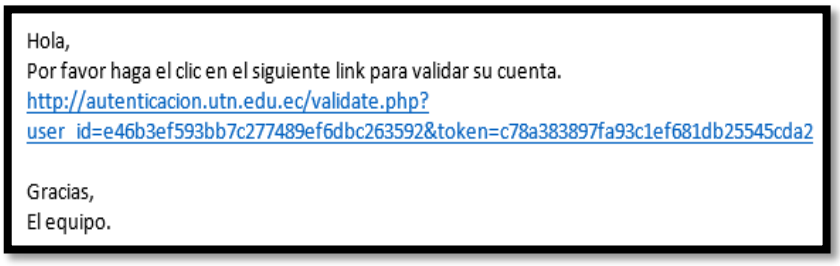


Figura 249 Link de validación de la cuenta del cliente que se ha registrado

Fuente: Correo Electrónico del cliente

Wifidog interactúa con un servidor de correos y envía al mail de registro un link para validar la nueva cuenta. Si en caso de no validar la cuenta dentro del periodo de gracia que es de 20 minutos, no podrá navegar a Internet porque la validación del correo y la cuenta han expirado como se indica en la Figura 250

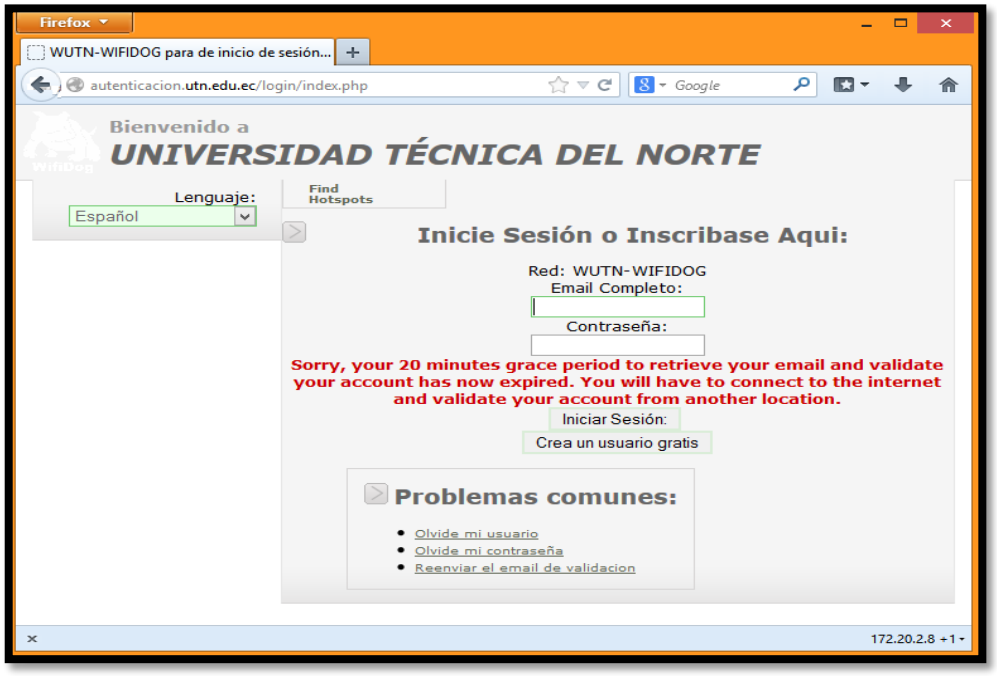


Figura 250 Proceso de validación expirado

Fuente: Navegador web del cliente

Control de Ancho de Banda

Después de editar el primer nodo en el servidor, es necesario modificar el perfil del administrador en el menú “Administración de servidores - User Roles – Editar Roles” y habilitar la opción “NETWORK_PERM_EDIT_DYNAMIC_ABUSE_CONTROL” para que pueda modificar las configuraciones de control de abuso y saturación de red.

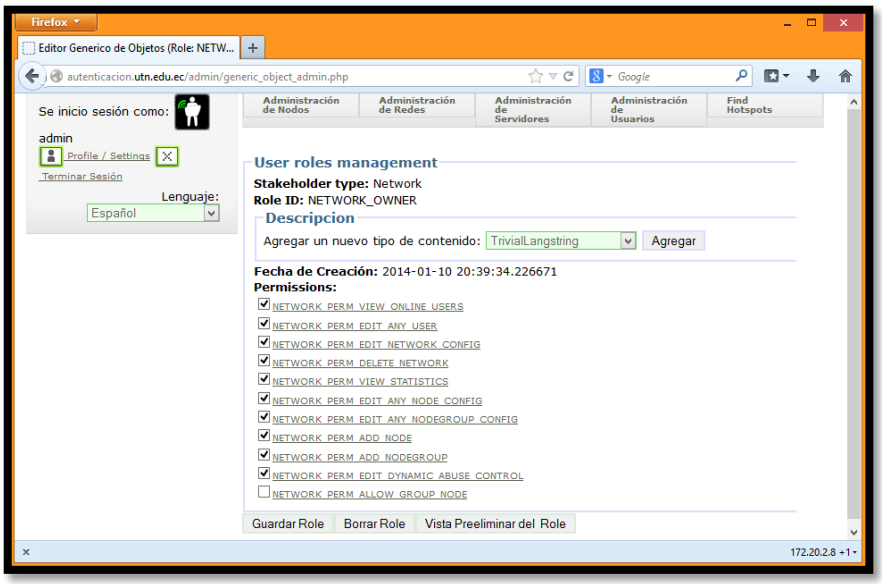


Figura 251 Configuración de roles de usuario

Fuente: Menú de opciones de configuración de Wifidog

Wifidog provee algunas formas de establecer una autenticación del usuario. Para este proyecto se ha utilizado la autenticación interna, que utiliza información guardada en la base de datos PostgreSQL para registrar nuevos usuarios o para identificar usuarios existentes. Además de este tipo de autenticación, Wifidog permite establecer comunicación con servidores LDAP y RADIUS que pueden estar configurados en el mismo servidor o en uno externo. Con la configuración básica se puede denegar el registro de nuevos usuarios, permitiendo así solamente el uso de usuarios internos o simplemente manejar el ancho de banda de los usuarios sin necesidad de que inicien sesión en el servidor.

El control de ancho de banda y el tiempo de navegación es una de las características más importantes del sistema de Portal Cautivo Wifidog, ya que con esta característica se puede controlar la cantidad de ancho de banda que un usuario puede utilizar en un nodo y en una red en general, además permite definir el tiempo máximo de duración de una conexión. Si un usuario sobrepasa el límite de alguna de estas características se le denegara el uso de la red automáticamente. Otra característica es que pasado el tiempo definido por el administrador los contadores volverán a estar en cero y el usuario podrá volver a trabajar con la red. Esta característica se llama “Abuse Control” y se configura de la siguiente manera.

Tabla 74 Control de conexiones con Dynamic Abuse Control

TIPO DE CONTRO	PARÁMETRO	ESCRIPCIÓN
Abuse control window	1 day	Lapso de tiempo para que los contadores se reinicien en 0.
Network max total bytes Transfered	500000000	Máximo de ancho de banda permitido para enviar y recibir en la red en Bytes (500 MB).
Network max connection Duration	08:00:00	Duración máxima permitida de una conexión en la red, hasta que los contadores se reinicien en 0 (8 horas).
Node max total bytes transfered	100000000	Máximo ancho de banda permitido para enviar y recibir en el nodo en que se conecta el cliente (100 MB).
Node max connection duration	02:00:00	Duración máxima permitida de una conexión en un nodo, hasta que los contadores se reinicien en 0 (2 horas).

Fuente: Menú de opciones de configuración de Wifidog

Cada vez que un usuario se conecte a la red tendrá un máximo de 100 MB disponibles de ancho de banda en el nodo que se conecte, y de ser el caso si el usuario cambia de nodos tendrá 500 MB en toda la red. Además tendrá un máximo de conexión de 2 horas en cada nodo y 8 horas en toda la red. Estos contadores se reiniciaran diariamente.

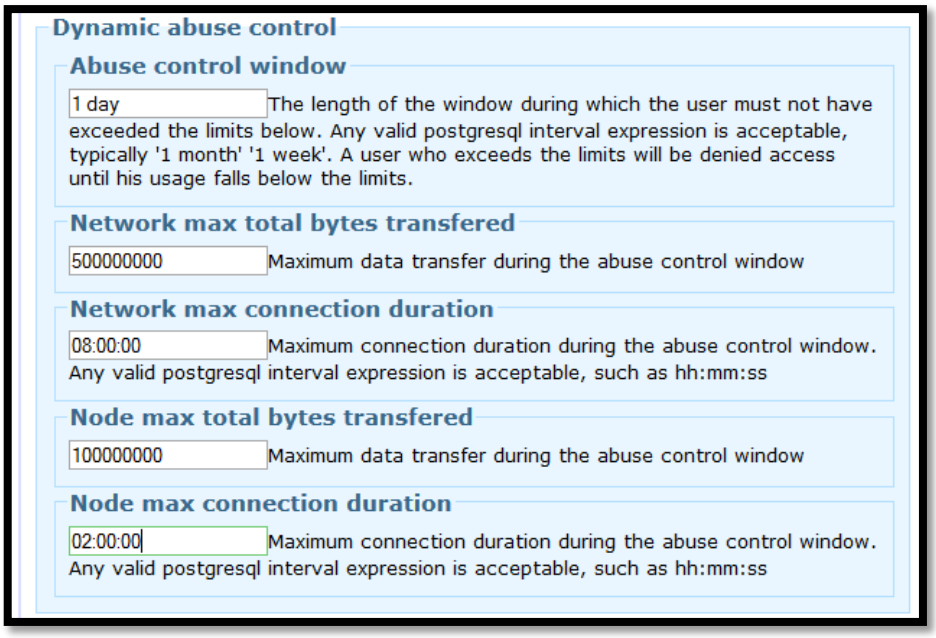


Figura 252 Configuración de Dynamic abuse control para control de ancho de banda y tiempo de conexión de cada usuario

Fuente: Menú de opciones de configuración de Wifidog

Para finalizar la configuración de “Dynamic Abuse Control” es necesario insertar un aviso para que cuando el usuario se conecte a la red sea informado del ancho de banda disponible y el utilizado así como el tiempo que lleva conectado en la red. Para esto se debe agregar el tipo de contenido “*UIAllowedBandwidth*” en la página de configuración de la red.

Figura 253 Agregar un nuevo tipo de contenido de Dynamic Abuse Control

Fuente: Menú de opciones de configuración de Wifidog

Al igual que la ventana de “Abuse Control” es posible agregar diferentes tipos de contenido y publicarlos en la página principal del portal cautivo o en la página que aparece después de haber iniciado sesión.

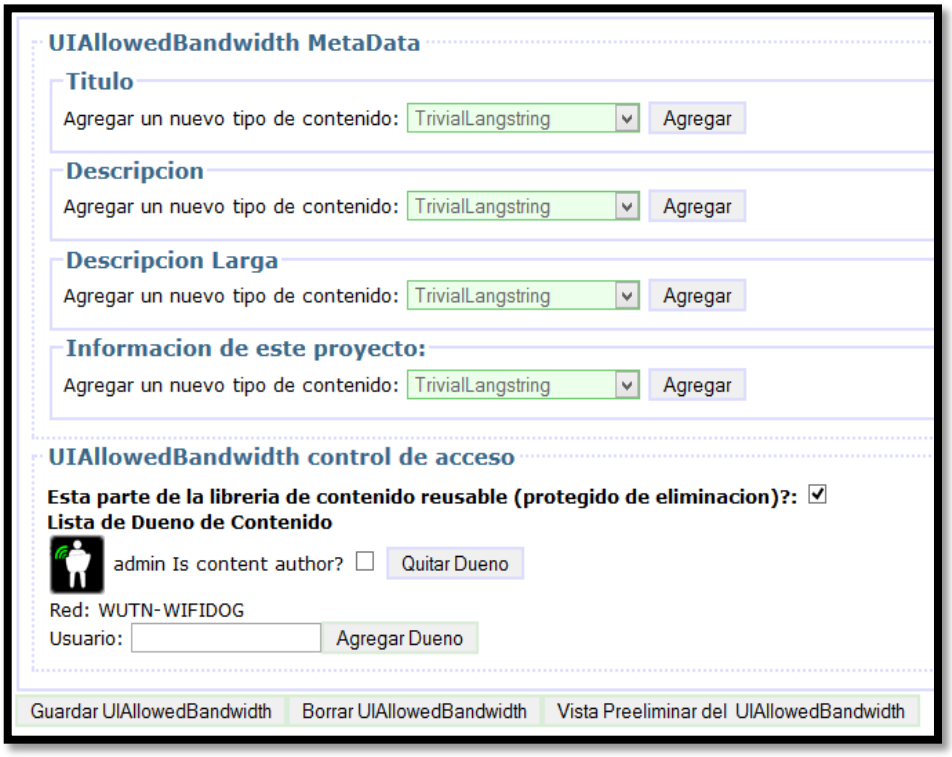


Figura 254 Edición de contenido de publicación a los clientes

Fuente: Menú de opciones de configuración de Wifidog

Al finalizar las configuraciones anteriormente descritas, el Servidor de Autenticación del Portal Cautivo Wifidog estará listo para ser utilizado.

ANEXO 8

IPTABLES PROXY PORTAL CAUTIVO WIFIDOG

```
#!/bin/sh
# IPTABLES PROXY script for the Linux 2.4 kernel.
# This script is a derivitive of the script presented in
# the IP Masquerade HOWTO page at:
# www.tldp.org/HOWTO/IP-Masquerade-HOWTO/firewall-examples.html
# It was simplified to coincide with the configuration of
# the sample system presented in the Guides section of
# www.aboutdebian.com
# This script is presented as an example for testing ONLY
# and should not be used on a production proxy server.
# PLEASE SET THE USER VARIABLES
# IN SECTIONS A AND B OR C
echo -e "\n\nSETTING UP IPTABLES PROXY..."

# === SECTION A ===
# FOR EVERYONE SET THE INTERFACE DESIGNATION FOR THE NIC CONNECTED TO YOUR INTERNAL NETWORK
# The default value below is for "eth0". This value
# could also be "eth1" if you have TWO NICs in your system.
# You can use the ifconfig command to list the interfaces
# on your system. The internal interface will likely have
# have an address that is in one of the private IP address
# ranges.
# Note that this is an interface DESIGNATION - not
# the IP address of the interface.
# Enter the internal interfaces designation for the INTIF variable

INTIF="eth1"

# SET THE INTERFACE DESIGNATION FOR YOUR "EXTERNAL" (INTERNET) CONNECTION
# The default value below is "ppp0" which is appropriate
# for a MODEM connection.
# If you have two NICs in your system change this value
```

```
# to "eth0" or "eth1" (whichever is opposite of the value
# set for INTIF above). This would be the NIC connected
# to your cable or DSL modem (WITHOUT a cable/DSL router).
# Note that this is an interface DESIGNATION - not
# the IP address of the interface.
# Enter the external interfaces designation for the EXTIF variable:

EXTIF="eth0"

# ! ! ! ! ! Use ONLY Section B *OR* Section C depending on
# ! ! ! ! the type of Internet connection you have.
# === SECTION B
# ----------- FOR THOSE WITH STATIC PUBLIC IP ADDRESSES
# SET YOUR EXTERNAL IP ADDRESS
# If you specified a NIC (i.e. "eth0" or "eth1" for
# the external interface (EXTIF) variable above,
# AND if that external NIC is configured with a
# static, public IP address (assigned by your ISP),
# UNCOMMENT the following EXTIP line and enter the
# IP address for the EXTIP variable:

EXTIP="172.16.2.8"

# === SECTION C
# ---------- DIAL-UP MODEM, AND RESIDENTIAL CABLE-MODEM/DSL (Dynamic IP)
USERS
# SET YOUR EXTERNAL INTERFACE FOR DYNAMIC IP ADDRESSING
# If you get your IP address dynamically from SLIP, PPP,
# BOOTP, or DHCP, UNCOMMENT the command below.
# (No values have to be entered.)
# Note that if you are uncommenting these lines then
# the EXTIP line in Section B must be commented out.
#EXTIP="`/sbin/ifconfig ppp0 | grep 'inet addr' | awk '{print $2}' | sed -e 's/.*://'`"
# -------- No more variable setting beyond this point --------

echo "Loading required stateful/NAT kernel modules..."
/sbin/depmod -a
/sbin/modprobe ip_tables
/sbin/modprobe ip_conntrack
```

```
/sbin/modprobe ip_conntrack_ftp
/sbin/modprobe ip_conntrack_irc
/sbin/modprobe iptable_nat
/sbin/modprobe ip_nat_ftp
/sbin/modprobe ip_nat_irc
echo " Enabling IP forwarding..."
echo "1" > /proc/sys/net/ipv4/ip_forward
echo "1" > /proc/sys/net/ipv4/ip_dynaddr
echo " External interface: $EXTIF"
echo " External interface IP address is: $EXTIP"
echo " Loading proxy server rules..."

# Clearing any existing rules and setting default policy

iptables -P INPUT ACCEPT
iptables -F INPUT
iptables -P OUTPUT ACCEPT
iptables -F OUTPUT
iptables -P FORWARD DROP
iptables -F FORWARD
iptables -t nat -F

#This is where you would probably want to put rules banning MAC addresses of naughty
users

#################################################################
## Permitir todas las conexiones de salida que existen ##
##### Y se relacionan con la conexiones de entrada ######
#################################################################
iptables -A FORWARD -i $EXTIF -o $INTIF -m state --state ESTABLISHED,RELATED -j
ACCEPT
iptables -A FORWARD -i $INTIF -o $EXTIF -j ACCEPT

#################################################################
## Denegacion del Puerto 22 (SSH) a los clientes Wireless ##
#################################################################
iptables -A INPUT -p tcp -i $INTIF --dport 22 -j DROP
```

```
#########################################################################
#Enmascaramiento de la red local para que puedan salir hacia la WAN#
###### Enabling SNAT (Masquerade) funcionality on $EXTIF ############
#########################################################################
iptables -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE

echo -e " Proxy server rule loading complete\n\n"

echo -e " We are now starting the DHCP server on eth1 \n\n"
```

ANEXO 9

ARCHIVO DE CONFIGURACIÓN PARA EL GATEWAY DE WIFIDOG

```
# $Id: wifidog.conf 1375M 2009-09-25 14:56:55Z (local) $
# WiFiDog Configuration file

# Parameter: GatewayID
# Default: default
# Optional
#
# Set this to the node ID on the auth server
# This is used to give a customized login page to the clients and for
# monitoring/statistics purpose. If you run multiple gateways on the same
# machine each gateway needs to have a different gateway id.
# If none is supplied, the mac address of the GatewayInterface interface will be used,
# without the : separators

GatewayID default

# Parameter: ExternalInterface
# Default: NONE
# Optional
#
# Set this to the external interface (the one going out to the Inernet or your larger LAN).
# Typically vlan1 for OpenWrt, and eth0 or ppp0 otherwise,
# Normally autodetected

ExternalInterface eth0

# Parameter: GatewayInterface
# Default: NONE
# Mandatory
#
# Set this to the internal interface (typically your wifi interface).
# Typically br0 for whiterussian, br-lan for kamikaze (by default the wifi interface is bridged
with wired lan in openwrt)
# and eth1, wlan0, ath0, etc. otherwise
# You can get this interface with the ifconfig command and finding your wifi interface
```

```
GatewayInterface eth1

# Parameter: GatewayAddress
# Default: Find it from GatewayInterface
# Optional
#
# Set this to the internal IP address of the gateway.  Not normally required.

#GatewayAddress 172.16.2.8

# Parameter: HtmlMessageFile
# Default: wifidog-msg.html
# Optional
#
# This allows you to specify a custome HTML file which will be used for
# system errors by the gateway. Any $title, $message and $node variables
# used inside the file will be replaced.
#
# HtmlMessageFile /opt/wifidog/etc/wifidog-.html
HtmlMessageFile /usr/local/wifidog/wifidog-msg.html

# Parameter: AuthServer
# Default: NONE
# Mandatory, repeatable
#
# This allows you to configure your auth server(s).  Each one will be tried in order, untill
one responds.
# Set this to the hostname or IP of your auth server(s), the path where
# WiFiDog-auth resides in and the port it listens on.
#AuthServer {
#       Hostname                (Mandatory; Default: NONE)
#       SSLAvailable            (Optional; Default: no; Possible values: yes, no)
#       SSLPort                 (Optional; Default: 443)
#       HTTPPort                (Optional; Default: 80)
#       Path                    (Optional; Default: /wifidog/ Note:  The path must be both prefixed
and suffixed by /.  Use a sin$
```

```
#   LoginScriptPathFragment  (Optional; Default: login/? Note:  This is the script the user will be sent to for login.)
#   PortalScriptPathFragment (Optional; Default: portal/? Note:  This is the script the user will be sent to after a successfull l$
#   MsgScriptPathFragment    (Optional; Default: gw_message.php? Note:  This is the script the user will be sent to upon error to $
#   PingScriptPathFragment    (Optional; Default: ping/? Note:  This is the script the user will be sent to upon error to read a r$
#   AuthScriptPathFragment    (Optional; Default: auth/? Note:  This is the script the user will be sent to upon error to read a r$
#}

AuthServer {
    Hostname autenticacion.utn.edu.ec
    SSLAvailable no
    Path /
}

#AuthServer {
#    Hostname auth2.ilesansfil.org
#    SSLAvailable yes
#    Path /
#}

# Parameter: Daemon
# Default: 1
# Optional
#
# Set this to true if you want to run as a daemon
# Daemon 1

# Parameter: GatewayPort
# Default: 2060
# Optional
#
# Listen on this port
#GatewayPort 2060
```

```
# Parameter: HTTPDName
# Default: WiFiDog
# Optional
#
# Define what name the HTTPD server will respond
#HTTPDName default

# Parameter: HTTPDMaxConn
# Default: 10
# Optional
#
# How many sockets to listen to
# HTTPDMaxConn 10

# Parameter: HTTPDRealm
# Default: WiFiDog
# Optional
#
# The name of the HTTP authentication realm. This only used when a user
# tries to access a protected WiFiDog internal page. See HTTPUserName.
# HTTPDRealm WiFiDog

# Parameter: HTTPDUserName / HTTPDPassword
# Default: unset
# Optional
#
# The gateway exposes some information such as the status page through its web
# interface. This information can be protected with a username and password,
# which can be set through the HTTPDUserName and HTTPDPassword parameters.
# HTTPDUserName admin
# HTTPDPassword secret

# Parameter: CheckInterval
# Default: 60
# Optional
#
```

```
# How many seconds should we wait between timeout checks.  This is also
# how often the gateway will ping the auth server and how often it will
# update the traffic counters on the auth server.  Setting this too low
# wastes bandwidth, setting this too high will cause the gateway to take
# a long time to switch to it's backup auth server(s).

CheckInterval 60

# Parameter: ClientTimeout
# Default: 5
# Optional
#
# Set this to the desired of number of CheckInterval of inactivity before a client is logged
out
# The timeout will be INTERVAL * TIMEOUT
ClientTimeout 100

# Parameter: TrustedMACList
# Default: none
# Optional
#
# Comma separated list of MAC addresses who are allowed to pass
# through without authentication
#TrustedMACList 00:00:DE:AD:BE:AF,00:00:C0:1D:F0:0D

# Parameter: FirewallRuleSet
# Default: none
# Mandatory
#
# Groups a number of FirewallRule statements together.

# Parameter: FirewallRule
# Default: none
#
# Define one firewall rule in a rule set.

# Rule Set: global
#
```

```
# Used for rules to be applied to all other rulesets except locked.
FirewallRuleSet global {
    ## To block SMTP out, as it's a tech support nightmare, and a legal liability
    #FirewallRule block tcp port 25

    ## Use the following if you don't want clients to be able to access machines on
    ## the private LAN that gives internet access to wifidog.  Note that this is not
    ## client isolation;  The laptops will still be able to talk to one another, as
    ## well as to any machine bridged to the wifi of the router.
    # FirewallRule block to 192.168.0.0/16
    # FirewallRule block to 172.16.0.0/12
    # FirewallRule block to 10.0.0.0/8

    ## This is an example ruleset for the Teliphone service.
    #FirewallRule allow udp to 69.90.89.192/27
    #FirewallRule allow udp to 69.90.85.0/27
    #FirewallRule allow tcp port 80 to 69.90.89.205
}

# Rule Set: validating-users
#
# Used for new users validating their account
FirewallRuleSet validating-users {
    FirewallRule allow to 0.0.0.0/0
}

# Rule Set: known-users
#
# Used for normal validated users.
FirewallRuleSet known-users {
    FirewallRule allow to 0.0.0.0/0
}

# Rule Set: unknown-users
#
# Used for unvalidated users, this is the ruleset that gets redirected.
#
```

```
# XXX The redirect code adds the Default DROP clause.
FirewallRuleSet unknown-users {
    FirewallRule allow udp port 53
    FirewallRule allow tcp port 53
    FirewallRule allow udp port 67
    FirewallRule allow tcp port 67
}

# Rule Set: locked-users
#
# Not currently used
FirewallRuleSet locked-users {
    FirewallRule block to 0.0.0.0/0
}
```

ANEXO 10
INSTALACIÓN DEL SISTEMA OPERATIVO CENTOS 6

PROCEDIMIENTO DE INSTALACIÓN DEL SISTEMA OPERATIVO CENTOS 6.5

Antes de comenzar, determine primero los siguientes puntos:

- **Finalidad productiva**: ¿Va ser un servidor, estación de trabajo o escritorio? ¿Qué uso va tener el equipo? ¿Qué servicios va a requerir? Idealmente lo que se establezca en este punto debe prevalecer sin modificaciones a lo largo de su ciclo productivo.
- **Ciclo de producción**. ¿Cuánto tiempo considera que estará en operación el equipo? ¿Seis meses, un año, dos años, cinco años?

