UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de fin de carrera titulado:

"ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UNA ARQUITECTURA DE SEGURIDAD PARA EL CONTROL DE ACCESO A LA RED INALÁMBRICA DE LA UNIVERSIDAD INTERNACIONAL SEK - ECUADOR EN EL CAMPUS MIGUEL DE CERVANTES"

Realizado por:

LUIS ALBERTO DARIK MUÑOZ ALVAREZ

Director del proyecto:

ING. EDISON ESTRELLA, MBA.

Como requisito para la obtención del título de:

INGENIERO EN TELECOMUNICACIONES

Quito, Agosto del 2015

DECLARACIÓN JURAMENTADA

Yo, LUIS ALBERTO DARICK MUÑOZ ALVAREZ, con cédula de identidad #1722945688, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en el documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa vigente.

_____

Luis Alberto Darik Muñoz Alvarez
C.I.: 1722945688

DECLARATORIA

El presente trabajo de investigación titulado:

"ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UNA ARQUITECTURA DE SEGURIDAD PARA EL CONTROL DE ACCESO A LA RED INALÁMBRICA DE LA UNIVERSIDAD INTERNACIONAL SEK - ECUADOR EN EL CAMPUS MIGUEL DE CERVANTES"

Realizado por:

LUIS ALBERTO DARIK MUÑOZ ALVAREZ

Como requisito para la obtención del título de:

INGENIERO EN TELECOMUNICACIONES

Ha sido dirigido por el docente:

ING. EDISON ESTRELLA, MBA.

Quien considera que constituye un trabajo original de su autor

_____

Ing. Edison Estrella, MBA.

DIRECTOR

DECLARATORIA

El profesor informante:

ING. JUAN GRIJALVA

Después de revisar el trabajo presentado,

lo ha calificado como apto para su defensa oral ante

el tribunal examinador

_____

Ing. Juan Grijalva, MSC.

Quito, 6 de Agosto de 2015

DEDICATORIA

Dedico el presente proyecto de investigación de manera muy especial a mis padres y a mis hermanos que con su constante e incondicional apoyo han sido y serán siempre la base fundamental en mi vida.

A mis familiares y amigos más cercanos por su afecto y cariño en todo momento.

Y a un gran amigo que siempre estuvo a mi lado aunque ya no esté presente.

AGRADECIMIENTO

A Dios.

A mis padres.

A mis hermanos.

A mis familiares.

A mis amigos.

A mi tutor.

A mis profesores.

A la Universidad.

ÍNDICE GENERAL

ÍNDICE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente trabajo de investigación tiene el objeto de mostrar el análisis, diseño e implementación de una arquitectura de seguridad para el control de acceso a la red inalámbrica de la Universidad Internacional SEK en el campus Miguel de Cervantes, el cual permite solventar los problemas y necesidades debido a la inexistencia de seguridad en la red inalámbrica de la institución. La implementación de la propuesta de solución proporciona un esquema de control y gestión de acceso de usuarios, consiguiendo que el uso de la red sea exclusivamente utilizado por usuarios vinculados a la institución; haciendo que la administración de la red sea eficiente y garantice la disponibilidad de recursos y servicios. El análisis y el diseño de la arquitectura de seguridad fueron propuestos en base a las necesidades de adaptabilidad a las herramientas administrativas y de infraestructura de red de la institución. La etapa de desarrollo se sustentó en la implementación de prueba de un servidor de autenticación RADIUS que proporciona servicios de autenticación, autorización y contabilidad (AAA) para el acceso de usuarios registrados. Con ello se consigue una optimización del uso de ancho de banda y la disminución del tráfico en la red. También se utilizaron los roles y servicios disponibles por el sistema operativo base, certificados digitales, un directorio activo y una base de datos en SQL Server. Las herramientas de desarrollo e implementación fueron de software propietario. Por tanto, se presenta como resultado final un esquema administrable de seguridad para un adecuado control y gestión acceso de los usuarios.

Palabras clave: RADIUS, Ubiquiti, Autenticación, Autorización, Contabilidad, Certificado digital.

ABSTRACT

This research has the object to show the analysis, design and implementation of a security architecture for access control to the wireless network of the International University SEK in Miguel de Cervantes campus, which allows to solve the problems and needs due to the lack of security in the wireless network of the institution. The implementation of the proposed solution provides a scheme for controlling and managing user access, getting the use of the network is used exclusively for users linked to the institution; making efficient the network management and ensure the availability of resources and services. The analysis and design of security architecture were proposed based on adaptability to the needs of administrative and network infrastructure tools of the institution. The stage of development was based on the test implementation of a RADIUS authentication server that provides services of authentication, authorization and accounting (AAA) for access to registered users. Thereby optimizing the use of bandwidth and reduced network traffic is achieved. Roles and services available from the base operating system, digital certificates, an active directory and a database in SQL Server were also used. Development tools and implementation were of proprietary software. Therefore, the end result is presented as a manageable security scheme for proper management and control user access.

Keywords: RADIUS, Ubiquiti, Authentication, Authorization, Accounting, Digital Certificate.

CAPÍTULO I

INTRODUCCIÓN

1.1 El Problema de Investigación

1.1.1 Planteamiento del Problema

El desarrollo de sistemas, redes de telecomunicaciones, tecnología, medios de comunicación y diversos factores han permitido el desarrollo y avance de la sociedad en distintos campos como las TICs. Ahora las redes informáticas y de telecomunicaciones se establecen con mayor frecuencia debido a la necesidad de comunicación de la sociedad; es por eso que la seguridad es un factor que se vuelve muy importante al momento de garantizar una estabilidad, integridad, confiabilidad, disponibilidad, y sobretodo protección de los recursos. Hoy en día un sin número de organizaciones, corporaciones, instituciones bancarias y académicas, etc., al tener un manejo y gestión de la red que utilizan requieren tener un control que permita conocer que o quienes pueden tener acceso a la misma.

En la Universidad Internacional SEK la red de comunicación constituye la red alámbrica e inalámbrica gestionada mediante diversas herramientas de administración, y para el control de la seguridad se utiliza un firewall, que determina los accesos de conexión

al sistema otorgando las debidas autorizaciones que proporcionan una comunicación segura.

La red inalámbrica se encuentra gestionada por herramientas básicas para el control de conexión, sin embargo, los accesos a la misma no son controlados, siendo expuesto contra riesgos tanto por vulnerabilidades internas de seguridad como también por las constantes amenazas presentes en el exterior.

Los equipos que constituyen los puntos de acceso a la red inalámbrica, proveen el servicio de conexión a internet a los usuarios de la institución cuyo acceso es directo sin ningún tipo de restricción debido a que la red se encuentra abierta para el público ocasionando mayor tráfico en la red al haber mayor número mayor de usuarios.

El crecimiento y aparición de nuevas redes de comunicaciones con tendencia hacia redes inalámbricas hace necesario tener o emplear un esquema de seguridad y gestión de riesgo tanto para los administradores como para los usuarios, que deben confirmar su autenticación para acceder a los recursos que estén establecidos a su disposición con las respectivas autorizaciones; permitiendo tener un registro continuo de las actividades y el tráfico generado de modo seguro evitando así que intrusos puedan ingresar y obtener información confidencial de la Institución o de sus usuarios.

Por lo tanto una administración de los usuarios mediante un servicio de gestión, integrado con un servidor de dominio, un servidor de directorios, un servidor de

autenticación y un servidor de base de datos ofrecerá mejores prestaciones en la arquitectura de seguridad para la gestión de control de accesos y autenticación en la red institucional.

1.1.2 Objetivo General

Analizar, diseñar e implementar una arquitectura de seguridad para el control y autenticación de los usuarios, que permita una adecuada gestión de las cuentas de los usuarios en un sistema de control general brindando mayor eficiencia y reduciendo al máximo los riesgos en la red inalámbrica del campus Miguel de Cervantes de la Universidad Internacional SEK.

1.1.3 Objetivos Específicos

- Conocer el estado actual de la arquitectura, seguridad e infraestructura de red de la Universidad Internacional SEK.

- Plantear una arquitectura de seguridad para la gestión y control de acceso de los usuarios a la red inalámbrica de la Institución.

- Unificar la arquitectura de seguridad a la red inalámbrica para la gestión del control de acceso de los usuarios.

- Implementar el modo de autenticación y control de usuarios gestionado por un servicio de directorio para cuentas de usuarios.

- Determinar un sistema de monitoreo que permita el control de acceso en la red de la institución académica.

1.1.4 Justificación

Ahora la propuesta de análisis, diseño e implementación de una arquitectura de seguridad en la red inalámbrica del campus Miguel de Cervantes de la Universidad Internacional SEK para el control y autenticación de los usuarios (estudiantes, profesores, invitados y la administración) a través de un sistema de gestión permitirá un eficiente uso de la red dando mejor disponibilidad, control y organización tanto de la información y el tráfico generado logrando un correcto desempeño de toda la red.

Para obtener grandes ventajas en el control y autenticación en el uso de la red, y diversas aplicaciones y servicios en general de la Institución; es necesario un análisis de diseño e implementación de un esquema que permita tener un control general que abarque: autenticación, autorización y contabilidad en base a una arquitectura de red que incluirá algunos factores a considerar como son:

- Servidor Radius: Permite proporcionar 3 servicios: autenticación, autorización y contabilidad (AAA) de manera centralizada.

- Certificados Digitales: Permite mejorar la seguridad en el control de accesos a la red, y el cifrado de las comunicaciones.
- Sistema de Gestión de Acceso y Control: Utilización del protocolo RADIUS/LDAP que brindará una mejor organización en el acceso de servicios de directorio ordenado y distribuido.

El diseño e implementación de la arquitectura de seguridad para la gestión de control y autenticación de accesos en la red involucran distintos procesos que se llevan a cabo dentro de la institución (Universidad Internacional SEK), los cuales deberán ser considerados al realizar las pruebas correspondientes.

1.1.5 Alcance

El presente proyecto permitirá obtener una arquitectura de seguridad más robusta para el control de acceso a la red inalámbrica, siendo una base para implementarse en otro campus de la institución. Adicionalmente se busca una optimización en la gestión de control de los usuarios a la red inalámbrica y la correcta distribución de los canales de comunicación hacia los usuarios para un eficiente y efectivo desempeño de la red de la Universidad Internacional SEK en el campus Miguel de Cervantes.

1.2 Marco Teórico

1.2.1 Estado actual del conocimiento sobre el tema

Debido al ingreso constante de estudiantes nuevos, visitantes, docentes y el personal como tal de la institución (UISEK), han dado lugar a que el control de acceso tanto a la red alámbrica como inalámbrica se vuelva muy amplia y extensa. Actualmente el estado en el cual se encuentra la gestión para el control y seguridad de acceso a las redes es básico de acuerdo a los nuevos estándares.

La gestión para el control de acceso y seguridad hacia la red inalámbrica de la Universidad Internacional SEK se volvería incontrolable dejando toda la carga hacia el firewall que posee la institución. El uso de nuevas tecnologías que provean un sistema de gestión más óptimo con servicios de directorio sería una ayuda y sobretodo una solución.

El problema con la red inalámbrica de la Universidad Internacional SEK se centra en la falta de una implementación de una arquitectura de seguridad que como base posea un control de usuarios que acceden o accederán a la red de la Institución.

Una de las medidas que se podría efectuar para dar solución al problema es la implementación de un control de acceso para todos los usuarios de la red inalámbrica considerando:

- El número de usuarios promedio que acceden a la red.

- El tráfico ocasionado por el uso de la red.
- Políticas de acceso y autenticación para todos los usuarios en general.
- Arquitectura de seguridad de red.
- Preferencias de acceso a la red.

Un gran inconveniente en la actualidad es la seguridad que pueda ofrecer una red de comunicación, el cual queda en evidencia en el poco control que se brinda al momento de acceder a la misma. Por lo tanto cada organización o institución educativa debe tener un modelo de seguridad que utilice herramientas para el control y la autenticación al momento de ingresar. Ahora la Universidad Internacional SEK no cuenta con una arquitectura de seguridad robusta para la red inalámbrica, por tal motivo el diseño e implementación de una arquitectura de seguridad para el control de acceso de los usuarios seria lo adecuado.

La Implementación de una arquitectura de seguridad para la gestión de control de acceso por medio de los protocolos LDAP o RADIUS, deberá orientarse a establecer una adecuada organización que permita el acceso a la información almacenada y centralizada a través de la red. Esto habilita un mejor control de accesos mediante autenticación a través de cuentas de usuarios de manera individual siendo gestionados por un sistema de manejo de directorio, donde la información de todos los usuarios puede ser categorizada y jerárquica incluyendo atributos como nombres, directorios, números telefónicos, e información general.

De igual manera para una correcta implementación se tienen distintos estándares relacionados con un sistema de gestión para el control que son aplicables, considerando puntos como: el marco de autenticación, protección de los datos del directorio, definición de accesos y servicios, procesos para operaciones distribuidas, especificación de protocolos de acceso y sistema, tipos de atributos seleccionados y clases de objetos seleccionados.

X.500, es un servicio de directorio global cuyos componentes gestionan la información de objetos como organizaciones, personas, equipos, y proporciona una búsqueda de información por nombre. Dicha información se mantiene en una base de información de directorio (DIB). Las entradas en el DIB se estructuran en un árbol de información de directorio (DIT).

Cómo LDAP está basado en el servicio de directorio X.500, que después pasó a ser un conjunto de estándares de redes de ordenadores que brindaban indicaciones sobre servicios de directorio y la manera de estructurar directorios globales.

Los protocolos definidos por X.500 incluyen: protocolo de acceso al directorio (DAP), el protocolo de sistema de directorio, el protocolo de ocultación de información de directorio, y el protocolo de gestión de enlaces operativos de directorio. Otro de los estándares es X.509, que hace referencia a certificados de clave pública.

También otro Protocolo a considerar dentro del diseño de una Arquitectura es RPC (Remote Procedure Call, Llamada a Procedimiento Remoto) que permite a un programa de

ordenador ejecutar código en otro ordenador remoto sin tomar en consideración las comunicaciones entre ambos.

El avance tecnológico ha ocasionado que la información que se maneja sea demasiado extensa con un alto grado de crecimiento por año. El gran volumen de información ocasiona un problema que hace difícil una óptima organización, recuperación de datos y gestión de usuarios. Adicionalmente en redes tanto informáticas como de telecomunicaciones en cada organización, corporación, institución, o empresa en general, es indispensable que contengan redes de ordenadores en constante operación para sus actividades, que no solo se limiten a un lugar específico o compartan recursos entre sí; sino también que alcancen una adecuada y confiable comunicación, además de otros aspectos.

Entre los aspectos principales esta la administración de los usuarios de una red por medio de un sistema de base de datos o directorio activo que permitan mantener la información actualizada de forma instantánea y sea accesible desde cualquier lugar.

Por lo general, se hace necesario en las organizaciones e instituciones que las redes de comunicaciones contengan un directorio centralizado con las cuentas de usuarios respectivas para que de forma individual puedan iniciar una sesión desde cualquier estación de trabajo perteneciente a un mismo dominio sin que conlleve a la creación innecesaria de nuevas cuentas de manera local; alcanzando así un mayor y mejor control de recursos, y sobre todo de los usuarios que se agregan o desagregan de la red.

Para el presente proyecto se pretende explicar el diseño e implementación de un esquema de seguridad que se debería efectuar en un ambiente cotidiano dado por lo general en entidades que prestan un servicio de acceso a internet a través de la red inalámbrica.

Durante el ciclo del proyecto, al orientarse al control de acceso y seguridad en la red inalámbrica se utilizará el estándar IEEE 802.1x que indica normas para el control de acceso a la red basado en puertos, permitiendo la autenticación de los usuarios. Con lo cual ayuda en el análisis y diseño de la solución del proyecto.

También se considerará las tecnologías para acceso seguro mediante Wi-Fi Protected Access 2 (WPA2) utilizado tanto en organizaciones privadas como públicas y EAP, el cual es un protocolo que al permitir múltiples métodos de autenticación, los usuarios pueden autenticarse, enviar o recibir información en ambientes inalámbricos como: EAP-TLS, EAP-SIM, EAP-AKA, PEAP, LEAP y EAP-TTLS.

Todos estos mecanismos y tecnologías se integrarán con los protocolos RADIUS (Remote Authentication Dial In User Service) y LDAP (Lightweight Directory Access Protocol), donde permitirán una administración de los usuarios ya sea por medio de una plataforma de gestión web o directamente desde el servidor de directorios a través de la plataforma de administración; además de llevar un registro de actividades y proporcionar permisos o la restricción de los recursos independientemente a cada usuario o grupo de usuarios determinado.

Para el proyecto de investigación se utilizarán herramientas de software como: SQL Server, RADIUS, LDAP, entre otros. También se tendrá siempre en consideración tanto los estándares como las tecnologías en el transcurso del desarrollo del proyecto para proporcionar directivas y lineamientos que se ajusten al ambiente en progreso, y una interoperabilidad informática que favorezca sobre todo a satisfacer las necesidades de una organización y de sus usuarios brindando soluciones óptimas a los problemas.

1.3 Marco Conceptual

1.3.1 Sistema Operativo

Un sistema operativo (SO) es un programa y parte de un sistema computacional que cumple distintas funciones, donde su objetivo es simplificar la gestión, el manejo y la utilización de los recursos del ordenador ya sea a nivel de hardware o software brindando eficiencia y seguridad. Actualmente los sistemas operativos han ido evolucionando dando nuevas funcionalidades como: interfaces gráficas, protocolos de comunicación, etc.

Las funciones principales que desempeña un sistema operativo son:

- Gestión de recursos de la equipo (ordenador)
- Ejecución de servicios para los programas o aplicaciones
- Ejecución de procesos dado por los usuarios

1.3.2 Servicios del Sistema Operativo

Un sistema operativo al crear un entorno para la ejecución de programas, procesos o tareas, proporciona servicios a los programas y a los usuarios de dichos programas. Estos servicios posibilitan la comodidad del programador y facilitan la programación. Entre los principales servicios se encuentran los siguientes:

- Ejecución de programas: el sistema permite la carga del programa en memoria para ejecutarlo.
- Operaciones de E/S: un programa en ejecución podría requerir E/S; lo que implicaría el uso de un archivo o dispositivo de E/S. Por tanto el sistema operativo deberá proporcionar un mecanismo para realizar E/S.
- Manipulación del sistema de archivos: los programas requieren la lectura y escritura de archivos al igual que la creación, modificación y eliminación de archivos.
- Comunicaciones: cuando un proceso necesita el intercambio de información con otro, la comunicación se puede efectuar entre procesos que se ejecutan en un mismo ordenador o en diferentes ordenadores conectados a una red. Para ello, la comunicación puede darse mediante memoria compartida o por transferencia de mensajes, donde el sistema operativo traslada paquetes de información entre los procesos.
- Detección de errores: un sistema operativo necesita estar pendiente en todo momento de posibles errores en el hardware, software y sobretodo en la red. El sistema operativo deberá tomar acciones apropiadas para asegurar el correcto funcionamiento de todo el sistema computacional.

1.3.3 Sistemas Distribuidos

Un sistema distribuido es un conjunto de ordenadores físicamente separados que están conectados en red para proporcionar a los usuarios el acceso a distintos recursos del sistema. Ciertos sistemas operativos recurren a funciones de red, otros toman los accesos de red como un tipo de acceso de archivo, entre otros modos, por ejemplo: FTP y NFS. Ahora las funcionalidades de un sistema distribuido dependerán de la red, y de los protocolos utilizados en efecto.

Los sistemas distribuidos al ser establecidos permiten la entrega de diversas funcionalidades como:

- Recursos compartidos: ofrece mecanismos para compartir archivos de forma remota, procesar información de una base de datos distribuida, impresión de archivos, procesamiento de información y de operaciones; como por ejemplo: al haber distintos sitios conectados a través de la red, el usuario de un sitio puede utilizar los recursos que se encuentren disponibles en otro.
- Velocidad computacional: permite dividir un proceso o cálculo en sub procesos o sub cálculos para una ejecución más rápida, debido que al distribuirse una tarea en un sistema distribuido la carga computacional se vuelve compartida.
- Confiabilidad: en ocurrencia de un incidente en un sitio de un sistema distribuido, los demás sitios deberán seguir en funcionamiento ya que cada terminal que compone el sistema es autónomo.

- Comunicación: al estar conectados distintos puntos de una red de comunicaciones, los procesos que se ejecutan en diferentes sitios pueden efectuar el intercambio de información.

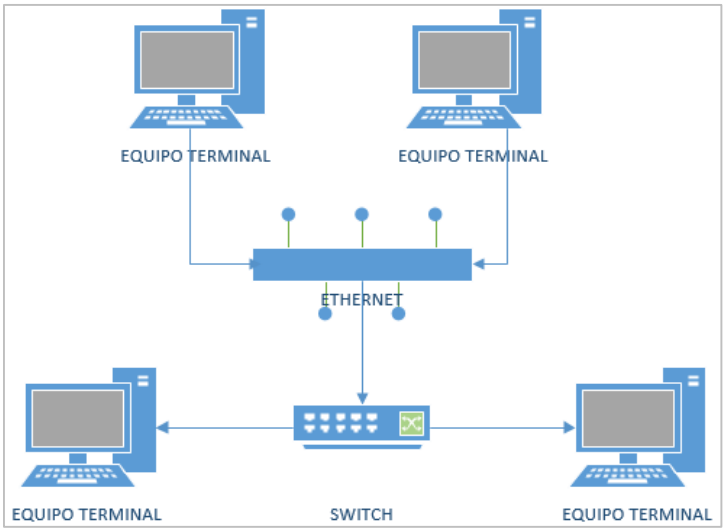
1.3.4 Hardware de red

Los sistemas distribuidos se construyen sobre las redes de computadoras, las cuales pueden ser principalmente las redes: LAN (Redes de área local), que cubren un edificio o un campus, y WAN (Redes de área amplia), que cubren una ciudad, país, o incluso continentes a nivel mundial. El tipo de LAN más importante es Ethernet, y para WAN seria Internet (aunque técnicamente es una red de redes).

En una red Ethernet, se toma en consideración la longitud máxima de cable y un número máximo de terminales (ordenadores) que se pueden conectar. Al momento de extender los límites de la red se requerirá mayor cableado que se conectarán por medio de dispositivos como puentes (bridges) para permitir que el tráfico pase de una red Ethernet a otra, y conmutadores (switches) para evitar colisiones, ya que cada ordenador tendrá su propio puerto de conexión.

Figura No. 1: Ethernet conmutada

Fuente: El autor



Para la red de internet que inició como ARPANET, tuvo un crecimiento rápido al abarcar cientos de terminales, que después se conectaban a redes de radio paquetes, redes satelitales, redes Ethernet dando lugar a la federación de redes denominada Internet.

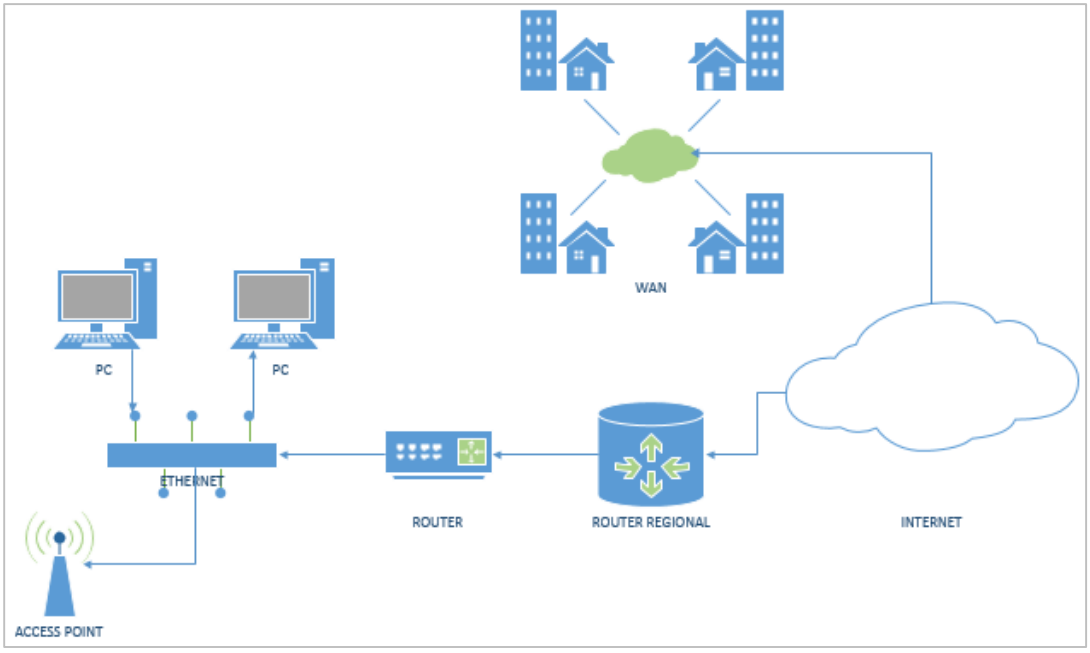
Internet principalmente abarca dispositivos como: concentradores (hubs), enrutadores (routers), anfitrión (host), etc. Los hosts son PCs, notebooks, dispositivos de bolsillo, servidores, mainframes y otros ordenadores que poseen los usuarios o empresas que desean conectarse a Internet. Los enrutadores son conmutadores especializados, que reciben paquetes de una de varias líneas entrantes, y los envían a través de muchas líneas salientes.

Los enrutadores se conectan entre sí en grandes redes, donde cada enrutador posee cables o fibras que conectan a otros enrutadores y hosts. Los ISPs (Proveedores de Servicio

de Internet) al igual que compañías telefónicas operan extensas redes de comunicaciones para sus clientes.

Figura No. 2: Internet

Fuente: El autor



En redes de comunicaciones se da una clasificación en base a: la tecnología de transmisión y escala. Existen dos tipos de tecnología de transmisión: los enlaces de difusión (broadcast) y los enlaces de punto a punto. Una red punto a punto conectan pares individuales de ordenadores, y en una red de difusión todas los equipos comparten el canal de comunicación; una red inalámbrica es un ejemplo de una red de difusión.

Por su escala las redes se clasifican en redes de área personal, destinadas a una persona. Después se encuentran redes más grandes, divididas en redes de área local, de área metropolitana y de área amplia, cada una con mayor tamaño que la anterior.

1.3.4.1 PAN

Las redes de área personal PAN (Personal Area Network) permiten la comunicación de dispositivos dentro del rango de una persona. Por ejemplo: una red inalámbrica que conecta a un ordenador con sus periféricos.

1.3.4.2 LAN

Las redes de área local, LAN (Local Area Networks), son redes de propiedad privada que operan dentro de un solo edificio, casa, oficina. Las redes LAN se utilizan para conexión de ordenadores para compartir recursos e intercambiar información.

1.3.4.3 WAN

Una Red de Área Amplia, WAN (Wide Area Network), son redes que constituyen una extensa área geográfica, país o continente.

1.3.5 Redes inalámbricas

Una red inalámbrica es una red en la que dos o más terminales se pueden comunicar sin necesidad de una conexión por cable. Las redes inalámbricas permiten al usuario mantenerse conectado al desplazarse en una determinada área geográfica. Las redes inalámbricas se basan en enlaces que utilizan ondas electromagnéticas en lugar del cableado. Las tecnologías utilizadas son diferentes de acuerdo a la frecuencia, alcance y

velocidad de transmisión. Las redes inalámbricas se clasifican de acuerdo al área de cobertura desde la que un usuario se conecta a la red.

1.3.5.1 Redes de área local inalámbricas (WLAN)

Una red de área local inalámbrica (WLAN), abarca un área equivalente a una red local de una empresa, con un alcance aproximado de 100 metros. Con lo cual las terminales que se encuentran dentro de un área de cobertura determinada puedan conectarse entre sí.

1.3.5.2 Tecnología Wi-Fi

Una red Wi-Fi (marca de Wi-Fi Alliance) es una red de comunicación de datos que permite conectar equipos como: servidores, ordenadores, etc., sin necesidad de cableado.

Una red Wi-Fi permite una interoperabilidad de los equipos de una red según la norma IEEE 802.11, siendo compatibles con cualquier fabricante que utilice estos estándares. Los componentes básicos de una red Wi-Fi son:

- Punto de acceso (AP): permiten la unión entre redes cableadas y una red Wi-Fi, o entre varias redes Wi-Fi, que actúa entonces como repetidor de la señal entre estas zonas (celdas).
- Antena: se conectan al punto de acceso.

- Terminal Wi-Fi: puede ser un dispositivo externo, que se instala en un equipo terminal, o puede estar integrado en equipos terminales portátiles y móviles.

1.3.5.3 Estándares Wi-Fi

IEEE (International Electrical and Electronic Engineers), Instituto Internacional de Ingenieros Eléctricos y Electrónicos), es un organismo encargado de la publicación de artículos, realización de conferencias y redacción de estándares. El IEEE proporciona una extensa familia de estándares relacionados con las redes de área local como la 802.