- **Capacidad del equipo**. ¿A cuántos usuarios simultáneos se brindará servicio? ¿Tiene el equipo la cantidad suficiente de RAM y poder de procesamiento suficiente?

- **Particiones del disco duro**. Determine cómo administrará el espacio disponible de almacenamiento.

- **Limitaciones**. Tenga claro que CentOS al igual que sucede con Red Hat Enterprise Linux es un sistema operativo diseñado y enfocado específicamente para ser utilizado como sistema operativo en servidores, desarrollo de programas y estaciones de trabajo. Salvo que posteriormente se añada algún almacén YUM como EPEL, Remi, AL Server o RPMFusion.

Descargue la imagen ISO del DVD de CentOS 6.5 para arquitectura i386 o bien arquitectura x86_64 (sólo es necesario el DVD 1 el cual encontrará en el siguiente URL:

- http://mirror.centos.org/centos/6/isos/

Inserte el disco DVD de instalación de CentOS 6.5 (recuerde que para ejecutar el DVD hay que configurar el BIOS) y espere 60 segundos para el inicio automático o bien pulse la tecla “ENTER” para iniciar de manera inmediata o la tecla “TAB” e ingrese a las opciones de instalación deseadas. Seleccionamos “Install or upgrade an existing system” para instalar o actualizar el sistema operativo Linux CentOS.

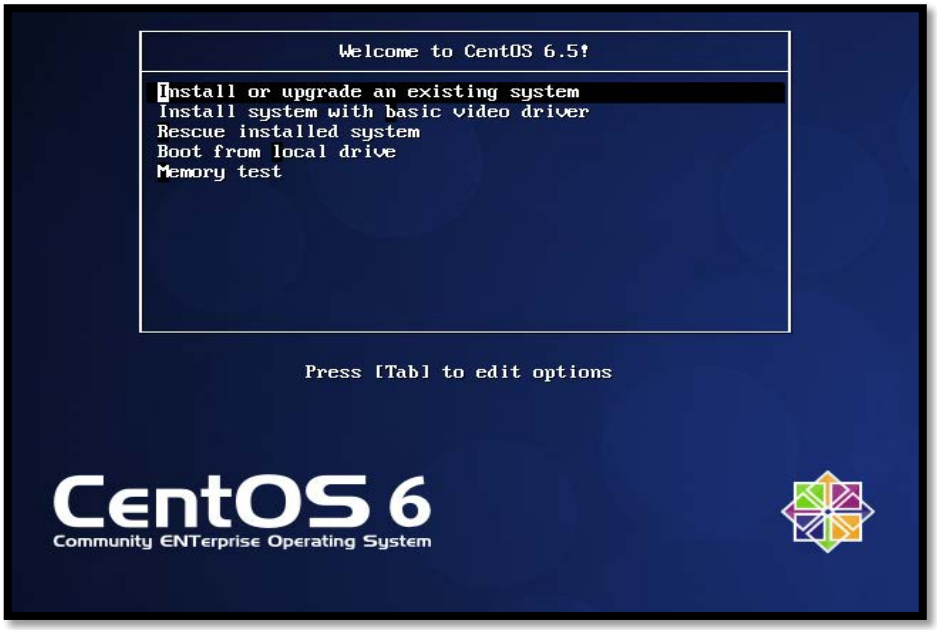


Figura 255 Opciones de instalación del sistema operativo

Fuente: Instalación del sistema operativo CentOS 6.5

Esperamos a que cargue el modo gráfico de instalación

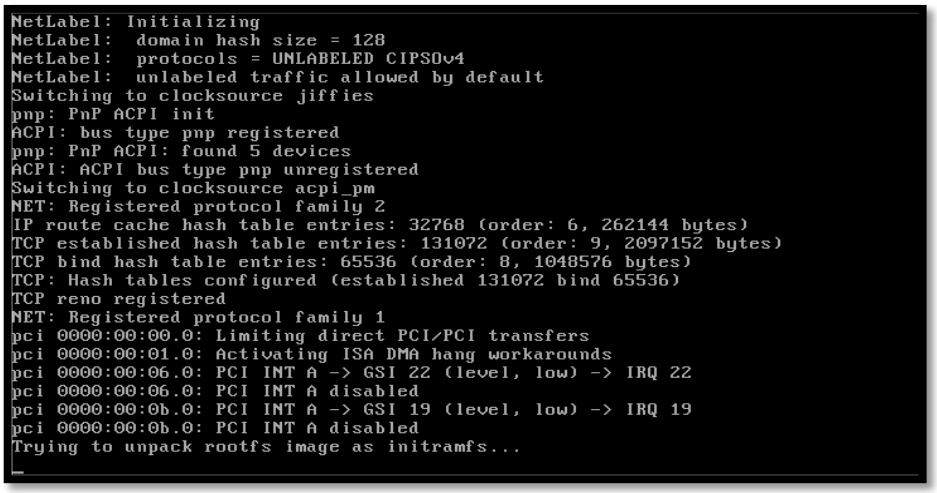


Figura 256 Cargando modo gráfico de instalación

Fuente: Instalación del sistema operativo CentOS 6.5

La primera pantalla que aparecerá le preguntará si desea verificar la integridad del medio de instalación. Si descargó una imagen ISO desde Internet y la grabó en un disco compacto o DVD, es buena idea verificar medios de instalación. Si está haciendo la instalación desde una máquina virtual con una imagen ISO y la suma MD5 coincide, descarte verificar.

Si desea verificar la integridad del medio de instalación (DVD o conjunto de discos compactos), a partir del cual se realizará la instalación, seleccione “OK” y pulse la tecla ENTER, considere que esto puede demorar varios minutos. Si está seguro de que el disco está en buen estado, pulse la tecla “TAB” para seleccionar “Skip” y pulse la tecla ENTER.

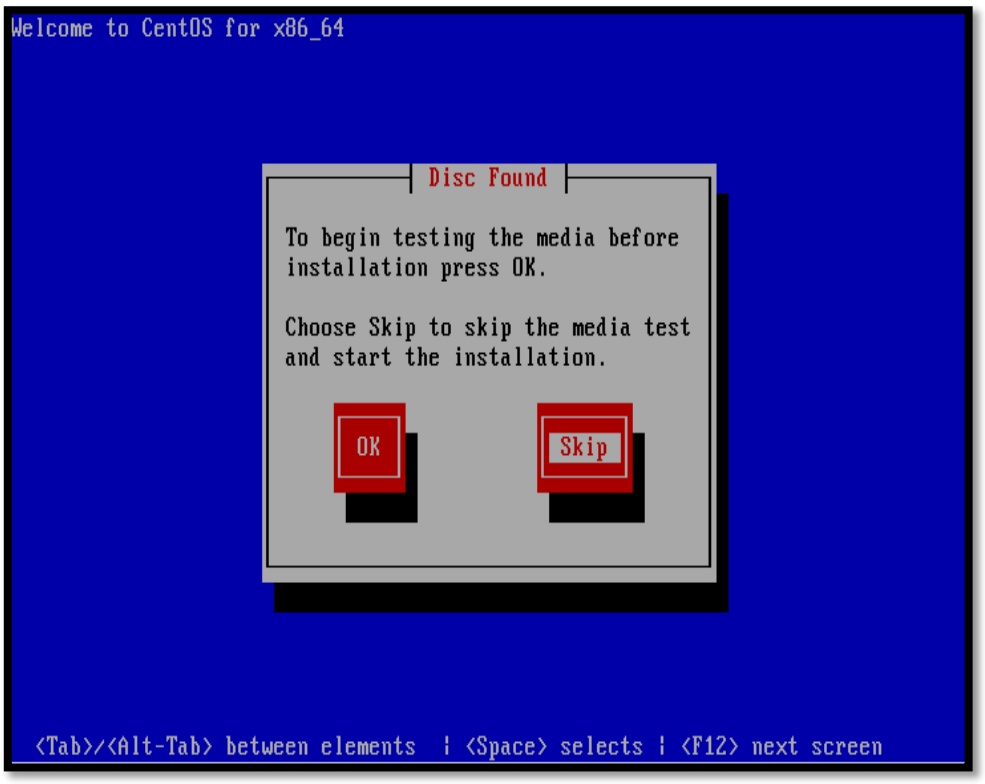


Figura 257 Verificación del medio de instalación

Fuente: Instalación del sistema operativo CentOS 6.5

Haga clic sobre el botón “Next”, en cuanto aparezca la pantalla de bienvenida de CentOS.

Figura 258 Pantalla de bienvenida de CentOS

Fuente: Instalación del sistema operativo CentOS 6.5

Seleccione “Spanish” o bien “Español”, como idioma para ser utilizado durante la instalación.

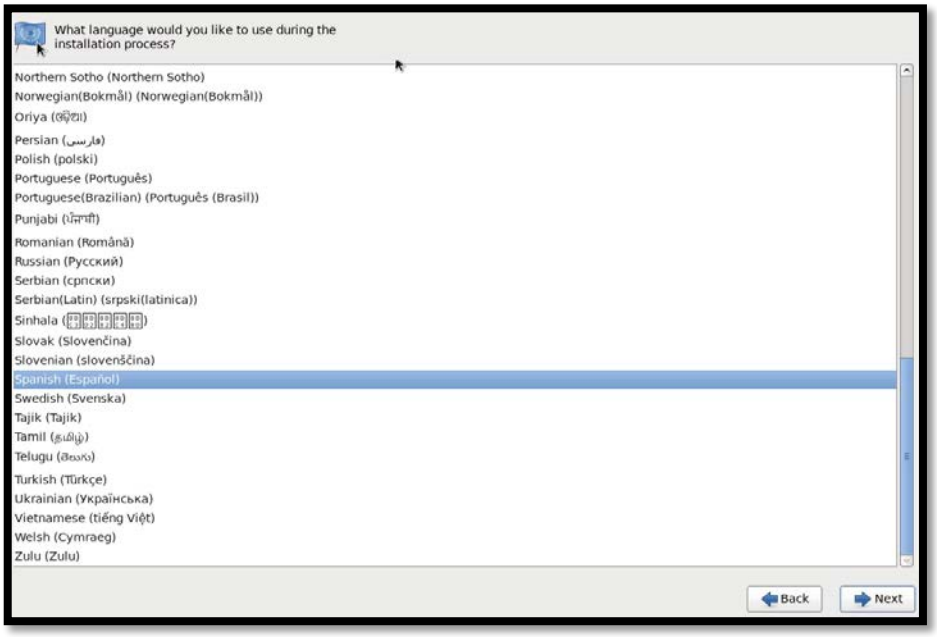


Figura 259 Idioma a utilizar durante el proceso de instalación

Fuente: Instalación del sistema operativo CentOS 6.5

A partir de este punto, todos los textos deberán aparecer en español. Seleccione el idioma de teclado. Elija el teclado en “Español” o bien el teclado “Latinoamericano”, de acuerdo a lo que corresponda. Al terminar, haga clic sobre el botón denominado “Siguiente”.

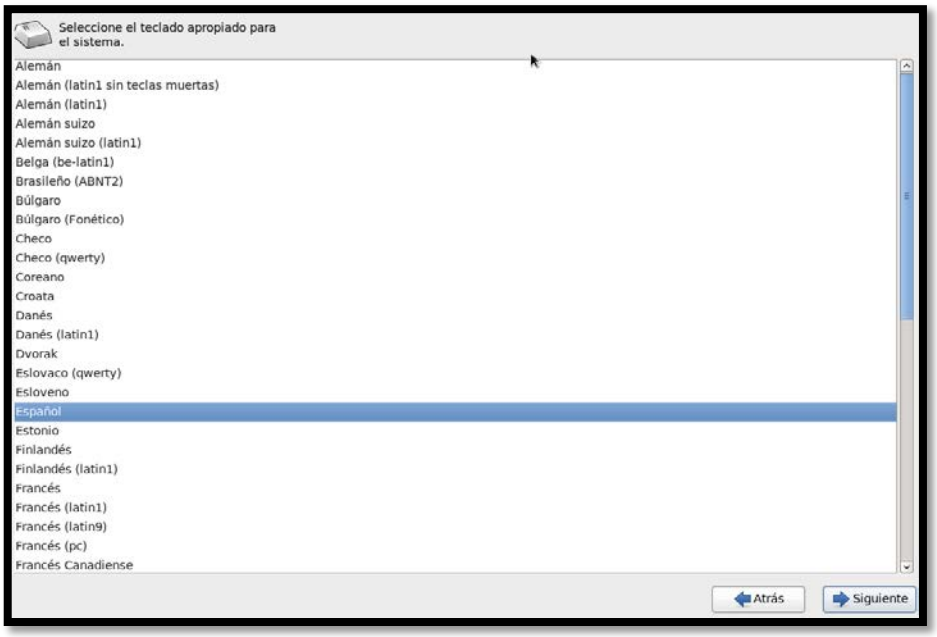


Figura 260 Selección del teclado apropiado para el sistema

Fuente: Instalación del sistema operativo CentOS 6.5

CentOS 6.5 incluye soporte para realizar una instalación sobre dispositivos de almacenamiento especializados, como Redes de Área de Almacenamiento (SAN), como FCoE, iSCSI y zFCP. Obviamente requiere disponer de un SAN en la red de área local para poder hacer uso de este tipo de dispositivos de almacenamiento. Si sólo dispone de discos duros en el equipo donde se realizará la instalación, elija la opción predeterminada, es decir “Dispositivos de almacenamiento básicos” y haga clic sobre el botón denominado “Siguiente”.

Figura 261 Elección de tipo de dispositivos de almacenamiento

Fuente: Instalación del sistema operativo CentOS 6.5

Mensaje de advertencia sobre el dispositivo de almacenamiento que puede contener datos, en el cual seleccionamos la opción “Si, descarte todos los datos”.

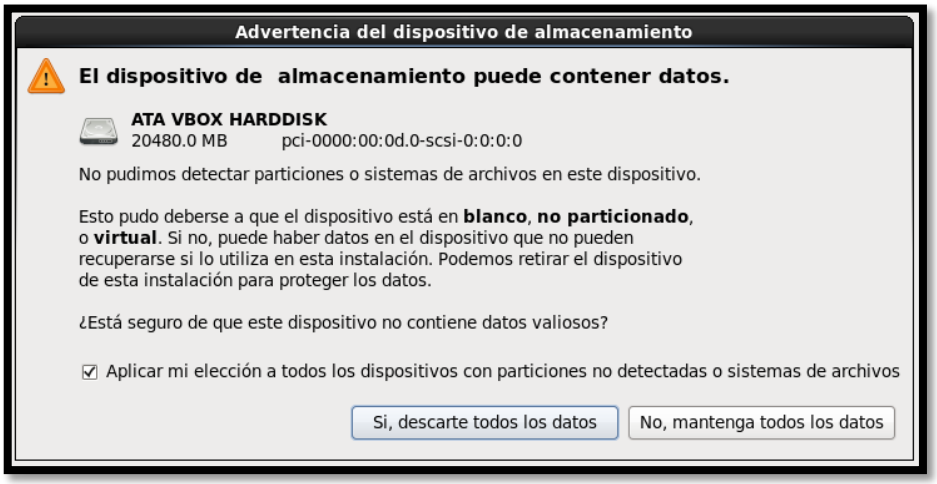


Figura 262 Advertencia del dispositivo de almacenamiento

Fuente: Instalación del sistema operativo CentOS 6.5

Defina el nombre de anfitrión en el siguiente formato: “nombre.dominio.tld”. Procure que el nombre de anfitrión sea corto, de hasta a 12 caracteres más el dominio y que esté resuelto en un servidor DNS. Si está indeciso al respecto, deje el valor predeterminado como “localhost.localdomain” y haga clic sobre el botón denominado “Siguiente”.

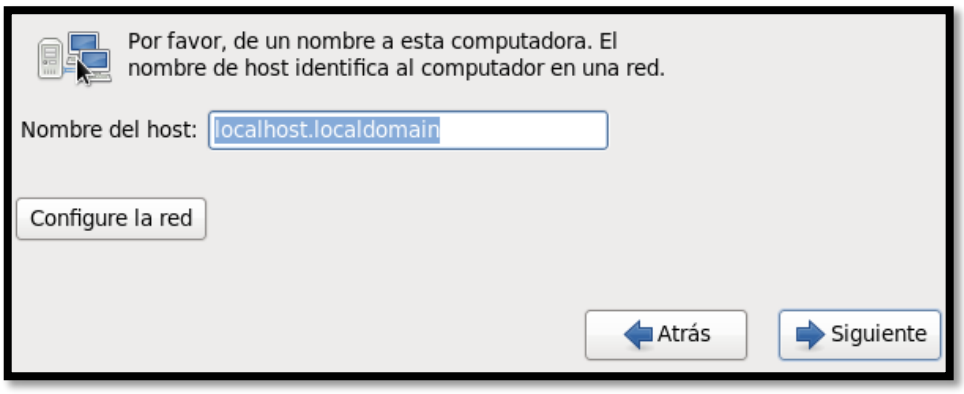


Figura 263 Nombre del host

Fuente: Instalación del sistema operativo CentOS 6.5

Seleccione la zona horaria que corresponda a su localidad, haciendo clic sobre cualquier punto en el mapamundi. Se recomienda dejar seleccionada la casilla “El reloj del sistema utiliza UTC”. Ésto último significa que el reloj del sistema utilizará UTC (Tiempo Universal Coordinado), que es el sucesor de GMT (Greenwich Mean Time, que significa Tiempo Promedio de Greenwich) y es la zona horaria de referencia respecto a la cual se calculan todas las otras zonas horarias del mundo. Al terminar, haga clic sobre el botón “Siguiente”.

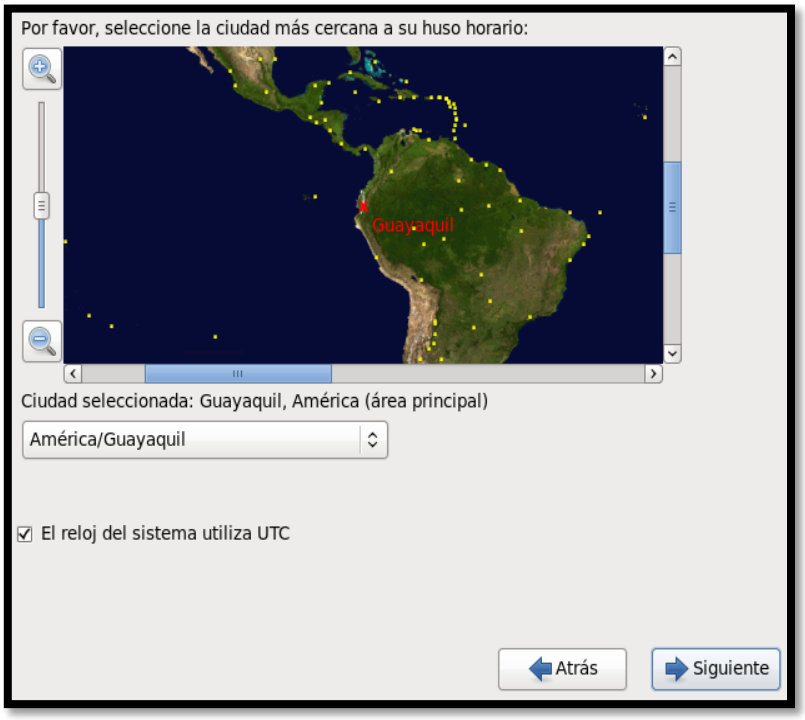


Figura 264 Selección de la zona horaria

Fuente: Instalación del sistema operativo CentOS 6.5

Defina y confirme la contraseña para el usuario root, cuenta que será utilizada para la administración del sistema. Al terminar, haga clic sobre el botón “Siguiente”.

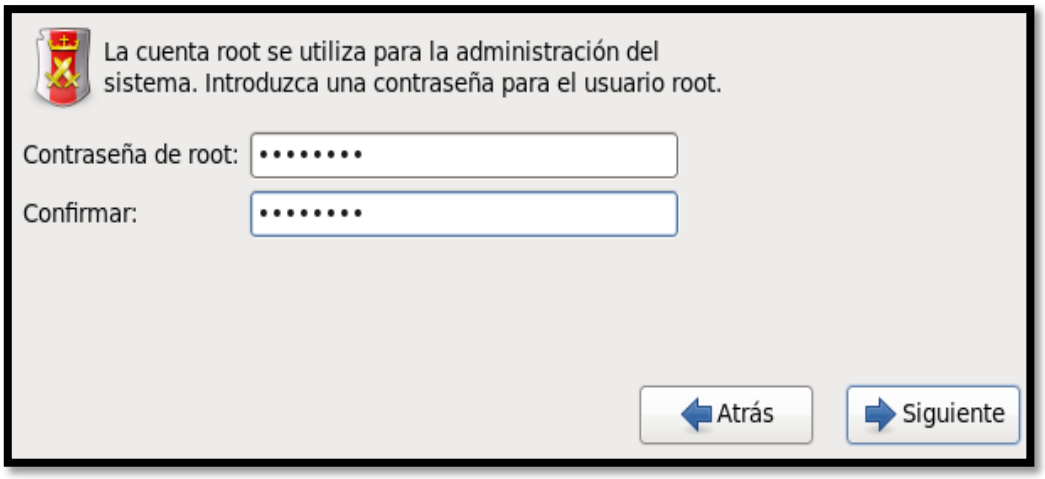


Figura 265 Definición de la contraseña root para la administración del sistema
Fuente: Instalación del sistema operativo CentOS 6.5

La siguiente pantalla le dará a elegir las opciones para crear las particiones en el disco duro. Salvo que elija “Crear un diseño personalizado”, invariablemente se aplicará un diseño predeterminado, el cual consistirá en:

- Una partición estándar de 200 MB para /boot
- Un volumen lógico para /, que utilizará la mayor parte del espacio disponible y que posteriormente permitirá hacer crecer el sistema añadiendo otro disco duro, con unidades físicas que se añadirán al volumen lógico.
- Un volumen lógico para la partición de memoria de intercambio (swap), que en equipos con menos de 1 GB en RAM, utilizará un espacio equivalente al doble de RAM físico del sistema o bien en equipos con más de 1 GB en RAM, utilizará un espacio equivalente a la suma del RAM físico del sistema, más 2 GB.

Seleccionaremos “Crear un diseño personalizado” que permitirá elegir las particiones estándar o volúmenes lógicos de acuerdo a los requerimientos del usuario.

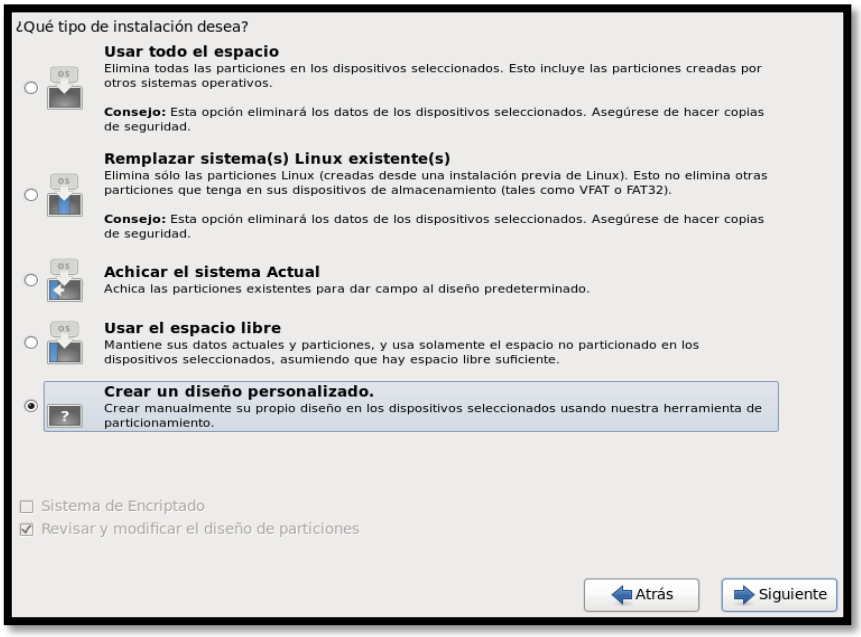


Figura 266 Tipo de instalación

Fuente: Instalación del sistema operativo CentOS 6.5

Se mostrará la tabla de particiones actual, mostrando el espacio libre disponible para crear nuevas particiones. Haga clic sobre el botón “Crear”.

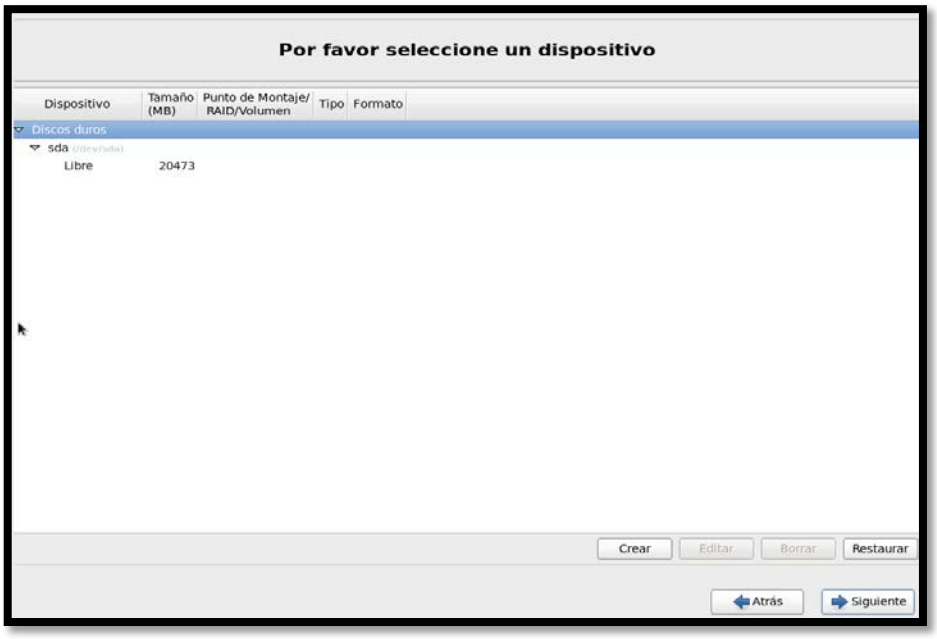


Figura 267 Lista de particionamiento por defecto

Fuente: Instalación del sistema operativo CentOS 6.5

Se abrirá una ventana donde podrá definir el tipo de partición a crear. Elija crear una “Partición estándar”. Al terminar, haga clic sobre el botón “Crear”.

Figura 268 Tipo de partición estándar a crear

Fuente: Instalación del sistema operativo CentOS 6.5

En la ventana que aparece sobre la tabla de particiones, defina /boot como punto de montaje, mantenga el formato ext4, mantenga el tamaño de 200 MB y active la casilla de opción denominada “Forzar a partición primaria”. Al terminar, haga clic sobre el botón “Aceptar”.

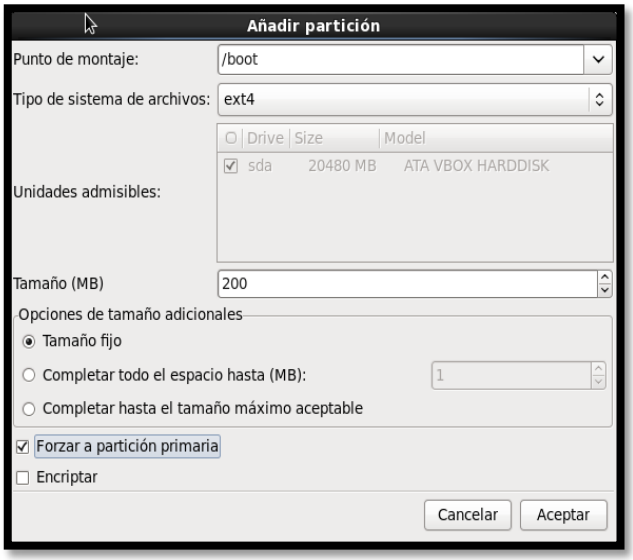


Figura 269 Definición de /boot como punto de montaje

Fuente: Instalación del sistema operativo CentOS 6.5

En la ventana que aparece sobre la tabla de particiones, defina / como punto de montaje, mantenga el formato ext4, defina su tamaño y active la casilla de opción “Forzar a partición primaria”. Al terminar, haga clic sobre el botón “Aceptar”.

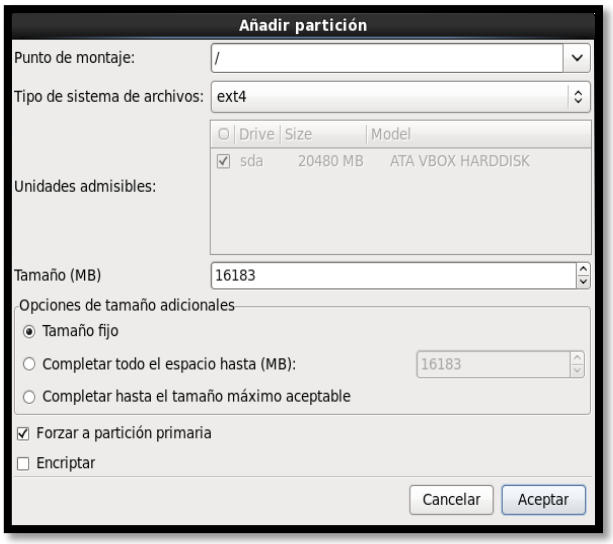


Figura 270 Definición de / como punto de montaje

Fuente: Instalación del sistema operativo CentOS 6.5

Para el tamaño de la partición de memoria de intercambio (swap), siga las siguientes reglas:

- Si el sistema tiene menos de 1 GB en RAM: Defina una cantidad equivalente a dos veces la cantidad de memoria RAM física. Ejemplos:
- Si el sistema tiene más de 1 GB en RAM: Defina una cantidad equivalente a la suma de la cantidad de memoria RAM física, más 2 GB. Ejemplos:

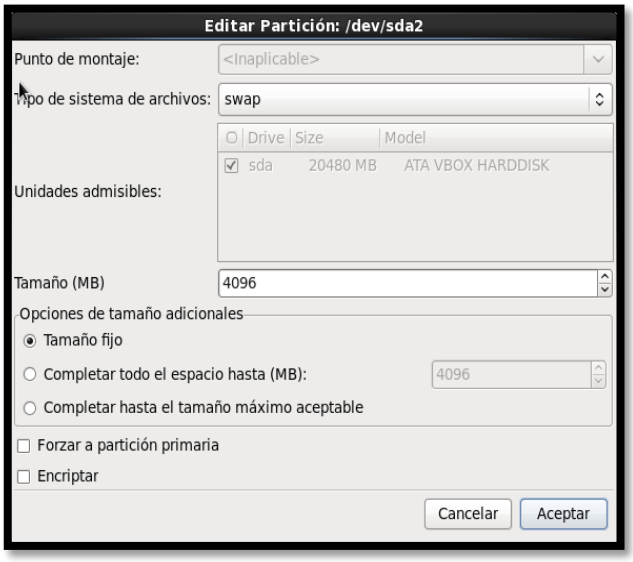


Figura 271 Definición del área de intercambio swap

Fuente: Instalación del sistema operativo CentOS 6.5

Se mostrará la tabla de particiones y si está conforme con el diseño haga clic en el botón “Siguiente”.

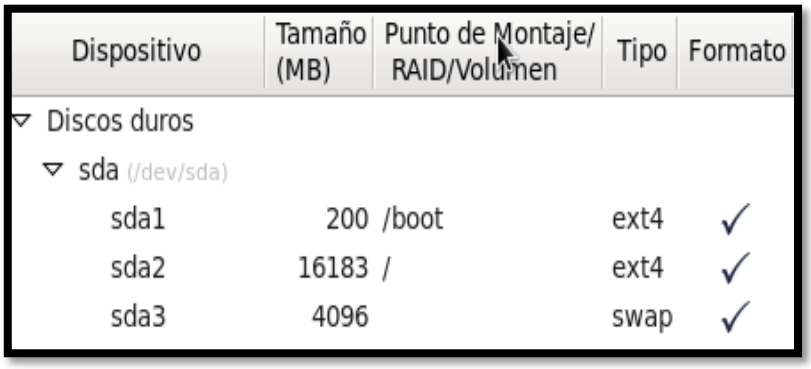


Figura 272 Tabla de particiones

Fuente: Instalación del sistema operativo CentOS 6.5

Se solicitará que confirme de manera explícita que se procederá a eliminar o dar formato a particiones existentes en el medio de almacenamiento. Si desea proceder, haga clic sobre el botón “Formato”.

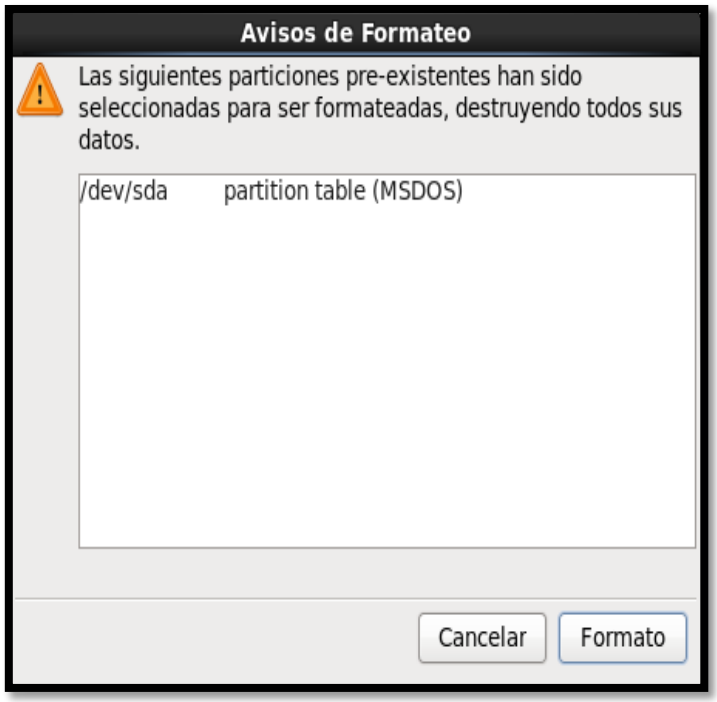


Figura 273 Avisos de formateo

Fuente: Instalación del sistema operativo CentOS 6.5

Se solicitará confirme que desea escribir los cambios al disco duro. Si desea proceder, haga clic sobre el botón “Escribir cambios al disco”.

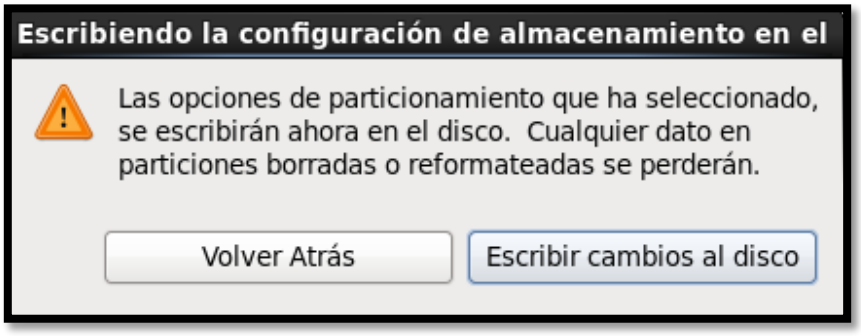


Figura 274 Configuración de cambios en el disco

Fuente: Instalación del sistema operativo CentOS 6.5

Espere algunos minutos mientras se guarda la tabla de particiones y se da formato a todas las particiones definidas en los pasos anteriores.

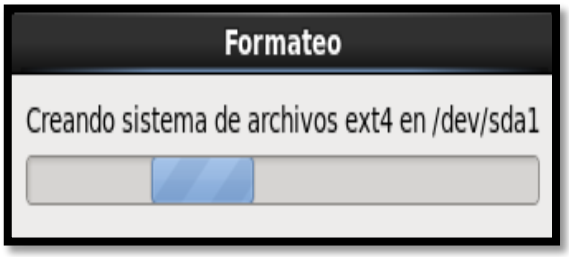


Figura 275 Procesando cambios de la tabla de particiones

Fuente: Instalación del sistema operativo CentOS 6.5

Por seguridad, conviene asignar una contraseña al gestor de arranque. Ésto tiene como finalidad el de evitar que cualquiera que tenga acceso físico al sistema, pueda modificar los parámetros de arranque del gestor de arranque e iniciar en modo mono-usuario (nivel de ejecución 1). Si desea proceder, haga clic sobre la opción “Usar la contraseña del gestor de arranque”.

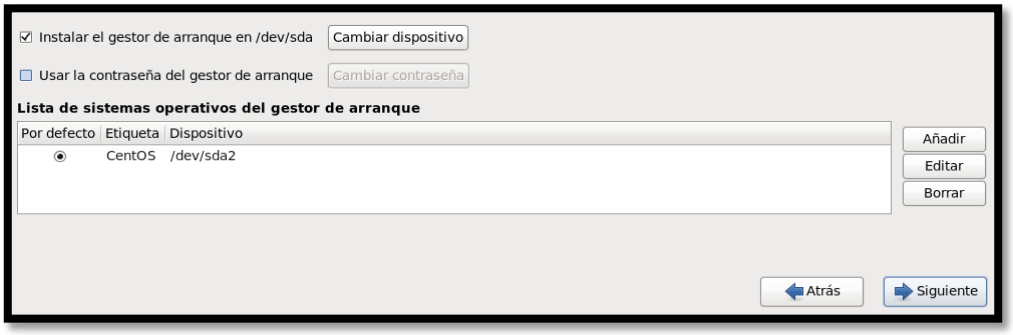


Figura 276 Parámetros del gestor de arranque

Fuente: Instalación del sistema operativo CentOS 6.5

Asigne y confirme una contraseña para el gestor de arranque. A continuación hacemos clic en “Siguiente”.

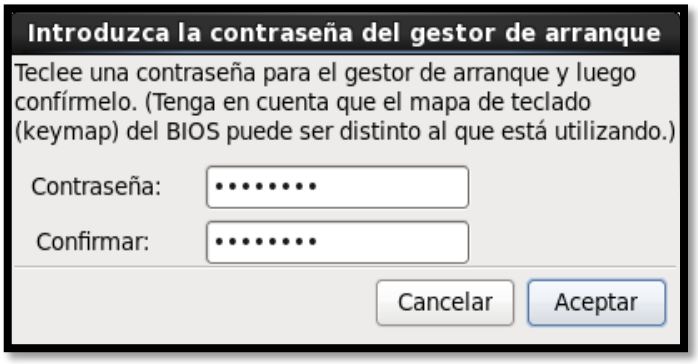


Figura 277 Contraseña del gestor de arranque

Fuente: Instalación del sistema operativo CentOS 6.5

Elija el tipo de instalación requerido por el usuario. Como la instalación se encuentra enfocada para uso de servidor escogeremos la opción “Minimal” que es la instalación predeterminada de CentOS. Para elegir grupos específicos de paquetes, haga clic sobre la casilla de opción “Personalizar ahora”. Al terminar, haga clic sobre el botón denominado “Siguiente”.

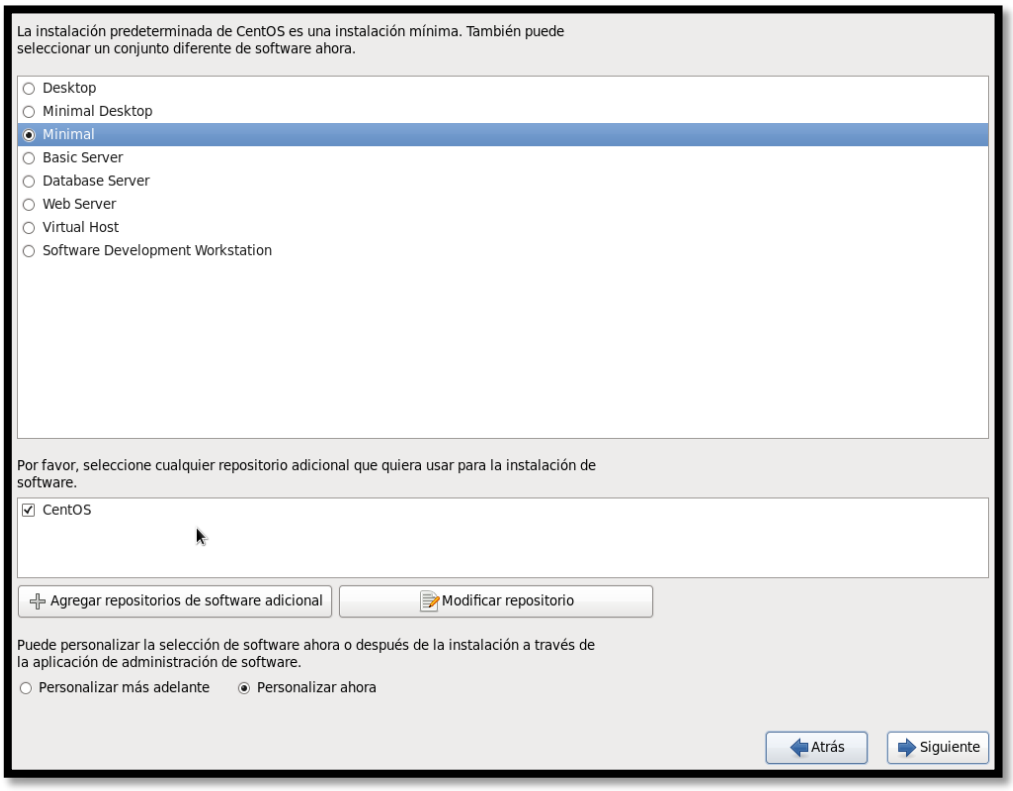


Figura 278 Tipo de instalación Minimal

Fuente: Instalación del sistema operativo CentOS 6.5

Podrá seleccionar cualquier grupo de paquetes que sirva a necesidades particulares. Prefiera conservar el diseño de instalación mínima y añadir el grupo de paquetes para ciertos parámetros.