1.3.5.4 Estándar 802.1x

El estándar IEEE 802.1x se define como un protocolo de control de acceso y autenticación basada en una arquitectura cliente-servidor, que impide que los clientes (usuarios) se conecten a una red LAN a través de puertos de acceso público sin ser autenticados.

1.3.5.5 IEEE 802.1x y EAP

El protocolo de autenticación IEEE 802.1x (conocido como Port-Based Network Access Control) es un entorno desarrollado en principio para redes cableadas, tiene mecanismos de autenticación, autorización y distribución de

claves; además de incluir controles de acceso para usuarios de una red. La arquitectura IEEE 802.1x está compone 3 entidades funcionales:

- suplicante que se une a la red.
- autenticador que controla el acceso.
- servidor de autenticación que realiza la autorización.

En las redes inalámbricas, el punto de acceso se lo considera como autenticador. Cada puerto físico o virtual en redes inalámbricas, se divide en dos puertos lógicos, formando un PAE (Port Access Entity). El PAE de autenticación se encuentra siempre abierta y da paso a procesos de autenticación, en cambio el PAE de servicio sólo se abre al haber una autenticación satisfactoria como por ejemplo una autorización. El servidor de autenticación (puede ser un servidor RADIUS) toma la decisión de otorgar el permiso de acceso.

Ahora el estándar 802.11i realiza modificaciones a la IEEE 802.1x para que las redes inalámbricas puedan estar protegidas contra incidentes de robo de identidades. La autenticación de los mensajes asegura de que tanto el suplicante como el autenticador prevean sus claves secretas y activen la encriptación previo acceso a la red. El suplicante y el autenticador se comunican mediante el protocolo basado en EAP. El autenticador simplemente se limita a enviar todos los mensajes al servidor de autenticación.

EAP es un entorno dirigido al transporte de varios métodos de autenticación con un número limitado de mensajes (Request, Response, Success, Failure), mientras que otros mensajes intermedios dependen del método de autenticación seleccionado: EAP-TLS, EAP-TTLS, PEAP, EAP-SIM etc. Al completarse el proceso, tanto el suplicante como el servidor de autenticación tendrán una clave secreta. El protocolo utilizado en redes inalámbricas para el transporte EAP se denomina EAPOL (EAP Over LAN), y para comunicaciones entre el autenticador y un servidor de autenticación se utilizan protocolos de nivel más alto, como Radius, etc.

1.3.6 Software de red

Gran número de redes se organizan como una pila de niveles, dichos niveles difieren entre una red y otra. El propósito de cada nivel es proporcionar ciertos servicios a los niveles superiores, es decir, cada nivel ofrece servicios al nivel que se encuentra encima.

1.3.7 Servicios de conexión

Los niveles proporcionan 2 tipos distintos de servicio a los niveles superiores: orientado a conexión y sin conexión.

1.3.7.1 Servicio orientado a conexión

Este servicio surge a partir del sistema telefónico. Un servicio de red orientado a conexión, el usuario del servicio establece una conexión, que la utiliza

y luego la libera; de modo que se conserva el orden de los bits desde que fueron enviaron.

1.3.7.2 Servicio orientado sin conexión

Este servicio surge a partir del sistema postal. En un servicio de red orientado sin conexión, cada paquete tiene la dirección de destino completa, y cada uno es direccionado hacia nodos intermedios dentro del sistema, de manera independiente a todos los paquetes subsecuentes.

1.3.7.2.1 UDP

UDP (User Data Protocol), es un protocolo a nivel de transporte que se basa en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin establecerse una conexión previa.

1.3.8 Arquitectura de seguridad

AAA (Authentication, Authorization and Accountig) es una arquitectura de seguridad, que se divide en tres módulos: Autenticación, Autorización, Contabilidad que trabajan en conjunto, proporcionando una conexión de red eficiente y segura. Entre sus funcionalidades se encuentra:

- Autenticación: ofrece el método de identificación de usuarios, que incluye nombre de usuario, contraseña, soporte de mensajería, y, dependiendo del protocolo de seguridad escogido, ofrece un cifrado.
- Autorización: ofrece el método para control de acceso remoto, que incluye autorización total o por cada servicio, perfil por usuario, lista de cuentas, soporte de grupos, etc.
- Contabilización: ofrece el método de recopilación y envió de información a un servidor de seguridad, que es usado en facturación, auditoria y reporte de: nombres de usuario, tiempo de inicio y fin, cantidad de paquetes enviados, número de bytes.

AAA provee ciertas ventajas como arquitectura de seguridad:

- Control de configuraciones de acceso y mayor flexibilidad.
- Uso de métodos de autorización estandarizados, como RADIUS, TACACS+, etc.
- Variedad de sistemas de apoyo (backup).

1.3.9 Modelo de referencia TCP/IP

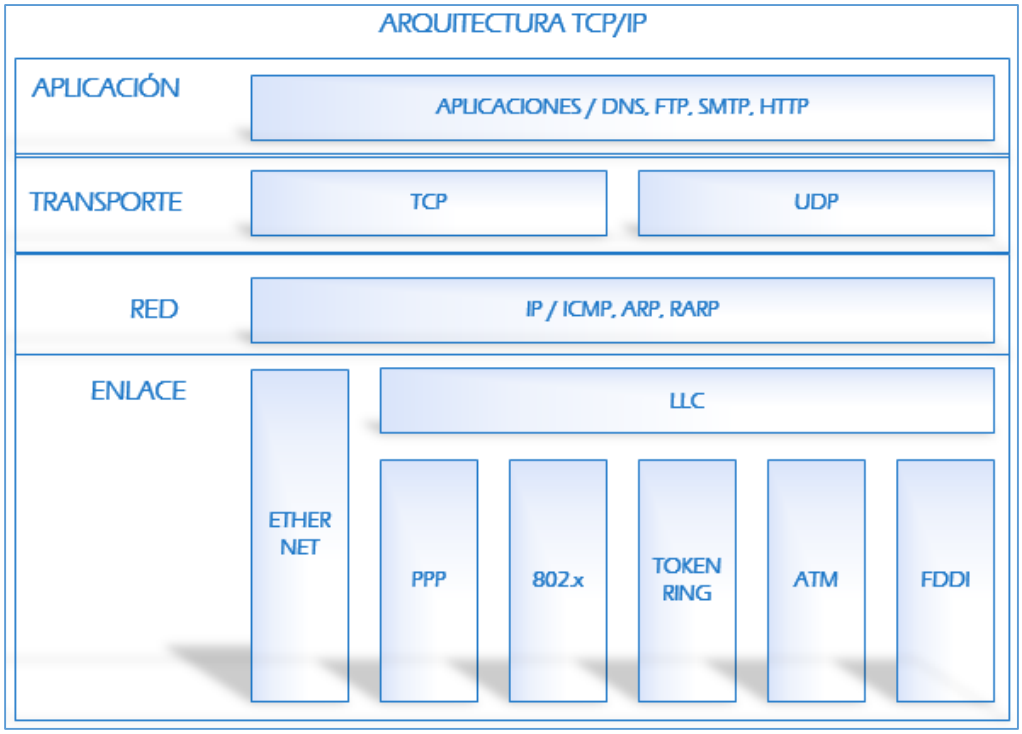
Este modelo se basa en la necesidad de que la información y los datos organizados en forma de paquetes recorran a su destino independientemente de la condición de cualquier nodo o red determinado. TCP/IP constituye 4 niveles: nivel de aplicación, nivel de transporte, nivel de red y nivel de enlace.

- Nivel de enlace: realiza el manejo de datos hacia o desde el medio físico.
- Nivel de red: realiza el envío de los datos desde el origen al destino.
- Nivel de transporte: realiza el manejo de comunicaciones entre los equipos de extremo a extremo.

- Nivel de aplicación: realiza el manejo de implementación de aplicaciones de usuarios.

Figura No. 3: Modelo TCP/IP

Fuente: El autor



1.3.10 Seguridad en redes inalámbricas

1.3.10.1 Autenticación

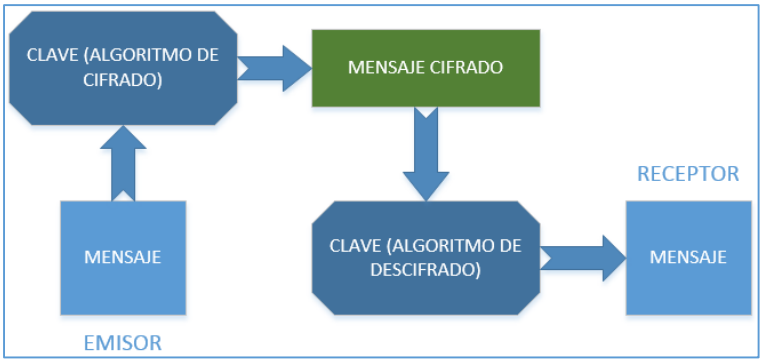
La autentificación permite verificar la identidad de un usuario o un proceso mediante el uso de credenciales que contengan: usuario y contraseña, hasta el uso de firmas o certificados digitales.

1.3.10.2 Criptografía

La criptografía se basa en el cifrado o descifrado de la información digital mediante el empleo de técnicas matemáticas. En el proceso de encriptación, un mensaje contiene información que es cifrada y solo puede ser descifrada por quien posea la clave, resultando un proceso de des encriptado.

Figura No. 4: Criptografía de datos

Fuente: El autor



Los métodos de encriptación se dividen en:

1.3.10.2.1 Criptografía de Clave Simétrica

Se utiliza una misma clave secreta en el emisor y receptor para encriptar y desencriptar la información transmitida, dicha clave será intercambiada entre los equipos a través de un canal seguro. El uso de algoritmos simétricos se hace útil para el cifrado de datos. Entre los principales algoritmos simétricos se encuentran:

- DES: Basado en un sistema mono alfabético, que utiliza un algoritmo de cifrado que aplica permutaciones y sustituciones sucesivamente.
- IDEA: Basado en el uso de bloques de texto de 64 bits, y opera con números de 16 bits mediante operaciones XOR, también utiliza suma y multiplicación de enteros.
- RC5: Basado en la aplicación de operaciones XOR sobre los datos. Utiliza diferentes longitudes de clave, iteraciones, y funciona como generador de números aleatorios.
- AES: Basado en la aplicación de bloques y claves de longitud variable.

1.3.10.2.2 Criptografía de Clave Asimétrica

Se utiliza 2 llaves diferentes uno para el emisor y otro para el receptor. Cada usuario tendrá una clave privada y una clave pública; donde la clave privada será secreta y estará protegida por el propio usuario, en cambio la clave pública será accesible para todos los usuarios que constituyen el sistema de comunicación. Este tipo de criptografía ofrece integridad y autenticidad. Los algoritmos asimétricos se basan en funciones matemáticas, y entre los principales se encuentran:

- Diffie-Hellman: Basado en la generación de una clave privada simétrica en el emisor y receptor que se comunican por un canal de comunicación inseguro.

- RSA: Basado en el problema de factorización de números enteros para la resolución del problema de distribución de llaves simétricas y muy utilizado en firmas digitales.

1.3.10.3 Algoritmos de Autentificación HASH

Los algoritmos de autenticación hash constituyen un método de generación de claves que representan un conjunto de datos. Una función hash es una operación matemática realizada sobre el conjunto de datos, y cuya salida es una huella digital independiente del tamaño del conjunto de datos original. El cifrado de una huella digital se denomina como una firma digital.

- MD5: Es una función hash de 128 bits que no permite el cifrado de un mensaje, donde la información original no es recuperable.
- SHA-1: Compone un bloque de 160 bits donde la función de compresión es compleja haciéndolo más robusto y seguro.
- SHA-2: Su diseño es mejorado con respecto a SHA-1 siendo más seguro, y por ende más lento en su procesamiento y uso.

1.3.11 Servicio de Directorio

Un servicio de directorio (SD) es una aplicación o conjunto complejo de componentes que trabajan de forma conjunta para prestar un servicio que almacena y

organiza la información de los usuarios de una red, mediante la gestión del acceso de los usuarios a los recursos de la red.

Los directorios generalmente contienen información detallada en base a atributos y filtrado pero no soportan transacciones complejas ni esquemas de Roll Back como en los sistemas de bases de datos; ya que las actualizaciones de los directorios son cambios simples.

Un servicio de directorio proporciona una interfaz de acceso a los datos, la cual la autenticación de los accesos al servicio de forma segura y centralizada para el acceso a los recursos del sistema que manejan los datos del directorio.

1.3.12 Certificado Digital

Es un conjunto de credenciales de autentificación cifradas que se identifican mediante una clave pública que verifica la firma digital incluida. Los certificados digitales evitan la visualización de información que se intercambia en la red al momento del envío o recepción de datos. Un certificado digital constituye 3 partes importantes que incluyen:

- Una clave pública.
- Identidad del remitente (nombre y datos generales).
- Una firma privada otorgada por una autoridad certificadora reconocida.

El estándar que establece el formato de uso de un certificado digital es el X509. Un certificado digital entonces además de autenticar a un usuario de red permite:

- Autenticar al usuario al momento de identificarse.
- Firmar digitalmente un documento digital.
- Manejar documentos digitales que están firmados digitalmente considerando la confiabilidad del remitente y del destinatario.
- Mantener la integridad, confidencialidad y disponibilidad de la información (documento digital) entre el remitente y el receptor.
- Realizar transacciones comerciales con seguridad y legalidad.

A la entidad que otorga certificados digitales se denomina autoridad de certificación.

1.3.13 Autoridad Certificadora CA

Es la autoridad encargada de firmar los certificados y confirmar que el propietario de un certificado es quien dice ser. Una autoridad certificadora puede certificar identidades de otras autoridades certificadoras. El proceso se detiene cuando una autoridad no tiene quién la certifique, por lo que el certificado lo debe firmar la misma, siendo un certificado de raíz.

La Autoridad Certificadora administra, determina el tiempo de validez y mantiene listas de certificados no válidos.

1.3.14 Renovación de Certificados

Es el proceso de actualización de datos del usuario que posee el certificado. Este proceso se realiza cuando las claves han expirado o la seguridad ha sido vulnerada.

1.3.15 Revocación de Certificados

Es el proceso en el cual la autoridad certificadora notifica a todas las entidades cuando un certificado es suspendido o revocado.

1.3.16 PEAP

El Protocolo de autenticación extensible protegido (PEAP), utiliza una seguridad de nivel de transporte (TLS) para crear un canal cifrado y seguro entre un cliente de autenticación PEAP como un equipo inalámbrico, y un autenticador PEAP como un servicio de autenticación de internet (IAS) o un servidor de autenticación (RADIUS). PEAP no especifica un método de autenticación, pero proporciona seguridad adicional para protocolos de autenticación EAP, como EAP-MSCHAPv2, que operan a través de un canal cifrado de TLS proporcionado por PEAP. El protocolo PEAP se implementa como un método de autenticación para equipos cliente inalámbricos 802.11, sin embargo, no admite clientes de red privada virtual o clientes de acceso remoto.

1.3.17 LDAP

LDAP (Lightweight Directory Access Protocol), es un protocolo a nivel de aplicación basado en el estándar X.500 (conjunto de estándares de redes de ordenadores de la ITU-T sobre el servicio de directorios) que permite el acceso a un servicio de directorio ordenado y distribuido en un entorno de red. Este protocolo se ejecuta sobre TCP/IP o sobre otros servicios de transferencia orientados a conexión; con lo cual proporciona acceso a la información del directorio para su búsqueda.

LDAP es similar a una base de datos que permite el procesamiento de consultas, y al ser un sistema cliente - servidor puede usar diversas bases de datos para almacenar un directorio, para operaciones de lectura rápida de gran volumen.

A menudo se almacena información de los usuarios que pertenecen a una red de ordenadores, como por ejemplo el nombre de usuario, contraseña, directorio, etc., sin embargo es posible almacenar también otro tipo de información tal como, el número de teléfono celular, fecha de nacimiento, ubicación de los recursos de la red, permisos, certificados, etc.

Cuando un cliente LDAP se conecta a un servidor LDAP puede consultar un directorio, o modificarlo. Al transcurrir la consulta, el servidor, puede contestarla localmente o dirigir la consulta a un servidor LDAP que tenga la respuesta. Si el cliente intenta modificar información en un directorio LDAP, el servidor realiza una verificación y confirmación de que el usuario tiene permiso para realizar el cambio para luego añadir o actualizar la

información. Entonces, LDAP es un protocolo de acceso unificado a un conjunto de información sobre los usuarios de una red de comunicación de ordenadores.

1.3.18 RADIUS

RADIUS (Remote Authentication Dial-In User Server), es un protocolo que permite la gestión para la "autenticación, autorización y registro" de usuarios remotos para el uso de un determinado recurso, o aplicaciones de acceso a la red e IP. RADIUS para establecer conexiones de comunicación utiliza los puertos 1812 y 1813 UDP.

Cuando el tamaño de una red es grande y se necesita proporcionar un servicio de acceso centralizado, las organizaciones optan por hacerlo mediante diversos servidores RADIUS. El brindar acceso a internet o conexión con otras redes corporativas con diferentes tipos de tecnologías de red (VPNs, WIFI, MÓDEMs, Xdsl, redes inalámbricas) mediante éste protocolo no sólo se centra en la gestión de acceso a la propia red sino también para servicios de Internet como el correo electrónico, la web o en el proceso de señalización SIP en VoIP.

Por ejemplo, en el proceso de conexión con un ISP a través de un medio de conexión como: módem, DSL, cable módem, Ethernet o Wi-Fi, se envía información (nombre de usuario y contraseña) que es transferido a un dispositivo NAS (Network Access Server) sobre el protocolo PPP, el cual re direcciona la petición a un servidor RADIUS sobre el protocolo RADIUS.

El servidor RADIUS realiza una comprobación de la información verificando que sea correcta mediante esquemas de autenticación como: PAP, CHAP o EAP, donde al ser aceptado, el servidor dará autorización para acceder al sistema ISP asignándole recursos de red como una dirección IP, parámetros como L2TP, etc.

Ahora ya existe un nuevo protocolo llamado DIAMETER, que proporciona manejo de errores y comunicación entre dominios; siendo ya el sustituto de RADIUS.

1.3.19 Servidor de Base de Datos

Un servidor de base de datos es aquel utilizado para la ejecución de gestores de BD donde múltiples usuarios pueden efectuar operaciones sobre ellas al mismo tiempo, en lugares diferentes; teniendo acceso a las BD por las aplicaciones instaladas en las estaciones de trabajo que sean clientes.

1.3.20 SQL Server

SQL (Structured Query Language), es un lenguaje de consulta estructurado utilizado para definir, controlar, acceder, manipular, recuperar y almacenar información en sistemas de bases de datos relacionales

Todos los sistemas de gestión de bases de datos relacionales como: DB2, MySQL, Access, Oracle, Sybase, Informix, PostgreSQL y SQL Server utilizan el lenguaje SQL como base de datos estándar.

El SQL es un lenguaje universal empleado en cualquier sistema gestor de base de datos relacional, y en principio es un leguaje orientado únicamente a la definición y al acceso a los datos por lo que no se puede considerar como lenguaje de programación ya que no incluye funcionalidades como estructuras condicionales, bucles, etc, aunque cada vez hay avance continuo.

Se puede ejecutar directamente en modo interactivo o embebido en programas escritos en lenguajes de programación convencionales.

1.3.21 Servidor DNS

Un servidor DNS (Domain Name System) traduce nombres de dominio a direcciones IP y viceversa. En las redes TCP/IP, cada PC dispone de una dirección IP para poder comunicarse con el resto de PCs. Es equivalente a las redes de telefonía en las que cada teléfono dispone de un número de teléfono que le identifica y le permite comunicarse con el resto de teléfonos.

1.3.22 Servidor DHCP

El protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) permite la simplificación de la administración de configuración IP de equipos de una red. Un servidor DHCP es un servidor que recibirá peticiones de clientes solicitando una configuración de red IP. El servidor responderá a dichas peticiones proporcionando la configuración requerida a los usuarios. El servidor proporcionara al usuario una dirección IP, y máscara de subred principalmente.

1.3.23 NAS

Un NAS (Network Access Server) es un sistema que proporciona acceso a la red, y controla el acceso a un recurso que se encuentra protegido.

1.3.24 Active Directory

Un servicio de directorio es una aplicación o conjunto de aplicaciones que gestionan objetos de red de manera jerárquica, como usuarios, servicios y recursos de red y permite tener un control centralizado que determina los accesos verificando la contraseña y los datos correspondientes a cada usuario.

CAPÍTULO II

MÉTODO

2.1 Análisis

2.1.1 Estudio Preliminar

En el transcurso de la investigación del proyecto en cuestión los requerimientos necesarios para el desarrollo fueron entregados por auspicio de la institución.

En el proceso de análisis sobre la situación actual de la red inalámbrica de la institución se tomó en consideración diversos aspectos como:

- Número de usuarios que se conectan a la red institucional.
- Tráfico generado en la red inalámbrica por los estudiantes, profesores, personal administrativo, y visitantes, etc.
- Infraestructura y arquitectura actual de la red inalámbrica de la institución del campus en cuestión.
- Estado de seguridad de la red inalámbrica de la institución.

Las propuestas solicitadas para el desarrollo del proyecto comprenden:

- Adaptación de la propuesta de solución sobre la arquitectura e infraestructura de la red inalámbrica de la universidad del campus en cuestión.
- Determinación de herramientas tanto hardware y software necesarias para pruebas e implementación.
- Autenticación y autorización en la red inalámbrica de la institución únicamente para los usuarios vinculados a la misma.
  - Gestión y registro de los usuarios pertenecientes a la institución.
  - Control del trafico

2.1.2 Estudio de Factibilidad

2.1.2.1 Operativa

Desde un punto de vista operativo, la propuesta de una arquitectura que se adapte a la establecida en la infraestructura de la institución tendrá un impacto positivo para todos los usuarios considerando que no tendrán mayor complejidad al iniciar el uso del sistema de autenticación de seguridad para la red inalámbrica de la institución.

Entre algunos aspectos adicionales a considerar se encuentran:

- La idea principal surge de la necesidad detectada por los administradores de la red de la institución que gestionan la red inalámbrica, donde el acceso a la red es libre para cualquier usuario sea parte o no de la institución. Para lo cual, ésta

propuesta está destinada a brindar un sistema más seguro en la red inalámbrica de la institución dando la resolución del problema planteado por los involucrados.

- La implementación de la arquitectura de seguridad será adaptada en la red establecida de la institución, y no representará un cambio significativo que obligue a realizar cambios en la estructura de la red existente.

- La arquitectura de seguridad planteada será gestionable mediante un sistema alojado en un servidor, el cual presentará una interfaz gráfica de administración no tan compleja y simple de gestionar.

- Hoy en día el manejo de dispositivos inteligentes de todo tipo y la navegación en la red de internet se han vuelto conceptos muy cotidianos en la vida de la personas. Considerando la premisa mencionada, se analizó que los usuarios en general no se verán afectados al momento de utilizar el nuevo sistema de autenticación para la red inalámbrica de la institución.

- La gestión y administración de la nueva arquitectura de seguridad por medio de un sistema gestor y herramientas adicionales administrativas permitirán tener un constante control del uso de la red, del tráfico de la red y sobretodo de la cantidad de usuarios activos dentro de la red. También se tendrá información estadística de la red.

Una vez evaluado el favorable estudio del problema y en base a las conversaciones y entrevistas sostenidas con el personal especializado de tecnología se acordó el apoyo y coordinación del departamento de redes y sistemas de la institución para el desarrollo del proyecto; demostrando que no hubo oposición al posible y futuro cambio de manera que la propuesta de solución es viable y será factible operacionalmente.

2.1.2.2 Técnica

La factibilidad técnica consistió en evaluar los recursos técnicos existentes en la institución para desarrollar la propuesta de solución que permitió consolidar y demostrar los siguientes puntos:

- La nueva arquitectura de seguridad es adaptable a la infraestructura actual de la red de la institución.
- La institución cuenta con los componentes técnicos necesarios para el desarrollo del proyecto.
- Antes de la implementación se tendrá una etapa de pruebas para la demostración del funcionamiento.
- El desarrollo de la propuesta de solución se limita como parte de la evaluación al campus: Miguel de Cervantes de la Universidad Internacional SEK, con un crecimiento a futuro donde pueda ya contener a toda la red institucional.
- También habrá una etapa de implementación en la red inalámbrica de la institución del campus en cuestión, a partir del término de la etapa de pruebas.

- Se consideró si la institución tiene el personal con experiencia técnica requerida para manejar, implementar, operar y mantener la arquitectura de seguridad propuesta.
- Se consideraron también planes de desarrollo y contingencia en caso de haber problemas al momento de la implementación de la propuesta de solución, sin que ocasione problemas o pérdida de información crítica.

2.1.2.3 Tecnológica

Para la factibilidad tecnológica se determinó los recursos tecnológicos necesarios para la implementación de la arquitectura de seguridad para la red inalámbrica existente.

También se planteó y demostró que la tecnología empleada permitirá tener practicidad y fácil manejo para los usuarios (los usuarios deberán ser informados y preparados para el nuevo modo de conexión a la red inalámbrica); ya que al momento de la autenticación en la red inalámbrica de la institución, la interfaz de conexión que permite la interacción entre el usuario y la red solicitará credenciales de acceso como: usuario y contraseña. Cabe mencionar que las credenciales requeridas estarán pre definidas para cada usuario del nuevo sistema de autenticación de la institución.

De acuerdo a los requerimientos tecnológicos para la arquitectura del nuevo sistema de control se consideró dos puntos: hardware y software. En cuanto a hardware, el equipo (servidor) donde estará instalado el sistema propuesto deberá contemplar requisitos mínimos para su correcto funcionamiento.

- Procesador Intel Core i5 2.5GHz.
- Tarjeta madre.
- 2 GB de memoria RAM.
- Disco duro de 50 GB.
- Tarjeta de red.
- Monitor, teclado y mouse.
- Unidad de protección UPS.

Examinando el hardware existente y los requerimientos mínimos necesarios, la institución no requirió realizar una inversión inicial para la adquisición de nuevos equipos ni para actualizar los ya existentes, ya que cuenta con la debida infraestructura y recursos que satisfacen los requerimientos establecidos tanto para el desarrollo como para la implementación de la propuesta de solución.

La red institucional en el campus Miguel de Cervantes constituye una parte cableada para la red alámbrica y otra parte no cableada para la red inalámbrica a través de puntos de acceso. Ambas partes se unen a la red provista por el

proveedor de servicio de Internet conformando una red con topología en malla y estrella.

En cuanto a software, la institución cuenta con todos los programas y aplicaciones, además del convenio de "Campus Agreement" con Microsoft para la gestión de licencias. Todos estos recursos mencionados estarán a la disposición para el desarrollo del proyecto y el funcionamiento del sistema de seguridad; con lo cual no hace necesario una inversión para la adquisición de los mismos.

El servidor que alojará un entorno Windows con el sistema operativo Windows Server 2008 R2, además de una consola de administración web para los puntos de acceso de la red inalámbrica, también para el progreso de las actividades de la propuesta de solución se tendrán herramientas de escritorio como navegadores, editores, etc.

Tabla No. 1: Software disponible

Fuente: El autor

Cantidad	Descripción
1	Campus Agreement Microsoft
1	Sistema Operativo Windows Server 2008 R2
1	Sistema Operativo Windows Server 2012
1	Navegadores Internet
1	Herramientas de Escritorio Office 2013
1	Sistemas Administrativos
1	Antivirus

2.1.2.4 Económica

Para el estudio de factibilidad económica para el desarrollo de la propuesta se determinaron los recursos de implementación, gestión y mantenimiento para un correcto desempeño, además del análisis de costos para el mismo.

2.1.2.4.1 Análisis Costos – Beneficios

El análisis permitió determinar los costos recurrentes al proyecto, considerando también lo mencionado previamente en el estudio de factibilidad tecnológica; que indica que la institución cuenta con todas las herramientas necesarias para no recurrir a un gasto de inversión inicial.

Sin embargo, por motivos de conocimiento general se presenta un listado con los costos intrínsecos para la propuesta de solución, los costos de implantación y los costos de operación.

Tabla No. 2: Presupuesto de Costos aproximados

Fuente: El autor

Costos intrínsecos / implantación / operación				
Recursos Materiales / Varios				
Item	**Descripción**	**Cantidad**	**Valor Unitario ($)**	**Total ($)**
Material de oficina	Paquete de hojas	1	$5.00	$5.00
	Disco duro externo 2TB	1	$200.00	$200.00
	Memoria Flash	1	$20.00	$20.00
	CD	10	$1.50	$15.00
Subtotal				**$240.00**
Recursos Humanos				
Cargo	**Descripción**	**Cantidad**	**Valor Unitario ($)**	**Total ($)**
Administrador de red	N/A	1	-	N/A
Administrador de sistemas	N/A	1	-	N/A
Jefe de Proyecto	N/A	1	-	N/A
Analista de desarrollo	N/A	1	-	N/A
Subtotal				**N/A**
Recursos Tecnológicos				
Item	**Descripción**	**Cantidad**	**Valor Unitario ($)**	**Total ($)**
Hardware	Servidor	1	$1,500.00	$1,500.00
	Antenas Unifi	2	$190.00	$380.00
	Router	1	$500.00	$500.00
	Switch	1	$100.00	$100.00
	Equipo terminal	1	$1,500.00	$1,500.00
	Equipo terminal móvil	1	$1,200.00	$1,200.00
Software	Licencias	2	$800.00	$1,600.00
Subtotal				**$6,780.00**
Costo total aproximado del Proyecto				
Descripción				**Total ($)**
Recursos Materiales / Varios				$240.00
Recursos Humanos				N/A
Recursos Tecnológicos				$6,780.00
Total				**$7,020.00**

2.1.2.4.2 Beneficios

- Optimización de la red inalámbrica del campus Miguel de Cervantes de la Universidad Internacional SEK.
- Mejor distribución de la señal del servicio de internet en la red inalámbrica.

- Flexibilidad en la gestión y manejo del número de usuarios.
- Control y monitorización de los usuarios conectados a la red inalámbrica.
- Solo los usuarios registrados en la base de datos podrán tener acceso a la red inalámbrica mediante credenciales de autenticación.
- Segmentación de la red inalámbrica para diferentes grupos de usuarios.

2.2 Diseño

2.2.1 Esquema General de la Solución Técnica

A través de la implementación del protocolo RADIUS, el cual es un protocolo con una arquitectura cliente/servidor, permite plantear una comunicación entre usuarios con servicios entregados por un servidor. Cuando se establece un servidor RADIUS como solución de seguridad, posibilita el manejo de clientes RADIUS como por ejemplo: puntos de acceso en una red inalámbrica, los mismos que serán elementos de acceso a la red como un NAS; donde la comunicación se basa en el protocolo de datagrama de usuario UDP. El cliente RADIUS es comúnmente un NAS y el servidor RADIUS es generalmente un proceso daemon ejecutado en UNIX o Windows. Un cliente o varios clientes RADIUS pasarán la información del usuario o usuarios (mediante credenciales de autenticación) al servidor o servidores RADIUS. El servidor RADIUS recibe las peticiones de conexión de los usuarios, para posteriormente autenticar a cada uno, devolver la información de configuración requerida consiguiendo que el cliente o clientes RADIUS entreguen el servicio al usuario. Las transacciones entre el cliente y un servidor RADIUS son autenticadas a través del uso de un secreto compartido, que nunca se envía por la red.

Para el inicio de la solución técnica se considera criterios de diseño que se adapten a la red.

Tabla No. 3: Criterios de solución

Fuente: (TechNet, 2004)

Factor	Pautas
Seguridad	Autenticación de los usuarios inalámbricos.
	Control de acceso que proporcione acceso a la red inalámbrica a usuarios autorizados.
	Cifrado del tráfico de red inalámbrica.
	Administración segura de claves de cifrado.
Escalabilidad	Diseño básico que permita escalabilidad ascendente y descendente para la institución.
Número mínimo/máximo de usuarios admitidos	de 700 a 1500 (o más) usuarios (estudiantes) de WLAN.
	de 500 a 800 (o más) usuarios (personal administrativo e institucional, profesores, invitados).
Uso de componentes (en base a la infraestructura existente)	Utilización de Active Directory, DHCP, DNS, servicios de red y clientes con Microsoft Windows® Server 2008 R2.
	Compatibilidad con otras aplicaciones de acceso a la red (por cable 802.1X y VPN) por medio de la infraestructura de autenticación.
	Compatibilidad con otras aplicaciones, como el sistema de archivos cifrados (EFS, Encrypting File System) y VPN, por medio de PKI.
Disponibilidad	Afectación mínima ante errores de enlace de red o de componentes individuales.
Extensibilidad	Ampliable para admitir normas futuras (por ejemplo, 802.1x, 802.11a, 802.11i y WPA para WLAN).
	Infraestructura de servicios de Certificate Server extensible para usos comunes de certificados de claves públicas (por ejemplo, correo electrónico seguro, inicio de sesión mediante una tarjeta inteligente, seguridad de servicio Web, etc.).
Administración	Adaptabilidad con soluciones de gestión y administración institucional existentes (control del sistema y del servicio, creación de copias de seguridad, administración de recursos administrativos y configuración, etc.).
Normas	Uso de estándares actuales y capacidad de adaptación ante migración a estándares futuros.

Figura No. 5: Diagrama de solución

Fuente: El autor

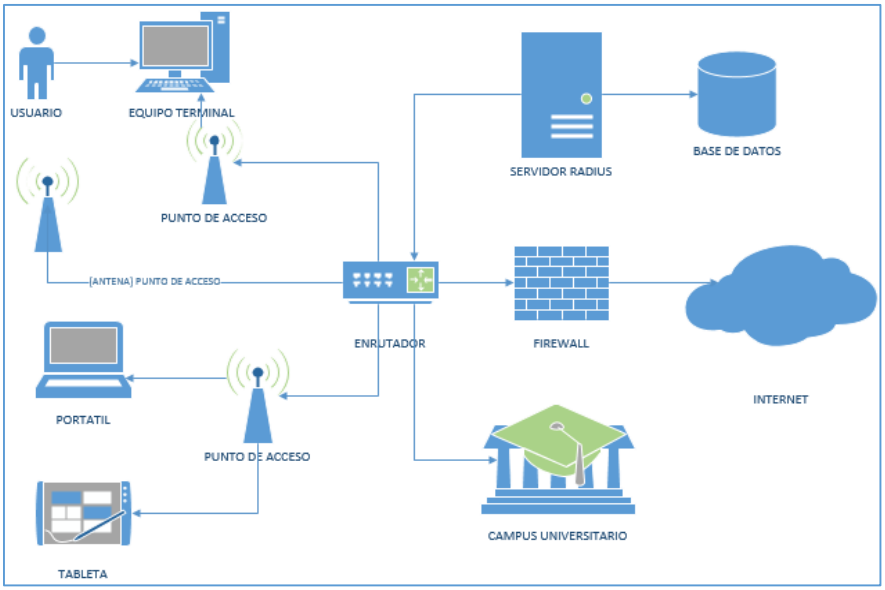


Figura No. 6: Diagrama de comunicación entre usuarios – clientes - RADIUS

Fuente: El autor

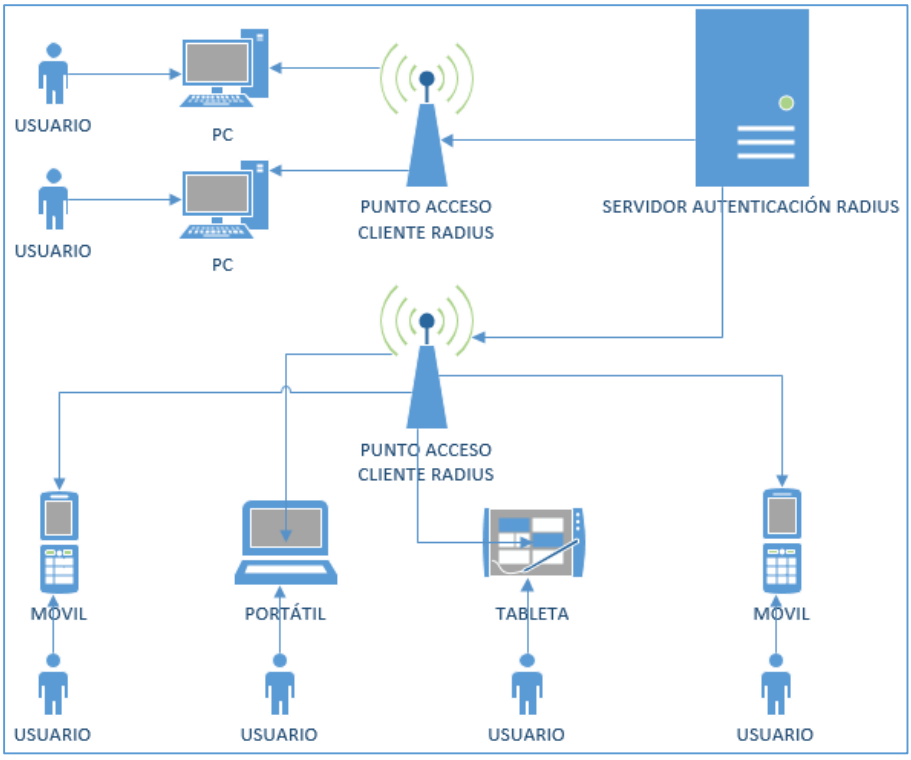
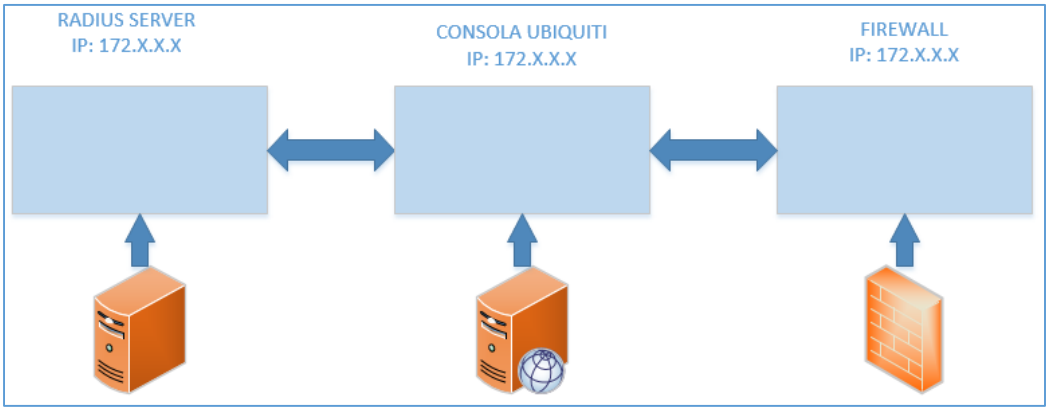


Figura No. 7: Diagrama de validación

Fuente: El autor



CAPÍTULO III

RESULTADOS

3.1 CONSTRUCCIÓN

El desarrollo del proyecto tuvo base en la necesidad de solventar un problema de seguridad en la red inalámbrica de la Universidad Internacional SEK del campus Miguel de Cervantes. Para lo cual se planteó una propuesta de solución mediante una arquitectura de seguridad que se adapte a la tecnología e infraestructura de la institución.

El proyecto incluyó varias etapas generales:

- Análisis y estudio de la situación inicial.
- Diseño de propuestas de solución.
- Ejecución de pruebas en base a las propuestas planteadas.
- Control de pruebas.
- Implementación de la propuesta de solución.
- Control de pruebas iniciales.
- Finalización de la entrega de la propuesta de solución.

En principio se analizó la arquitectura de la red inalámbrica de la institución, la conectividad, operatividad, desempeño de la red y el modo de administración, entre otros factores como: tecnología existente, infraestructura, equipos, etc.

Además se constató que la red inalámbrica en el campus Miguel de Cervantes brinda el acceso a los usuarios al servicio de internet mediante puntos de acceso distribuidos en todo el lugar en cuestión.

Dichos puntos de acceso son antenas tanto indoor como outdoor que permiten la comunicación en la red inalámbrica, y son una parte fundamental de la red. Por lo tanto uno de los puntos principales para el desarrollo de la propuesta de solución del proyecto radica en la configuración de los puntos de acceso en base a la nueva arquitectura de seguridad.

El diseño de la nueva arquitectura consistió en definir la factibilidad de las opciones de solución, costos, y adaptabilidad con la arquitectura de red existente.

Se plantearon como base 2 opciones:

- Mediante software libre.
- Mediante software propietario.

Ambas opciones permitieron determinar el servidor de autenticación a implementar. Los servidores de autentificación principalmente realizan la administración

del acceso a recursos de forma directa o remota. También entregan un servicio de gran fiabilidad dependiendo de los recursos. Por consiguiente se presentó una lista de servidores de autentificación:

- RADIUS.
- LDAP.
- NPS.
- IAS (Internet Authentication Service).

Para el desarrollo e inicio de pruebas se optó por el servidor de autenticación RADIUS. El proceso de pruebas iniciales se efectuó a partir de software libre como: Zeroshell, que es una herramienta que dispone de un servidor RADIUS y ofrecer ciertos servicios requeridos en una red LAN o WLAN.

Sin embargo, en el proceso de configuración y pruebas, la opción no se adaptaba de forma adecuada a la arquitectura de red de la institución, por tal motivo se optó por una solución a través de software propietario de Microsoft, puesto que la institución cuenta con todas las licencias y equipos necesarios.

Las posteriores pruebas de implementación tienen base en un servidor que aloja al servidor RADIUS para su funcionamiento, al igual que servicios (roles) como: DNS, DHCP, LDAP, CERTIFICADOS, etc.

Además, una de las necesidades de la institución es mantener el uso de la consola de gestión de AP para la red inalámbrica, ya que proporciona un sistema de administración estable y seguro que se acopla a lo requerido.

La consola de gestión y administración UBIQUITI de AP, está diseñada para el control y manejo de equipos de comunicación inalámbrica de tipo empresarial en tiempo real, con lo cual la propuesta de solución debe ser adaptable a la misma.

Otro punto importante es la posibilidad que ofrece la consola para vincular un servidor o varios servidores externos para la seguridad al momento de implementar o complementar la arquitectura de la red, dicho servidor puede ser de correo o de autenticación. Como es el caso, se determinó que el servidor asociado a la consola será uno de autenticación denominado RADIUS. Por lo cual, en el proceso de administración continuo de la consola, la gestión de los AP tendría una conexión previa con el servidor de autenticación RADIUS para proveer un determinado servicio de la red inalámbrica a los usuarios.

3.2 IMPLEMENTACIÓN

Dada la elección por el servidor de autenticación RADIUS y software propietario Microsoft, es fundamental determinar las herramientas tecnológicas a nivel de hardware y software para el progreso de la propuesta de solución. Los procesos, configuraciones y

funcionamiento de las herramientas fueron investigados debidamente, de modo que se da paso a la implementación.

3.2.1 Hardware

Para la implementación de pruebas se utilizó un AP UNIFI Enterprise Wi-Fi System modelo UAP-LR (Long Range), de propiedad de la Universidad Internacional SEK.

3.2.1.1 Antena Unifi AP

La antena Unifi es un punto de acceso diseñado para entidades, organizaciones u empresas grandes de fácil despliegue y administración. El equipo incluye un software controlador cuya operatividad es administrable a través de una consola de gestión desplegada en cualquier navegador web. Integra además el estado de los puntos de acceso en tiempo real, carga de mapas, y opciones de seguridad avanzadas.

Figura No. 8: Access Point UAP-LR (Long Range)

Fuente: El autor

3.2.1.2 Características generales

- Diseño estético con un LED único que proporciona una guía para seguimiento y alertas de ubicación para cada punto de acceso.
- Utiliza un controlador de hardware y software.
- Despliegue tanto en PC, Mac, Linux, nube privada, servicio público en la nube.
- Tecnología MIMO WiFi 802.11ac, con velocidades de gigabit y rangos de hasta 600 pies (183m).
- Tecnología MIMO WiFi 802.11n con velocidades de hasta 300 Mbps; para rendimiento superior en bandas de 2,4 y o 5 GHz.
- Consola de administración e interfaz de usuario de controlador, para configuraciones, y organización de los puntos de acceso (AP).
- Escalabilidad ilimitada y ampliable.
- Construcción de la red inalámbrica grande o pequeña según sea lo requerido.
- Firmware actualizable.
- Sistema de gestión unificada.
- Alimentación a través de Ethernet (PoE).

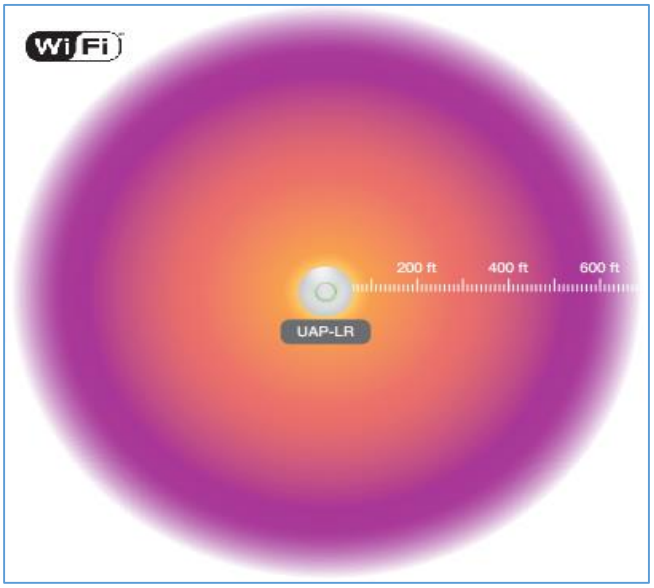
3.2.1.3 Controlador UNIFI

- Permite provisionar a uno o varios puntos de acceso Unifi, trazar redes, gestión rápida del tráfico del sistema y provisionar puntos de acceso adicionales.

- Presenta informes configurables y análisis para el control y manejo de grandes cantidades de usuarios agilizando problemas.
- Posee una funcionalidad de enlace ascendente que permite conectividad inalámbrica entre puntos de acceso y adopción de dispositivos inalámbricos y cambios en tiempo real de la topología de la red.
- Portal de invitados personalizable con autenticación, además capacidad de utilizar su propio servidor de portal externo.
- Permite aplicar diferentes velocidades de ancho de banda, limita el uso total de datos para carga y descarga, y limita la duración del uso.
- Gestión de configuración flexible para grandes despliegues.
- Creación de múltiples grupos WLAN y asignación al radio o zona de cobertura de un punto de acceso.
- Zero Handoff Roaming, que mantiene las conexiones estables para los usuarios en movimiento por medio del cambio a un AP más cercano.
- Zero Handoff Roaming permite la aparición de múltiples puntos de acceso como un solo AP, trabajando con cualquier cliente.
- Importación de mapas de ubicación del lugar donde se indicará la posición de cada AP de la red inalámbrica.
- Organización, estadística y visualización gráfica del tráfico de red en tiempo real.
- Instalación, configuración y gestión de todos los puntos de acceso desde una única ubicación.

Figura No. 9: AP rango de cobertura

Fuente: (UNIFI, User Guide)



3.2.1.4 Características Técnicas

A continuación se detallan las características técnicas en el siguiente cuadro.

Tabla No. 4: Características técnicas antena AP Unifi (Ubiquiti)

Fuente: (UNIFI, User Guide)

Especificaciones (UAP-LR) UniFi AP Largo Alcance	
Dimensiones	200 x 200 x 36.5 mm (7,87 x 7,87 x 1,44 in)
Peso	290 g (10,23 oz) sin Kits de montaje, 430 g (15,17 oz) con kits de montaje
Interfaz de red	(1) Puerto Ethernet 10/100
Botones	Reset (restablecer)
Antenas	Integrado 3 dBi Omni (Soporta MIMO 2x2 con Diversidad espacial)
Estandares WI-FI	802.11 b / g / n *
Método de alimentación	Fuente pasiva sobre Ethernet (12-24V)
Fuente de alimentación	de 24V, con adaptador PoE 0.5A
Máximo Consumo de energía	6 W
Máxima Potencia	TX 27 dBm
BSSID	hasta cuatro por Radio
Ahorro de energía	Compatible
Seguridad Inalámbrica	WEP, WPA-PSK, WPA-Enterprise (WPA / WPA2, TKIP / AES)
Certificaciones	CE, FCC, IC
Montaje	de pared / techo (Kits incluidos)
Temperatura de funcionamiento	-10 a 70 ° C (14 a 158 ° F)
Humedad de funcionamiento	5 - 80% sin condensación
Gestión de Tráfico Avanzado	
VLAN	802.1Q
QoS avanzada	Rango limitado por usuario
Aislamiento Invitado Tráfico	Compatible
WMM	Voz, Vídeo, Best Effort, y Background
Clientes concurrentes	100+
Rango datos admitidos (Mbps)	
Estándar	**Rango de Datos**
802.11n	6.5 Mbps a 300 Mbps (MCS0 - MCS15, HT 20/40)
802.11b	1, 2, 5.5, 11 Mbps
802.11g	6, 9, 12, 18, 24, 36, 48, 54 Mbps * 2.4 GHz

3.2.2 Software

Para la implementación del servidor RADIUS se utilizó como opción de prueba inicial la herramienta de software libre ZeroShell, y posteriormente como opción aceptada y definitiva la herramienta de Windows Server 2008 R2 a través de los servicios (roles) que incluye.

3.2.2.1 Zeroshell

Zeroshell es una distribución Linux para servidores y dispositivos embebidos que proporcionan servicios de red a una LAN o WLAN que lo requiera.

Disponible en forma de Live CD o imagen configurable y administrable utilizando un navegador web. También es una herramienta que permite el manejo de un servidor RADIUS de manera intuitiva con administración de certificados digitales.

Entre los servicios a destacar: DHCP, DNS, VLAN, VPN, RADIUS, LDAP, portal cautivo, firewall. Es configurable desde un terminal o vía ssh, y administrable vía remota desde un navegador con una interfaz web.

3.2.2.2 Windows Server 2008 R2

Es la segunda versión de Windows Server 2008, que añade características adicionales y mejoras a la versión existente. Dichas mejoras se dan para: virtualización, gestión, escalabilidad, fiabilidad, web, redes y acceso.

R2 (Release), hace referencia a una actualización del sistema Windows Server 2008, e incorpora paquetes de actualización SP1 y SP2. Esta herramienta permite dar un mayor control sobre la red y la infraestructura de servidores,

aumentar la seguridad para la protección el sistema operativo y el entorno de red, ofrece a los administradores de TI flexibilidad en la implementación y mantenimiento del sistema, también ofrece una plataforma segura para el desarrollo y alojamiento confiable de servicios y aplicaciones web, permite la virtualización de servidores, aplicaciones y cargas de trabajo.

Entre los roles que Windows Server 2008 R2 permite instalar se encuentran:

- Active Directory Lightweight Directory Services.
- Active Directory Rights Management Services.
- Hyper-V.
- Servicios de acceso y directivas de redes.
- Servicios de archivo.
- Servicios de certificados de Active Directory.
- Servicios de dominio de Active Directory.
- Servicios de escritorio remoto.
- Servicios de federación de Active Directory.
- Servicios de implementación de Windows.
- Servicios de impresión y documentos.
- Servidor de aplicaciones.
- Servidor de fax.
- Servidor DHCP.
- Servidor DNS.

- Servidor web (IIS).
- Windows Server Update Services.

En cuanto a requerimientos mínimos necesarios de presenta en el siguiente cuadro:

Tabla No. 5: Requerimientos

Fuente: El autor

	Mínimo	Recomendado	Óptimo
Procesador	1 GHz	2 GHz	3 GHz
Memoria	512 MB de RAM	1 GB de RAM	2 GB de RAM
Almacenamiento	8 GB	40 GB	80 GB
Unidad	Unidad de DVD-ROM		
Pantalla y perifericos	Super VGA (800 x 600) o superior		

3.2.3 Implementación Inicial

3.2.3.1 Instalación del controlador y consola de administración del AP

- Se ingresa el CD del controlador del AP en el equipo terminal (PC o servidor) donde será gestionada la consola de administración.

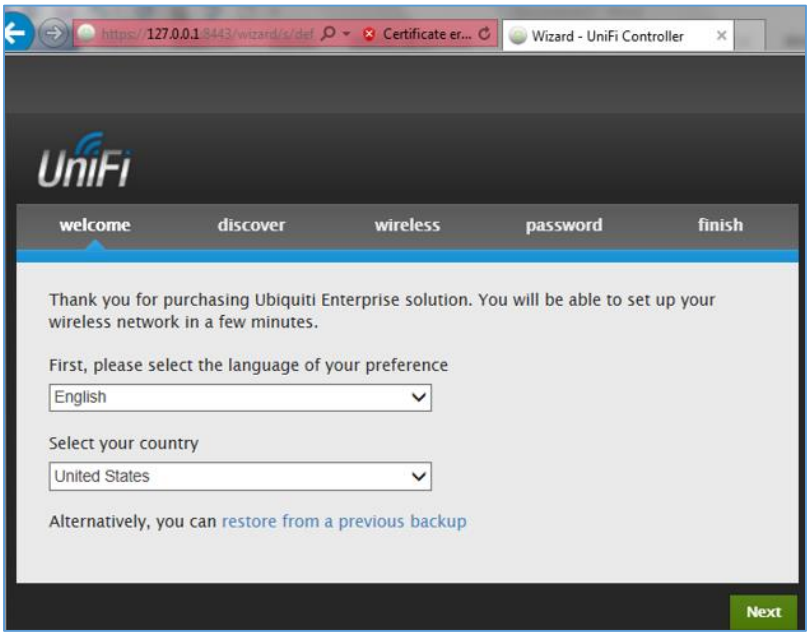
Figura No. 10: Arranque del controlador AP

Fuente: (UNIFI, User Guide)

- Escoger la opción "Launch a Browser to Manage Wireless Network" para obtener acceso a la interfaz de configuración web. Elegir el idioma y país de preferencia y continuar con la configuración.

Figura No. 11 Interfaz web de configuración

Fuente: (UNIFI, User Guide)



- En la siguiente pestaña de configuración se mostrarán todas las antenas que se encuentren conectadas a la red LAN / WLAN, también se visualizará la dirección o direcciones tanto MAC como IP dados por defecto.

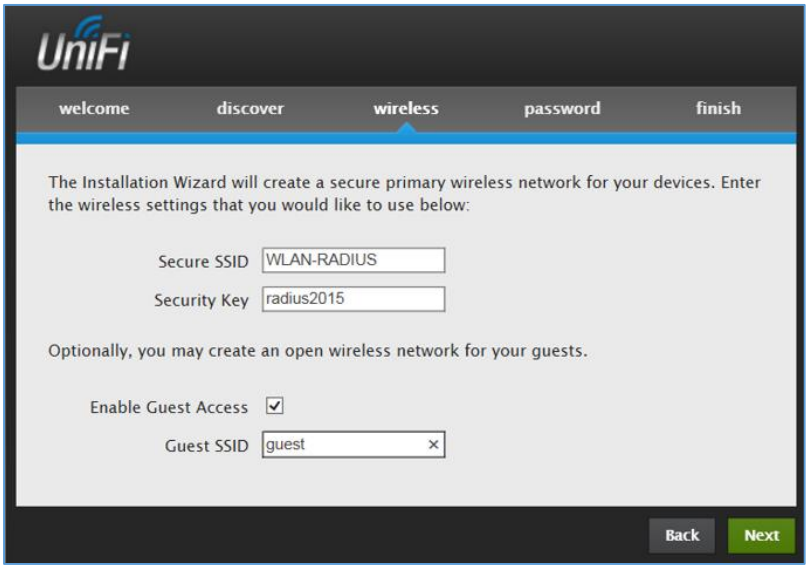
Figura No. 12: AP conectadas

Fuente: (UNIFI, User Guide)

- En la siguiente pestaña se ingresa las configuraciones para la red inalámbrica que se va a crear, indicando el SSID (Service Set Identifier) que es un identificador de la red inalámbrica. Proporcionar la clave de seguridad y asignar un SSID para una red de invitados si se desea y continuar.

Figura No. 13: Configuración del SSID

Fuente: (UNIFI, User Guide)



- Indicar datos de autenticación para el acceso a la consola de administración.

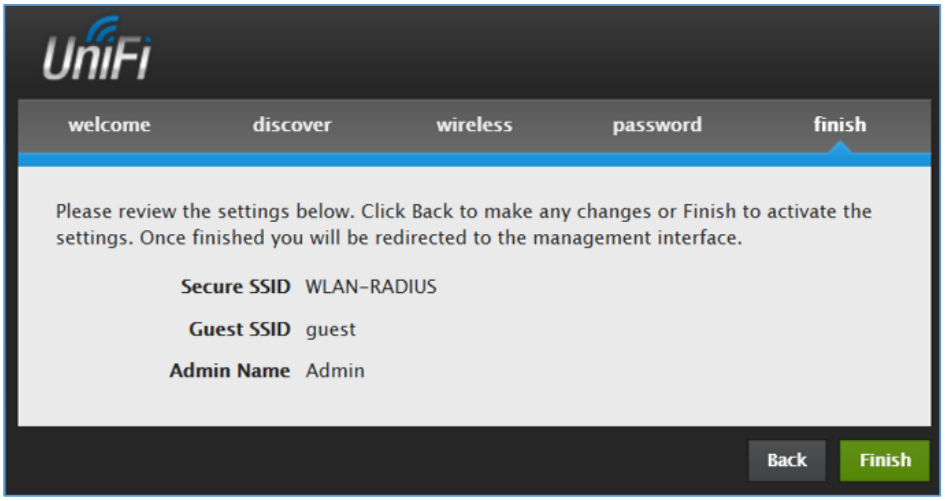
Figura No. 14: Configuración de administrador

Fuente: (UNIFI, User Guide)

- A continuación se mostrará el cuadro de confirmación final.