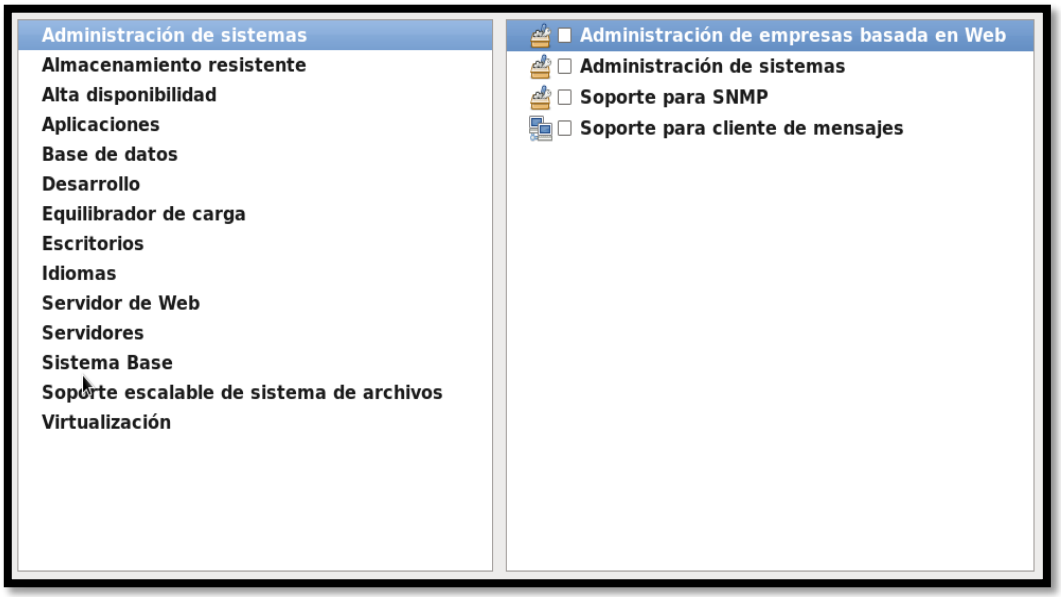


Figura 279 Administración de sistemas

Fuente: Instalación del sistema operativo CentOS 6.5

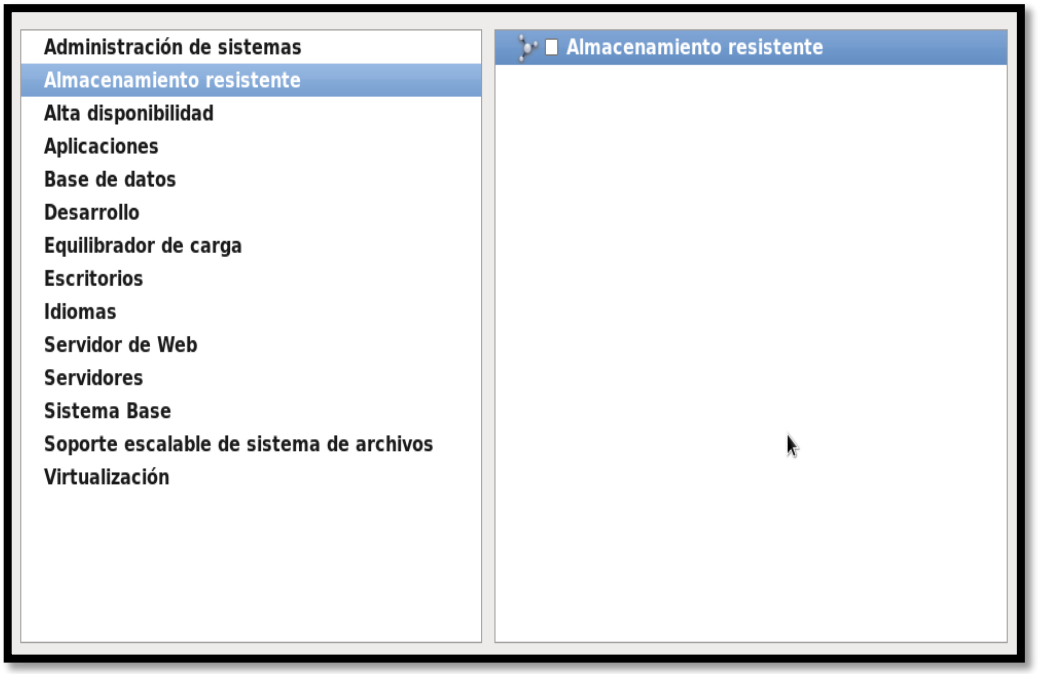


Figura 280 Almacenamiento resistente

Fuente: Instalación del sistema operativo CentOS 6.5

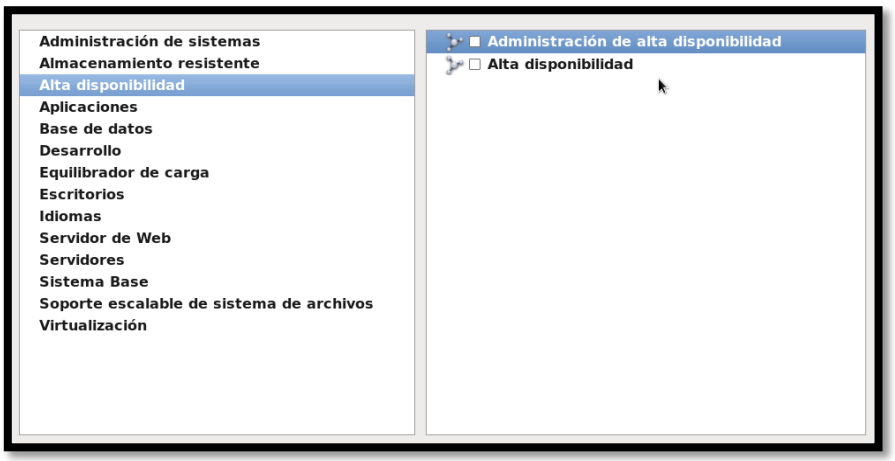


Figura 281 Alta disponibilidad

Fuente: Instalación del sistema operativo CentOS 6.5

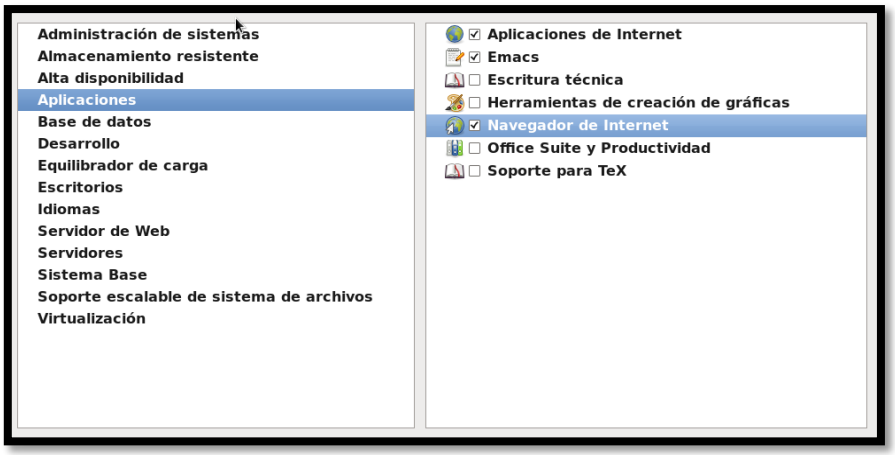


Figura 282 Aplicaciones

Fuente: Instalación del sistema operativo CentOS 6.5

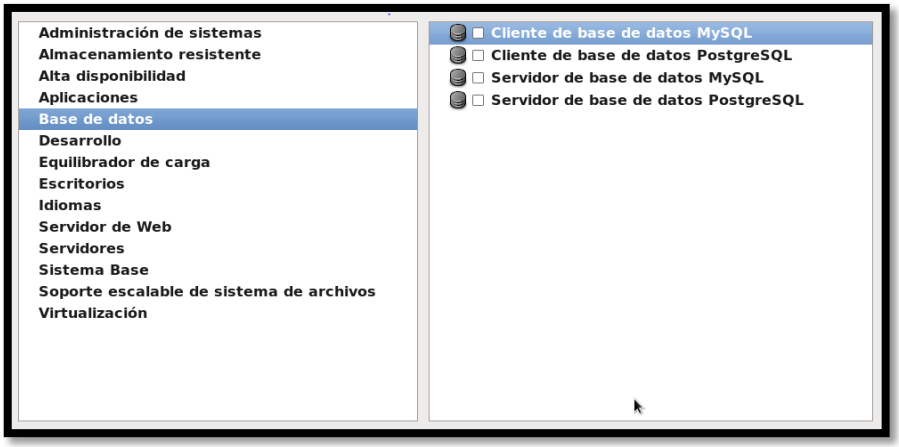


Figura 283 Base de datos

Fuente: Instalación del sistema operativo CentOS 6.5

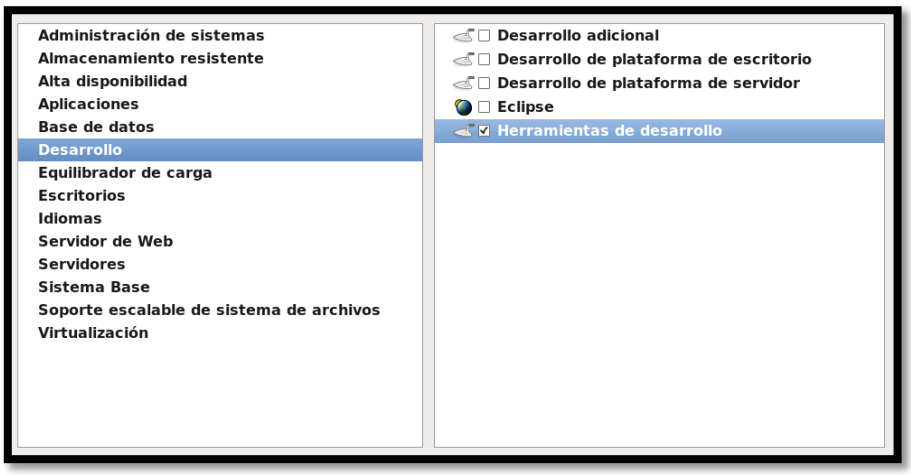


Figura 284 Desarrollo

Fuente: Instalación del sistema operativo CentOS 6.5

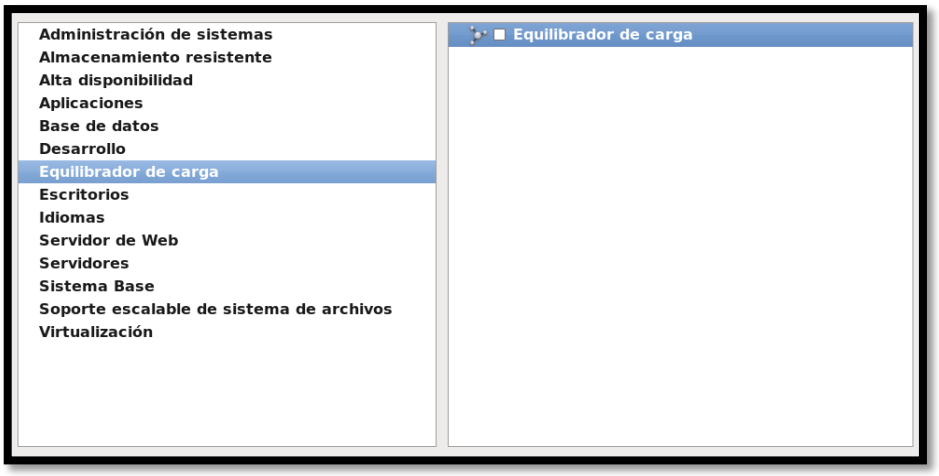


Figura 285 Equilibrador de carga

Fuente: Instalación del sistema operativo CentOS 6.5

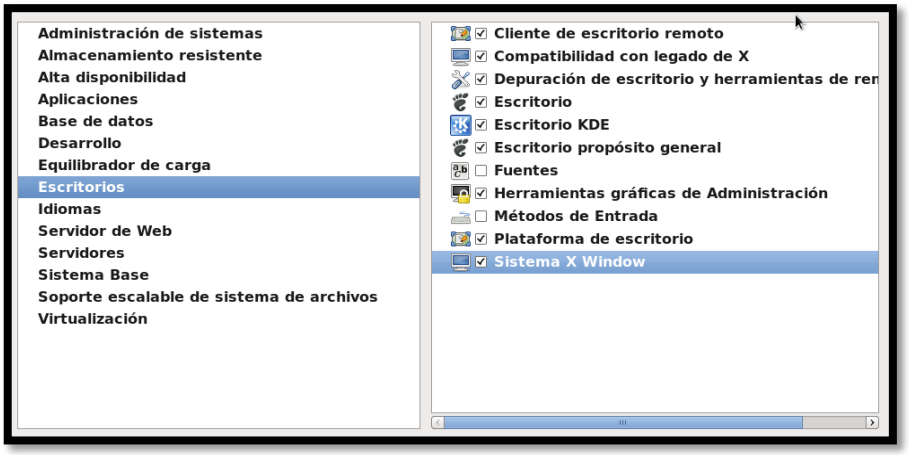


Figura 286 Escritorios

Fuente: Instalación del sistema operativo CentOS 6.5

Figura 287 Idiomas

Fuente: Instalación del sistema operativo CentOS 6.5

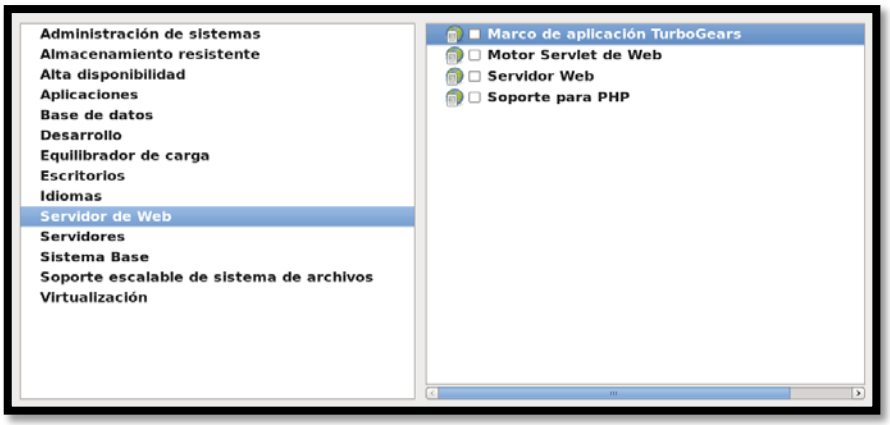


Figura 288 Servidor de Web

Fuente: Instalación del sistema operativo CentOS 6.5

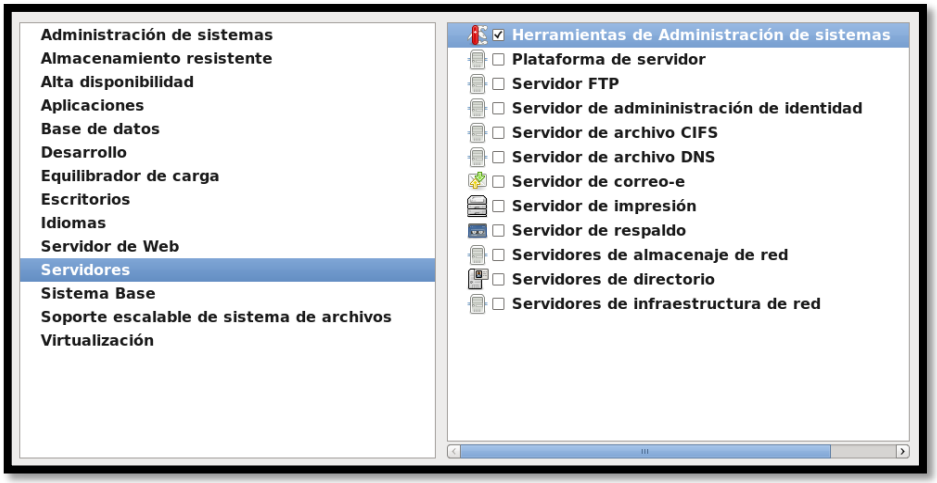


Figura 289 Servidores

Fuente: Instalación del sistema operativo CentOS 6.5

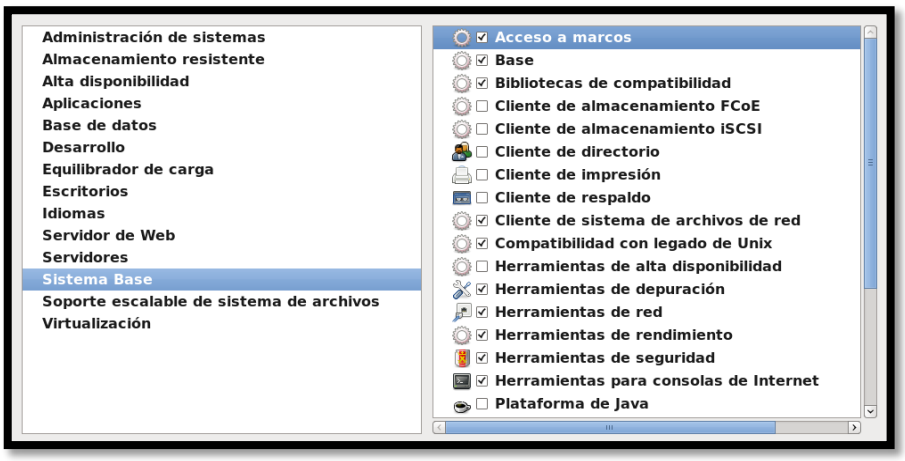


Figura 290 Sistema Base

Fuente: Instalación del sistema operativo CentOS 6.5

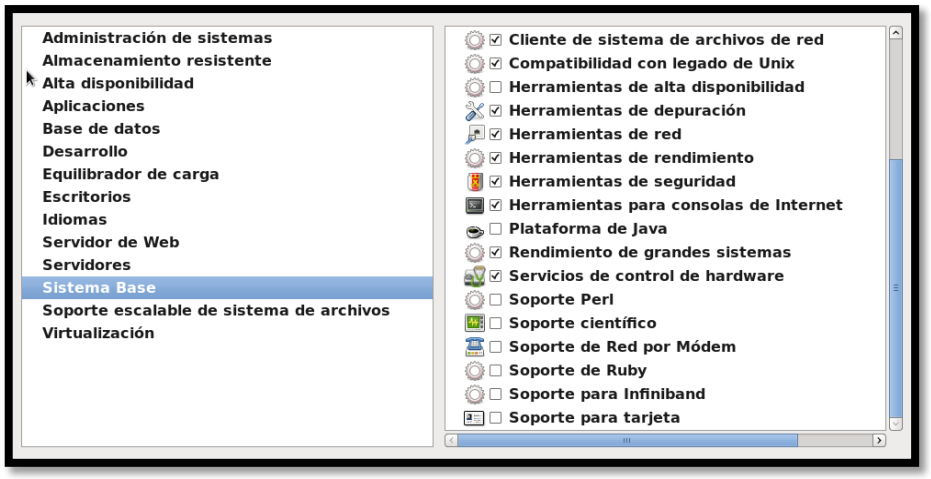


Figura 291 Sistema Base

Fuente: Instalación del sistema operativo CentOS 6.5

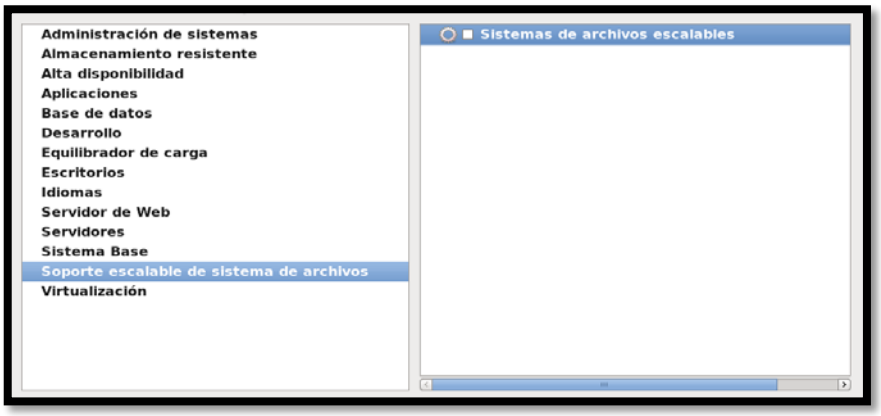


Figura 292 Soporte escalable de sistema de archivos

Fuente: Instalación del sistema operativo CentOS 6.5

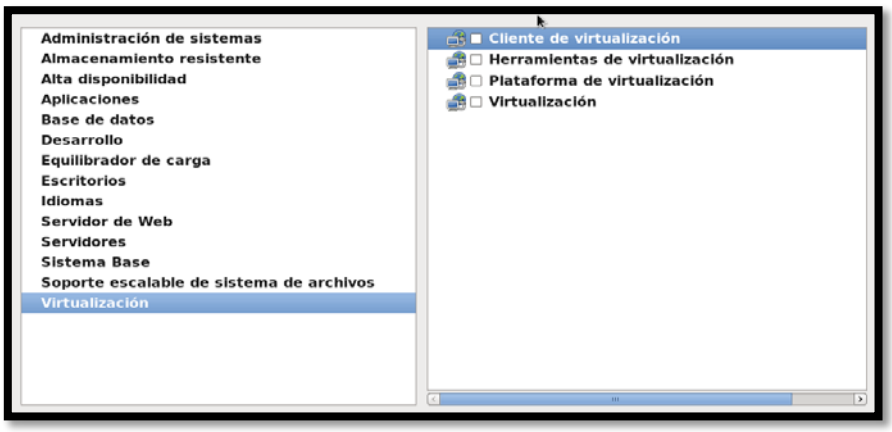


Figura 293 Virtualización

Fuente: Instalación del sistema operativo CentOS 6.5

Si está conforme y considera que ha terminado de seleccionar los grupos de paquetes, haga clic sobre el botón “Siguiente” y posterior a ello el sistema empezará a realizar una comprobación de las dependencias.

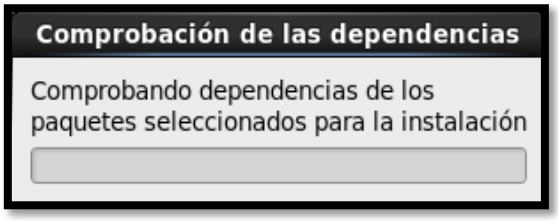


Figura 294 Comprobación de las dependencias

Fuente: Instalación del sistema operativo CentOS 6.5

Iniciará el proceso de instalación de paquetes. El tiempo que demore el proceso dependerá de la cantidad de grupos y paquetes que se hayan seleccionado.

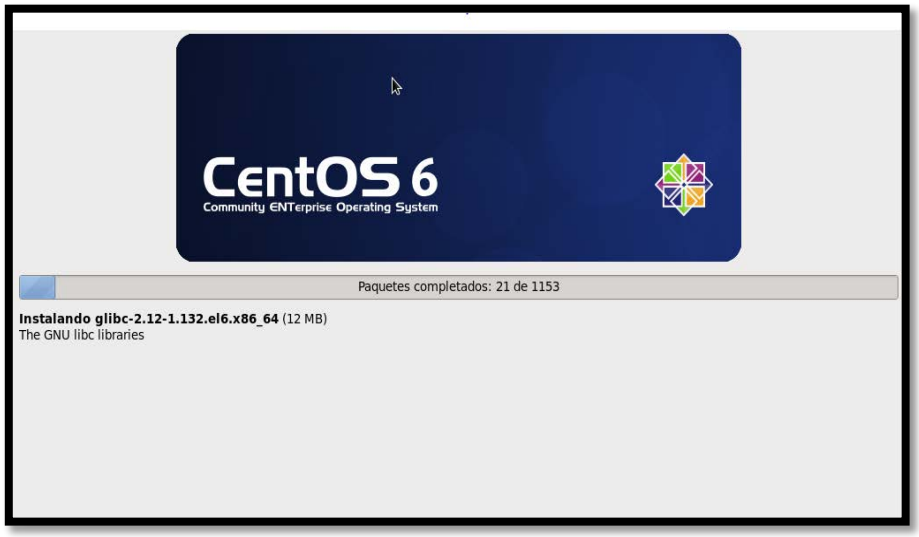


Figura 295 Proceso de instalación de paquetes

Fuente: Instalación del sistema operativo CentOS 6.5

Una vez completada la instalación, haga clic sobre el botón “Reiniciar”, y retire el DVD o disco compacto de la unidad óptica.

Figura 296 Finalización de la instalación de CentOS

Fuente: Instalación del sistema operativo CentOS 6.5

Una vez que se ha reiniciado el sistema operativo podemos verificar que se haya instalado en el equipo.

Figura 297 Cargando paquetes instalados

Fuente: Instalación del sistema operativo CentOS 6.5

Pantalla de bienvenida:

Figura 298 Pantalla de Bienvenida

Fuente: Instalación del sistema operativo CentOS 6.5

Aceptamos el acuerdo de la Licencia:

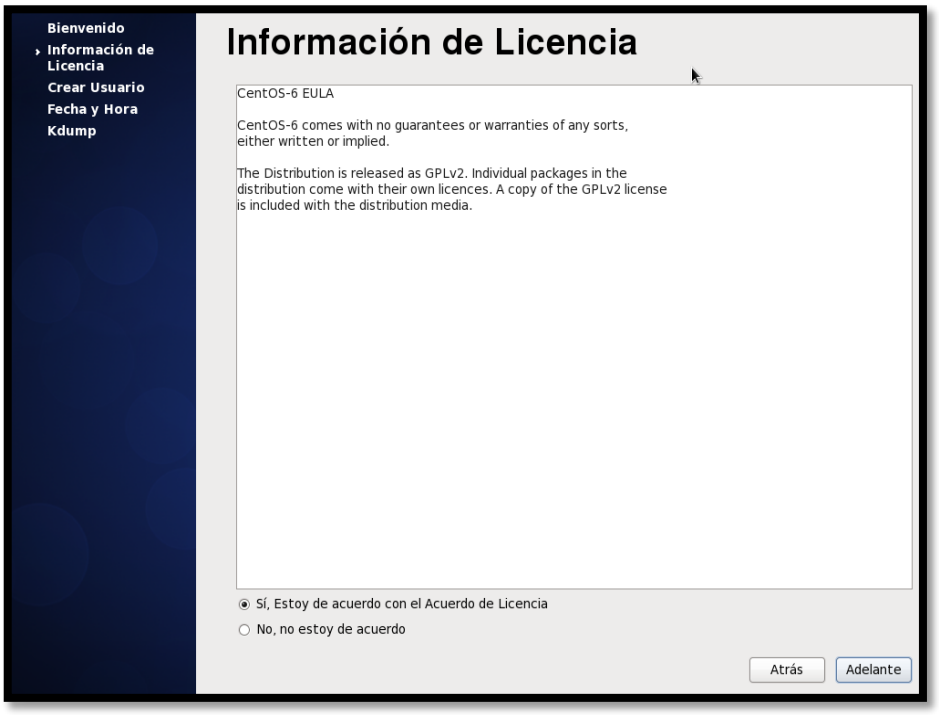


Figura 299 Información de Licencia

Fuente: Instalación del sistema operativo CentOS 6.5

Como la instalación está basada para uso de servidores, no creamos ningún usuario y lo único que hacemos es poner “Adelante”.

Figura 300 Creación de usuario

Fuente: Instalación del sistema operativo CentOS 6.5

Sincronización de la Fecha y hora del sistema.

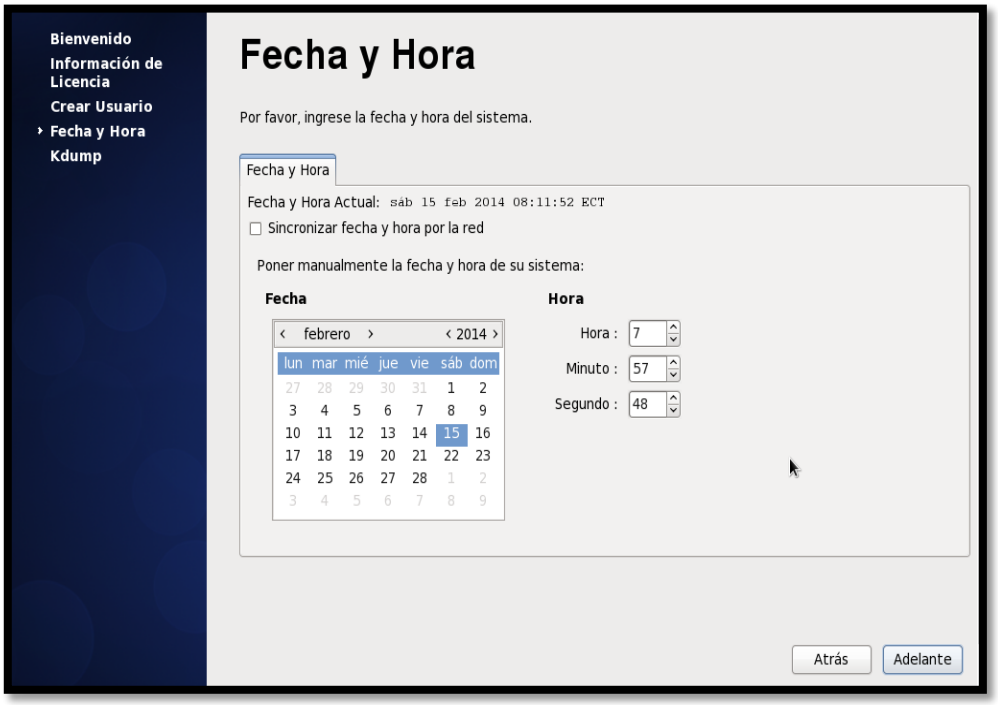


Figura 301 Sincronización de fecha y hora

Fuente: Instalación del sistema operativo CentOS 6.5

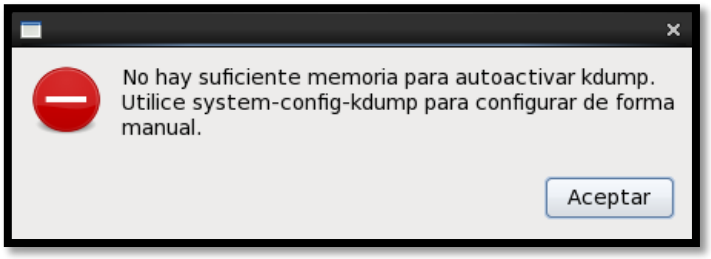


Figura 302 Error de la memoria Kdump

Fuente: Instalación del sistema operativo CentOS 6.5

Finalmente nos despliega el mecanismo de volcado de fallos del kernel donde Kdump capturará la información del sistema que puede ser invaluable para la determinación de la causa del fallo. Hacemos clic en “Finalizar”.

Figura 303 Configuración de Kdump

Fuente: Instalación del sistema operativo CentOS 6.5

ANEXO 11
MANUAL TÉCNICO LDAP

SERVIDOR DE DIRECTORIO LDAP

A continuación se detalla todo el proceso necesario para la instalación, configuración y funcionamiento de un servidor LDAP institucional:

INSTALACIÓN

La sesión se iniciará como usuario estándar con permisos de configuración restringidos, así que se debe añadir “sudo” frente a cada comando que requiera privilegios de administrador (root) o simplemente pasamos al modo root con el siguiente comando:

sudo su (luego solicitará usuario y contraseña)

Actualización de los paquetes del Sistema Operativo

Antes de instalar cualquier aplicación debemos tener acceso a Internet y actualizar los repositorios de Debian. El Software Manager de Debian es aptitude o apt tal como se indica a continuación:

sudo apt-get update

sudo apt-get upgrade

Instalación de Paquetes

Para iniciar con la instalación debemos abrir un terminal y loguearnos como root donde ejecutamos una orden de instalación de los siguientes paquetes:

apt-get install apache2 slapd ldap-utils phpldapadmin libapache2-mod-php5

```
root@debian:~# apt-get install apache2 slapd ldap-utils phpldapadmin libapache2-mod-php5
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libltdl7 libonig2 libperl5.10 libqdbm14
  libsasl2-modules libslp1 odbcinst odbcinst1debian2 openssl php5-cli php5-common
  php5-ldap php5-suhosin ssl-cert unixodbc
Paquetes sugeridos:
  apache2-doc apache2-suexec apache2-suexec-custom php-pear libsasl2-modules-otp
  libsasl2-modules-ldap libsasl2-modules-sql libsasl2-modules-gssapi-mit
  libsasl2-modules-gssapi-heimdal slpd openslp-doc ca-certificates openssl-blacklist
  libmyodbc odbc-postgresql tdsodbc unixodbc-bin
Se instalarán los siguientes paquetes NUEVOS:
  apache2 apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common ldap-utils
  libapache2-mod-php5 libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
  libltdl7 libonig2 libperl5.10 libqdbm14 libsasl2-modules libslp1 odbcinst
  odbcinst1debian2 openssl php5-cli php5-common php5-ldap php5-suhosin phpldapadmin
  slapd ssl-cert unixodbc
0 actualizados, 28 se instalarán, 0 para eliminar y 0 no actualizados.
Necesito descargar 14,3 MB de archivos.
Se utilizarán 41,1 MB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? S_
```

Figura 304 Instalación de los paquetes

Fuente: Sistema Operativo Debian 6.0.7

Ingresar Contraseña

Durante el proceso de instalación nos solicitará la contraseña de administrador para la configuración de nuestro directorio LDAP como se indica en la Figura 305. Por defecto el nombre del administrador es admin.

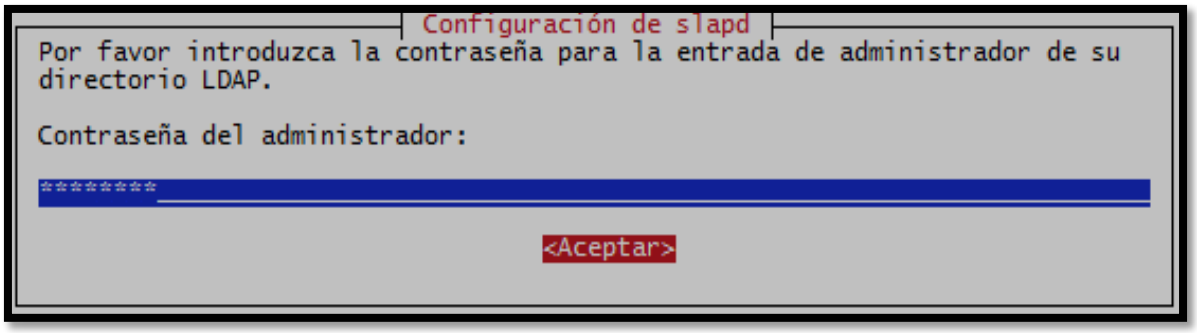


Figura 305 Contraseña del Administrador

Fuente: Sistema Operativo Debian 6.0.7

Verificar Contraseña

A continuación debemos ingresar nuevamente la contraseña para verificar que se ingresó correctamente por motivos de seguridad como se indica en la Figura 306.