Figura No. 15: Cuadro de confirmación

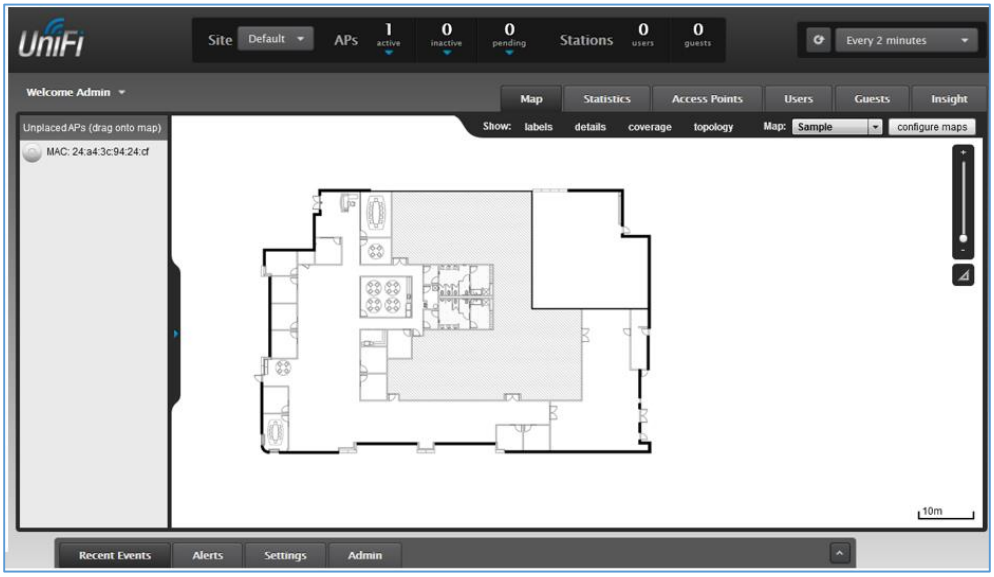
Fuente: (UNIFI, User Guide)



- La interfaz web permitirá visualizar la consola de administración.

Figura No. 16: Consola de administración web

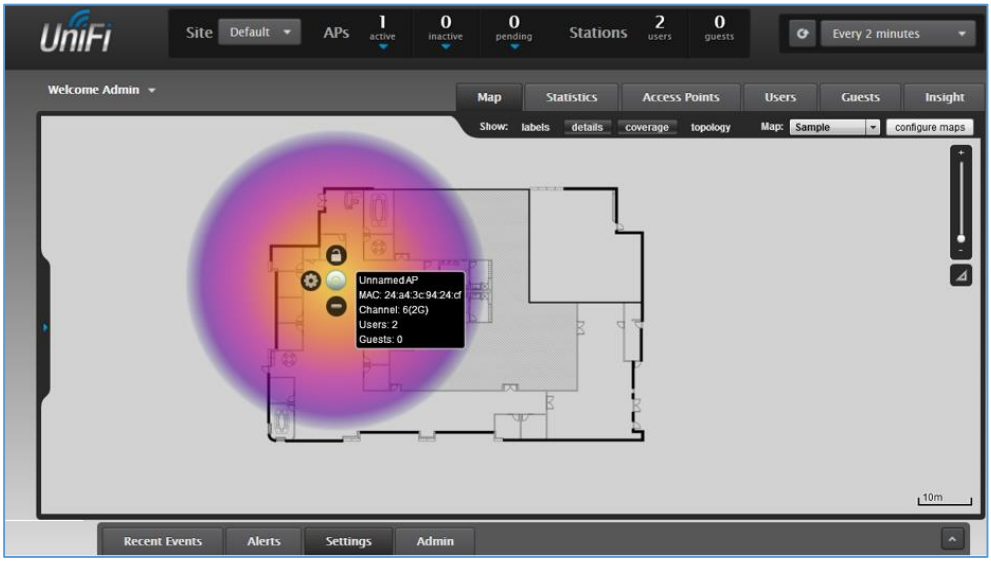
Fuente: (UNIFI, User Guide)



- Agregar la antena hacia el mapa por defecto para visualizar su cobertura, detalle de configuraciones y su funcionamiento en tiempo real.

Figura No. 17: Ingreso y visualización del AP

Fuente: (UNIFI, User Guide)



3.2.3.2 Instalación Zeroshell

- Descargar la imagen de la herramienta Zeroshell en: http://www.zeroshell.net/ para configurar en una máquina virtual sea: VMware o Virtual Box.

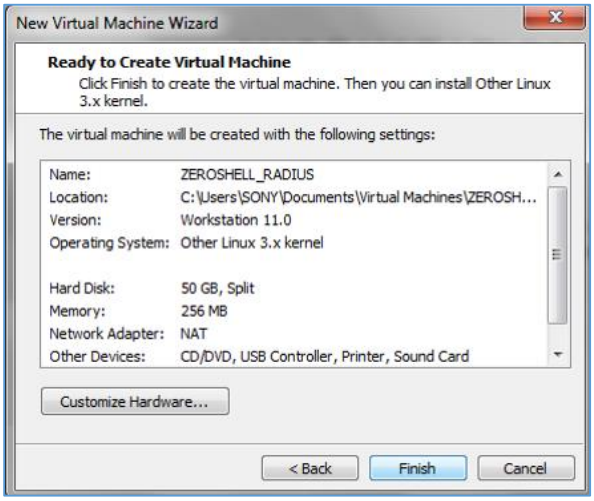
Figura No. 18: Creación de la máquina virtual (modo de instalación)

Fuente: (VMware)

- Cargar la imagen de Zeroshell, desde la ubicación en la que se encuentra y continuar. Elegir el tipo de sistema operativo, que se está instalando, asignar el nombre a la máquina virtual y el tamaño de disco y finalizar la instalación.

Figura No. 19: Resumen de máquina virtual

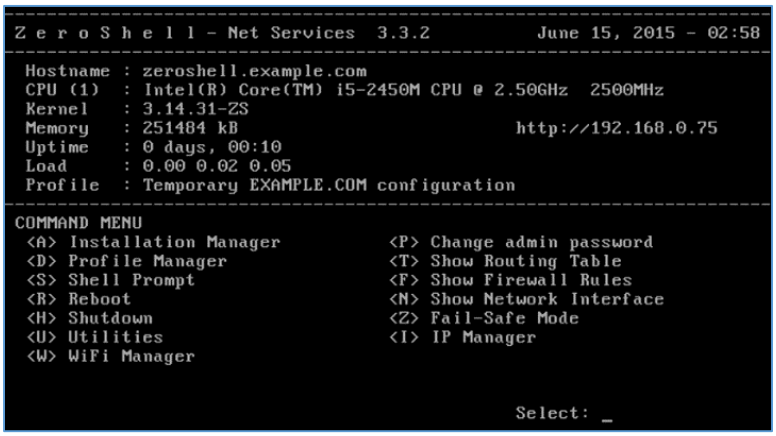
Fuente: (VMware)



- Al iniciar, se cargan los componentes del sistema y se presentará la pantalla de inicio de Zeroshell con el menú de opciones de configuración del servidor. Como opciones principales se tendrá: gestión IP (dirección y mascara de subred), interface de red, cambio de contraseña, puerta de enlace y gestión de perfiles.

Figura No. 20: Opciones de Configuración

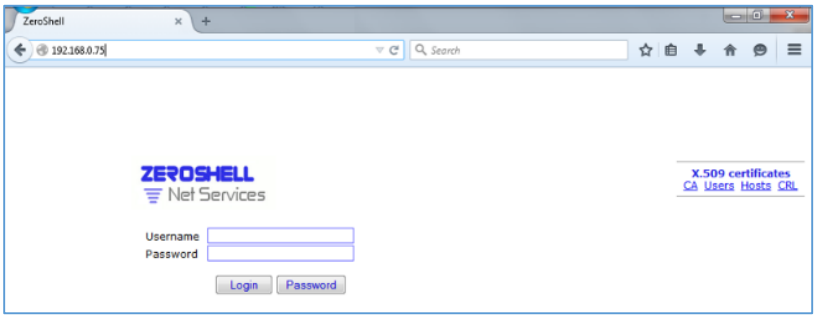
Fuente: (Zeroshell)



- Para comprobar el acceso a la interfaz web, se debe ingresar la dirección IP designada por defecto IP 192.168.0.75/24 en un navegador web.

Figura No. 21: Ingreso a interfaz web

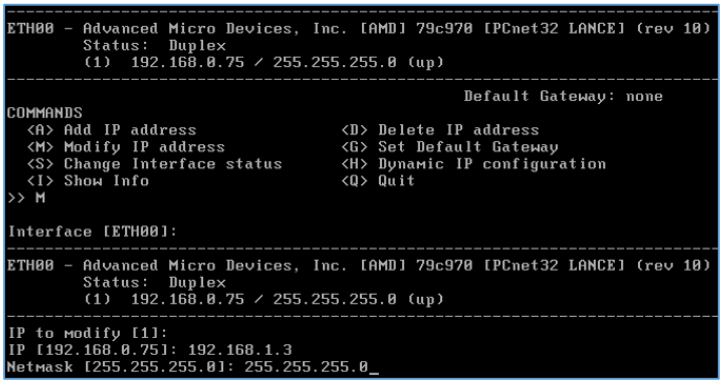
Fuente: (Zeroshell)



- Si se requiere cambiar la dirección IP del servidor, para el ingreso a su configuración mediante un navegador web; ingresar en la opción I, que mostrara las opciones de configuración de tarjeta de red del servidor. Luego ingresar en la opción M para modificar la dirección IP y mascara de subred configurados por defecto. También es posible la asignación de una puerta de enlace para el servidor, que permita la comunicación con los hosts de la red, seleccionando la opción G.

Figura No. 22: Modificación de la dirección IP

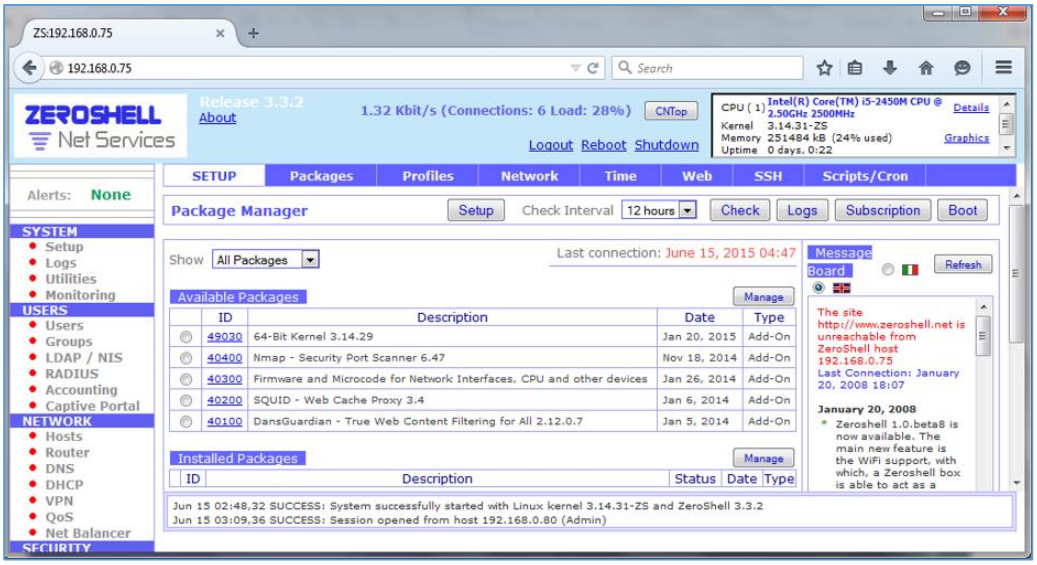
Fuente: (Zeroshell)



- Es necesario el cambio de contraseña de acceso para la configuración a través de la interfaz web de Zeroshell, que por defecto el usuario y contraseña es el mismo: ‘Admin’. Al ingresar a la interfaz, previa autenticación se visualizará la interfaz gráfica con todas las opciones que ofrece a un administrador de TI.

Figura No. 23: Interfaz web de Zeroshell

Fuente: (Zeroshell)



- Dentro de la interfaz es importante crear un perfil que almacenará todas las configuraciones y ajustes correspondientes. La creación de un perfil, permitirá en cada inicio de sesión que cargue la configuración por defecto. Ubicar la pestaña ‘Setup’ para seleccionar el disco duro para almacenar el nuevo perfil.

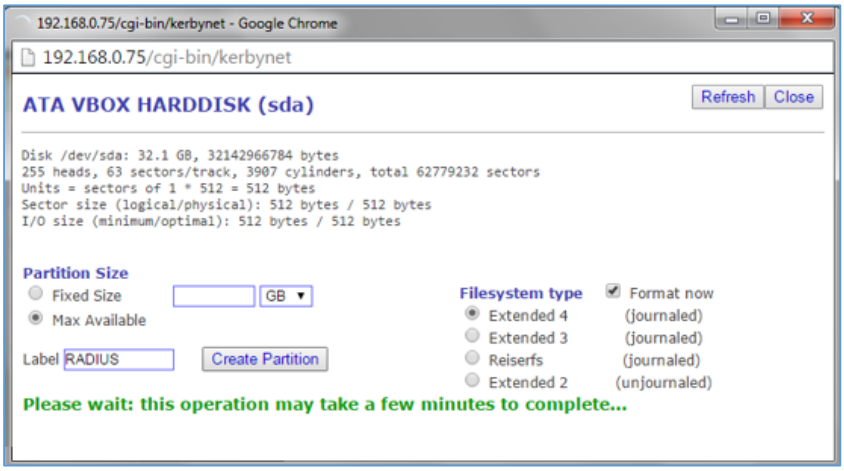
Figura No. 24: Creación perfil

Fuente: (Zeroshell)

- Crear una partición seleccionando 'Disk Model' y dar clic en "New partition". En la ventana desplegada ingresar el nombre del disco virtual en la opción 'Label' y seleccionar 'Create Partition'.

Figura No. 25: Creación de la partición

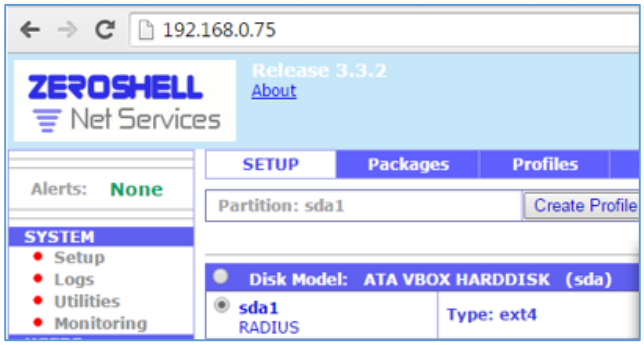
Fuente: (Zeroshell)



- Crear un perfil, seleccionando la partición creada previamente y elegir la opción 'Create Profile'.

Figura No. 26: Selección de partición creada

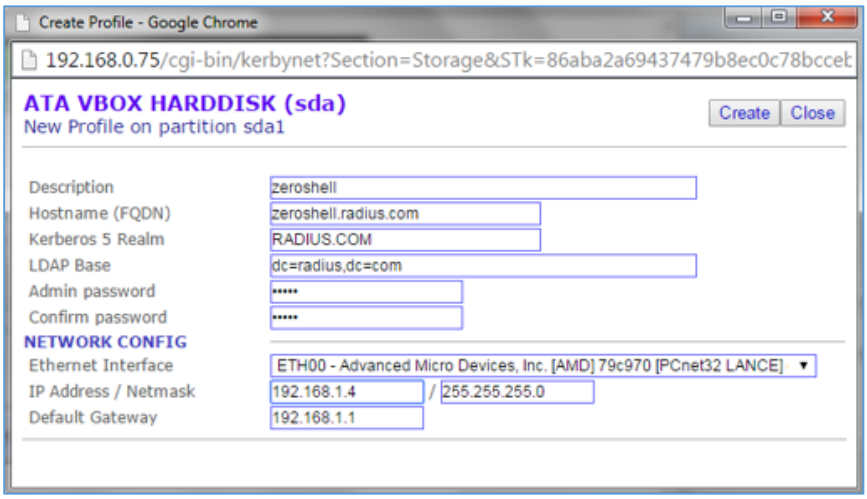
Fuente: (Zeroshell)



- En la ventana desplegada, ingresar una descripción, un Hostname, el Kerberos 5 Realm, un LDAP Base, la contraseña de administrador y la dirección IP del servidor y gateway con mascara de subred. A continuación seleccionar 'Create' para crear el perfil.

Figura No.27: Formulario de creación de perfil

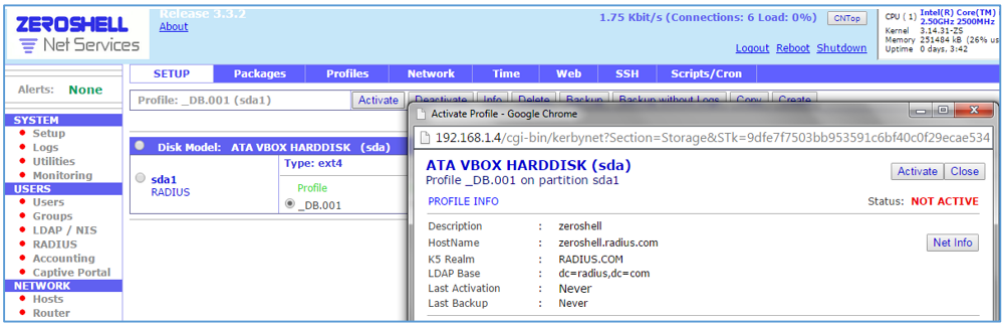
Fuente: (Zeroshell)



- Para activar el nuevo perfil, se selecciona el creado, para abrir una ventana de resumen donde el 'Status' se encuentra como no activo.

Figura No.28: Resumen del perfil creado

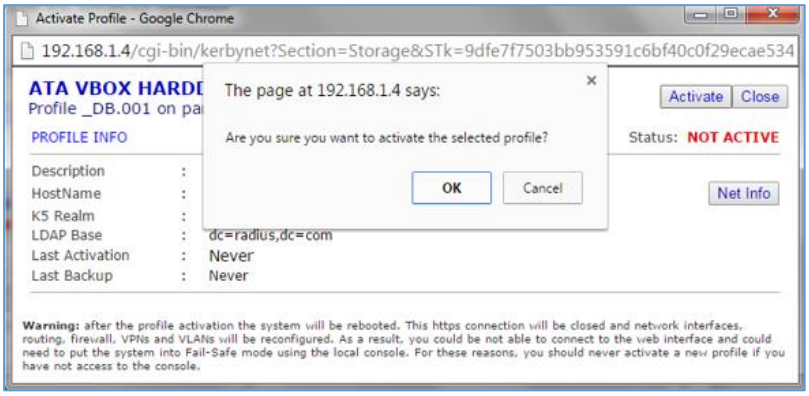
Fuente: (Zeroshell)



- Se selecciona ‘Activate’ para que el perfil se active dando un mensaje de confirmación.

Figura No. 29: Activación del nuevo perfil creado

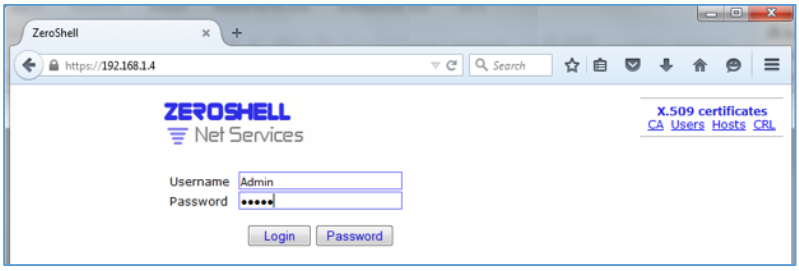
Fuente: (Zeroshell)



- Además se debe considerar que en la creación del perfil la dirección IP del servidor fue cambiada, por lo cual todos los equipos deben estar en la misma red. Se puede realizar una comprobación mediante el comando: ‘ipconfig’ (que permite obtener la dirección IP del equipo local), y ‘ping’ (que permite comprobar el estado de comunicación de un host con el resto de equipos de la red) en el terminal de consola. Al término del proceso reiniciar el sistema para que los cambios se apliquen e ingresar nuevamente.

Figura No. 30: Ingreso a la interfaz reiniciada

Fuente: (Zeroshell)

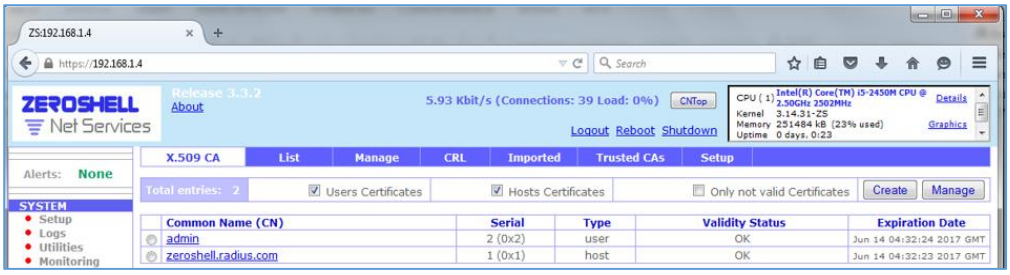


3.2.3.3 Autoridad Certificadora

- Para iniciar con la creación de una autoridad de certificación, seleccionar la pestaña X509 CA de la interfaz web.

Figura No. 31: Creación de CA

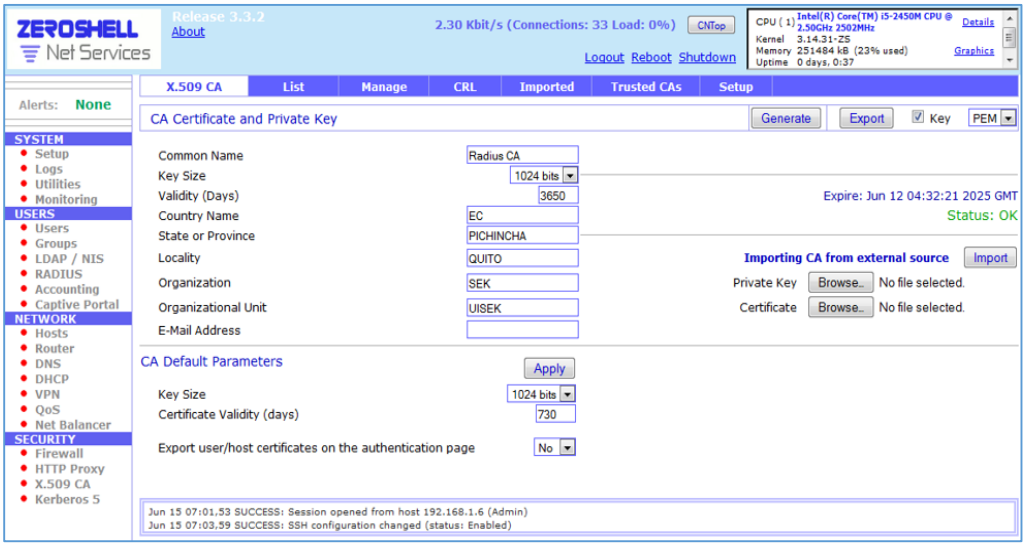
Fuente: (Zeroshell)



- A continuación se presenta una ventana con un formulario de ingreso de información, seleccionar la opción 'Generate', que generara el certificado de CA y continuar. Con ello la autoridad certificadora estará configurada.

Figura No. 32: Formulario para la creación de CA

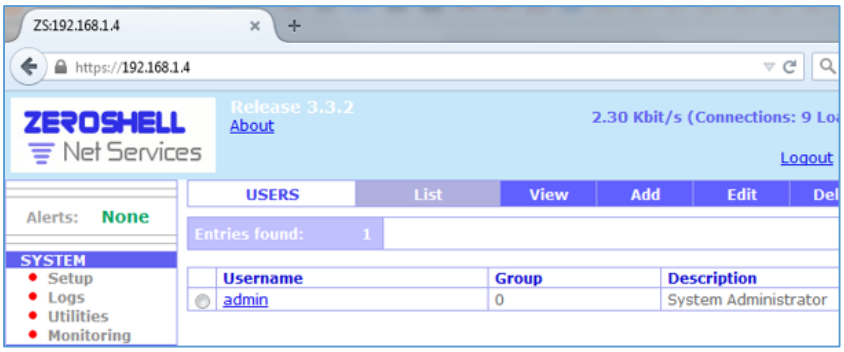
Fuente: (Zeroshell)



- Para la creación de usuarios de RADIUS, seleccionar la opción ‘Users’. Ahí se visualizará un único usuario administrador.

Figura No. 33: Lista de usuarios existentes

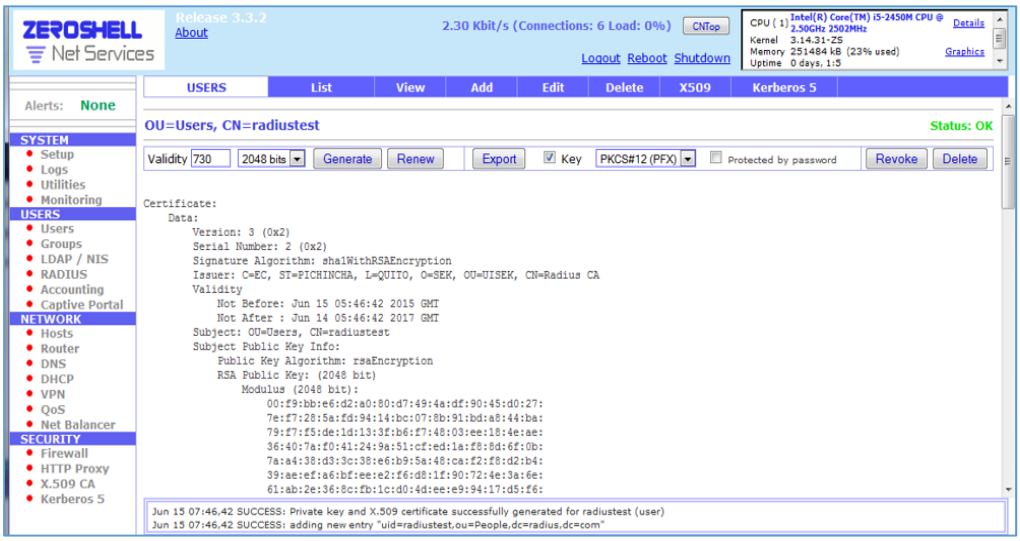
Fuente: (Zeroshell)



- Seleccionar la opción para generar el formulario de creación de usuario, y llenar los datos requeridos. Después dar clic en la opción 'Submit' que mostrará un resumen del certificado creado.

Figura No. 34: Resumen del certificado creado

Fuente: (Zeroshell)



3.2.3.4 Configuración del servidor RADIUS en Zeroshell

- Seleccionar la opción RADIUS, y marcar el recuadro 'enabled' para activar el estado del servidor.

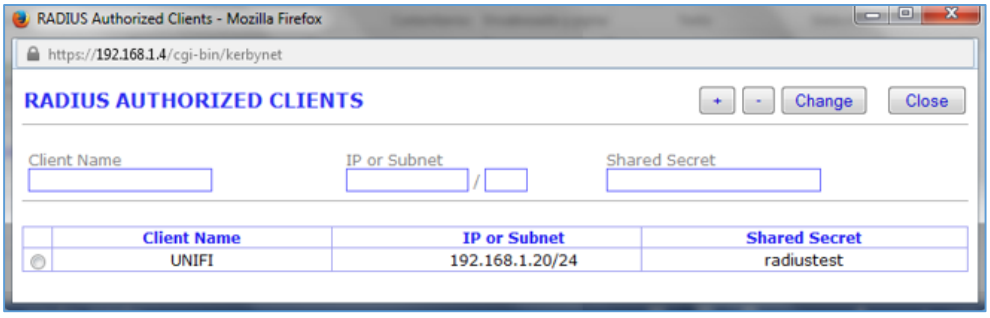
Figura No. 35: Activación del servidor RADIUS

Fuente: (Zeroshell)

- Ingresar a la opción RADIUS, y ubicar la pestaña ‘Authorized Clients’ para registrar y agregar los puntos de acceso deseados respectivamente.

Figura No. 36: Registro de clientes RADIUS

Fuente: (Zeroshell)



3.2.3.5 Clave Pública

Antes de realizar la importación de la clave pública, se debe exportar la clave pública del servidor, para instalarlo en cada uno de los clientes. Seleccionar la opción x.509 CA y elegir la pestaña ‘Trusted CAs’, donde se indica la autoridad certificadora. Al exportar se obtendrá un archivo ‘TrustedCA.pem’ descargable.

Figura No. 37: Clave pública descargada

Fuente: (Zeroshell)

- Para la importación de clave privada, seleccionar la opción ‘USERS’, en el cual se presentará los usuarios registrados en el sistema. Indicar el usuario cuya clave privada se va a exportar e ingresar a la opción X509 que indica un resumen de la clave privada a exportar. Al finalizar la exportación se obtendrá el archivo de la clave privada exportada.