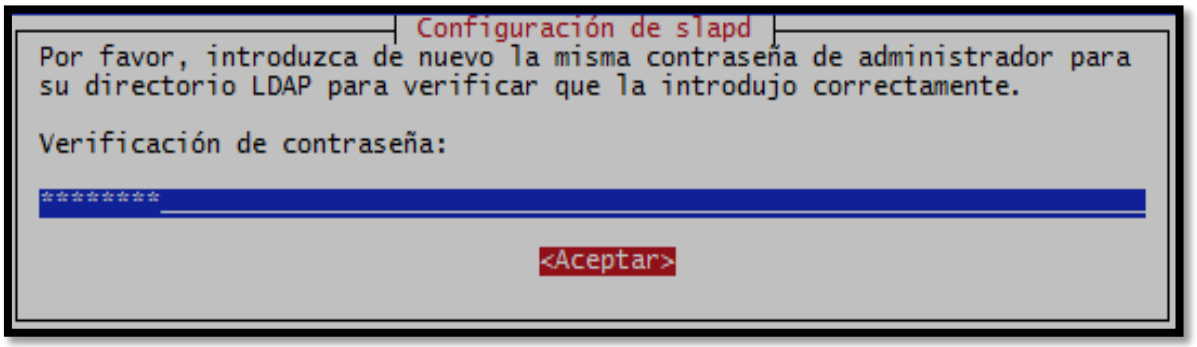


Figura 306 Verificación de la contraseña de Administrador

Fuente: Sistema Operativo Debian 6.0.7

Proceso de Instalación

Con la configuración de administración ingresada se empiezan a terminar de instalar los paquetes necesarios para el funcionamiento del servidor LDAP tal como se muestra en la Figura 307 y Figura 308.

Figura 307 Inicio del Proceso de Instalación

Fuente: Sistema Operativo Debian 6.0.7

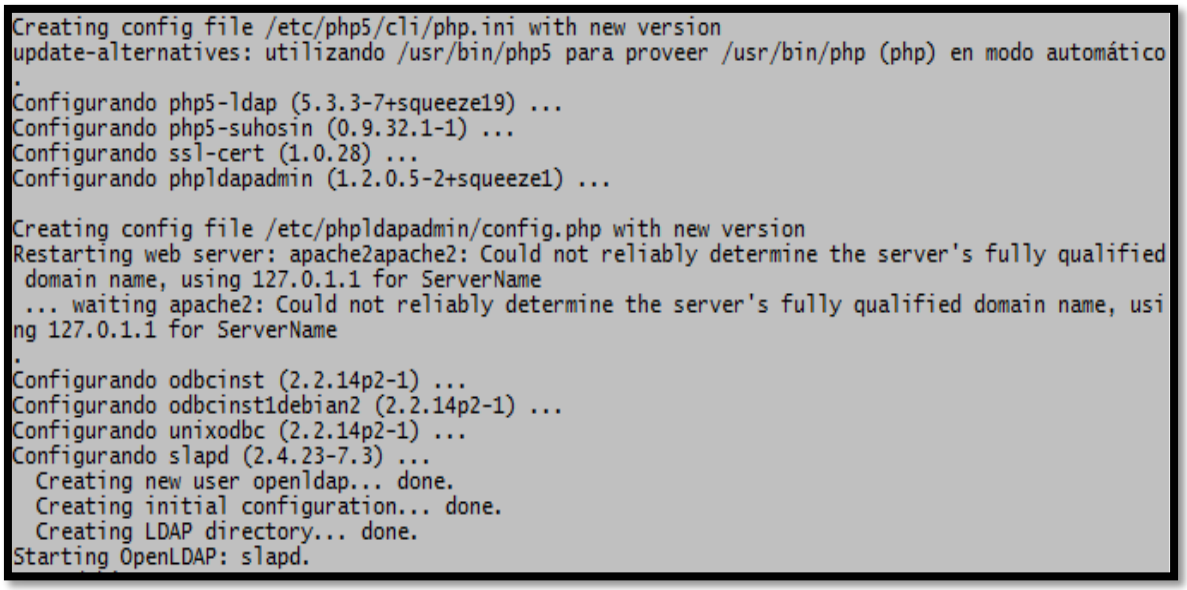


Figura 308 Finalización del Proceso de Instalación

Fuente: Sistema Operativo Debian 6.0.7

CONFIGURACIÓN

Configuración inicial del asistente de slapd

Los archivos de configuración del servidor LDAP se almacenan en la carpeta /etc/ldap/. En lugar de editar manualmente dichos archivos, es mejor lanzar el asistente de configuración de slapd. Para ello debemos ejecutar el siguiente comando:

dpkg-reconfigure slapd

Lo primero que nos pregunta el asistente es si deseamos omitir la configuración del servidor LDAP (Figura 309). Obviamente responderemos que no, porque lo que queremos es configurar el servicio.

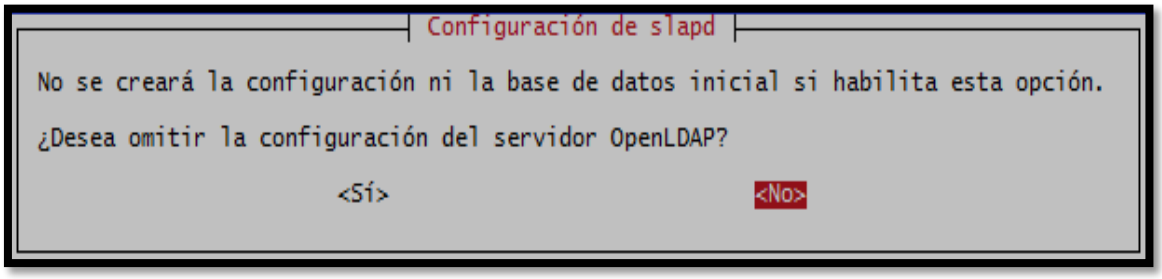


Figura 309 Inicio de configuración de slapd

Fuente: Sistema Operativo Debian 6.0.7

Nombre de Dominio DNS

Ahora el asistente nos pide que ingresemos el nombre de dominio DNS para construir el DN base del directorio LDAP (Figura 310).

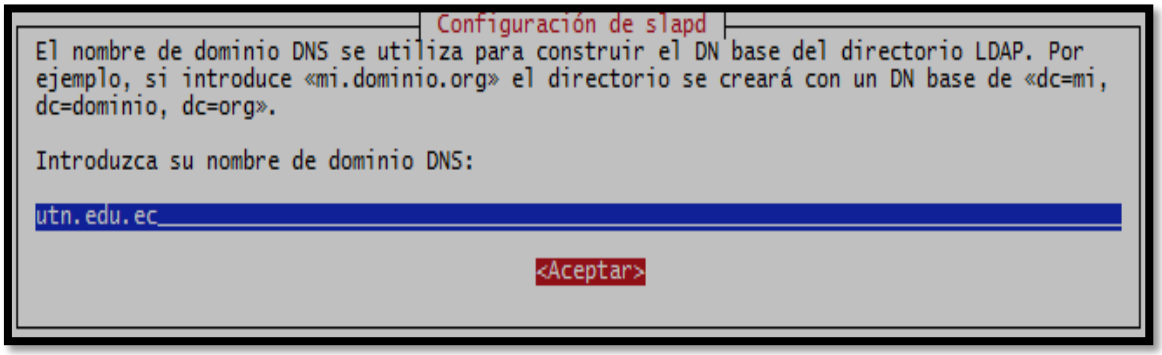


Figura 310 Nombre de dominio DNS

Fuente: Sistema Operativo Debian 6.0.7

Nombre de la Organización

Ingresamos el Nombre de la Organización a utilizar en el directorio LDAP a utn.edu.ec como se muestra en la Figura 311.

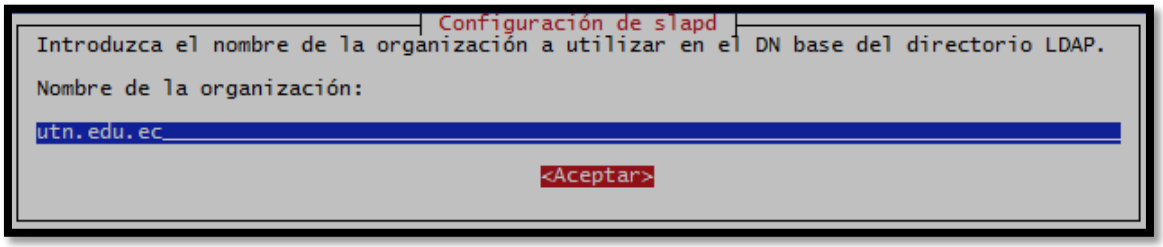


Figura 311 Nombre de la Organización

Fuente: Sistema Operativo Debian 6.0.7

Contraseña del Administrador

Para validar los cambios realizados procedemos a ingresar la contraseña del administrador (Figura 312).

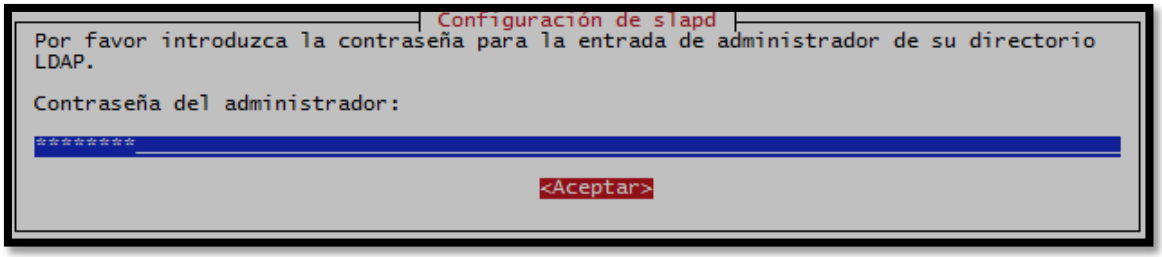


Figura 312 Contraseña del Administrador

Fuente: Sistema Operativo Debian 6.0.7

Verificación de Contraseña

Una vez ingresada la contraseña nos solicita la verificación de la misma para corroborar que se ha escrito correctamente (Figura 313).

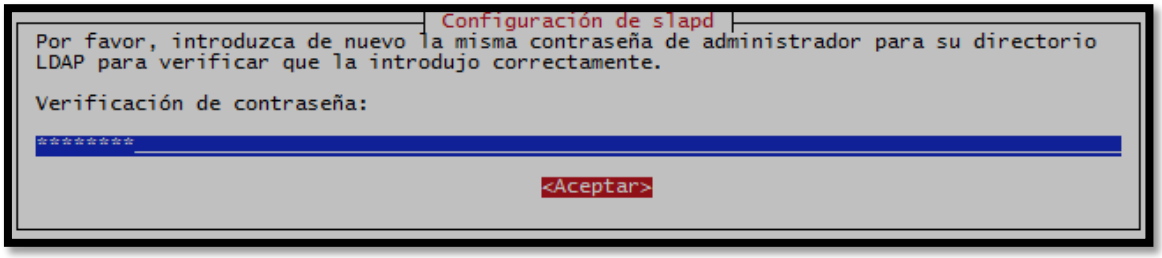


Figura 313 Verificación de contraseña

Fuente: Sistema Operativo Debian 6.0.7

Selección del Motor de la Base de Datos

Nos pregunta por el motor de la base de datos a utilizar, entre las opciones tenemos HDB y BDB. Se recomienda el uso de HDB (Figura 314).

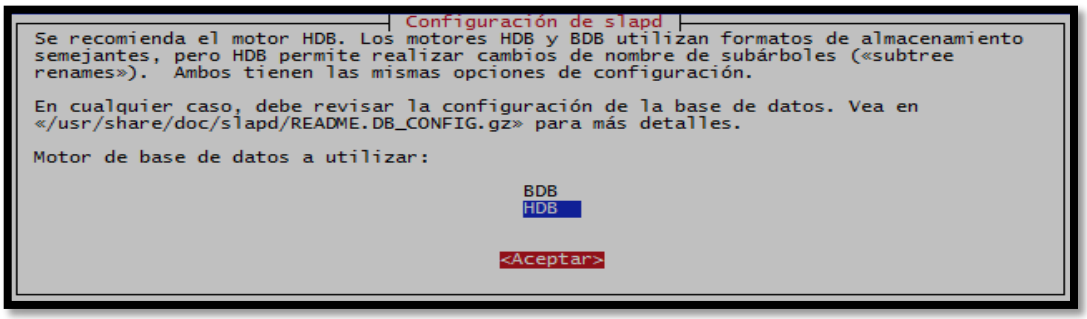


Figura 314 Motor de Base de Datos

Fuente: Sistema Operativo Debian 6.0.7

Purgue del paquete slapd

Una vez que hemos seleccionado el motor de la base de datos nos mostrará una ventana de configuración en modo pregunta a la cual responderemos que No (Figura 315).

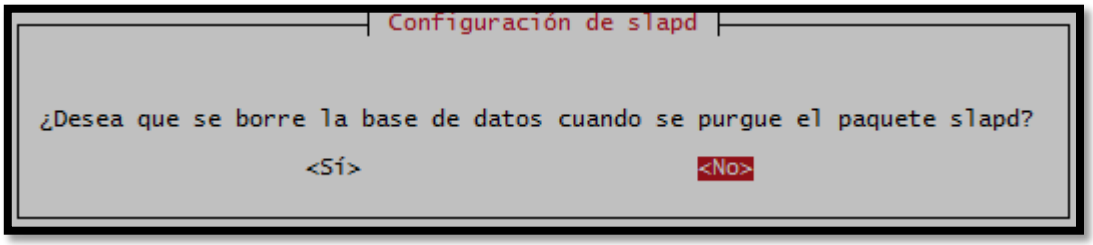


Figura 315 Purgue del paquete slapd

Fuente: Sistema Operativo Debian 6.0.7

Borrar la Base de Datos Antigua

En la siguiente ventana de configuración se elimina la base de datos creada por defecto al inicio de la instalación, para la cual seleccionamos Sí para poder crear la nueva base de datos.

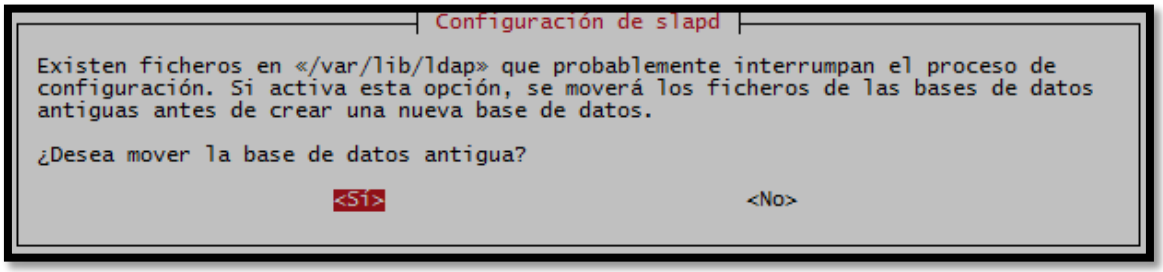


Figura 316 Borrar la Base de Datos Antigua

Fuente: Sistema Operativo Debian 6.0.7

Actualización del Protocolo LDAP

Nos pregunta si deseamos habilitar el soporte para la versión 2 del protocolo LDAP, seleccionamos No (Figura 317) debido a que la versión 2 está obsoleta y prácticamente no se usa.

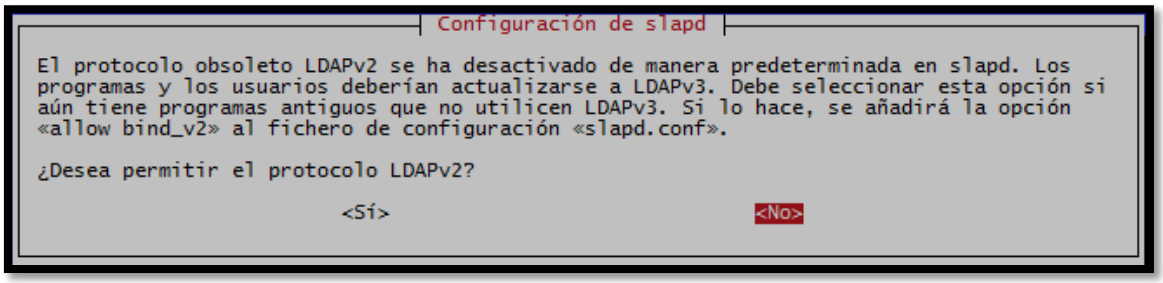


Figura 317 Habilitar o Deshabilitar el protocolo LDAPv2

Fuente: Sistema Operativo Debian 6.0.7

Finalización de la Configuración

Finalmente terminamos con la reconfiguración de slapd con los parámetros previamente ingresados (Figura 318).

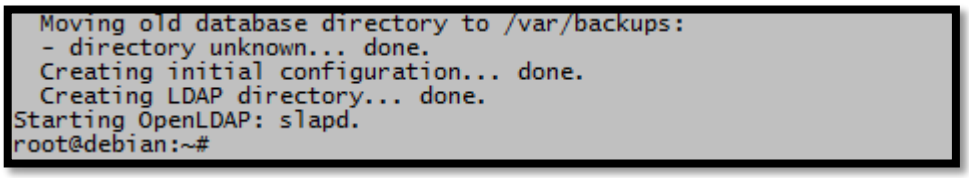


Figura 318 Finalización de la Configuración

Fuente: Sistema Operativo Debian 6.0.7

SCHEMA PARA USUARIOS UTN

Copiar openldap.schema

El esquema se lo puede obtener por medio de Internet o directamente del servidor freeradius que lo incluye por defecto en la instalación, para lo cual copiamos el archivo ubicado en /usr/share/doc/freeradius/examples/openldap.schema al directorio /etc/ldap/schema del servidor OpenLDAP.

```
cp /usr/share/doc/freeradius/examples/openldap.schema
/etc/ldap/schema/UsuariosLdapUtn.schema
```

Creación de un archivo temporal

A continuación creamos un archivo temporal UsuariosLdapUtn.conf dentro del directorio /tmp/ con el siguiente contenido:

include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/UsuariosLdapUtn.schema

Creación de un directorio temporal

Crear un directorio temporal que almacene toda la estructura de ficheros LDIF generados a partir del esquema radius:

mkdir /tmp/UsuariosLdap.d

Conversión al formato LDIF

El comando utilizado para la conversión es slaptest que se encarga de crear toda la estructura necesaria de ficheros LDIF con el siguiente comando:

slaptest -f /tmp/UsuariosLdapUtn.conf -F /tmp/UsuariosLdap.d/

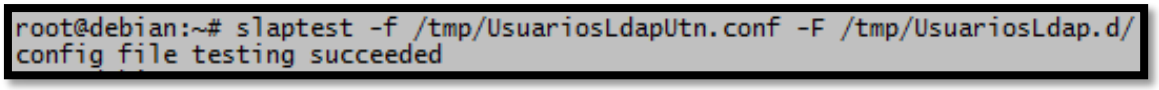


Figura 319 Conversión finalizada satisfactoriamente

Fuente: Sistema Operativo Debian 6.0.7

Modificaciones del fichero LDIF

Como resultado se obtiene el esquema radius en formato LDIF, el cual requiere un par de modificaciones en sus líneas para evitar posibles errores al momento de agregarlo al directorio. El fichero que se debe modificar es el siguiente:

/tmp/UsuariosLdap.d/cn\=config/cn\=schema/cn\=\{4\}UsuariosLdapUtn.ldif

Reemplazamos la siguiente configuración por defecto:

dn: cn={4}UsuariosLdapUtn
objectClass: olcSchemaConfig
cn: {4}UsuariosLdapUtn

Por la nueva configuración:

dn: cn=UsuariosLdapUtn,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: UsuariosLdapUtn

Las líneas finales del archivo, que incluyen los atributos de creación del objeto deben ser eliminadas:

structuralObjectClass: olcSchemaConfig

entryUUID: f48cf81e-ce38-1033-849a-bbdb76b78c0c

creatorsName: cn=config

createTimestamp: 20140911195250Z

entryCSN: 20140911195250.359816Z#000000#000#000000

modifiersName: cn=config

modifyTimestamp: 20140911195250Z

Añadir Esquema al Directorio LDAP

Finalmente, una vez que se han realizada los cambios pertinentes indicados en los pasos anteriores se añade el esquema al directorio principal LDAP usando el siguiente comando:

ldapadd -Q -Y EXTERNAL -H ldapi:/// -f /tmp/UsuariosLdap.d/cn\=config/cn\=schema/cn\=\{4\}UsuariosLdapUtn.ldif

Figura 320 Comando para añadir el esquema al Directorio LDAP

Fuente: Sistema Operativo Debian 6.0.7

Verificación del Esquema Radius

Para verificar que el esquema radius se agregó correctamente al directorio se puede usar los siguientes comandos que se indican en la Figura 321 y Figura 322:

ldapsearch -x -b "dc=utn,dc=edu,dc=ec"

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

# utn.edu.ec
dn: dc=utn,dc=edu,dc=ec
objectClass: top
objectClass: dcObject
objectClass: organization
o: utn.edu.ec
dc: utn

# admin, utn.edu.ec
dn: cn=admin,dc=utn,dc=edu,dc=ec
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

Figura 321 Verificación con ldapsearch -x -b "dc=utn,dc=edu,dc=ec"

Fuente: Sistema Operativo Debian 6.0.7

ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config

```
root@debian:~# ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config
dn: cn=schema,cn=config
objectClass: olcSchemaConfig
cn: schema
olcObjectIdentifier: OLcfg 1.3.6.1.4.1.4203.1.12.2
olcObjectIdentifier: OLcfgAt OLcfg:3
olcObjectIdentifier: OLcfgGlAt OLcfgAt:0
olcObjectIdentifier: OLcfgBkAt OLcfgAt:1
olcObjectIdentifier: OLcfgDbAt OLcfgAt:2
olcObjectIdentifier: OLcfgOvAt OLcfgAt:3
olcObjectIdentifier: OLcfgCtAt OLcfgAt:4
olcObjectIdentifier: OLcfgOc OLcfg:4
olcObjectIdentifier: OLcfgGlOc OLcfgOc:0
olcObjectIdentifier: OLcfgBkOc OLcfgOc:1
olcObjectIdentifier: OLcfgDbOc OLcfgOc:2
olcObjectIdentifier: OLcfgOvOc OLcfgOc:3
olcObjectIdentifier: OLcfgCtOc OLcfgOc:4
olcObjectIdentifier: OMsyn 1.3.6.1.4.1.1466.115.121.1
olcObjectIdentifier: OMsBoolean OMsyn:7
olcObjectIdentifier: OMsDN OMsyn:12
olcObjectIdentifier: OMsDirectoryString OMsyn:15
olcObjectIdentifier: OMsIA5String OMsyn:26
olcObjectIdentifier: OMsInteger OMsyn:27
olcObjectIdentifier: OMsOID OMsyn:38
olcObjectIdentifier: OMsOctetString OMsyn:40
```

Figura 322 Verificación con ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config

Fuente: Sistema Operativo Debian 6.0.7

INTEGRACIÓN DE LDAP CON EL SERVIDOR RADIUS

Configuración Módulo LDAP

Para que el servidor Radius local de la UTN consulte las credenciales de los usuarios admitidos para utilizar la red Eduroam se configura la dirección IP del servidor LDAP y los parámetros de autenticación de un usuario habilitado como administrador, por medio del cual se accederá al directorio para realizar las consultas y verificación de usuarios. El archivo de configuración es el siguiente:

```
/etc/freeradius/modules/ldap
ldap {
…
server = "172.20.1.4"
identity = "cn=admin,dc=utn,dc=edu,dc=ec"
password = ************
basedn = "dc=utn,dc=edu,dc=ec"
filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
base_filter = "(objectclass=radiusprofile)"
…
```

Además en el módulo de autenticación LDAP se va a utilizar como nombre de usuario el correo, es por ello que para no tener problemas en el acceso de cada usuario debemos cambiar la siguiente línea dentro del archivo LDAP:

```
filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
```

por,

```
filter = "(mail=%{User-Name})"
```

Configuración de LDAP en Freeradius

Para que el servidor freeradius realice la autenticación y autorización de usuarios mediante el servidor LDAP se debe habilitar algunos parámetros en los archivos de configuración de freeradius default e inner-tunnel ubicados dentro de /etc/freeradius/sites-available/, a continuación se muestra las respectivas configuraciones:

```
/etc/freeradius/sites-enabled/default
    authorize {
     …
```

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

/etc/freeradius/sites-enabled/inner-tunnel

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

Reiniciar el Servicio

Una vez que hemos realizado todos los cambios necesarios debemos iniciar, reiniciar o parar el servicio de LDAP de la siguiente manera:

```
invoke-rc.d slapd start
invoke-rc.d slapd restart
invoke-rc.d slapd stop
```

ó

```
/etc/init.d/slapd start
/etc/init.d/slapd restart
/etc/init.d/slapd stop
```

INTERFAZ DE ADMINISTRACIÓN PHPLDAPADMIN

PhpLDAPadmin es una herramienta basado en una interfaz WEB escrita en PHP, que permite administrar de una forma sencilla un servidor LDAP desde cualquier lugar, a través de un sencillo navegador WEB. Este cliente es phpLDAPadmin, aunque también se conoce de forma abreviada como PLA.

PhpLDAPadmin dispone de una vista con forma de árbol jerárquico que permite recorrer toda la estructura del directorio. Además, incorpora funciones de búsqueda avanzadas que lo convierten en una herramienta intuitiva para consultar y administrar el directorio LDAP.
Al inicio del manual se procedió a instalar phpLDAPadmin, por lo que nos resta realizar las configuraciones respectivas para establecer la conexión con el directorio LDAP.

Establecimiento de conexión de phpLDAPadmin con LDAP

Para establecer la conexión de phpLDAPadmin con el servidor LDAP debemos realizar unos cambios de configuración en el archivo config.php ubicado en el siguiente fichero:

/etc/phpLDAPadmin/config.php

Realizamos los cambios que nos permita evaluar el directorio “dc=utn,dc=edu,dc=ec”, tal como se indica en la Figura 323.

```
$servers->setValue('server','base',array('dc=example,dc=com'));
$servers->setValue('login','bind_id','cn=admin,dc=example,dc=com');
```

por,

```
$servers->setValue('server','base',array('dc=utn,dc=edu,dc=ec'));
$servers->setValue('login','bind_id','cn=admin,dc=utn,dc=edu,dc=ec');
```

```
/* A convenient name that will appear in the tree viewer and throughout
   phpLDAPadmin to identify this LDAP server to users. */
$servers->setValue('server','name','My LDAP Server');

/* Examples:
   'ldap.example.com',
   'ldaps://ldap.example.com/',
   'ldapi://%2fusr%local%2fvar%2frun%2fldapi'
           (Unix socket at /usr/local/var/run/ldap) */
$servers->setValue('server','host','127.0.0.1');

/* The port your LDAP server listens on (no quotes). 389 is standard. */
// $servers->setValue('server','port',389);

/* Array of base DNs of your LDAP server. Leave this blank to have phpLDAPadmin
   auto-detect it for you. */
$servers->setValue('server','base',      'dc=utn,dc=edu,dc=ec'));

/* Four options for auth_type:
   1. 'cookie': you will login via a web form, and a client-side cookie will
      store your login dn and password.
   2. 'session': same as cookie but your login dn and password are stored on the
      web server in a persistent session variable.
   3. 'http': same as session but your login dn and password are retrieved via
      HTTP authentication.
   4. 'config': specify your login dn and password here in this config file. No
      login will be required to use phpLDAPadmin for this server.

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

Figura 323 Conexión phpLDAPadmin - Servidor LDAP

Fuente: Sistema Operativo Debian 6.0.7

Login de Acceso

Una vez que hemos terminado de realizar las configuraciones respectivas podemos acceder a la interfaz WEB desde cualquier navegador ingresando la siguiente dirección:

http://172.20.1.4/phpldapadmin

Y automáticamente nos aparece la interfaz gráfica de phpLDAPadmin como se muestra en la Figura 324.

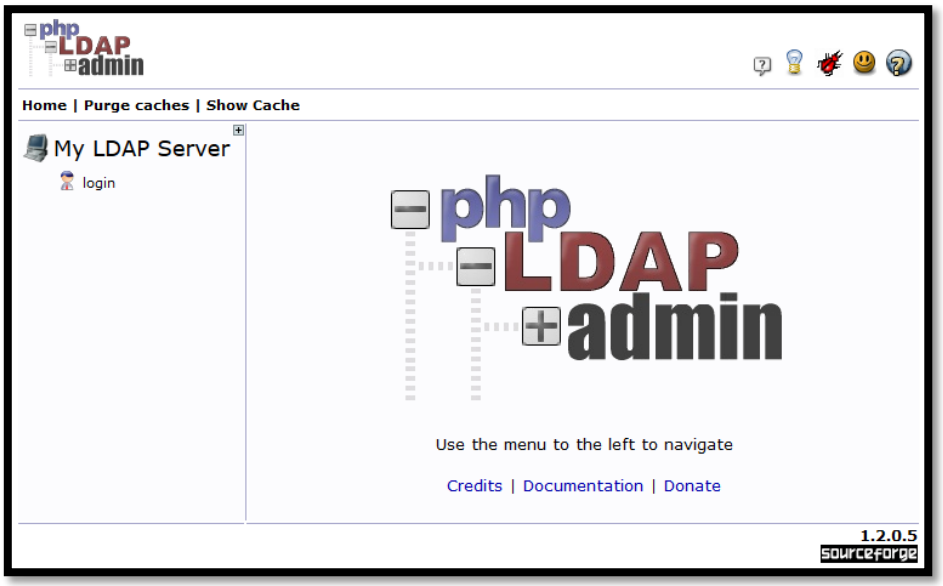


Figura 324 Interfaz principal phpLDAPadmin

Fuente: Sistema Operativo Debian 6.0.7

En la parte izquierda de la página principal hacemos clic en el icono de “login” donde ingresaremos la contraseña de administrador configurada en el fichero /etc/freeradius/modules/ldap (Figura 325).

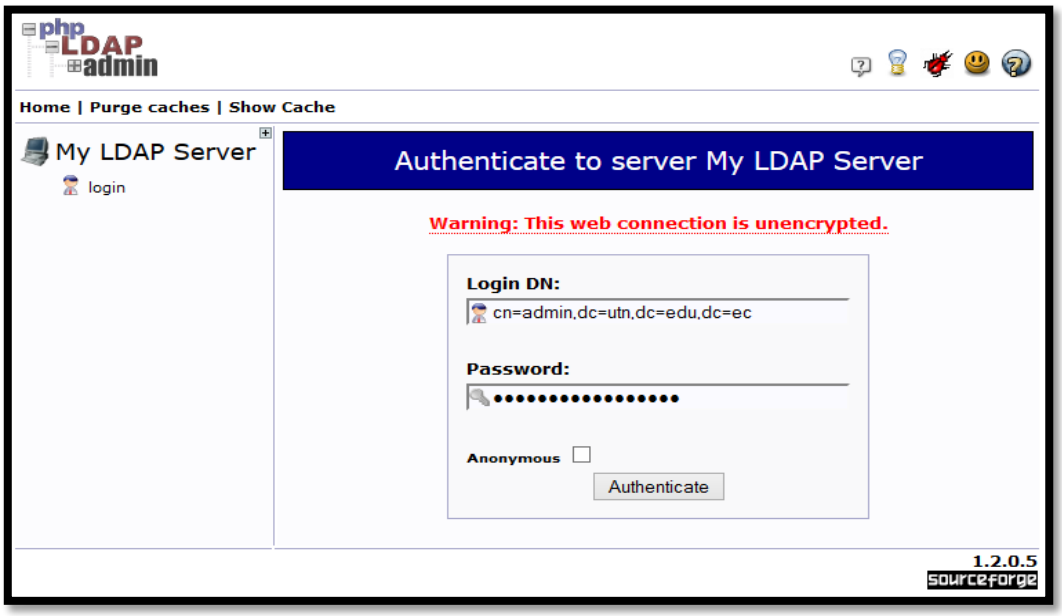


Figura 325 Ingreso de la contraseña de Administrador

Fuente: Sistema Operativo Debian 6.0.7

Ahora que hemos ingresado la contraseña de administrador, nos encontramos dentro de la interfaz gráfica donde se crearán algunos parámetros (unidades organizativas, grupos) que almacenarán todos los usuarios de la UTN a la red Eduroam.

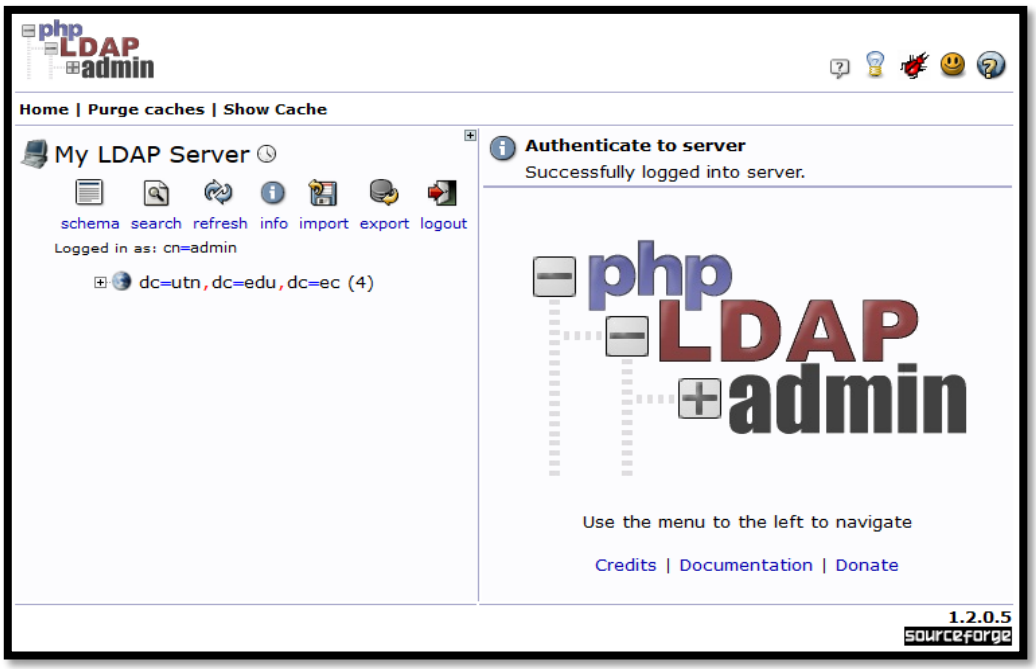


Figura 326 Login de Acceso realizado satisfactoriamente

Fuente: Sistema Operativo Debian 6.0.7

Creación de Unidades Organizativas

Para agregar una o varias Unidades Organizativas se debe crear un archivo con el formato ".ldif" con la información del nombre, el directorio raíz y los objetos principales de LDAP. A continuación se muestra el script de configuración de las Unidades Organizativas creadas:

```
dn: ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
objectClass: top
objectClass: organizationalUnit
ou: ESTUDIANTES

dn: ou=DOCENTES,dc=utn,dc=edu,dc=ec
objectClass: top
objectClass: organizationalUnit
ou: DOCENTES

dn: ou=ADMINISTRATIVOS,dc=utn,dc=edu,dc=ec
objectClass: top
objectClass: organizationalUnit
ou: ADMINISTRATIVOS
```

Para agregar el grupo de Unidades Organizativas hacemos clic en el icono "import" (Figura 327) que se encuentra en la parte superior izquierda que nos redirecciona a un template para importar los ficheros .ldif o ingresarlos manualmente

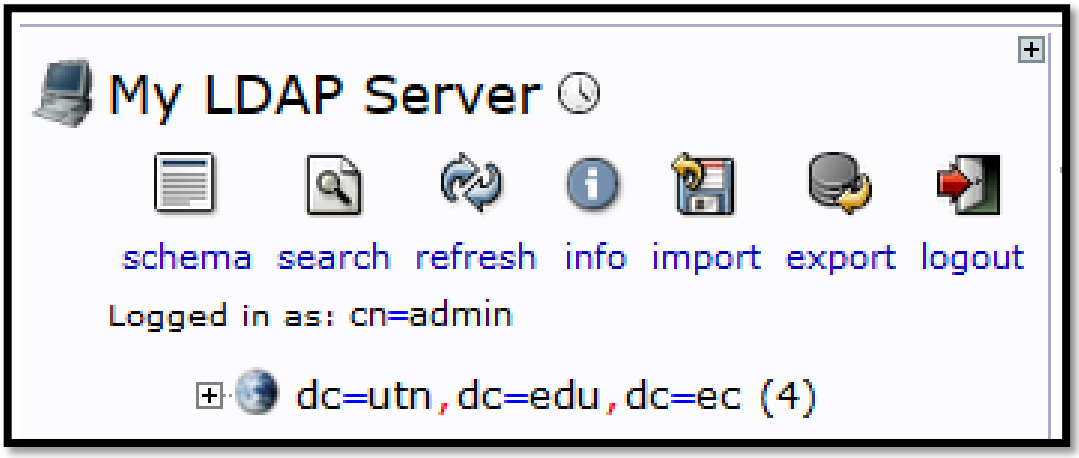


Figura 327 Seleccionamos el botón "import"

Fuente: Sistema Operativo Debian 6.0.7

Una vez que se visualiza la siguiente pantalla, para importar podemos hacerlo de dos maneras: la primera haciendo clic en "**Examinar**" donde seleccionamos el archivo .ldif y la segunda es ingresando todo el archivo de configuración en el espacio en blanco debajo de la siguiente sentencia "**Or paste your LDIF here**" (Figura 328).

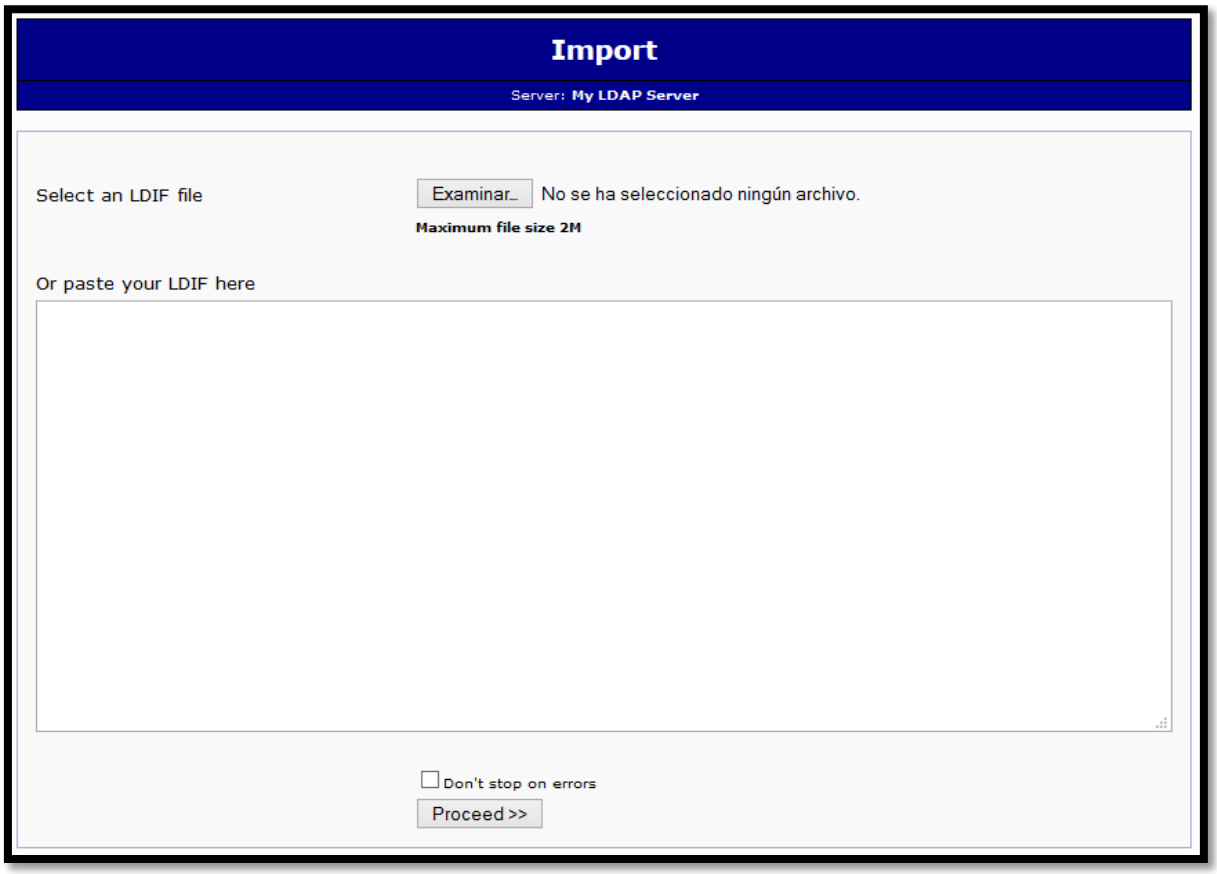


Figura 328 Selección del fichero .ldif

Fuente: Sistema Operativo Debian 6.0.7

Posteriormente luego de haber seleccionado el fichero, hacemos clic en el botón "**Proceed >>**" como se puede ver en la Figura 329.

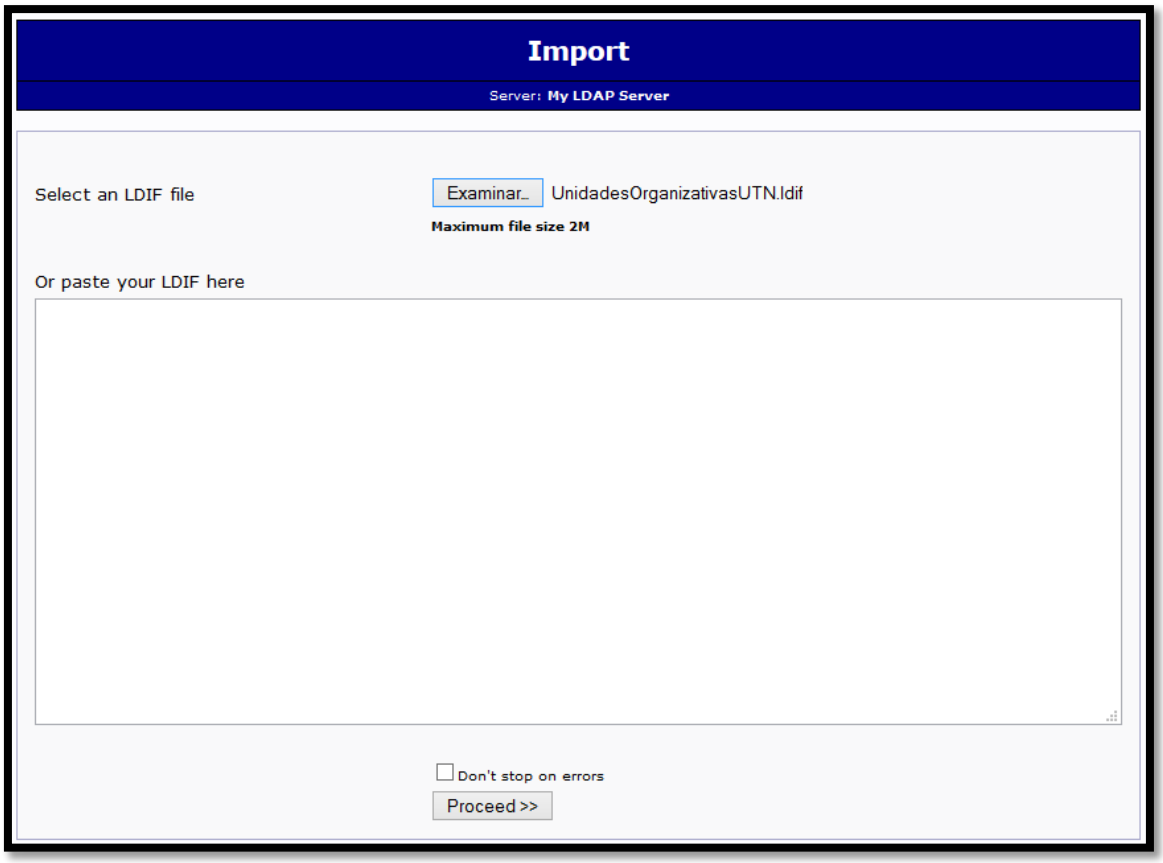


Figura 329 Cargar el archivo .ldif de las Unidades Organizativas de la UTN

Fuente: Sistema Operativo Debian 6.0.7

Para finalizar nos muestra un mensaje indicando que se agregado correctamente las Unidades Organizativas como se indica en la Figura 330.

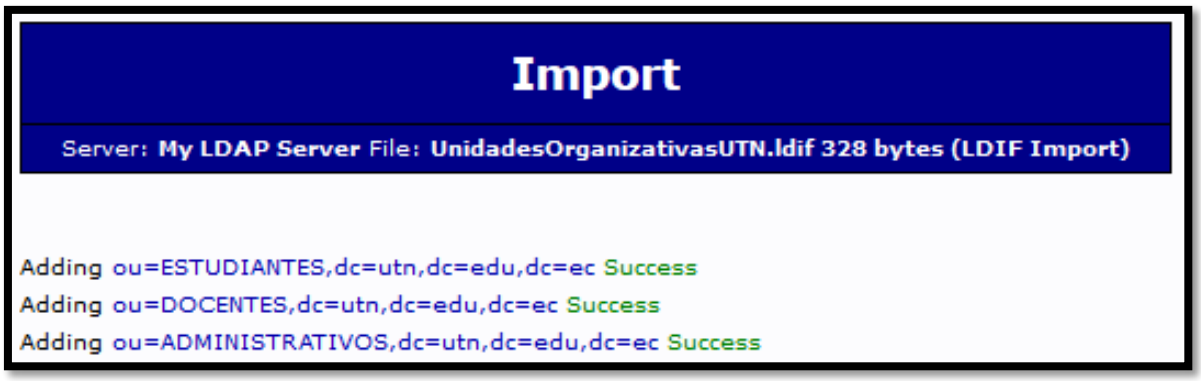


Figura 330 Carga exitosa de las Unidades Organizativas de la UTN

Fuente: Sistema Operativo Debian 6.0.7

Para verificar que se ha agregado las Unidades Organizativas de Estudiantes, Docentes y Administrativos, podemos fijarnos en el menú principal de phpLDAPadmin como se muestra en la Figura 331.

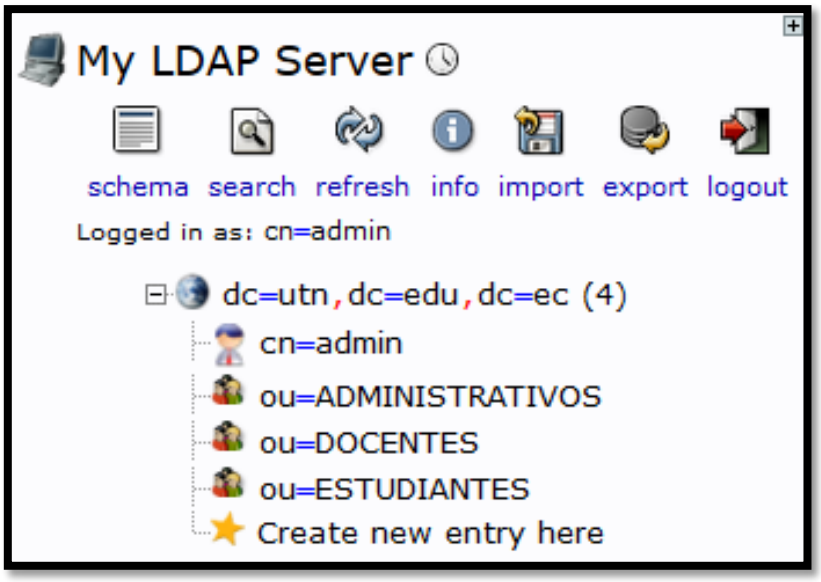


Figura 331 Unidades Organizativas de la UTN creadas

Fuente: Sistema Operativo Debian 6.0.7

Creación de Grupos por Facultades

Para agregar uno o varios grupos se debe crear un archivo con el formato ".ldif" con la información del nombre, el directorio raíz y los objetos principales de LDAP. A continuación se muestra el script de configuración de los Grupos por Facultades creados:

dn: cn=FICA,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec

objectclass: posixGroup

objectclass: top

cn: FICA

gidNumber: 100000

dn: cn=FACAE,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec

objectclass: posixGroup

objectclass: top

cn: FACAE

gidNumber: 100001

dn: cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec

objectclass: posixGroup

objectclass: top

cn: FECYT

gidNumber: 100002

dn: cn=FICAYA,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec

objectclass: posixGroup

objectclass: top

cn: FICAYA

gidNumber: 100003

dn: cn=FCCSS,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec

objectclass: posixGroup

objectclass: top

cn: FCCSS

gidNumber: 100004

Para agregar los Grupos por Facultades hacemos clic en el icono “import” (Figura 332) que se encuentra en la parte superior izquierda que nos redirecciona a un template para importar los ficheros .ldif o ingresarlos manualmente.

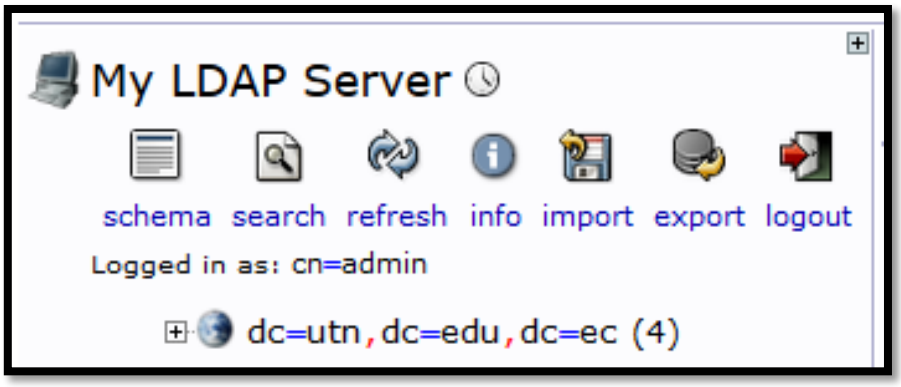


Figura 332 Seleccionamos el botón “import”

Fuente: Sistema Operativo Debian 6.0.7

Una vez que se visualiza la siguiente pantalla, para importar podemos hacerlo de dos maneras: la primera haciendo clic en "**Examinar**" donde seleccionamos el archivo .ldif y la segunda es ingresando todo el archivo de configuración en el espacio en blanco debajo de la siguiente sentencia "**Or paste your LDIF here**" (Figura 333).

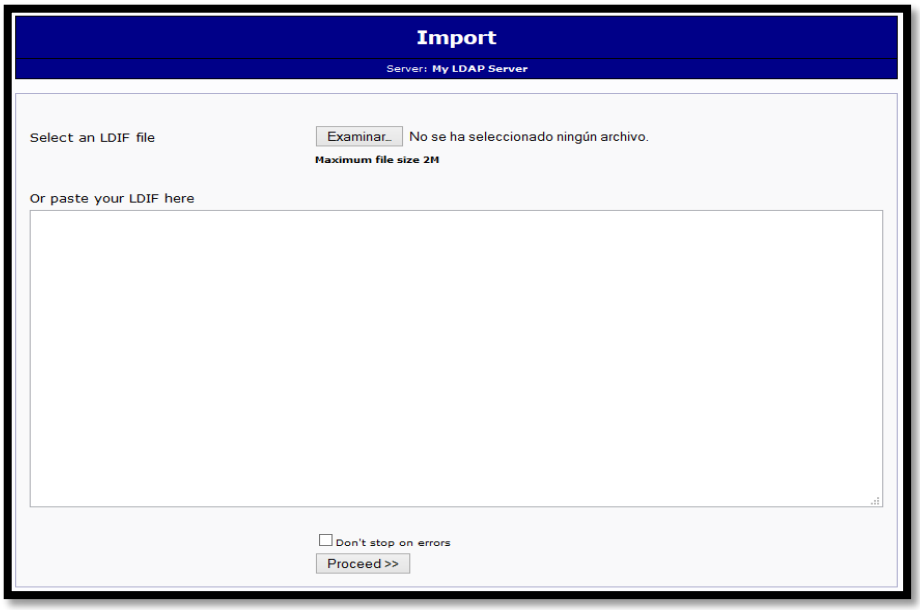


Figura 333 Selección del fichero .ldif

Fuente: Sistema Operativo Debian 6.0.7

Posteriormente luego de haber seleccionado el fichero, hacemos clic en el botón "**Proceed >>**" como se puede ver en la Figura 334.

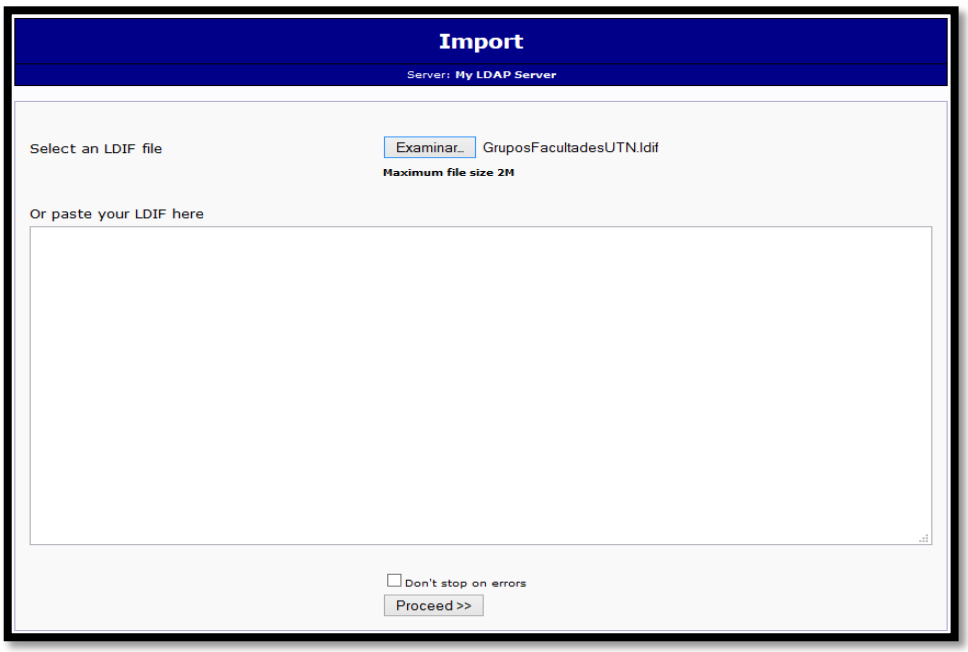


Figura 334 Cargar el archivo .ldif de los Grupos por Facultades

Fuente: Sistema Operativo Debian 6.0.7

Para finalizar nos muestra un mensaje indicando que se agregado correctamente las Unidades Organizativas como se indica en la Figura 335.

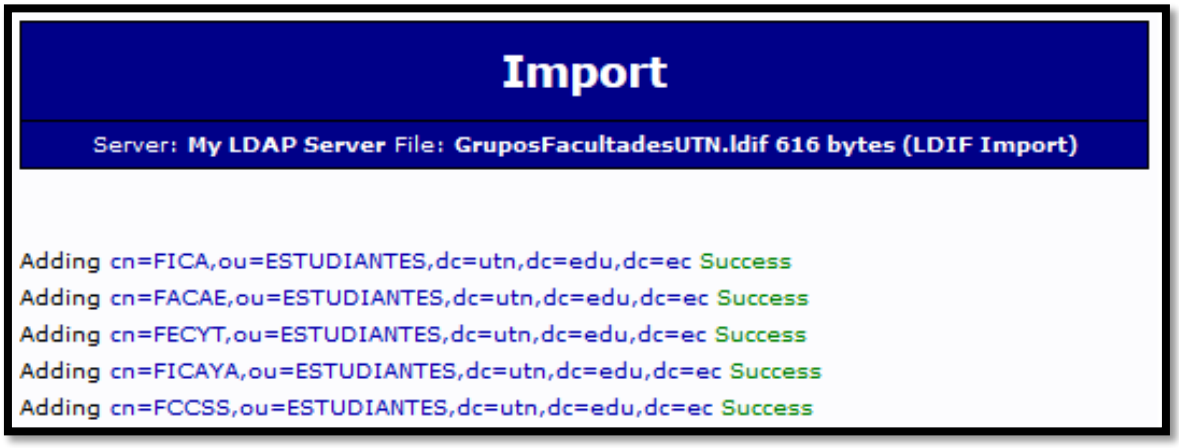


Figura 335 Carga exitosa de los Grupos por Facultades

Fuente: Sistema Operativo Debian 6.0.7

Para verificar que se han agregado los Grupos por Facultades, podemos fijarnos en el menú principal de phpLDAPadmin como se muestra en la Figura 336.

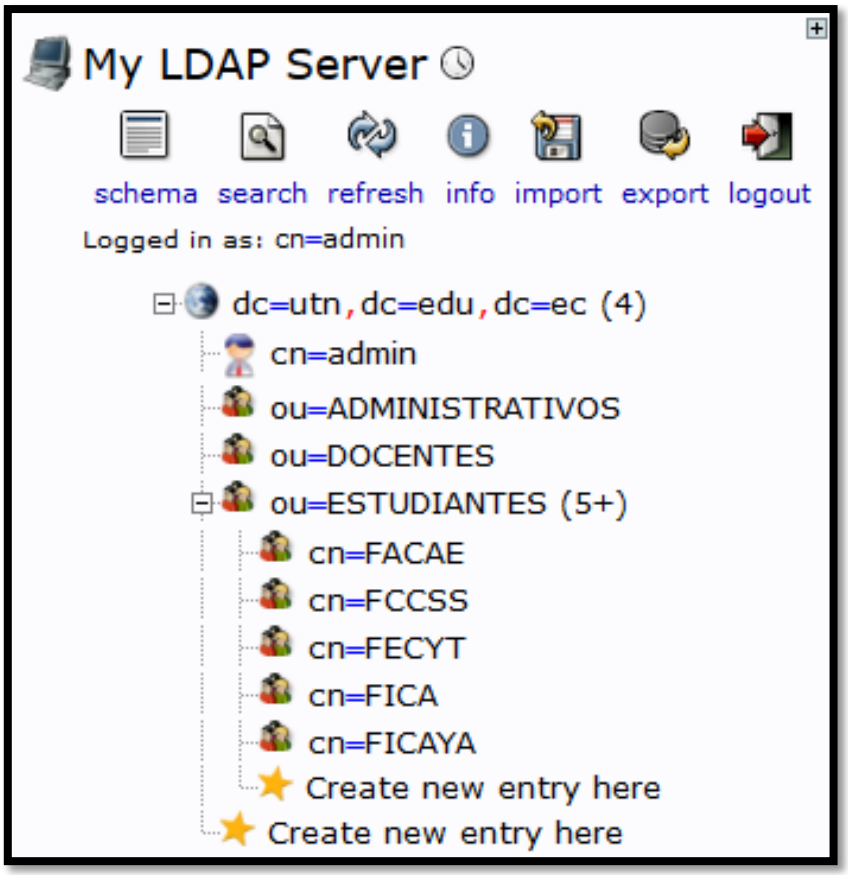


Figura 336 Grupos por Facultades creados

Fuente: Sistema Operativo Debian 6.0.7

Creación de Grupos por Carreras

Para agregar uno o varios grupos se debe crear un archivo con el formato “.ldif” con la información del nombre, el directorio raíz y los objetos principales de LDAP. A continuación se muestra el script de configuración de los Grupos por Carreras creados:

```
#####################################################
## FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS ##
#####################################################
dn: cn=CARRERA DE INGENIERIA EN ELECTRONICA Y REDES DE
COMUNICACION,cn=FICA,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA EN ELECTRONICA Y REDES DE COMUNICACION
gidNumber: 100000
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA EN
MECATRONICA,cn=FICA,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA EN MECATRONICA
gidNumber: 100000
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA EN SISTEMAS
COMPUTACIONALES,cn=FICA,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES
gidNumber: 100000
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA
INDUSTRIAL,cn=FICA,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA INDUSTRIAL
gidNumber: 100000
objectclass: posixGroup
objectclass: top
```

dn: cn=CARRERA DE INGENIERIA TEXTIL,cn=FICA,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA TEXTIL
gidNumber: 100000
objectclass: posixGroup
objectclass: top
##
FACULTAD DE CIENCIAS ADMINISTRATIVAS Y ECONÓMICAS
##
dn: cn=CARRERA DE INGENIERIA COMERCIAL,cn=FACAE,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA COMERCIAL
gidNumber: 100001
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA EN ADMINISTRACION PUBLICA DE GOBIERNOS SECCIONALES,cn=FACAE,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA EN ADMINISTRACION PUBLICA DE GOBIERNOS SECCIONALES
gidNumber: 100001
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA EN CONTABLIDAD Y AUDITORIA CPA,cn=FACAE,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA EN CONTABLIDAD Y AUDITORIA CPA PRESENCIAL
gidNumber: 100001
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA EN ECONOMIA MENCION FINANZAS,cn=FACAE,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA EN ECONOMIA MENCION FINANZAS
gidNumber: 100001
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA EN MERCADOTECNIA,cn=FACAE,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA EN MERCADOTECNIA
gidNumber: 100001
objectclass: posixGroup
objectclass: top

##
FACULTAD DE EDUCACIÓN CIENCIA Y TECNOLOGÍA
##
dn: cn=CARRERA DE INGENIERIA GESTION Y DESARROLLO SOCIAL,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA GESTION Y DESARROLLO SOCIAL
gidNumber: 100002
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA EN MANTENIMIENTO AUTOMOTRIZ,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA EN MANTENIMIENTO AUTOMOTRIZ
gidNumber: 100002
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA EN MANTENIMIENTO ELECTRICO,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA EN MANTENIMIENTO ELECTRICO
gidNumber: 100002
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE LICENCIATURA EN ARTES PLASTICAS,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE LICENCIATURA EN ARTES PLASTICAS
gidNumber: 100002
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE LICENCIATURA EN DISENO GRAFICO,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE LICENCIATURA EN DISENO GRAFICO PRESENCIAL
gidNumber: 100002
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE LICENCIATURA EN DISENO Y PUBLICIDAD,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE LICENCIATURA EN DISENO Y PUBLICIDAD PRESENCIAL
gidNumber: 100002
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE LICENCIATURA EN RELACIONES PUBLICAS,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE LICENCIATURA EN RELACIONES PUBLICAS
gidNumber: 100002
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE PSICOLOGIA,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE PSICOLOGIA
gidNumber: 100002
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE LICENCIATURA EN SECRETARIADO EJECUTIVO EN ESPANOL,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE LICENCIATURA EN SECRETARIADO EJECUTIVO EN ESPANOL
gidNumber: 100002
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA EN TURISMO,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec

cn: CARRERA DE INGENIERIA EN TURISMO
gidNumber: 100002
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE LICENCIATURA EN CONTABILIDAD Y
COMPUTACION,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE LICENCIATURA EN CONTABILIDAD Y COMPUTACION
gidNumber: 100002
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE LICENCIATURA EN EDUCACION
FISICA,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE LICENCIATURA EN EDUCACION FISICA
gidNumber: 100002
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE LICENCIATURA EN FISICO
MATEMATICO,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE LICENCIATURA EN FISICO MATEMATICO
gidNumber: 100002
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE LICENCIATURA EN
INGLES,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE LICENCIATURA EN INGLES
gidNumber: 100002
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE LICENCIATURA EN PSICOLOGIA EDUCATIVA Y O.
V.,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE LICENCIATURA EN PSICOLOGIA EDUCATIVA Y O. V.
gidNumber: 100002

objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE LICENCIATURA EN ENTRENAMIENTO DEPORTIVO,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE LICENCIATURA EN ENTRENAMIENTO DEPORTIVO
gidNumber: 100002
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE LICENCIATURA EN PARVULARIA,cn=FECYT,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE LICENCIATURA EN PARVULARIA
gidNumber: 100002
objectclass: posixGroup
objectclass: top

###
FACULTAD DE INGENIERÍA EN CIENCIAS AGROPECUARIAS Y AMBIENTALES
###
dn: cn=CARRERA DE INGENIERIA AGROINDUSTRIAL,cn=FICAYA,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA AGROINDUSTRIAL
gidNumber: 100003
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA EN AGRONEGOCIOS AVALUOS Y CATASTROS,cn=FICAYA,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA EN AGRONEGOCIOS AVALUOS Y CATASTROS
gidNumber: 100003
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA EN AGROPECUARIA,cn=FICAYA,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec

cn: CARRERA DE INGENIERIA EN AGROPECUARIA
gidNumber: 100003
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA EN BIOTECNOLOGIA,cn=FICAYA,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA EN BIOTECNOLOGIA
gidNumber: 100003
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA EN ENERGIAS RENOVABLES,cn=FICAYA,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA EN ENERGIAS RENOVABLES
gidNumber: 100003
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA EN RECURSOS NATURALES RENOVABLES,cn=FICAYA,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA EN RECURSOS NATURALES RENOVABLES
gidNumber: 100003
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE INGENIERIA FORESTAL,cn=FICAYA,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE INGENIERIA FORESTAL
gidNumber: 100003
objectclass: posixGroup
objectclass: top

##
FACULTAD DE CIENCIAS DE LA SALUD
##

dn: cn=CARRERA DE LICENCIATURA EN ENFERMERIA,cn=FCCSS,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE LICENCIATURA EN ENFERMERIA
gidNumber: 100004
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE LICENCIATURA EN TERAPIA FISICA MEDICA,cn=FCCSS,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE LICENCIATURA EN TERAPIA FISICA MEDICA
gidNumber: 100004
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE GASTRONOMIA,cn=FCCSS,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE GASTRONOMIA
gidNumber: 100004
objectclass: posixGroup
objectclass: top

dn: cn=CARRERA DE LICENCIATURA EN NUTRICION Y SALUD COMUNITARIA,cn=FCCSS,ou=ESTUDIANTES,dc=utn,dc=edu,dc=ec
cn: CARRERA DE LICENCIATURA EN NUTRICION Y SALUD COMUNITARIA
gidNumber: 100004
objectclass: posixGroup
objectclass: top

Nota: *El parámetro “gidNumber” hace referencia a un código único con el que se crearon los Grupos por Facultades; es decir, que cada carrera pertenece a su respectiva facultad.*

Para agregar los Grupos por Carreras hacemos clic en el icono “import” (Figura 337) que se encuentra en la parte superior izquierda que nos redirecciona a un template para importar los ficheros .ldif o ingresarlos manualmente.

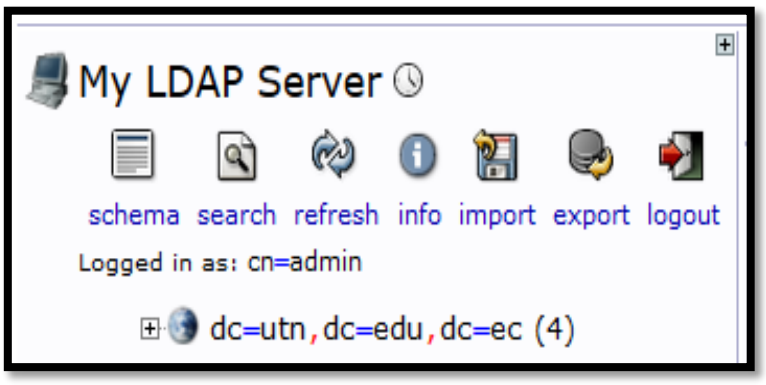


Figura 337 Seleccionamos el botón “import”

Fuente: Sistema Operativo Debian 6.0.7

Una vez que se visualiza la siguiente pantalla, para importar podemos hacerlo de dos maneras: la primera haciendo clic en “**Examinar**” donde seleccionamos el archivo .ldif y la segunda es ingresando todo el archivo de configuración en el espacio en blanco debajo de la siguiente sentencia “**Or paste your LDIF here**” (Figura 338).

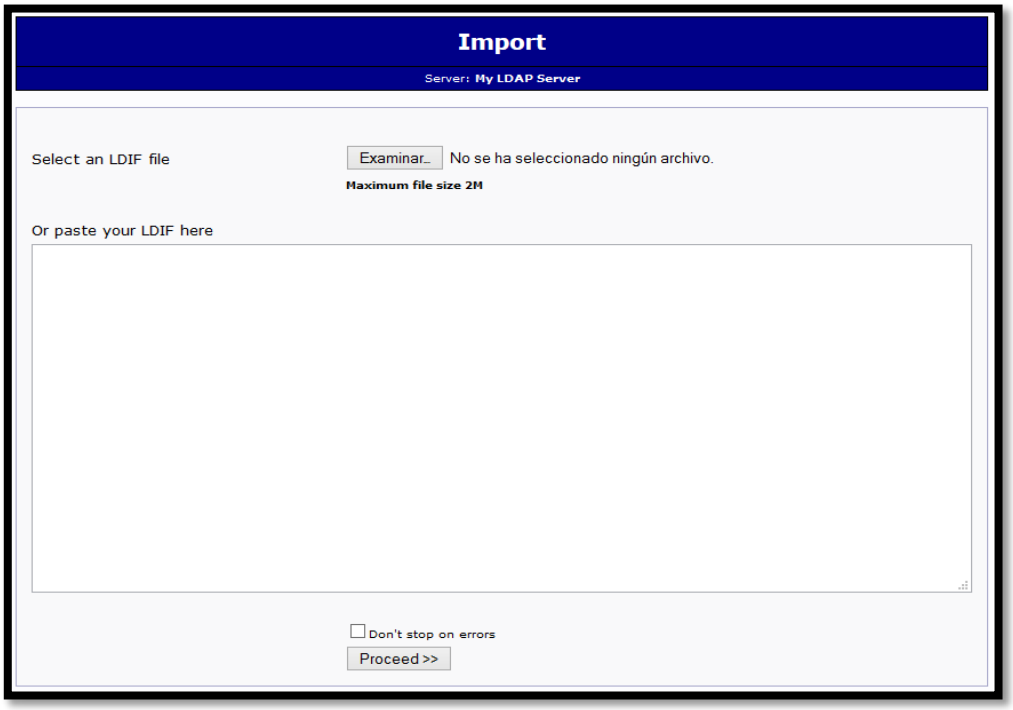


Figura 338 Selección del fichero .ldif

Fuente: Sistema Operativo Debian 6.0.7