Figura No. 38: Clave privada exportada

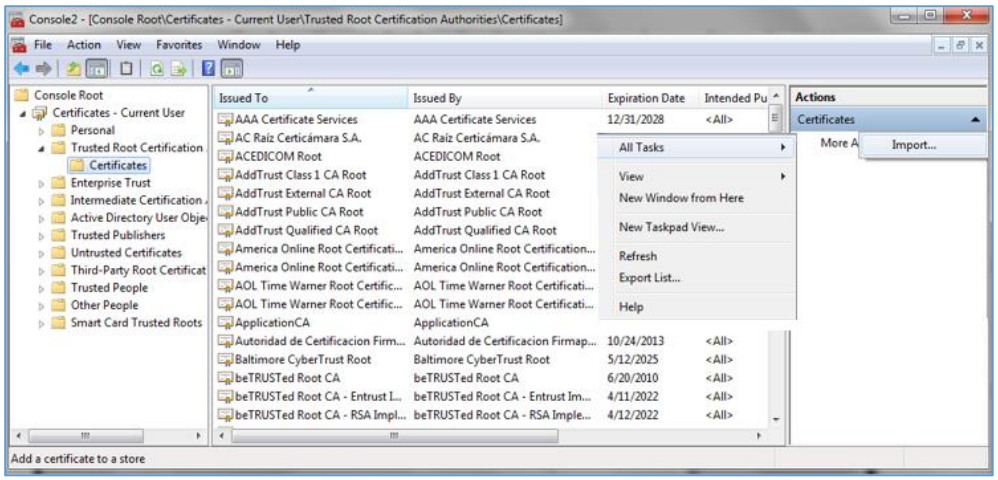
Fuente: (Zeroshell)

- El siguiente paso es la instalación de la clave pública, ingresando a la consola raíz ‘mmc’ para agregar complementos desde la opción ‘File’. El complemento que se va agregar es 'Certificates’. En el cual se marca la opción ‘My user account’ para la administración de certificados y continuar. Seleccionar la opción para que el complemento administre los certificados y finalizar.

- Al finalizar, desplegar el contenido de certificados del usuario actual, y seleccionar el directorio de entidades de certificación raíz donde se encuentran los certificados. Seleccionar la opción ‘Actions’ para realizar la importación.

Figura No. 39: Importación del certificado

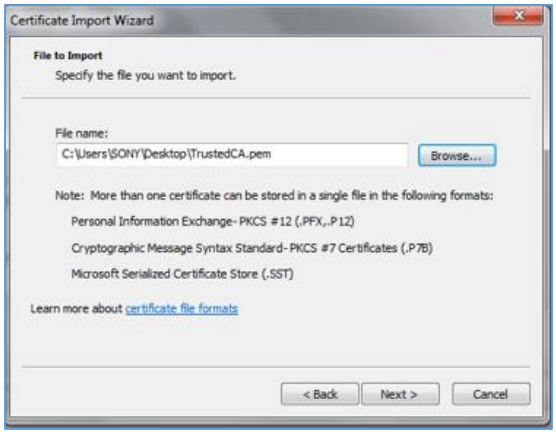
Fuente: (Zeroshell)



- Una vez importado el certificado se abrirá el asistente de importación de certificados, en el cual carga el certificado previamente descargado.

Figura No. 40: Carga de certificado

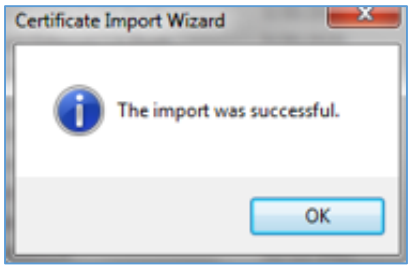
Fuente: (Zeroshell)



- Seleccionar el almacén de certificados 'Trusted Root Certification Authorities' y continuar. A continuación se mostrará un resumen y un mensaje de confirmación.

Figura No. 41: Mensaje de importación realizada

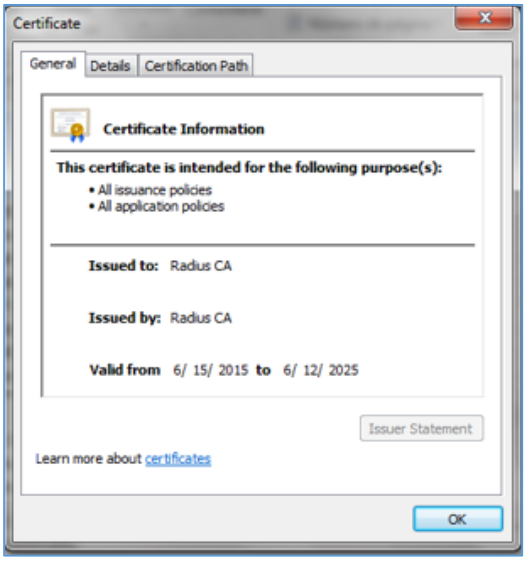
Fuente: (Zeroshell)



- El certificado importado estará añadido en la autoridad certificadora 'Radius CA'.

Figura No. 42: Detalle de Radius CA

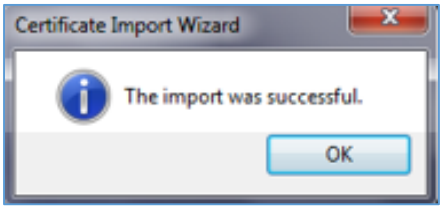
Fuente: (Zeroshell)



- Ahora para la instalación de clave privada, dar doble clic sobre el certificado exportado que abrirá el asistente de importación de certificados. Ubicar el archivo para cargarlo, e indicar la contraseña para la clave privada configurado anteriormente en la creación del certificado y marcar la inclusión de las propiedades extendidas. Elegir el almacén del certificado, examinar la ubicación y seleccionar como almacén el directorio 'Personal'. Al continuar se mostrará el resumen del certificado y un mensaje de confirmación de la importación realizada.

Figura No. 43: Mensaje de confirmación

Fuente: (Zeroshell)

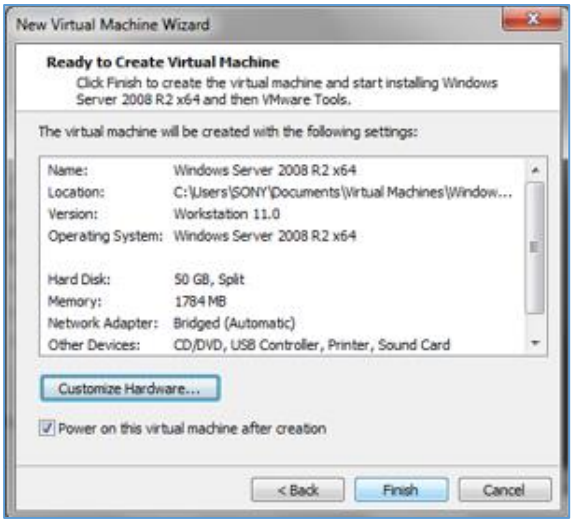


3.2.3.6 Instalación y configuración de Windows Server 2008 R2

- Crear una máquina virtual para la instalación de Windows Server 2008 R2, y al continuar con la creación se deberá cargar la imagen o CD de instalación. De igual forma se configura un mínimo de memoria para almacenamiento de 50 GB, el adaptador de red como 'Bridged', y la memoria RAM con un mínimo de 1 GB a 2 GB como principales configuraciones.

Figura No. 44: Creación de la máquina virtual en VMware

Fuente: (Microsoft)



- Al término de la creación de la máquina virtual, iniciará el proceso de instalación del sistema operativo Windows Server 2008 R2.

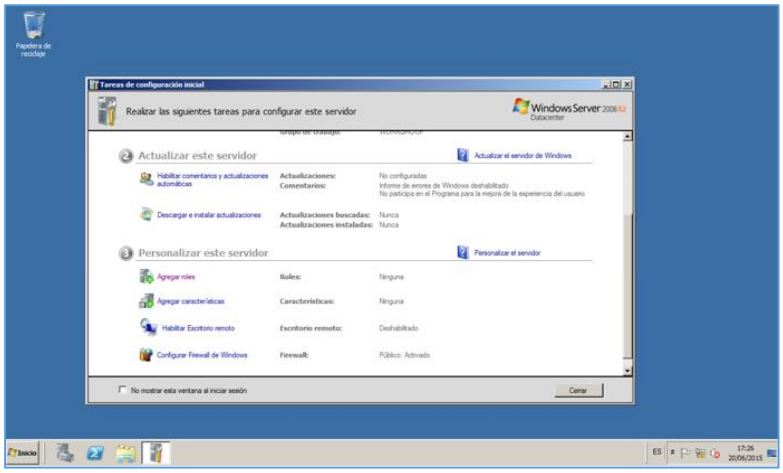
Figura No. 45: Instalación del Sistema Operativo

Fuente: (Microsoft)

- Al término de la instalación, se mostrara una ventana inicial de ayuda.

Figura No. 46: Ventana de tareas de configuración inicial

Fuente: (Microsoft)

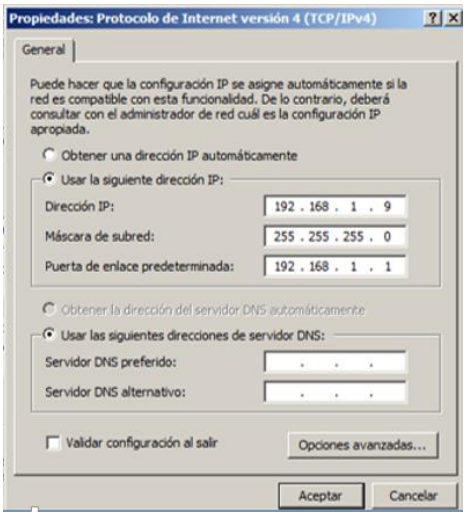


- Configurar en las propiedades del protocolo TCP/IP la dirección IP (192.168.1.9), máscara de subred (255.255.255.0), y puerta de enlace

(192.168.1.1) que tendrá el servidor para la implementación de prueba inicial en una red privada.

Figura No. 47: Configuración de direcciones del servidor

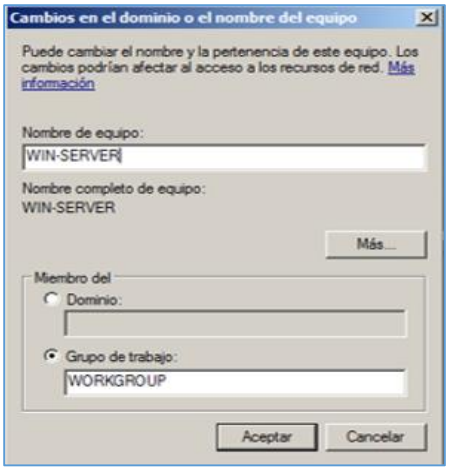
Fuente: (Microsoft)



- A continuación cambiar el nombre del equipo, que para este caso de prueba será: 'WIN-SERVER' mediante propiedades del sistema en la pestaña 'Nombre de equipo' y continuar.

Figura No. 48: Cambio del nombre del equipo (servidor)

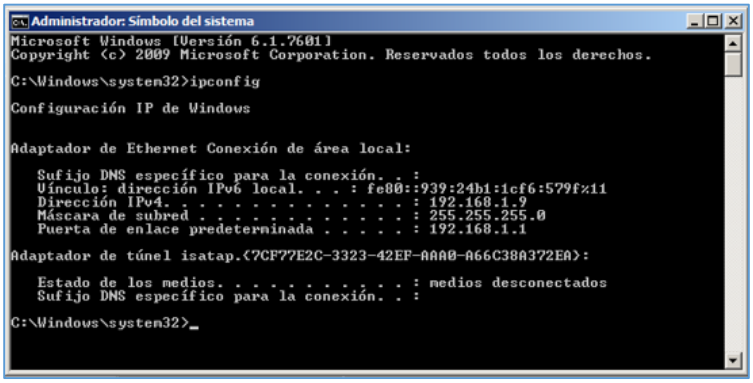
Fuente: (Microsoft)



- Para comprobar las recientes configuraciones realizadas, se puede verificar a través de la consola de comandos mediante el comando 'ipconfig'.

Figura No. 49: Comprobación de configuraciones (cmd)

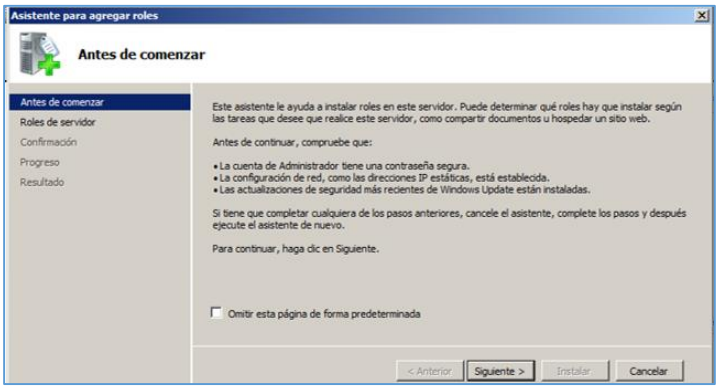
Fuente: El autor



- El servidor al ser instalado requiere de ciertos servicios (roles) para cumplir con su funcionamiento, para ello se puede recurrir a la ventana de tareas de configuración inicial. En la ventana de tareas seleccionar la opción 'Agregar roles' que abrirá el asistente de instalación.

Figura No. 50: Asistente para instalación de roles del servidor

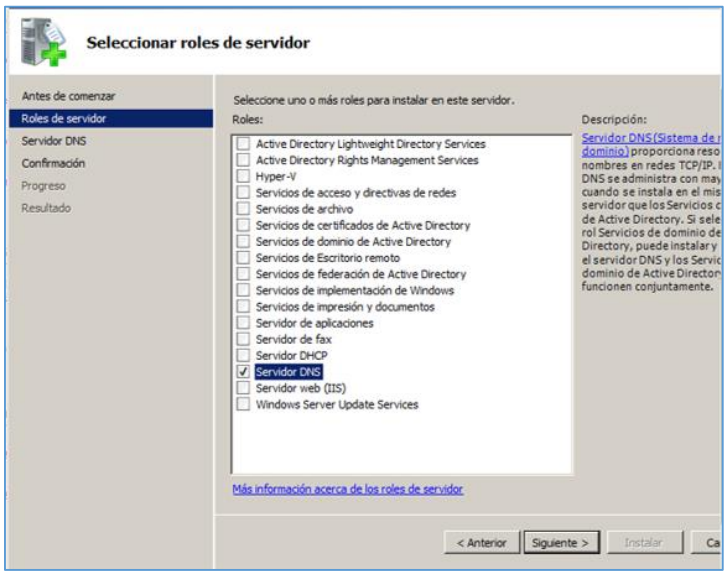
Fuente: (Microsoft)



- Para iniciar se va a instalar el rol de 'Servidor DNS', marcando el casillero correspondiente, y continuar con la confirmación y progreso de instalación.

Figura No. 51: Selección de rol

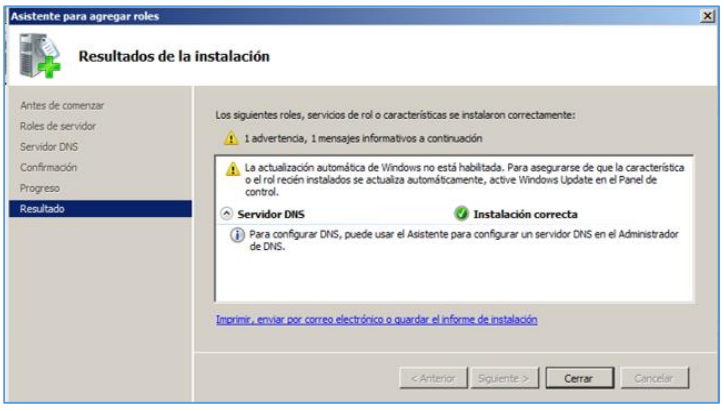
Fuente: (Microsoft)



- Después de instalar el rol aparecerá un mensaje de confirmación de 'instalación correcta'.

Figura No. 52: Resultados de la instalación

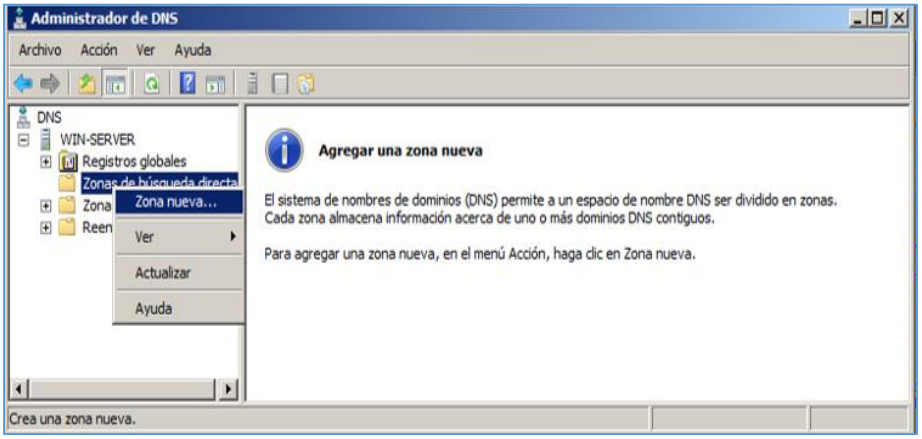
Fuente: (Microsoft)



- Ingresar desde inicio – herramientas administrativas – DNS, para abrir el administrador de DNS y crear una 'zona nueva'.

Figura No. 53: Administrador de DNS

Fuente: (Microsoft)



- Al crear una nueva zona en el directorio 'Zonas de búsqueda directa', un asistente ayudará en la creación.

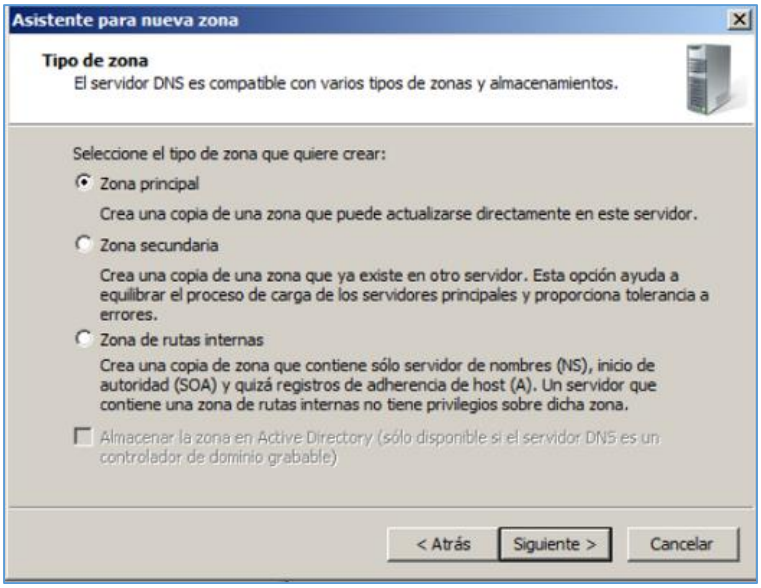
Figura No. 54: Asistente de nueva zona

Fuente: (Microsoft)

- Elegir el tipo de zona para el servidor DNS y Marcar como tipo de zona: a 'zona principal'.

Figura No. 55: Tipo de zona

Fuente: (Microsoft)



- Dar un nombre de zona que para el caso será radiussek.com

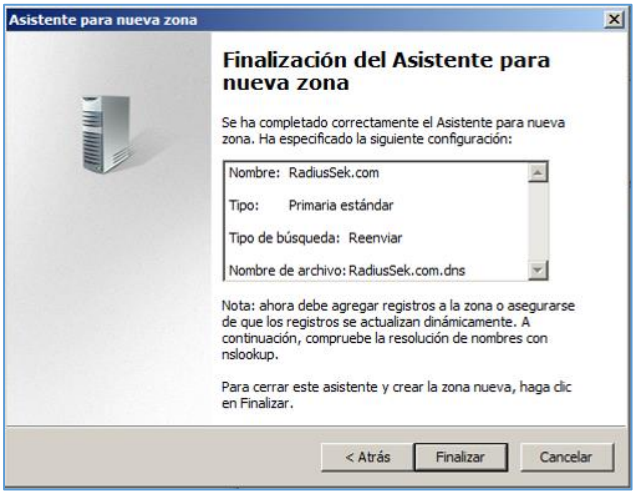
Figura No. 56: Nombre de zona

Fuente: (Microsoft)

- A continuación el asistente creará un archivo con el nombre designado en la nueva zona, y elegir la opción que permita 'actualizaciones dinámicas' y finalizar.

Figura No. 57: Finalización de creación de nueva zona

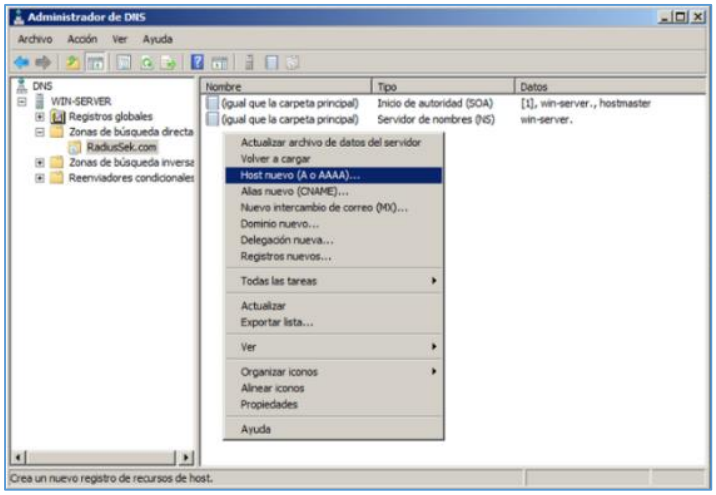
Fuente: (Microsoft)



- Una vez creada la nueva zona, seleccionar la misma y dar clic derecho en la opción 'Host nuevo (A o AAA)'.

Figura No. 58: Host nuevo

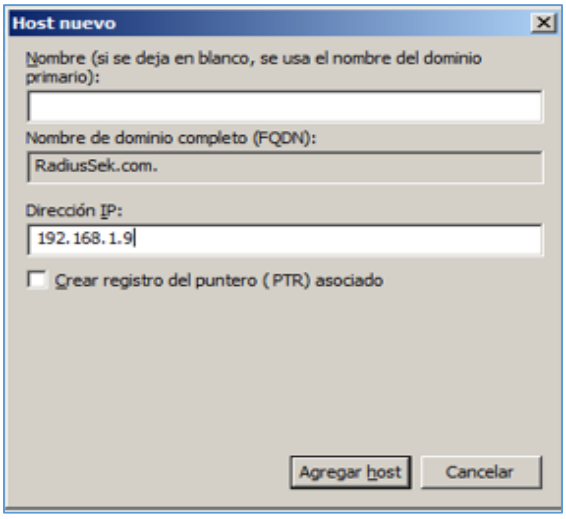
Fuente: (Microsoft)



- En la ventana desplegada ingresar la dirección IP que se asignó previamente (192.168.1.9).

Figura No. 59: Ingreso de IP en el host nuevo

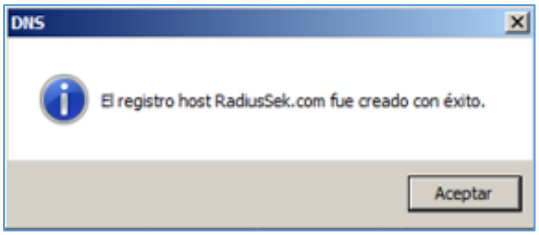
Fuente: (Microsoft)



- Mensaje de confirmación de registro de host ‘radiussek.com’.

Figura No. 60: Registro de host

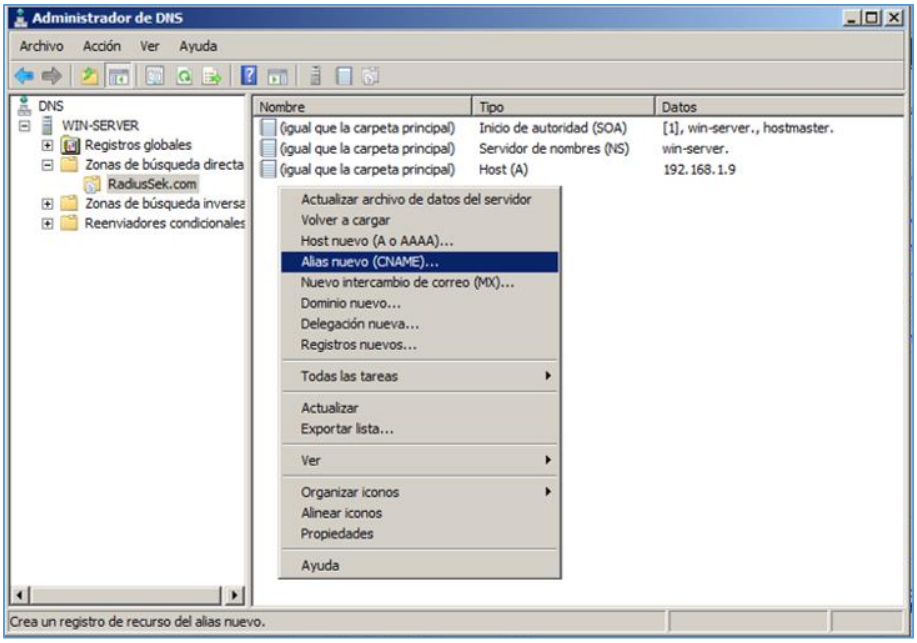
Fuente: (Microsoft)



- En la zona creada se podrá visualizar el registro del nuevo host, donde también se crea un ‘Alias nuevo (CNAME)’.

Figura No. 61: Alias nuevo

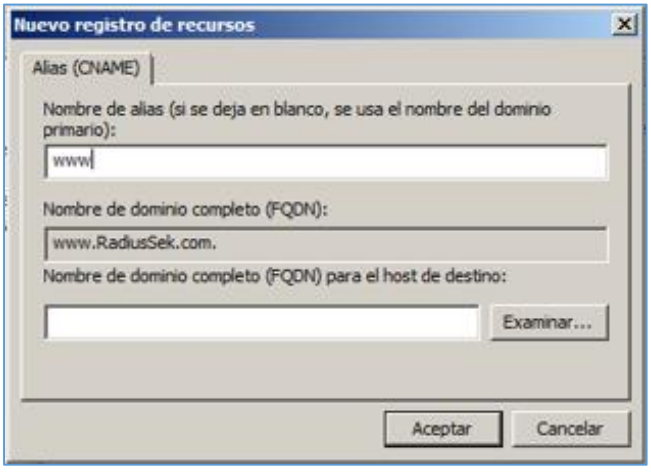
Fuente: (Microsoft)



- Especificar el nombre de alias que para el caso es: ‘www’.

Figura No. 62: Nombre de alias

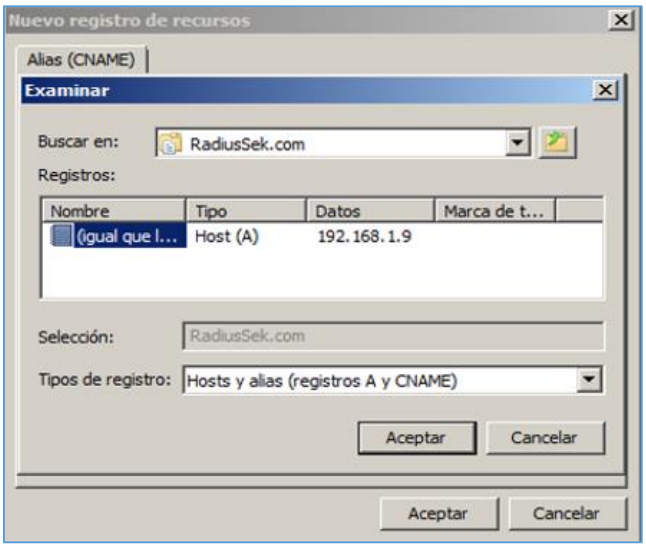
Fuente: (Microsoft)



- En la ventana de registro de nombre de alias, ubicar la opción 'Examinar', y buscar en la zona creada previamente 'radiussek.com' el host con la dirección IP designada y aceptar.

Figura No. 63: Nombre de dominio para host destino

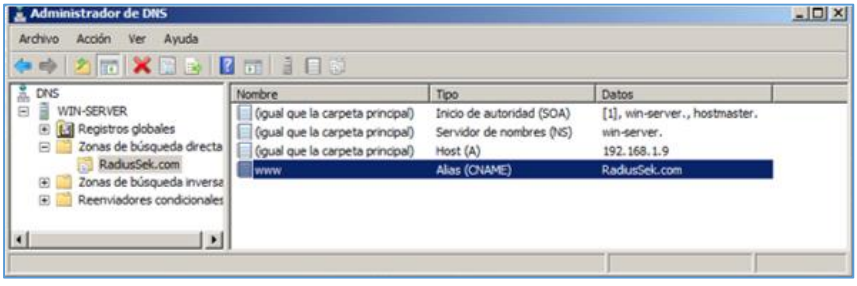
Fuente: (Microsoft)



- Se tendrá para la zona nueva 'radiussek.com', los nuevos registros tanto del host como del alias con sus respectivos datos.

Figura No. 64: Registros de host y alias

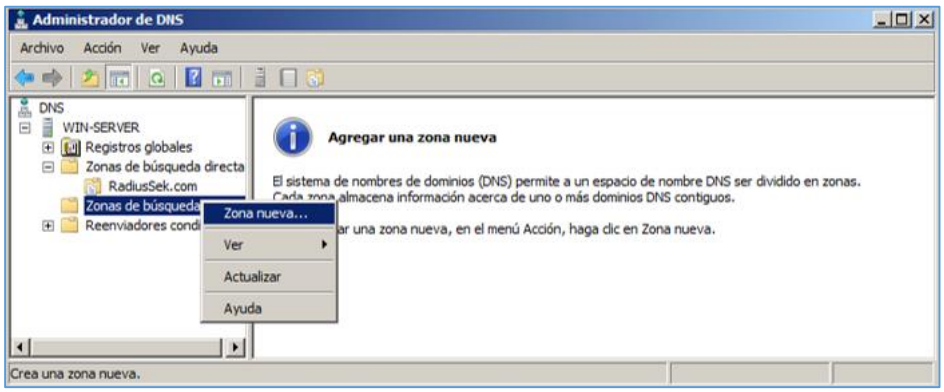
Fuente: (Microsoft)



- En el directorio 'Zona de búsqueda inversa', crear una zona nueva. Un asistente de ayuda se abrirá para el proceso de creación.

Figura No. 65: Creación de nueva zona

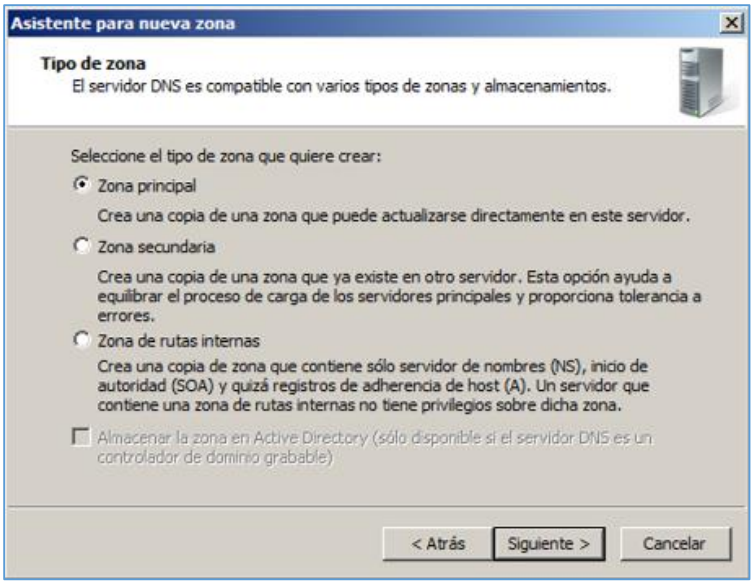
Fuente: (Microsoft)



- Indicar el tipo de zona como: 'Zona principal' para el servidor.

Figura No. 66: Tipo de zona de búsqueda inversa

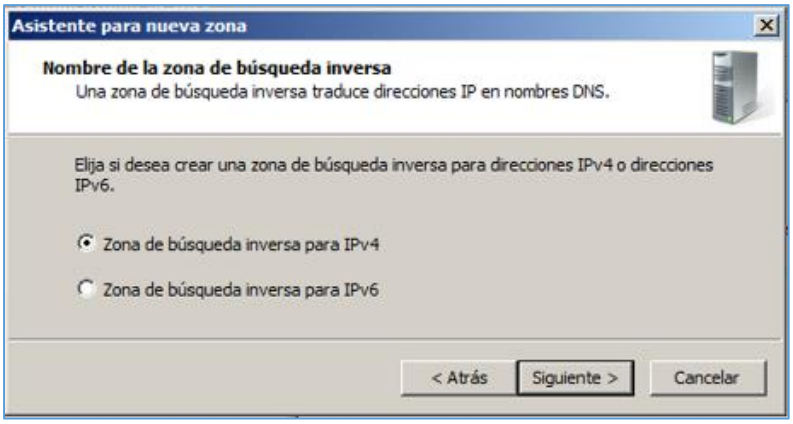
Fuente: (Microsoft)



- Especificar la zona de búsqueda inversa para IPv4 y continuar.

Figura No. 67: Nueva zona para IPv4

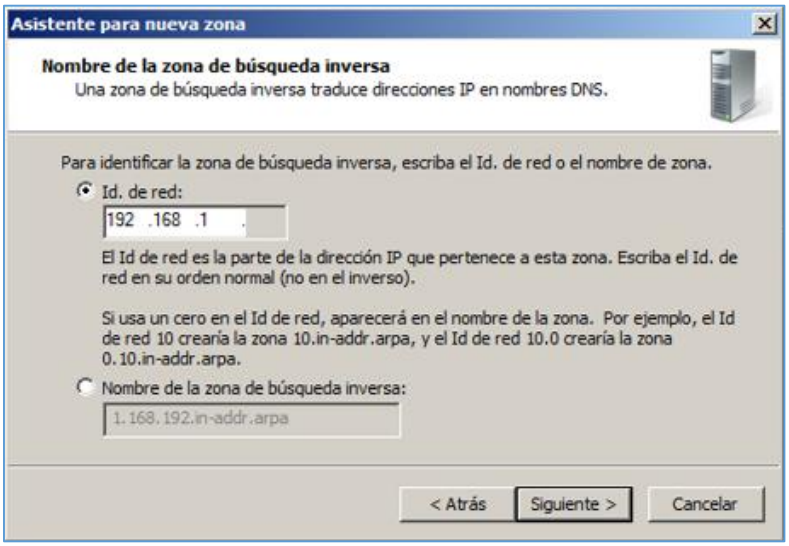
Fuente: (Microsoft)



- Ingresar el Id de red, que en este caso será 192.168.1. que permitirá identificar la zona de búsqueda inversa.

Figura No. 68: Id de red de zona nueva

Fuente: (Microsoft)



- Crear un archivo nuevo de zona, permitir todas las actualizaciones dinámicas, y finalizar el asistente de ayuda, el cual desplegará un resumen del proceso.

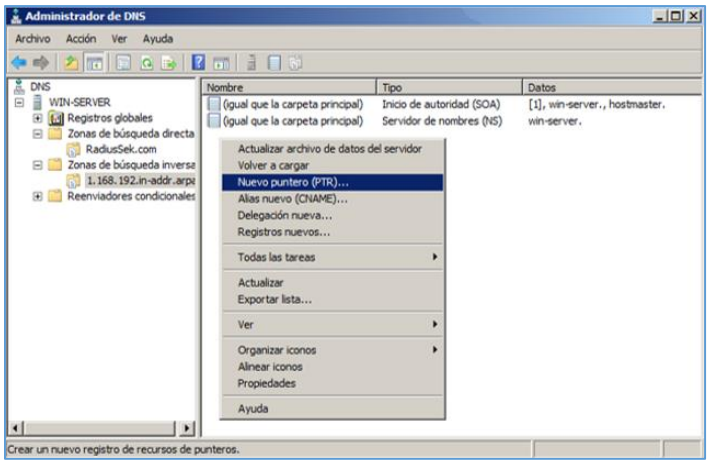
Figura No. 69: Finalización del asistente

Fuente: (Microsoft)

- En el Id de red creado, dar clic derecho para seleccionar la opción 'Nuevo puntero (PTR) para crear el puntero.

Figura No. 70: Nuevo puntero (PTR)

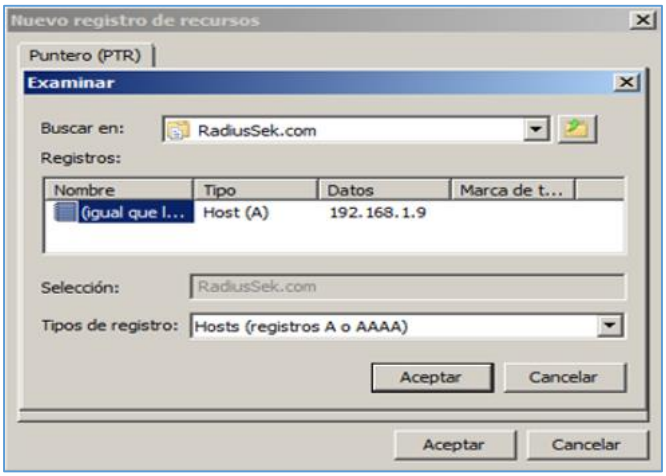
Fuente: (Microsoft)



- En la ventana desplegada buscar en zona de búsqueda directa la zona 'radiussek.com' y seleccionar la opción de host creada previamente y aceptar.

Figura No. 71: Configuración del puntero

Fuente: (Microsoft)



- Al aceptar se abre la ventana del nuevo registro de recursos, en la cual el nuevo puntero tendrá asignados una dirección IP de host, nombre de host.

Figura No. 72: Nuevo registro de recursos

Fuente: (Microsoft)

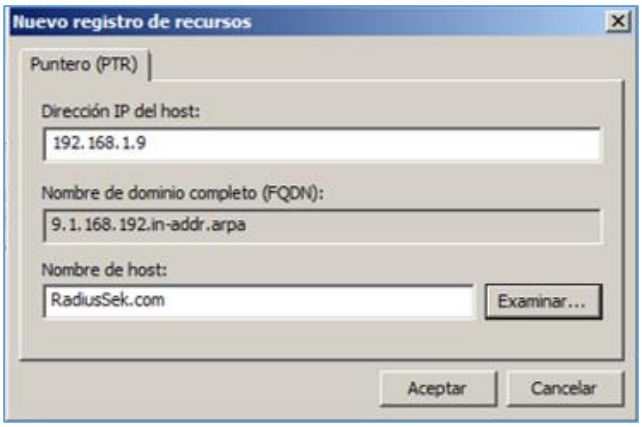
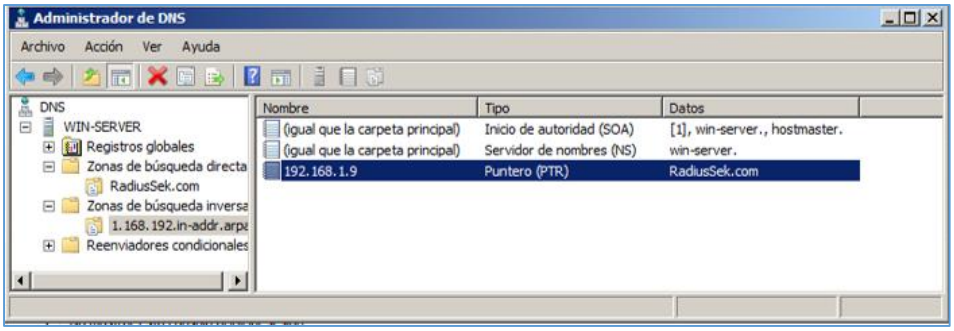


Figura No. 73: Nuevo puntero registrado

Fuente: (Microsoft)



- Configurar las propiedades del protocolo de internet de la máquina física, con una dirección IP estática y en la consola de comandos del servidor realizar una comprobación de conexión mediante el comando ‘ping’.

Figura No. 74: Configuración IP de la máquina física

Fuente: El autor

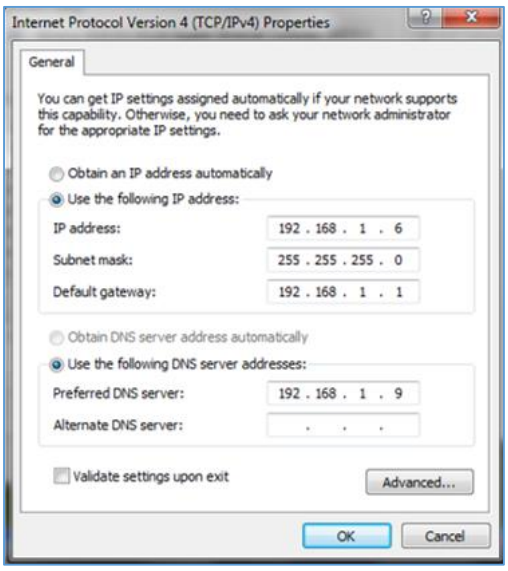
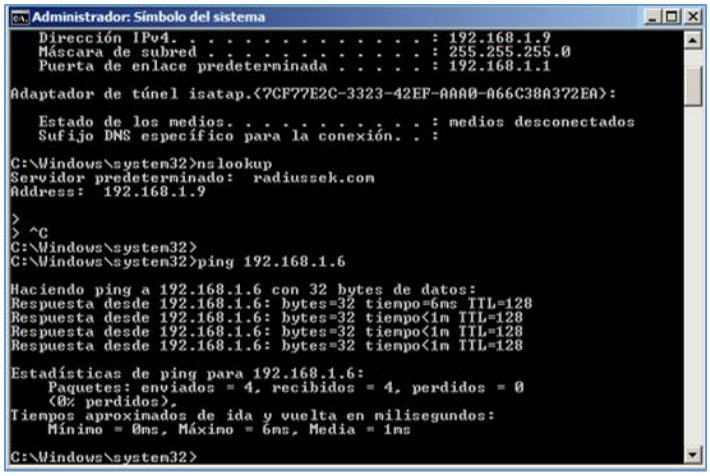


Figura No. 75: Comprobación de conexión

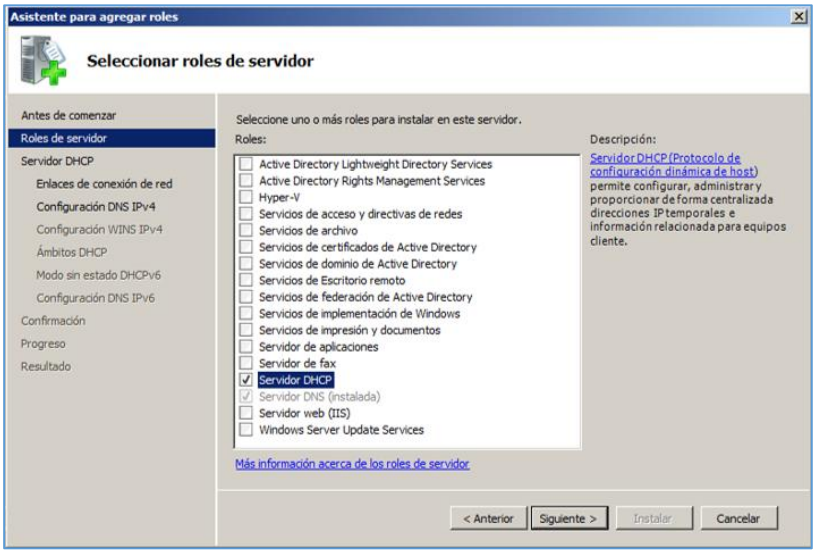
Fuente: El autor



- Abrir el asistente para agregar el nuevo rol: 'Servidor DHCP', para que los terminales en la red puedan obtener una dirección IP dinámica designada por el servidor y continuar.

Figura No. 76: Rol de Servidor DHCP

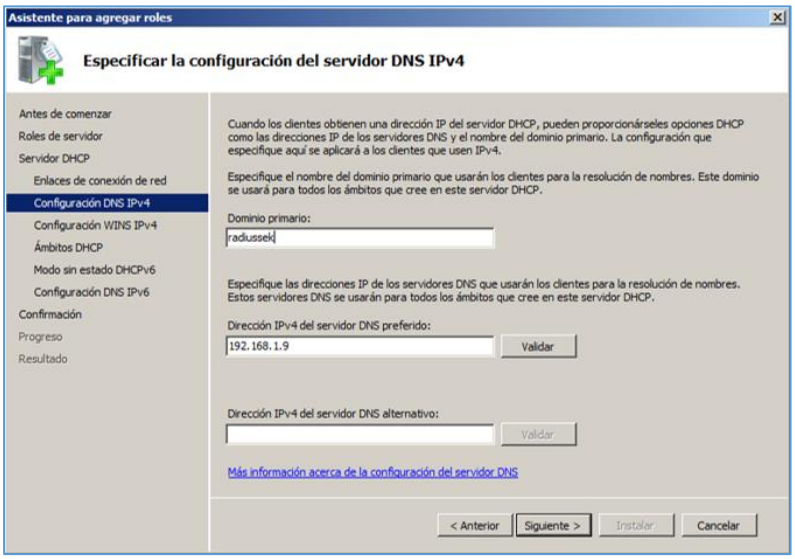
Fuente: (Microsoft)



- En el proceso de instalación, seleccionar la conexión de red (192.168.1.9), especificar la configuración del servidor DNS IPv4 ingresando el dominio primario: radiussek, dirección IPv4 del servidor DNS: 192.168.1.9.

Figura No. 77: Especificaciones de configuración para servidor DHCP

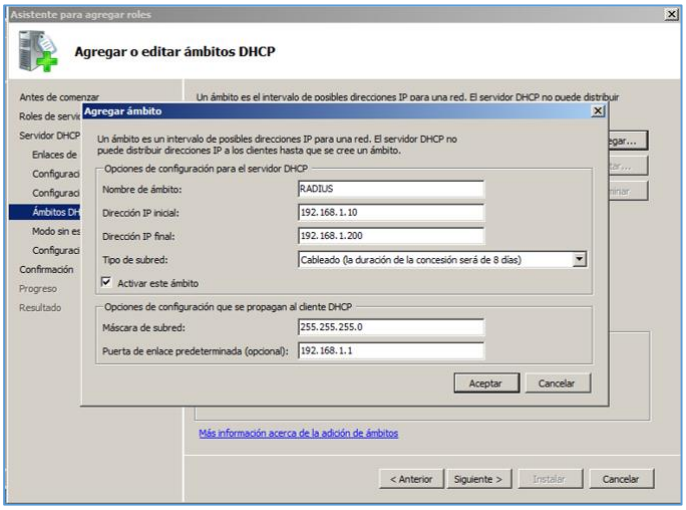
Fuente: (Microsoft)



- En la configuración de las especificaciones, indicar que no se requiere WINS para aplicaciones de la red y continuar. En la siguiente ventana agregar el nuevo ámbito ingresando los datos correspondientes como: nombre del ámbito, rango de direcciones IP, máscara de subred, puerta de enlace y aceptar.

Figura No. 78: Especificación de datos para nuevo ámbito

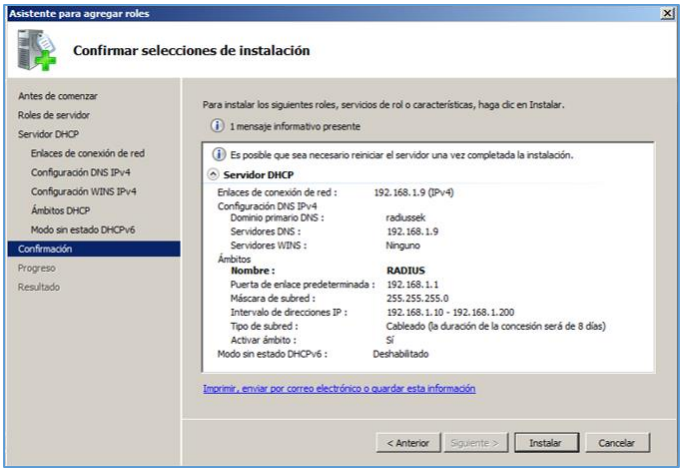
Fuente: (Microsoft)



- Al continuar, deshabilitar el modo ‘sin estado DHCPv6’ para el servidor. En el próximo cuadro de configuración marcar la opción ‘uso de credenciales actuales’ y finalizar la instalación.

Figura No. 79: Resumen informativo del rol instalado

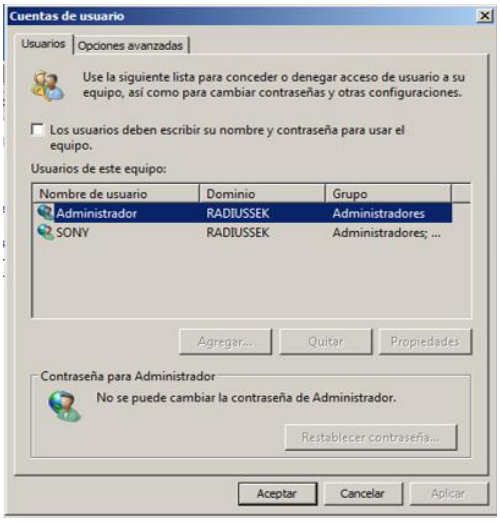
Fuente: (Microsoft)



- Ingresando al 'Panel de control' en la opción 'Cuentas de usuario' se verifica que los usuarios ya pertenecen al dominio creado previamente en el servidor.

Figura No. 80: Cuentas de usuario del servidor

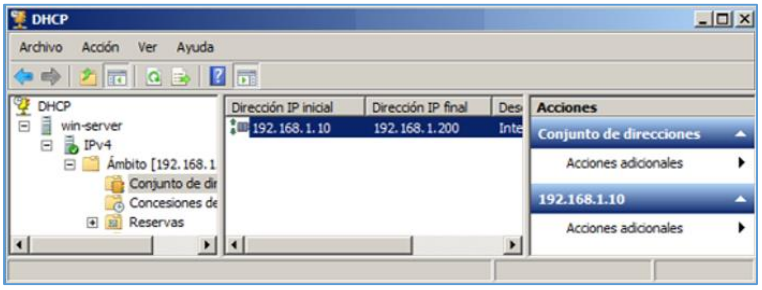
Fuente: (Microsoft)



- Abrir el servidor DHCP y verificar el ámbito configurado anteriormente.

Figura No. 81: Servidor DHCP

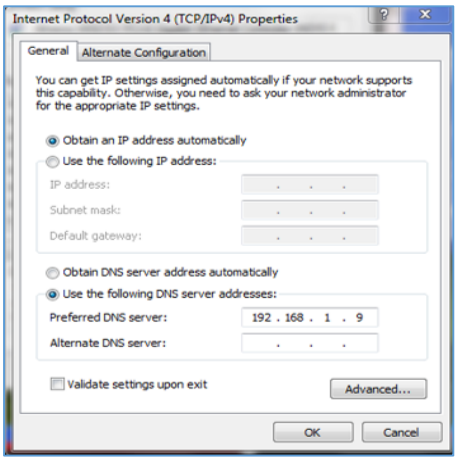
Fuente: (Microsoft)



- En la máquina física (ordenador) configurar las propiedades TCP/IP, asignando una dirección IP dinámica que será otorgado por el servidor DHCP; también indicar la dirección IP del servidor DNS (192.168.1.9).

Figura No. 82: Configuración IP de la maquina física

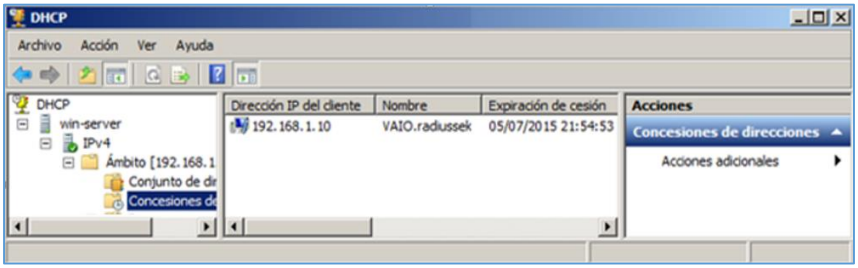
Fuente: El autor



- Ingresar nuevamente al servidor DHCP, donde se confirmará la asignación dinámica de direcciones IP del ámbito creado a un equipo terminal. El primer equipo con una dirección IP dinámica designada por DHCP es el equipo físico.

Figura No. 83: Concesión de dirección IP por DHCP

Fuente: (Microsoft)



- Ingresar a la consola de comandos del servidor alojado en la máquina virtual y realizar una comprobación del estado de conexión con el equipo físico (192.168.1.10) designado por DHCP. Después realizar el mismo procedimiento desde el equipo terminal físico hacia el servidor.

Figura No. 84: Estado de conexión desde servidor a equipo terminal

Fuente: (Microsoft)

- Comprobar si los servicios de dominio de 'Active Directory' están instalados y abrir el asistente de instalación.

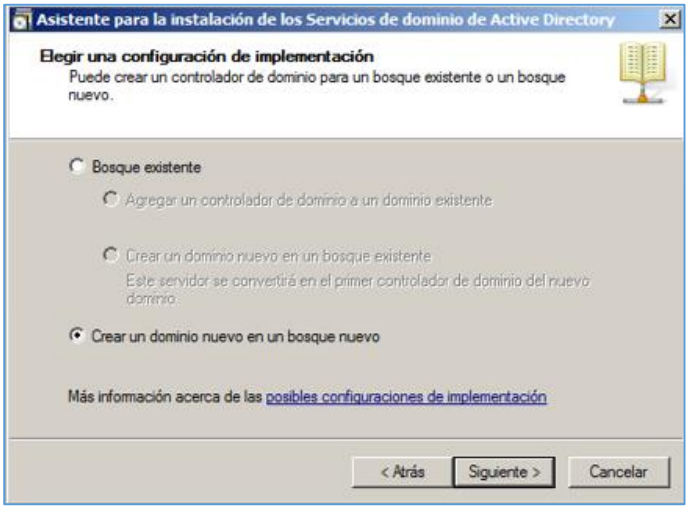
Figura No. 85: Asistente de instalación de servicios de dominio de AD

Fuente: (Microsoft)

- Seleccionar la opción de 'creación de un dominio nuevo en un bosque nuevo' y continuar.

Figura No. 86: Configuración de implementación

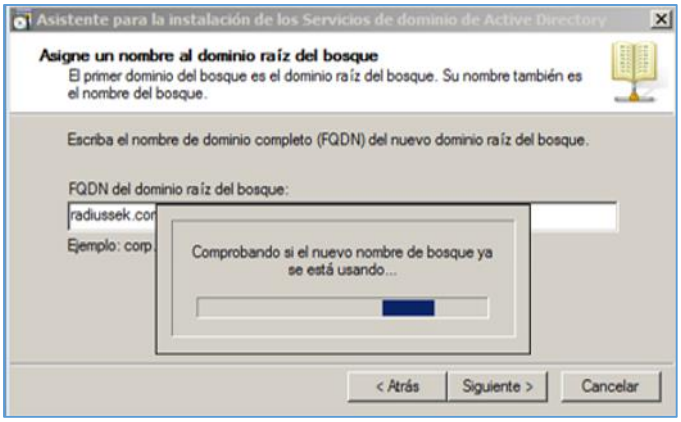
Fuente: (Microsoft)



- Se asignará un nombre al dominio raíz del bosque y se comprobará su utilización.

Figura No. 87: Asignación de nombre al dominio raíz del bosque

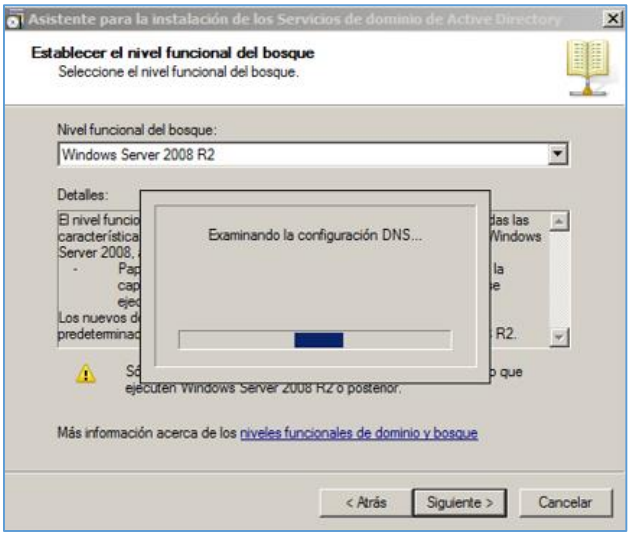
Fuente: (Microsoft)



- Establecer el nivel funcional del bosque seleccionando la opción 'Windows Server 2008 R2' y continuar.

Figura No. 88: Nivel funcional del bosque

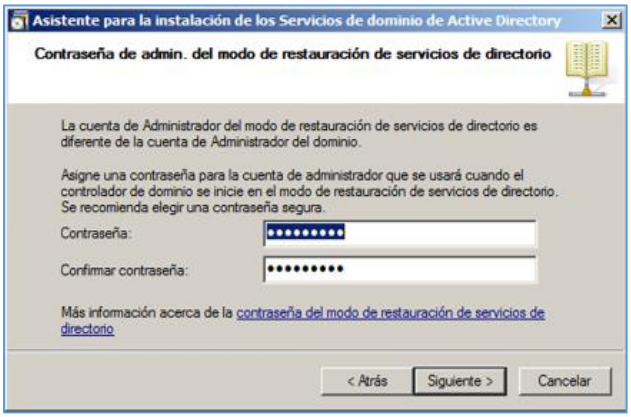
Fuente: (Microsoft)



- Verificar opciones adicionales del controlador de dominio, se mostrará la base de datos y archivo de registros de manera independiente y continuar. Después se ingresará la contraseña de administrador para el 'modo de restauración de servicios de directorio'.