Posteriormente luego de haber seleccionado el fichero, hacemos clic en el botón “**Proceed >>**” como se puede ver en la Figura 339.

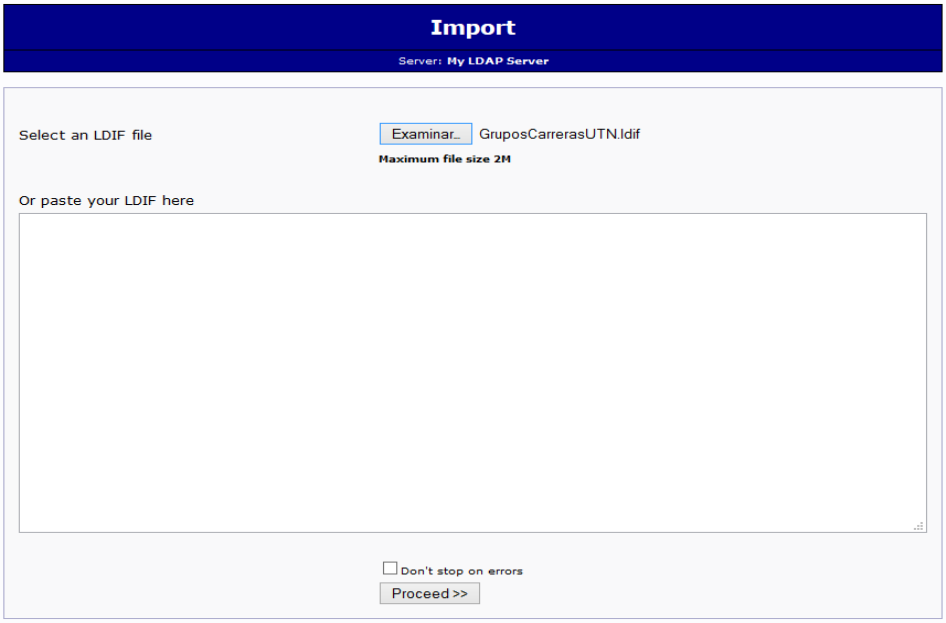


Figura 339 Cargar el archivo .ldif de los Grupos por Carreras

Fuente: Sistema Operativo Debian 6.0.7

Para finalizar nos muestra un mensaje indicando que se agregado correctamente las Unidades Organizativas como se indica en la Figura 340.

Figura 340 Carga exitosa de los Grupos por Carreras

Fuente: Sistema Operativo Debian 6.0.7

Para verificar que se han agregado los Grupos por Facultades, podemos fijarnos en el menú principal de phpLDAPadmin como se muestra en la Figura 336.

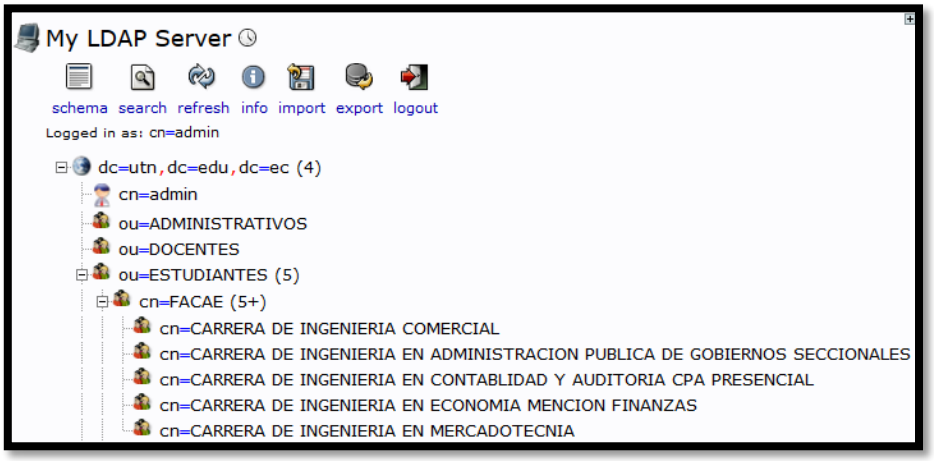


Figura 341 Grupos por Carreras creados

Fuente: Sistema Operativo Debian 6.0.7

Creación de Usuarios de la UTN

Para agregar uno o varios usuarios se debe crear un archivo con el formato “.ldif” con la información de nombres, apellidos, carrera, facultad, mail institucional, cédula, el directorio raíz y los objetos principales de LDAP. A continuación se muestra como ejemplo el script de configuración de un usuario creado:

dn: cn=Edwin Vinicio Guerra Morales,cn=CARRERA DE INGENIERIA EN ELECTRONICA Y REDES DE COMUNICACION,cn=FICA,ou=Estudiantes,dc=utn,dc=edu,dc=ec
cn: Edwin Vinicio Guerra Morales
description: Ingenieria En Electronica Y Redes De Comunicacion
mail: evguerram@utn.edu.ec
objectClass: person
objectClass: uidObject
objectClass: top
objectClass: radiusprofile
objectClass: inetOrgPerson
radiusTunnelMediumType: IEEE-802
radiusTunnelPrivateGroupId: 128
radiusTunnelType: VLAN
sn: Guerra Morales
uid: prueba@utn.edu.ec
userPassword: 0123456789

Para agregar uno o varios usuarios hacemos clic en el icono “import” (Figura 342) que se encuentra en la parte superior izquierda que nos redirecciona a un template para importar los ficheros .ldif o ingresarlos manualmente.

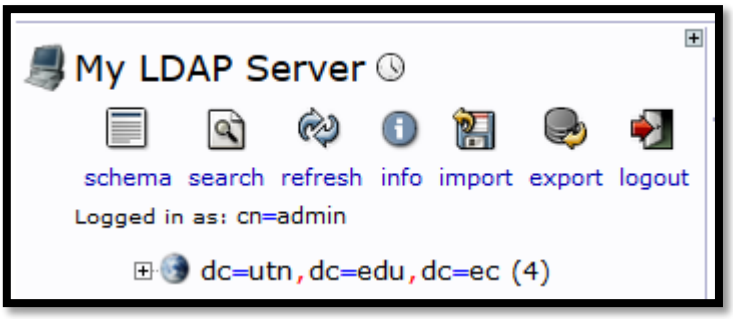


Figura 342 Seleccionamos el botón “import”

Fuente: Sistema Operativo Debian 6.0.7

Una vez que se visualiza la siguiente pantalla, para importar podemos hacerlo de dos maneras: la primera haciendo clic en “**Examinar**” donde seleccionamos el archivo .ldif y la segunda es ingresando todo el archivo de configuración en el espacio en blanco debajo de la siguiente sentencia “**Or paste your LDIF here**”. Posteriormente luego de haber ingresado el usuario, hacemos clic en el botón “**Proceed >>**” como se puede ver en la Figura 343.

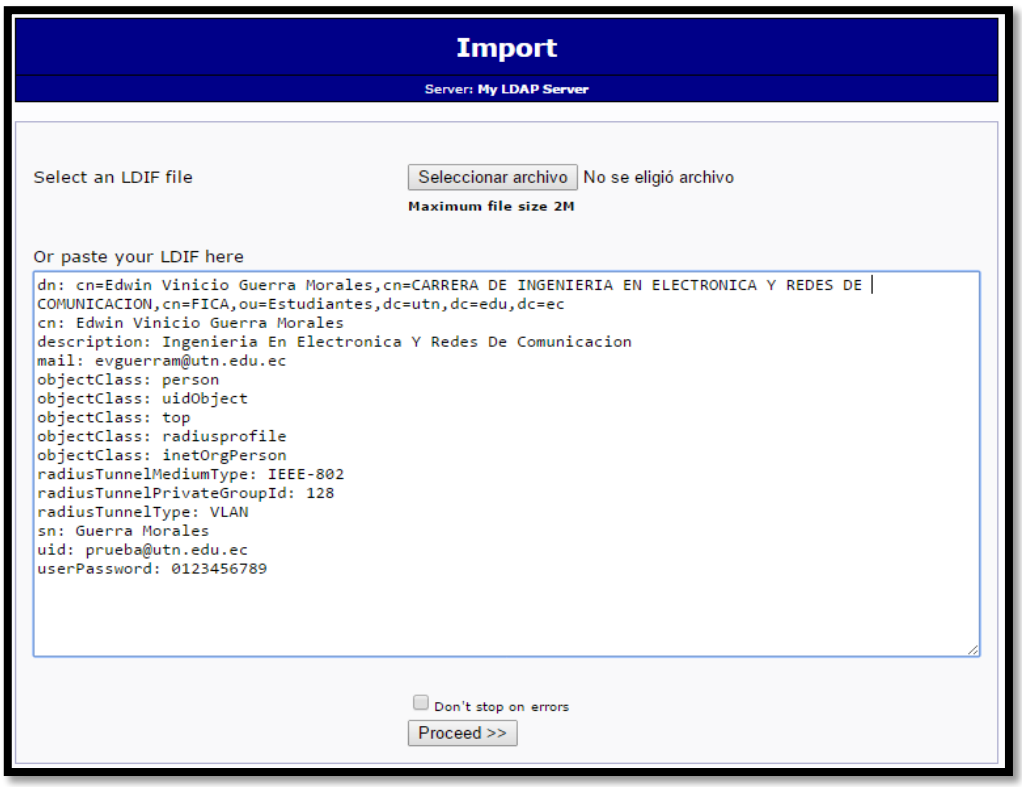


Figura 343 Cargar el archivo .ldif de un Usuario UTN

Fuente: Sistema Operativo Debian 6.0.7

Para finalizar nos muestra un mensaje indicando que se agregado correctamente el Usuario UTN en la Unidad Organizativa Estudiantes como se indica en la Figura 344.

Figura 344 Carga exitosa de un Usuario UTN

Fuente: Sistema Operativo Debian 6.0.7

Para verificar que el usuario se ha agregado, podemos fijarnos en el menú principal de phpLDAPadmin como se muestra en la Figura 345.

Figura 345 Usuario UTN creado

Fuente: Sistema Operativo Debian 6.0.7

Modificación de Grupos

En primer lugar para la creación de grupos debemos modificar el ID que se encuentra dentro del archivo siguiente:

/etc/phpldapadmin/templates/creation/posixGroup.xml

Una vez que hemos ingresado nos dirigimos a la siguiente línea:

<readonly>1</readonly>

En la cual reemplazamos el 1 por el 0 como se verifica a continuación:

<readonly>0</readonly>

Para editar la información nos ingresamos haciendo un clic en el grupo que deseamos modificar, donde nos visualizará la ventana que se indica en la Figura 346 en la cual seleccionamos “Default”. A continuación se presenta un ejemplo con el grupo “cn=FICA”.

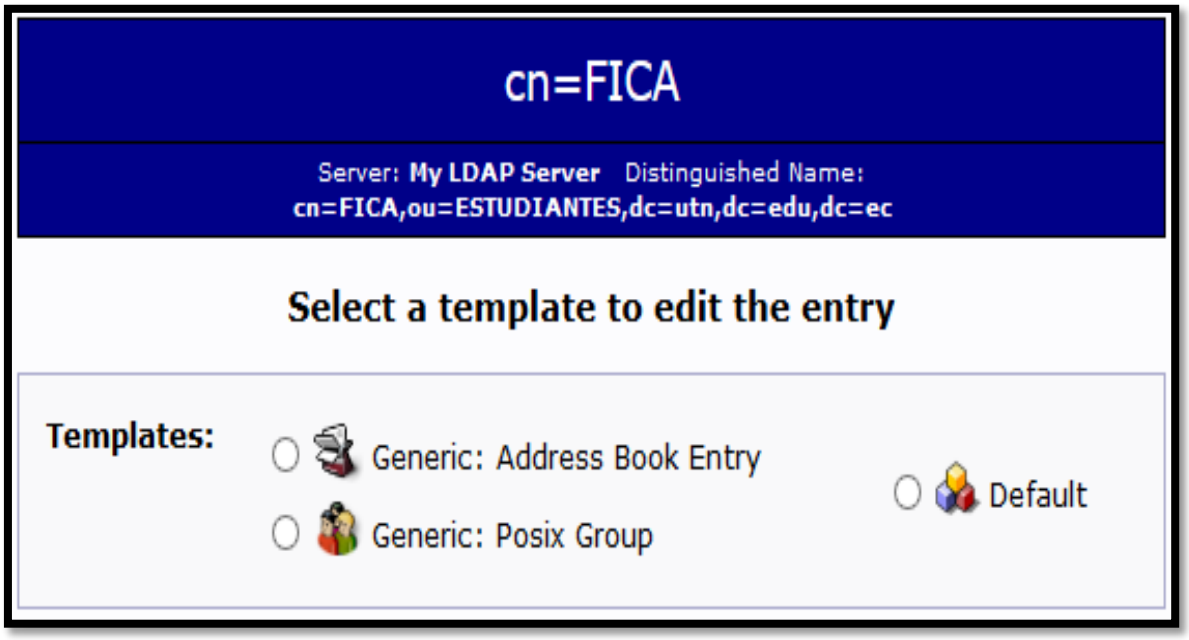


Figura 346 Ventana de Selección de un Template para editar o eliminar la entrada de un Grupo

Fuente: Sistema Operativo Debian 6.0.7

De esta manera ingresamos a los parámetros de configuración del grupo “cn=FICA” donde podemos realizar los cambios necesarios editando cada uno de los campos requeridos (Figura 347) y actualizamos haciendo clic en el botón “Update Object” ubicado en la parte inferior del mismo template.

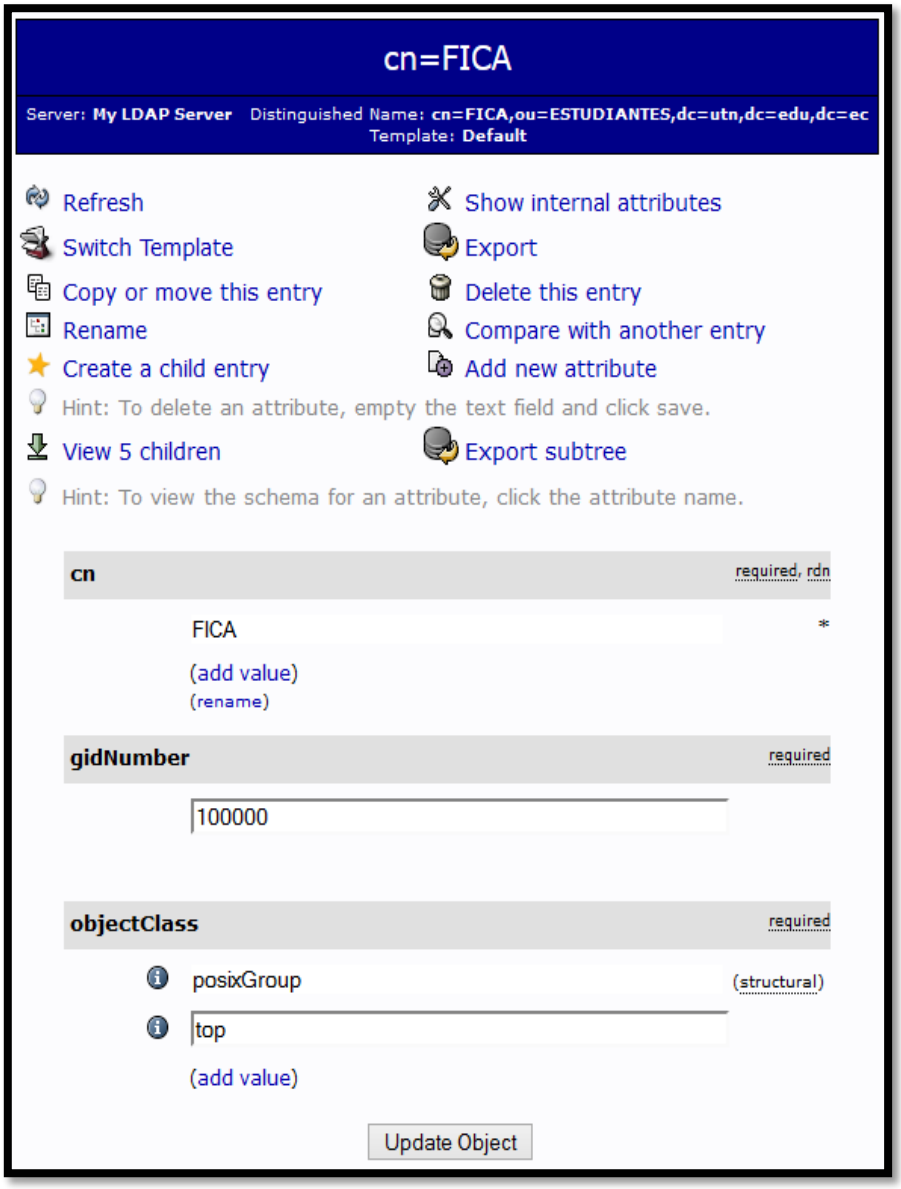


Figura 347 Información del Grupo “cn=FICA”

Fuente: Sistema Operativo Debian 6.0.7

Modificación de Usuarios

En primer lugar para la creación de usuarios debemos modificar el ID que se encuentra dentro del archivo siguiente:

/etc/phpldapadmin/templates/creation/posixAccount.xml

Una vez que hemos ingresado nos dirigimos a la siguiente línea:

<readonly>1</readonly>

En la cual reemplazamos el 1 por el 0 como se verifica a continuación:

<readonly>0</readonly>

Para editar la información nos ingresamos haciendo un clic en el usuario que deseamos modificar, donde nos visualizará la ventana que se indica en la Figura 348 en la cual seleccionamos “Default”. A continuación se presenta un ejemplo con el usuario “cn=Edwin Vinicio Guerra Morales”.

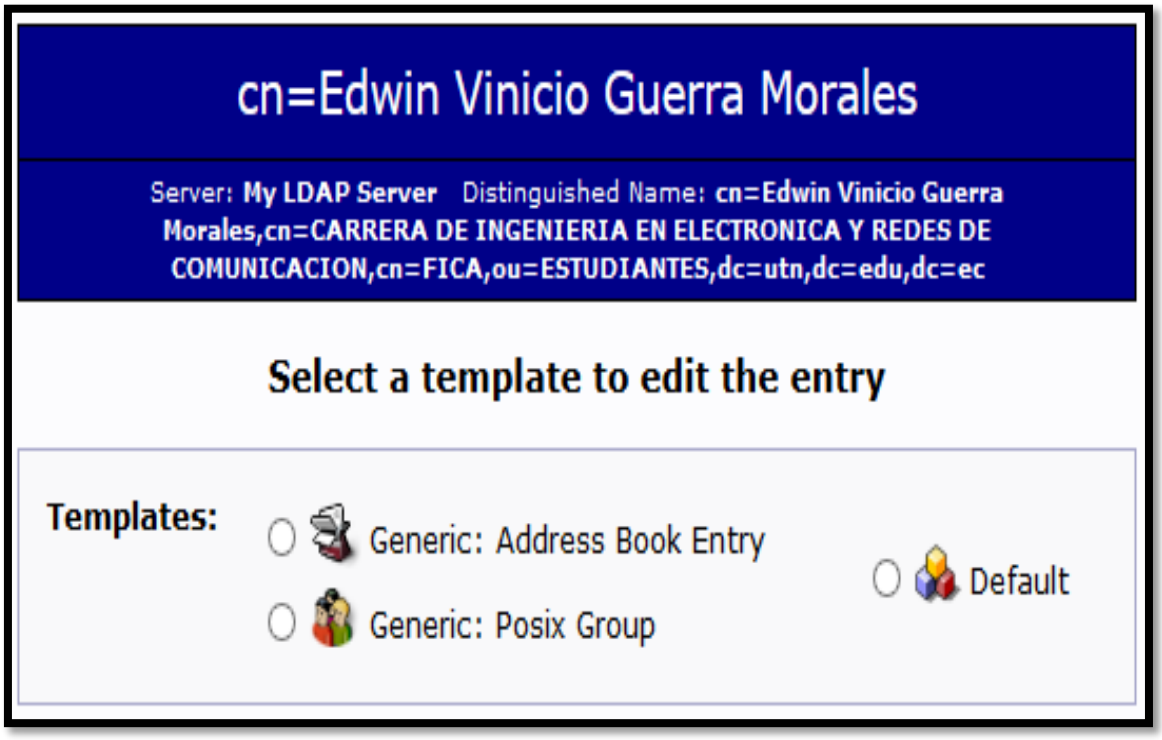


Figura 348 Ventana de Selección de un Template para editar o eliminar la entrada de un Usuario

Fuente: Sistema Operativo Debian 6.0.7

De esta manera ingresamos a los parámetros de configuración del usuario “cn=Edwin Vinicio Guerra Morales” donde podemos realizar los cambios necesarios editando cada uno de los campos requeridos (Figura 349) y actualizamos haciendo clic en el botón “Update Object” ubicado en la parte inferior del mismo template.

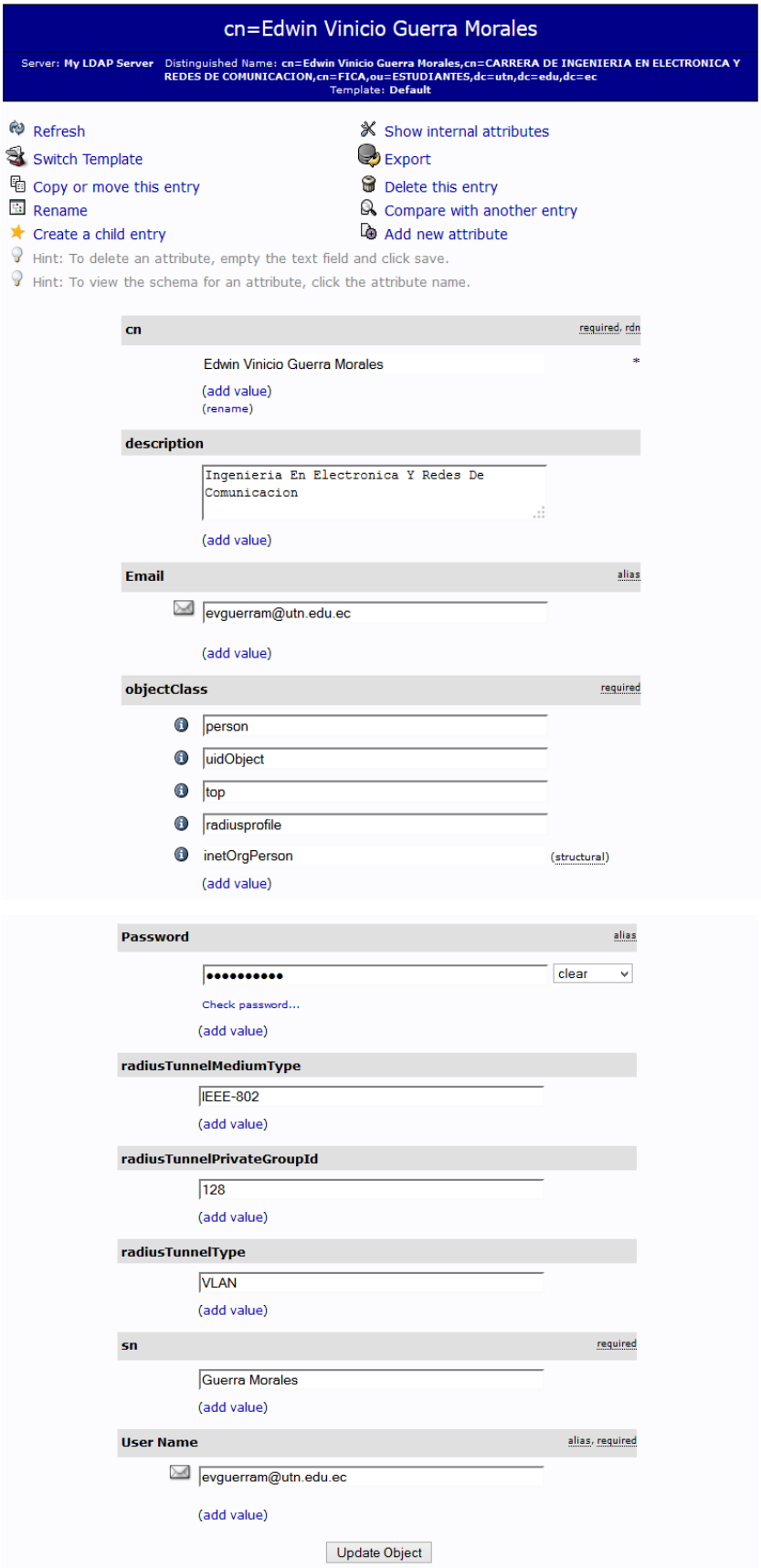


Figura 349 Información del Usuario “cn=Edwin Vinicio Guerra Morales”

Fuente: Sistema Operativo Debian 6.0.7

Eliminación de Grupos

Para eliminar un grupo hacemos clic sobre el mismo, donde nos visualizará la ventana que se indica en la Figura 350 en la cual seleccionamos “Default”. A continuación se presenta un ejemplo con el grupo “cn=CARRERA DE INGENIERIA EN ELECTRONICA Y REDES DE COMUNICACION”.

Figura 350 Ventana de Selección de un Template para editar o eliminar la entrada de un Grupo

Fuente: Sistema Operativo Debian 6.0.7

De esta manera ingresamos a los parámetros de configuración del grupo “cn= CARRERA DE INGENIERIA EN ELECTRONICA Y REDES DE COMUNICACION”, donde podemos realizar los cambios necesarios editando cada uno de los campos requeridos o para eliminar el grupo si así lo deseamos haciendo clic en “Delete this entry” como se muestra en la FIGURA 351.

FIGURA 351 Eliminar el Grupo “cn=CARRERA DE INGENIERIA EN ELECTRONICA Y REDES DE COMUNICACION”

Fuente: Sistema Operativo Debian 6.0.7

En la siguiente ventana de información nos pregunta si estamos seguros de que queremos eliminar el grupo “cn= CARRERA DE INGENIERIA EN ELECTRONICA Y REDES DE COMUNICACION”, si es así, hacemos clic en “Delete” como se indica en la Figura 352.

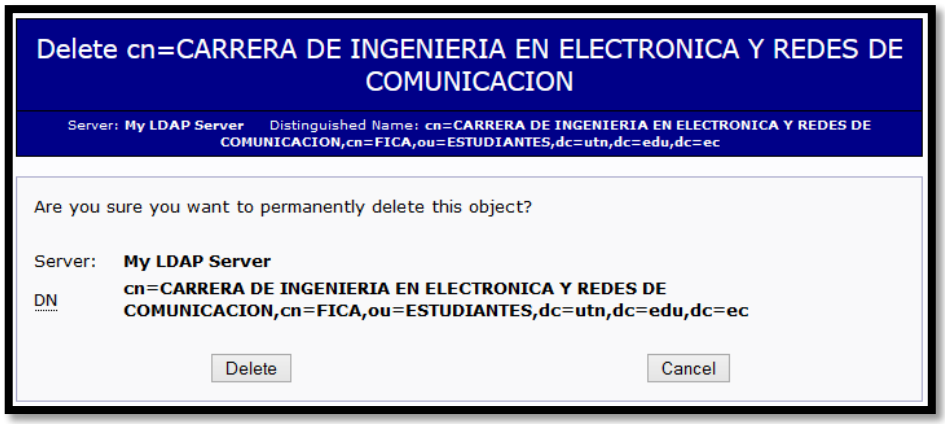


Figura 352 Confirmación para la eliminación de un Grupo

Fuente: Sistema Operativo Debian 6.0.7

Finalmente nos muestra un mensaje de confirmación de que se ha eliminado satisfactoriamente el grupo del directorio LDAP (Figura 353).

Figura 353 Mensaje de confirmación de que se ha eliminado el Grupo exitosamente

Fuente: Sistema Operativo Debian 6.0.7

Eliminación de Usuarios

Para eliminar un usuario hacemos clic sobre el mismo, donde nos visualizará la ventana que se indica en la Figura 354 en la cual seleccionamos “Default”. A continuación se presenta un ejemplo con el usuario “cn=Edwin Vinicio Guerra Morales”

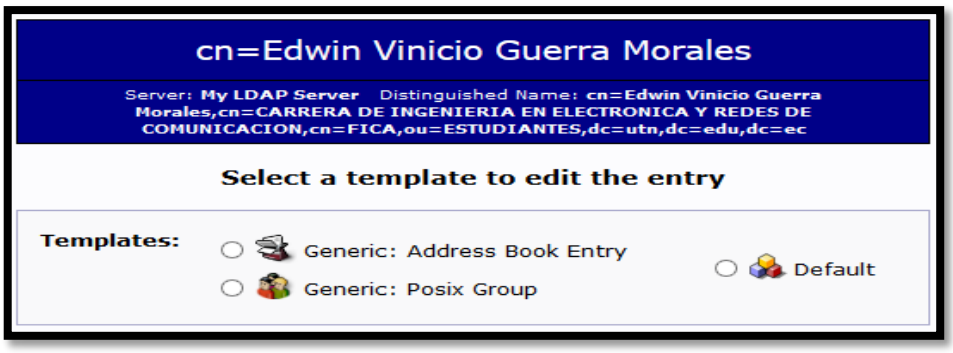


Figura 354 Ventana de Selección de un Template para editar o eliminar la entrada de un Grupo

Fuente: Sistema Operativo Debian 6.0.7

De esta manera ingresamos a los parámetros de configuración del usuario “cn=Edwin Vinicio Guerra Morales”, donde podemos realizar los cambios necesarios editando cada uno de los campos requeridos o para eliminar el usuario si así lo deseamos haciendo clic en “Delete this entry” como se muestra en la Figura 355.

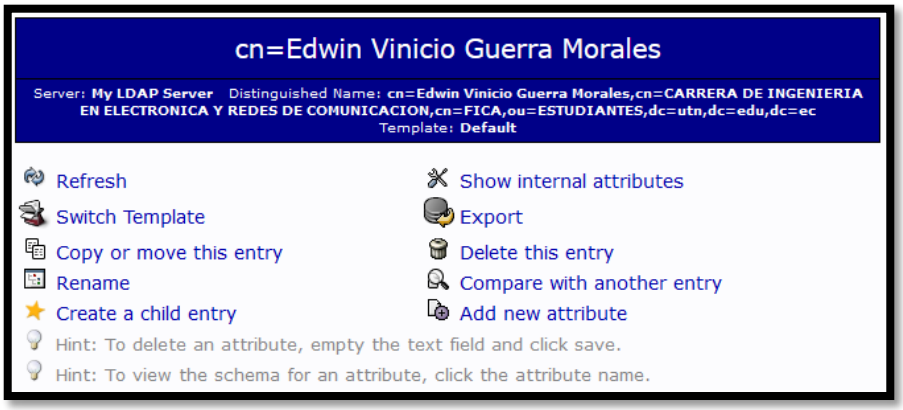


Figura 355 Eliminar el usuario “cn=Edwin Vinicio Guerra Morales”

Fuente: Sistema Operativo Debian 6.0.7

En la siguiente ventana de información nos pregunta si estamos seguros de que queremos eliminar el usuario “cn=Edwin Vinicio Guerra Morales”, si es así, hacemos clic en “Delete” como se indica en la Figura 356.

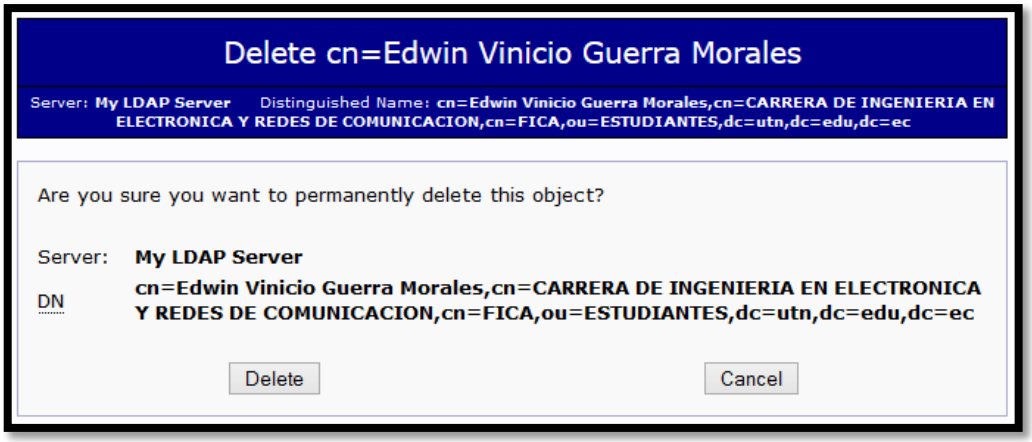


Figura 356 Confirmación para la eliminación de un Usuario

Fuente: Sistema Operativo Debian 6.0.7

Finalmente nos muestra un mensaje de confirmación de que se ha eliminado satisfactoriamente el usuario del directorio LDAP (FIGURA 357).

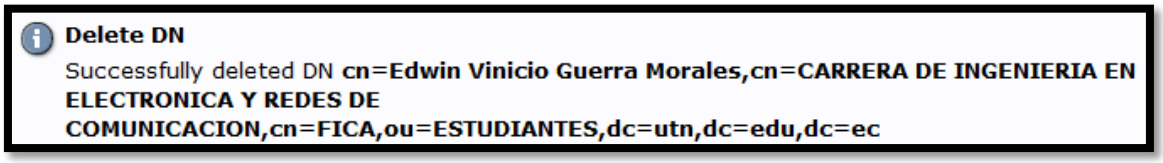


FIGURA 357 Mensaje de confirmación de que se ha eliminado el Usuario exitosamente

Fuente: Sistema Operativo Debian 6.0.7