Figura No. 89: Ingreso de contraseña

Fuente: (Microsoft)



- Al finalizar la instalación se presentará un cuadro de resumen de configuraciones y el asistente terminará el proceso.

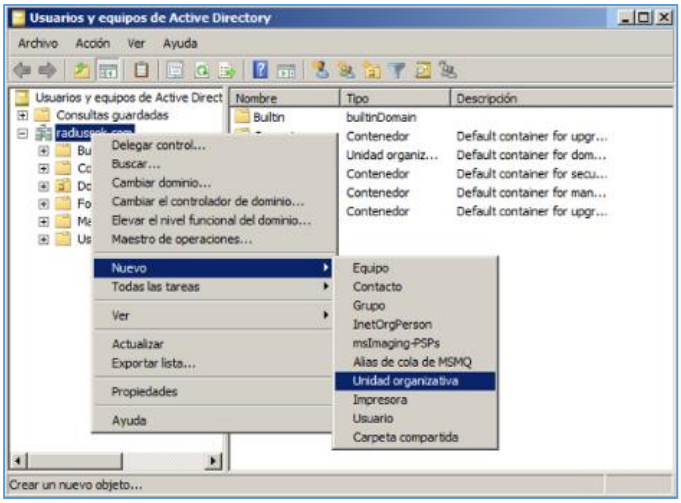
Figura No. 90: Finalización del asistente de instalación de AD

Fuente: (Microsoft)

- Ingresar a usuarios y equipos de Active Directory para iniciar el proceso de creación de usuarios y sus correspondientes configuraciones. En el dominio raíz de bosque creado (radiussek.com) dar clic derecho para crear una nueva 'Unidad organizativa' de prueba; que contendrá otros objetos sean equipos o usuarios.

Figura No. 91: Creación de Unidad organizativa en AD

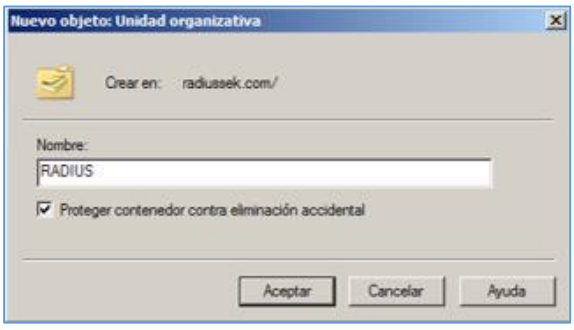
Fuente: (Microsoft)



- El nuevo objeto a crearse será una unidad organizativa de nombre: 'RADIUS'.

Figura No. 92: Unidad organizativa

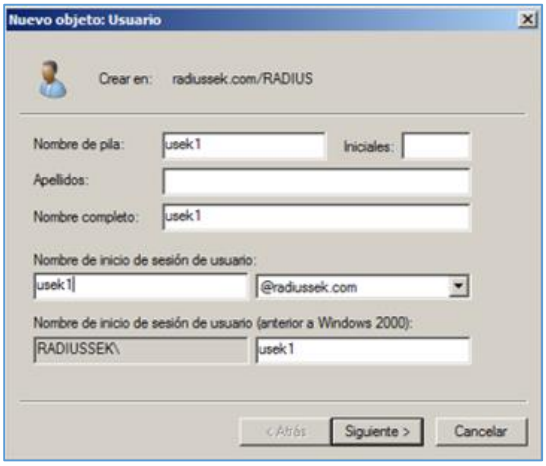
Fuente: (Microsoft)



- En la nueva unidad crear un nuevo usuario de prueba cuyo nombre será 'usek1' tanto para nombre completo como para nombre de inicio de sesión.

Figura No. 93 Creación de usuario dentro de la unidad

Fuente: (Microsoft)



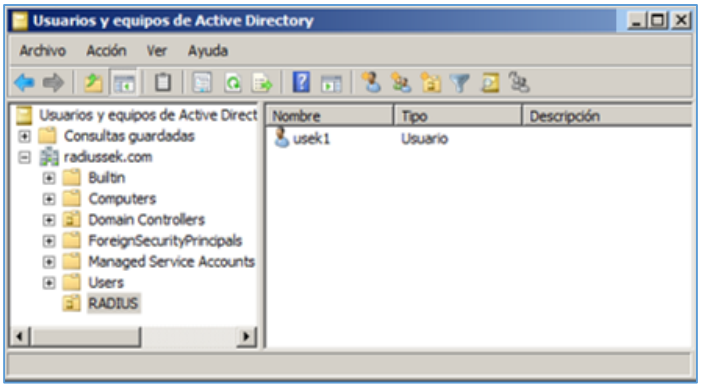
- Asignar una contraseña para el usuario creado, adicionalmente hay opciones de manejo de cuenta que dependerá de las políticas que establezca un administrador y continuar.

Figura No. 94: Asignación de contraseña del usuario

Fuente: (Microsoft)

Figura No. 95: Usuario creado en la unidad RADIUS en AD

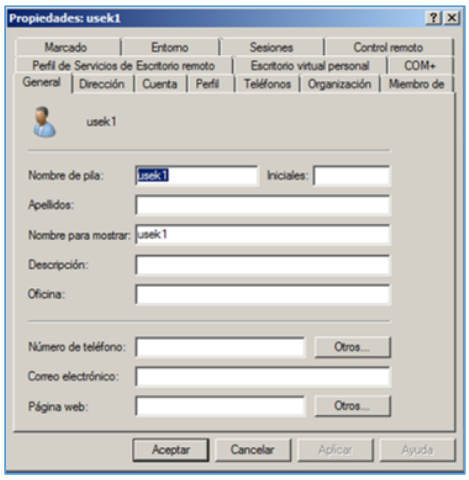
Fuente: (Microsoft)



- También se puede verificar las propiedades del usuario creado y se requiere cambiar ciertos parámetros en específico.

Figura No. 96: Propiedades del usuario creado

Fuente: (Microsoft)

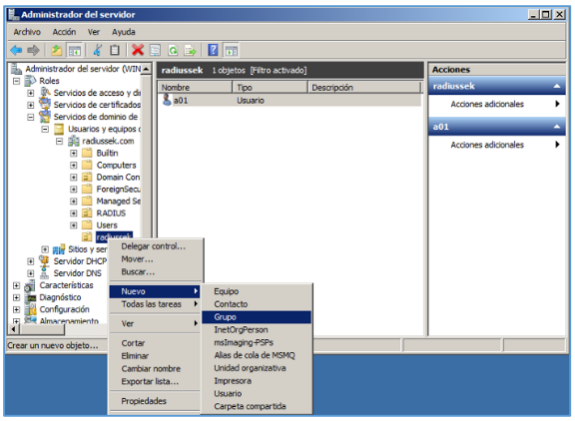


- Para el proceso de autenticación se crea nuevamente otra unidad organizativa ‘radiussek’ con un nuevo usuario ‘a01’. En la nueva unidad se deberá crear un

nuevo objeto de 'Grupo' que permita incluir tanto equipos como usuarios registrados en AD.

Figura No. 97: Creación de Grupo

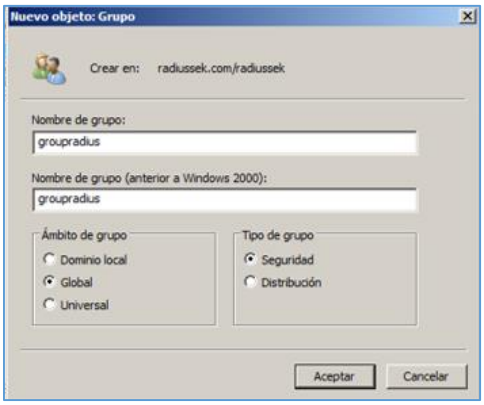
Fuente: (Microsoft)



- Proporcionar el nombre 'groupradius' al nuevo grupo correspondiente a la unidad organizativa 'radiussek'.

Figura No. 98: Nuevo grupo creado

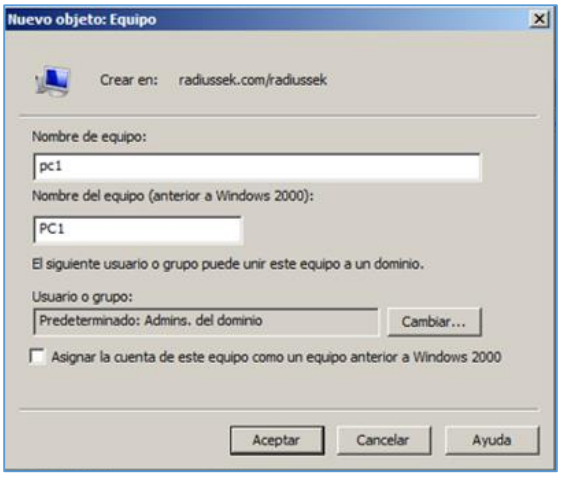
Fuente: (Microsoft)



- De igual manera crear un equipo en la unidad organizativa 'radiussek' cuyo nombre será 'pc1' que se incluirá en el grupo creado previamente.

Figura No. 99: Nuevo equipo creado

Fuente: (Microsoft)



- Para continuar ingresar a las propiedades del nuevo grupo creado seleccionando la pestaña de 'Miembros', dentro del cual se ingresara el nombre del usuario que fue credo anteriormente en la unidad organizativa, comprobar el nombre y elegir la opción del recuadro 'Tipos de objeto'.

Figura No.100: Configuración de propiedades de grupo

Fuente: (Microsoft)

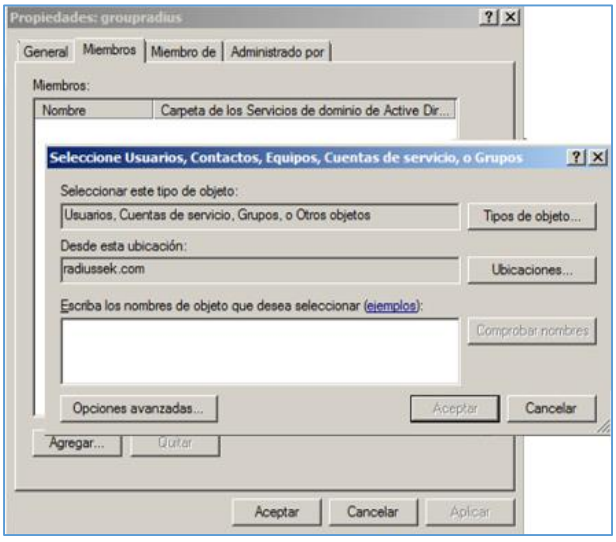
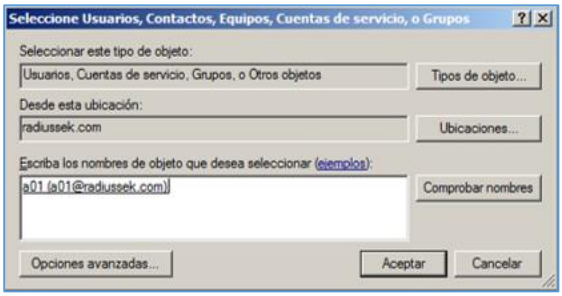


Figura No. 101: Ingreso de nombre de objeto

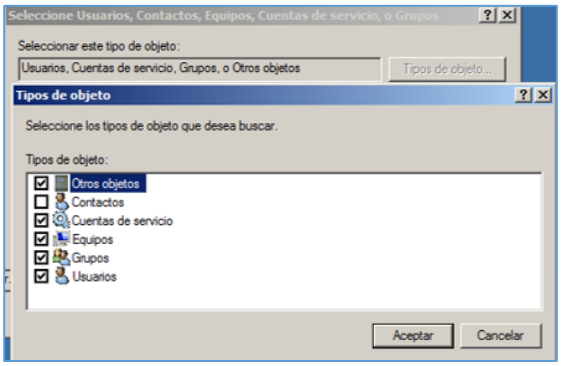
Fuente: (Microsoft)



- En la ventana desplegada de tipos de objeto, marcar el recuadro 'Equipos' y aceptar para volver a la ventana anterior.

Figura No. 102: Tipos de objeto

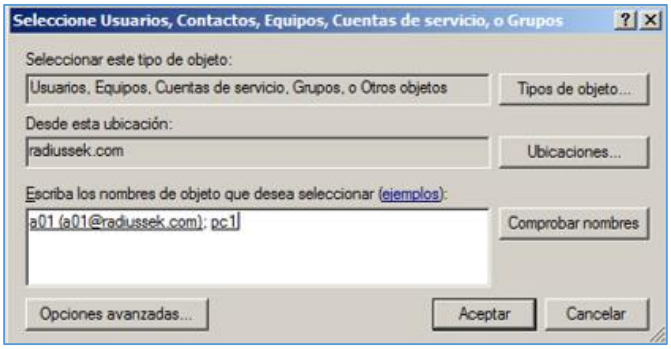
Fuente: (Microsoft)



- En la ventana de selección de objetos a incluir en el grupo, añadir el nombre del equipo creado junto al usuario y comprobar nuevamente los nombres, y continuar. Este proceso de configuración permitirá asignar un modo de conexión de un usuario determinado mediante su vinculación con un equipo para una autenticación en una arquitectura de seguridad de red inalámbrica.

Figura No. 103: Configuración de objetos del grupo 'groupradius'

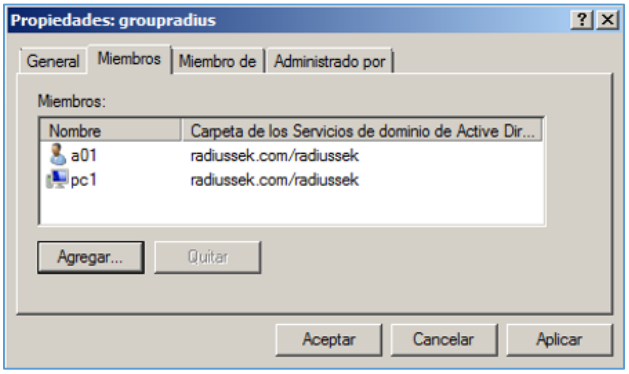
Fuente: (Microsoft)



- Al finalizar el proceso se visualizarán ambos objetos usuario y equipo como miembros del grupo 'groupradius'.

Figura No. 104: Miembros agregados al grupo

Fuente: (Microsoft)



- Ingresar al asistente del servidor para agregar nuevos roles. Instalar los roles: 'Servicios de certificado y dominio de Active Directory', y 'Servidor web (IIS)' hasta obtener los resultados de la instalación. De igual forma instalar el rol 'Servicios de acceso y directivas de redes', donde se marcará la opción 'servidor de directivas de redes' y continuar.

Figura No. 105: Instalación de roles en el servidor

Fuente: (Microsoft)

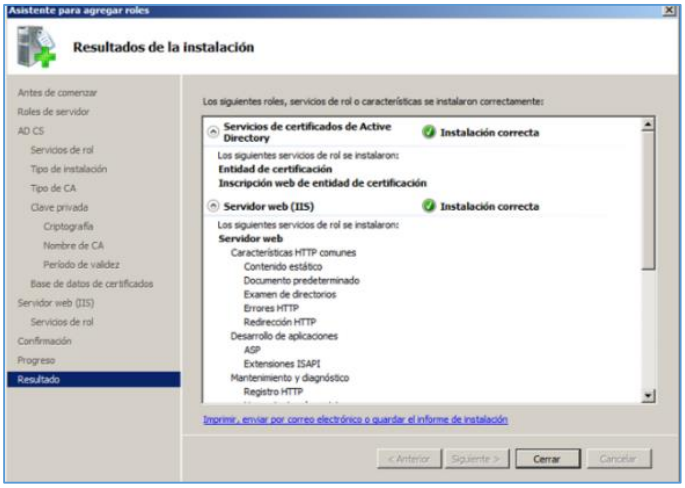
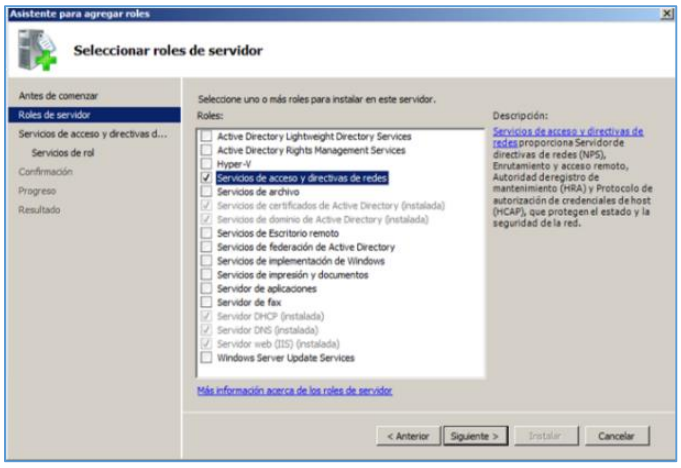


Figura No. 106: Instalación de roles adicionales en el servidor

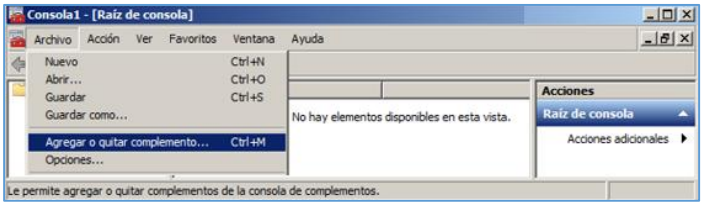
Fuente: (Microsoft)



- Finalizados los procesos de instalación de nuevos roles en el servidor, ir a inicio y escoger la opción ‘Ejecutar’ para abrir la consola raíz. Se iniciará la instalación de certificados para procesos de autenticación. En la consola raíz, ir a la pestaña de ‘Archivo’ y elegir ‘Agregar o quitar complemento’.

Figura No. 107: Consola raíz del sistema en el servidor RADIUS

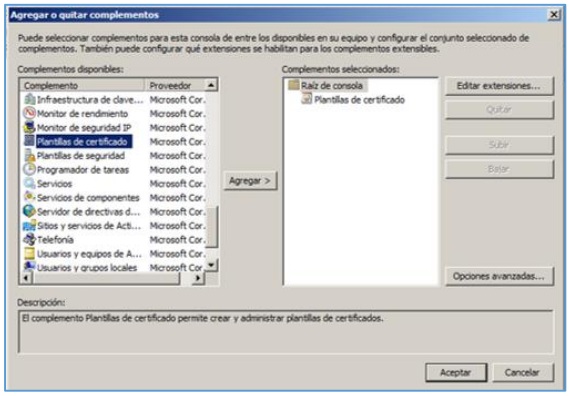
Fuente: (Microsoft)



- Ubicar el complemento 'Plantillas de certificado' y agregarlo.

Figura No. 108: Plantillas de certificado

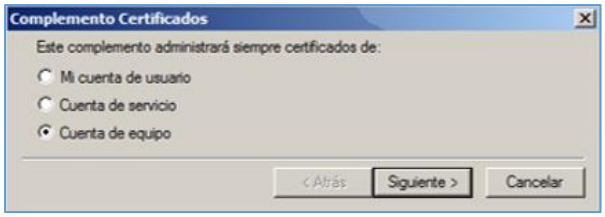
Fuente: (Microsoft)



- Cuando se agrega el complemento en mención, se configura adicionalmente que tipo de certificados de cuenta administrará. Para ello se escoge la opción 'Cuenta de equipo'.

Figura No. 109: Configuración de complemento de certificados

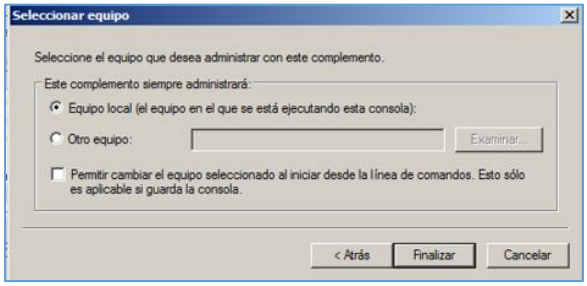
Fuente: (Microsoft)



- De igual manera se configura el equipo que administrará el complemento agregado, y escoger la opción de 'Equipo local'.

Figura No. 110: Configuración de selección de equipo

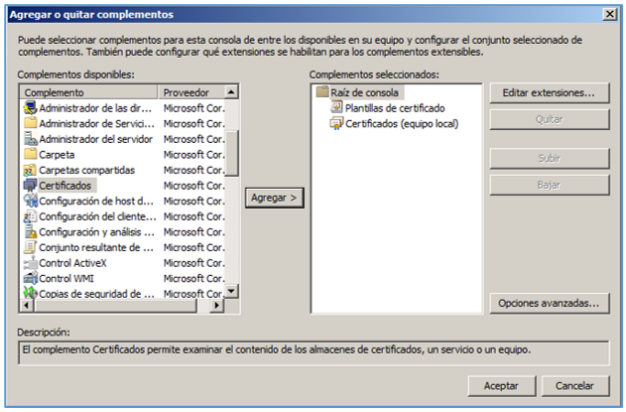
Fuente: (Microsoft)



- Para continuar, ubicar el complemento 'Certificados' para ser agregado a la lista de complementos requeridos.

Figura No. 111: Certificados

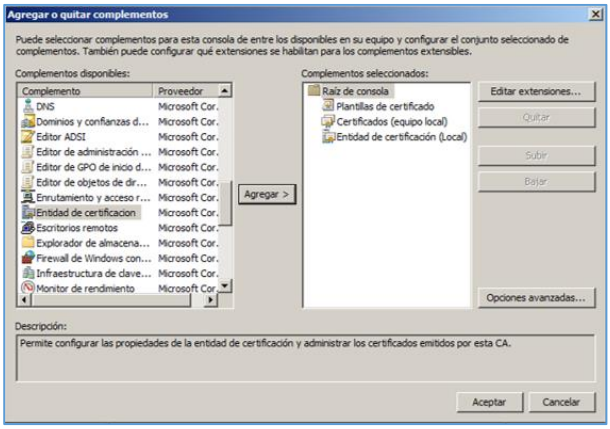
Fuente: (Microsoft)



- También agregar el complemento 'Entidad de certificación' e indicar que la administración será en el equipo local.

Figura No. 112: Entidad de certificación

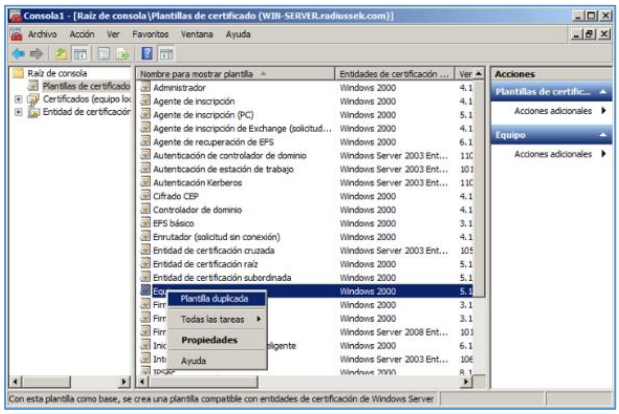
Fuente: (Microsoft)



- En la 'Raíz de consola' se habrán cargado los 3 complementos agregados anteriormente. Ubicar el complemento 'Plantillas de certificado' para abrir un listado de nombres de plantilla. Seleccionar la opción 'Equipo', dar clic derecho para escoger 'Plantilla duplicada'.

Figura No. 113: Selección de plantilla

Fuente: (Microsoft)



- En la ventana que se muestra escoger la opción 'Windows Server 2008 Enterprise'.

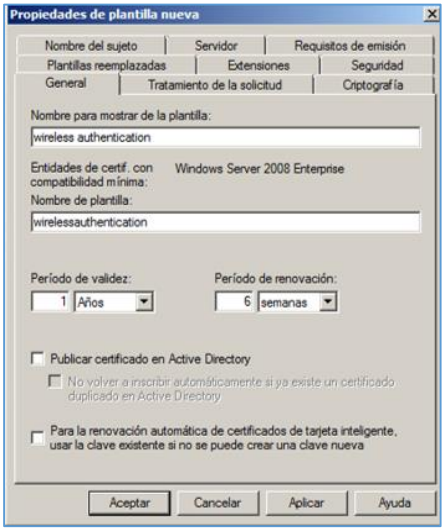
Figura No. 114: Plantilla duplicada

Fuente: (Microsoft)

- Nuevamente ingresar en la plantilla 'Equipo' y dar clic derecho para abrir las propiedades de la misma. En la pestaña 'General', dar un nuevo nombre a la plantilla como 'wireless authentication' e indicar el periodo de validez y renovación.

Figura No. 115: Propiedades de plantilla nueva

Fuente: (Microsoft)

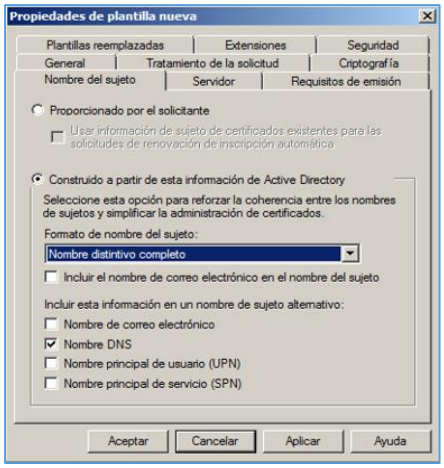


- En la misma ventana de propiedades, ubicar la pestaña 'Nombre del sujeto'. En dicha pestaña seleccionar como formato de nombre de sujeto la alternativa de

'Nombre distintivo completo'. Marcar como nombre de sujeto alternativo la opción 'Nombre DNS'.

Figura No. 116: Nombre del sujeto

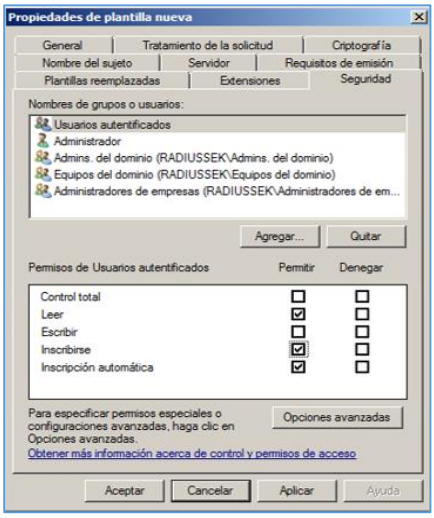
Fuente: (Microsoft)



- Elegir la pestaña 'Seguridad', ubicar 'Usuarios autentificados' y otorgar permisos de lectura, inscripción, e inscripción automática.

Figura No. 117: Seguridad para usuarios autentificados

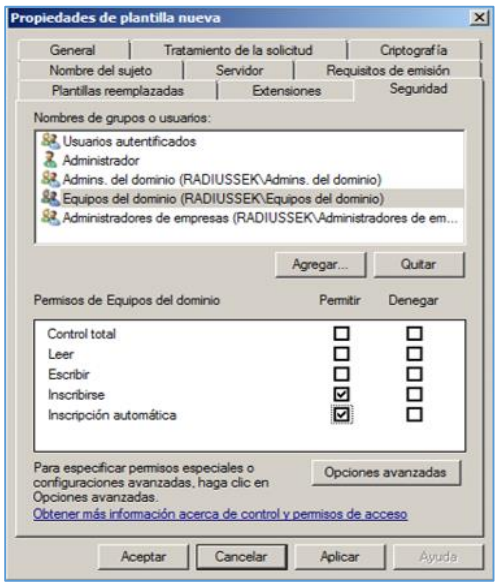
Fuente: (Microsoft)



- Continuando en la misma pestaña de seguridad, ubicar ‘Equipos del dominio’ y dar permisos de inscripción e inscripción automática. Aplicar y aceptar.

Figura No. 118: Seguridad para equipos del dominio

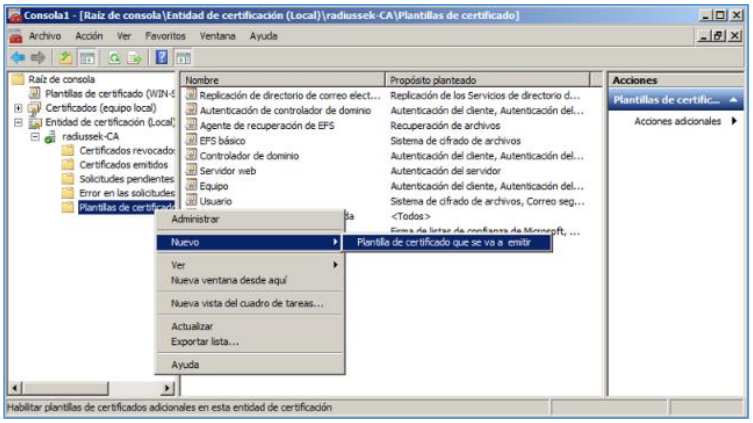
Fuente: (Microsoft)



- En la consola raíz ubicar el complemento de entidad de certificación, al ingresar se tiene la autoridad certificadora creada previamente como ‘radiussek-CA’. Dentro de la CA escoger ‘Plantillas de certificado’ y dar clic derecho en la opción ‘Nuevo’ para crear una nueva plantilla de certificado que será emitido.

Figura No. 119: Configuración de nueva plantilla

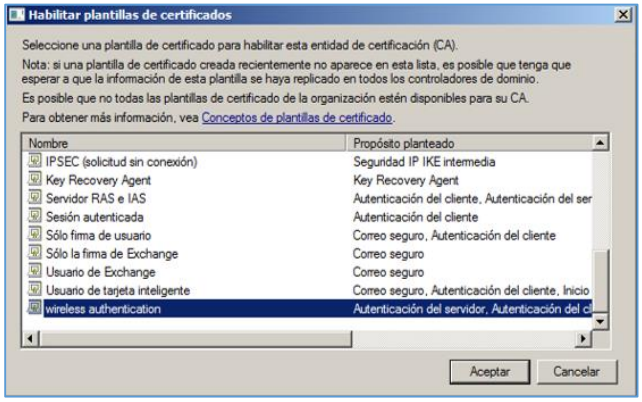
Fuente: (Microsoft)



- En la ventana siguiente seleccionar la plantilla de certificado que habilita la entidad de certificación CA. En este caso será la opción 'wireless authentication' configurado previamente, y continuar.

Figura No. 120: Selección de plantilla de certificado

Fuente: (Microsoft)

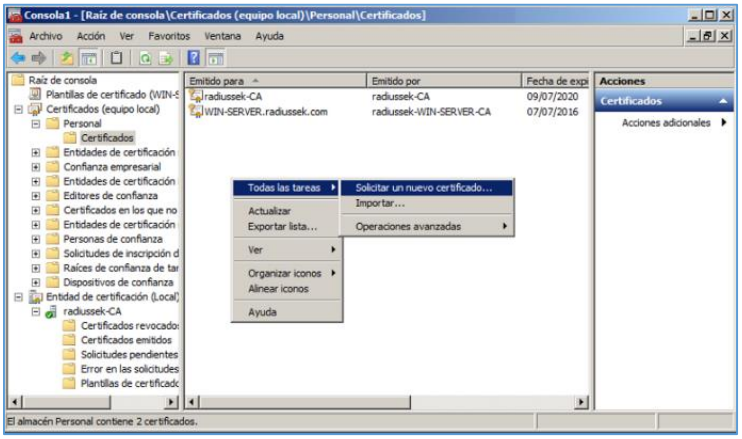


- Ubicar el complemento de certificados, acceder al directorio 'Personal' en la opción de 'Certificados'. Al abrirse el contenido en la ventana se visualizarán

los certificados ya configurados. Dar clic derecho, escoger 'Todas las tareas' y solicitar un nuevo certificado.

Figura No. 121: Solicitud de certificado nuevo

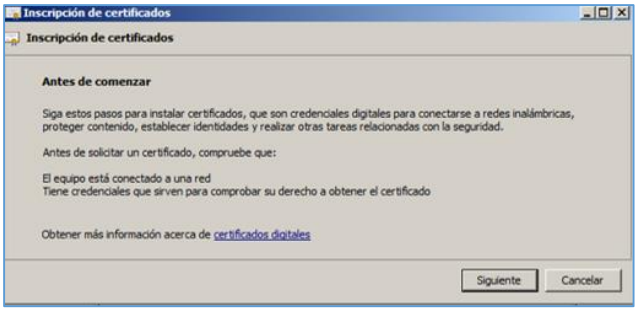
Fuente: (Microsoft)



- Se abrirá una ventana de inscripción de certificados y continuar.

Figura No. 122: Inscripción de certificados

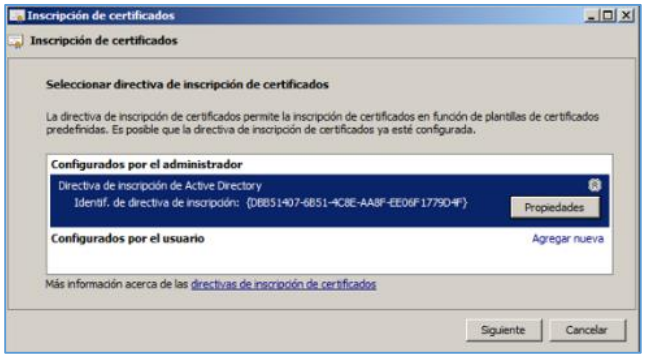
Fuente: (Microsoft)



- Escoger la directiva de inscripción de certificados, que para el caso serán los 'configurados por el administrador' y continuar.

Figura No. 123: Selección de directiva de inscripción de certificación

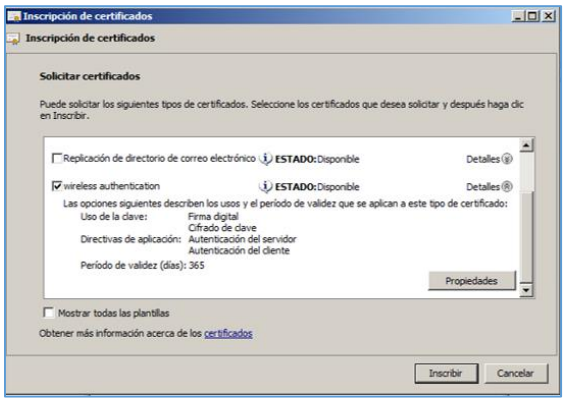
Fuente: (Microsoft)



- En la siguiente ventana en 'Directiva de inscripción de Active Directory' marcar el tipo de certificado 'wireless authentication' e ingresar a sus propiedades.

Figura No. 124: Solicitud de certificados

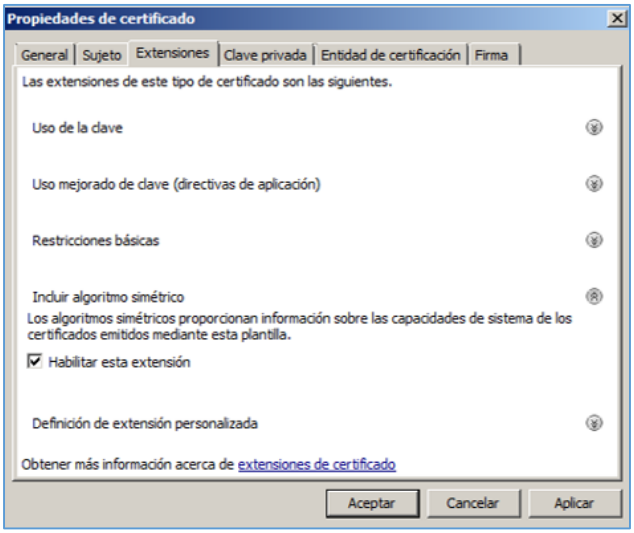
Fuente: (Microsoft)



- Las propiedades de certificado desplegados muestran varias pestañas de configuración, para lo cual se deberá seleccionar la pestaña 'Extensiones'. En ella marcar la opción 'Habilitar esta extensión' correspondiente al campo 'Incluir algoritmo simétrico'. Aplicar, aceptar e inscribir.

Figura No. 125: Propiedades de certificado elegido

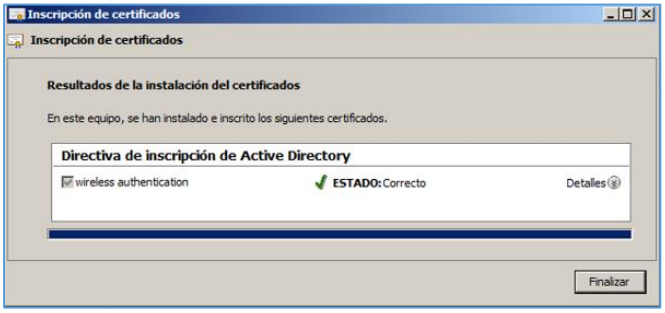
Fuente: (Microsoft)



- En la ventana siguiente se presentarán los resultados de instalación del tipo de certificado elegido.

Figura No. 126: Resultados de instalación de certificado

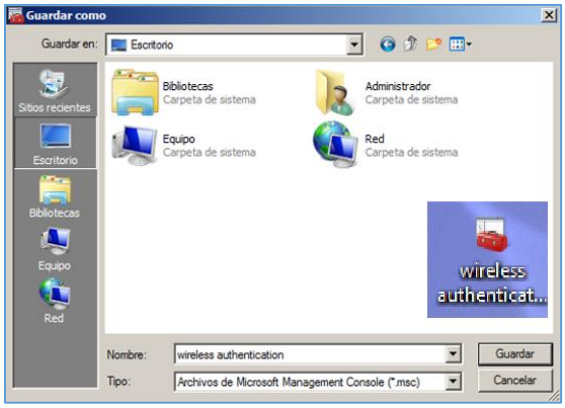
Fuente: (Microsoft)



- Guardar la configuración efectuada en el servidor.

Figura No. 127: Configuración almacenada en el servidor

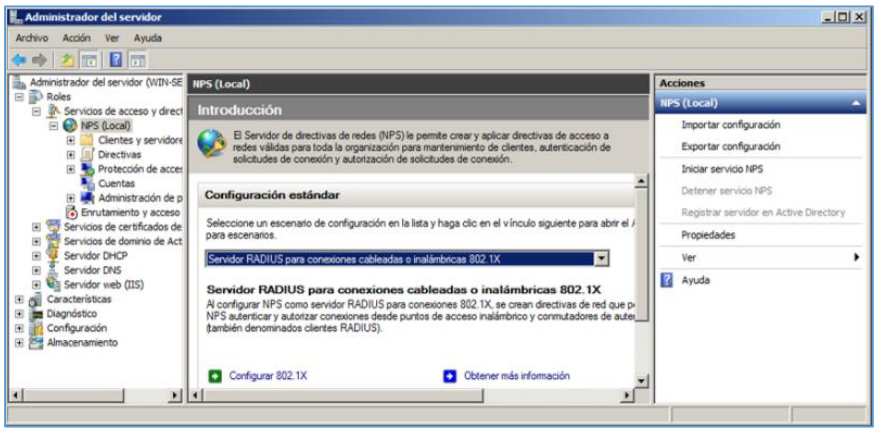
Fuente: (Microsoft)



- A partir de las anteriores configuraciones, abrir el administrador del servidor, acceder 'Roles' e ingresar a la opción NPS local (Network Policy Server) correspondiente a los servicios de acceso y directivas de redes instalado. En la ventana desplegada de NPS en 'Configuración estándar', seleccionar el escenario de configuración 'servidor RADIUS para conexiones cableadas o inalámbricas 802.1X'. Esto permitirá realizar una autenticación, autorización de solicitudes de conexión.

Figura No. 128: Configuración NPS (local)

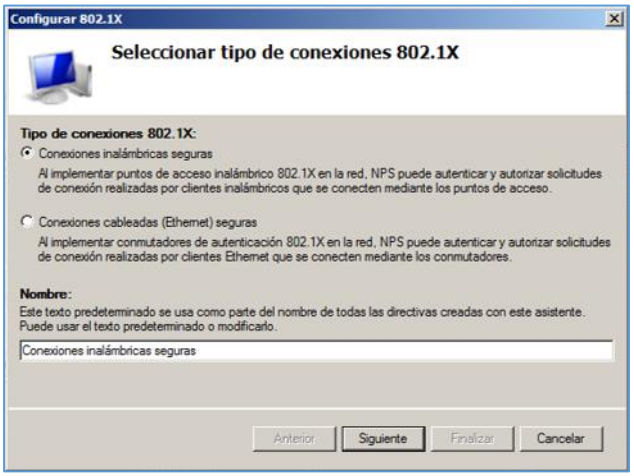
Fuente: (Microsoft)



- Dar clic en 'Configurar 802.1X', el cual despliega una ventana para seleccionar un tipo de conexión, en este caso será 'Conexiones inalámbricas seguras' y creará una conexión inalámbrica segura. La nueva conexión facultará un medio de comunicación estableciendo un canal de conexión. Como la nueva arquitectura de seguridad se enfoca en la red inalámbrica el tipo de conexión será el respectivo.

Figura No. 129: Selección del tipo de conexión 802.1X

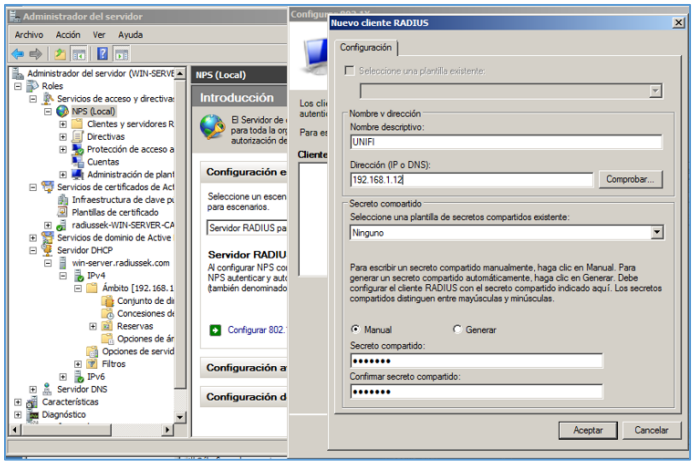
Fuente: (Microsoft)



- A continuación en la ventana desplegada se tendrá que especificar los conmutadores que serán agregados mediante la opción 'Agregar'. Ingresar los datos correspondientes para el nuevo cliente RADIUS como nombre, dirección IP (192.168.1.12) del punto de acceso (antena) de la red designado por el servidor DHCP e indicar una contraseña para el secreto compartido. Dicha contraseña compartida deberá ser la misma que posee el punto de acceso, permitiendo una comunicación entre el servidor RADIUS con el nuevo cliente.

Figura No. 130: Registro de datos del nuevo cliente RADIUS

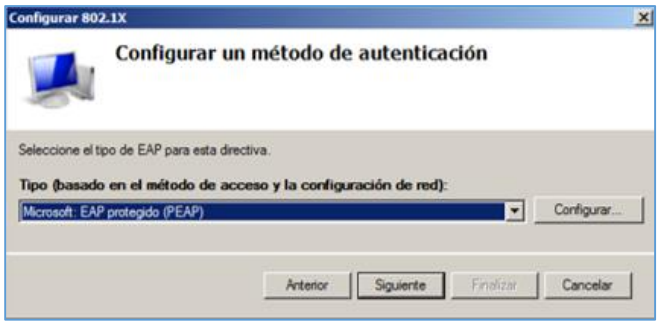
Fuente: (Microsoft)



- Configurar un método de autenticación, que para este caso es 'PEAP' que es un protocolo de autenticación protegida extendida.

Figura No. 131: Método de autenticación

Fuente: (Microsoft)

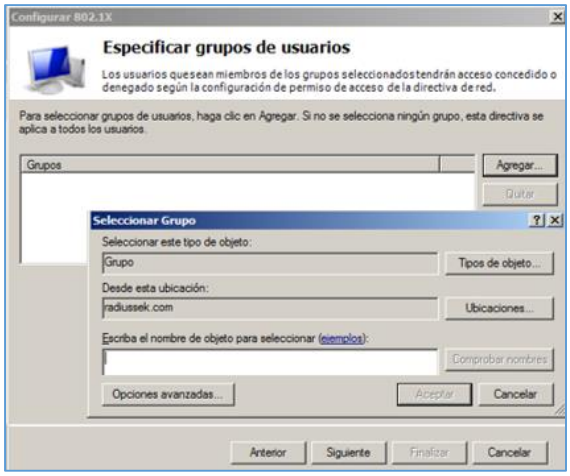


- Agregar en grupos de usuarios un nuevo grupo, el cual hará referencia al grupo creado para la unidad organizativa 'groupradius' de AD; donde todos los usuarios pertenecientes a dicho grupo tendrán la posibilidad de autenticarse e

ingresar a la red inalámbrica. Ir a opciones avanzadas en la ventana de selección de grupo.

Figura No. 132: Agregar grupo

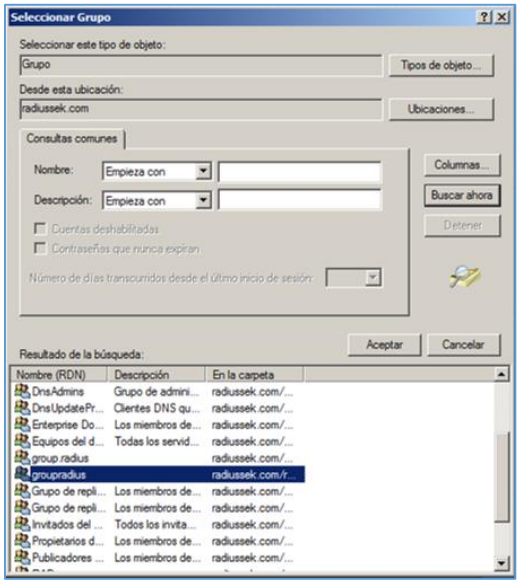
Fuente: (Microsoft)



- En la ventana seleccionar la opción 'Buscar ahora' y señalar el grupo 'groupradius' creado en AD y aceptar.

Figura No. 133: Selección de grupo de AD

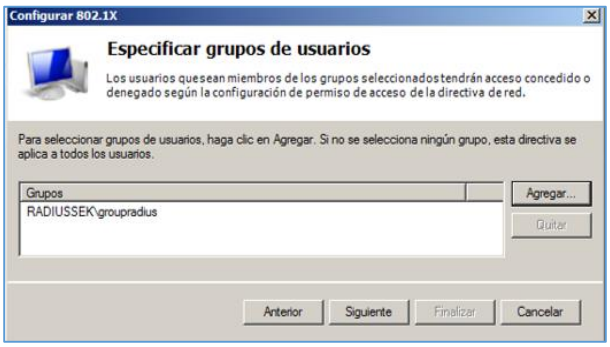
Fuente: (Microsoft)



- El grupo escogido se añadirá al cliente RADIUS con su respectivo canal de comunicación mediante la conexión inalámbrica segura establecida anteriormente.

Figura No. 134: Grupo agregado al cliente RADIUS

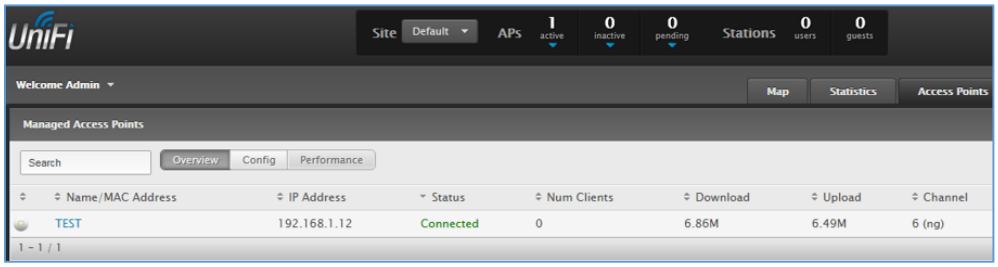
Fuente: (Microsoft)



- Finalizar la configuración 802.1X, el cual entregará un resumen de la nueva configuración para los clientes nuevos de RADIUS. Tomar en consideración que el punto acceso tendrá una dirección IP designada por DHCP.

Figura No. 135: Punto de acceso con dirección IP por DHCP

Fuente: (UNIFI, User Guide)



- A continuación se realiza la prueba de conexión con un usuario registrado en AD para su autenticación de acceso a la red inalámbrica. El usuario que se autentica

será: a01, que ingresará a la red inalámbrica desde diferentes equipos terminales sean móviles o estáticos. Una vez determinado el usuario se procede a la autenticación en la red y puede ser constatado de varias maneras. Una forma de verificación es mediante el servidor DHCP que debe asignar las direcciones IP a nuevos equipos que intentan obtener el acceso a la red inalámbrica. Las asignaciones de direcciones IP se visualizan en las 'concesiones de direcciones' del DHCP. Para el caso se realiza una prueba de acceso desde un equipo terminal estático de laboratorio de la institución.

Figura No. 136: Autenticación del usuario de prueba 'a01' en la red inalámbrica

Fuente: El autor

- En el proceso de acceso a la red inalámbrica 'WLAN-RADIUS' se presentará un formulario de autenticación enviado por el servidor RADIUS, al ingresar las credenciales respectivas, se enviará una solicitud de acceso hacia el servidor RADIUS a través del punto acceso. El servidor comprobará si el usuario se encuentra registrado en el directorio en su respectiva unidad organizativa con ayuda de la CA o autoridad certificadora. La CA al comprobar las credenciales,

confirmara el acceso y se genera un certificado de acceso que habilita el acceso al usuario en cuestión.

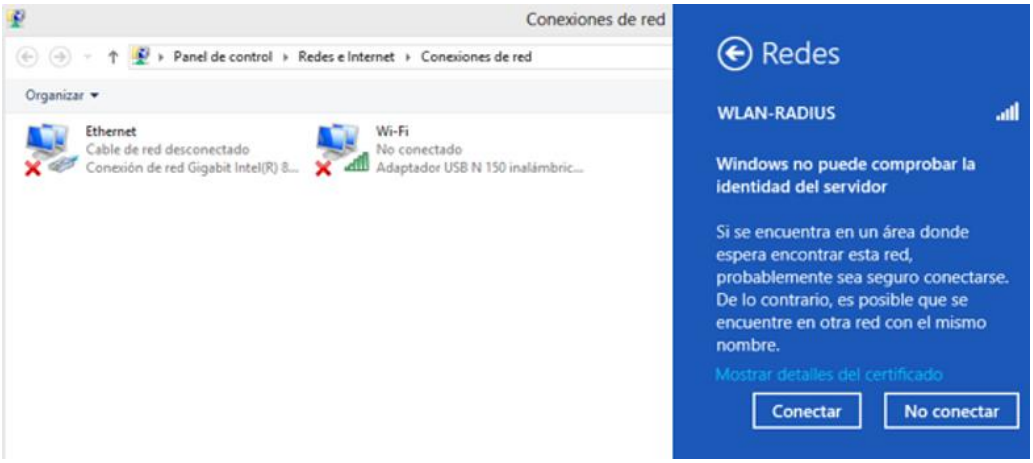
Figura No. 137: Ingreso de credenciales de autenticación

Fuente: El autor

- Al comprobarse las credenciales de acceso para la autenticación del usuario, proporcionará el enlace de conexión. Seleccionar la opción ‘Conectar’ para acceder a la red inalámbrica correspondiente.

Figura No. 138: Conexión a la red inalámbrica

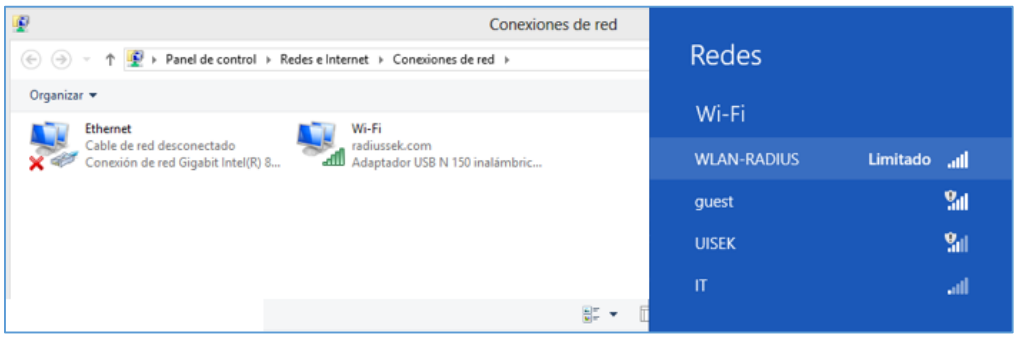
Fuente: El autor



- Finalmente el usuario de prueba al ya tener el acceso a la red inalámbrica, podrá disponer de los recursos de la misma. También es posible verificar el estado de conexión a una red.

Figura No. 139: Usuario autentificado y conectado a la red inalámbrica

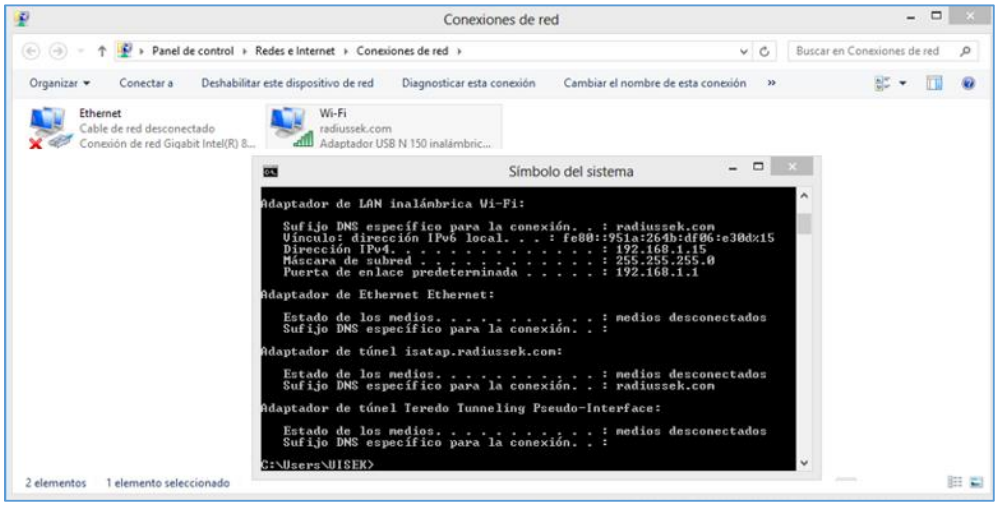
Fuente: El autor



- En el equipo terminal autenticado, ingresar a la consola de comandos y comprobar que dirección IP fue designado por DHCP (192.168.1.15), al conectarse a través del punto de acceso dado.

Figura No. 140: Dirección IP por DHCP del equipo terminal

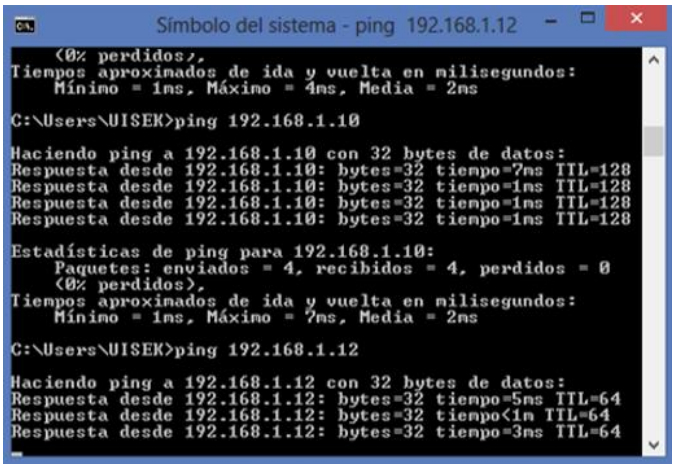
Fuente: El autor



- Comprobar que el usuario autenticado tiene acceso. En la consola de comandos hacer una comprobación de estado de conexión desde el equipo terminal hacia el servidor RADIUS (192.168.1.9); y punto de acceso (192.168.1.12).

Figura No. 141: Comprobación de estado de conexión desde equipo terminal

Fuente: El autor



- En el servidor DHCP se puede verificar la asignación de dirección IP al equipo terminal autenticado (192.168.1.15).

Figura No. 142: Asignación de direcciones IP por DHCP

Fuente: (Microsoft)

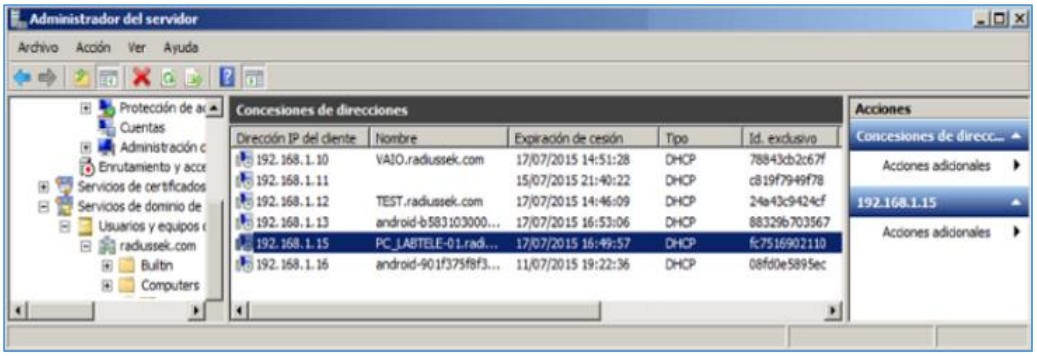
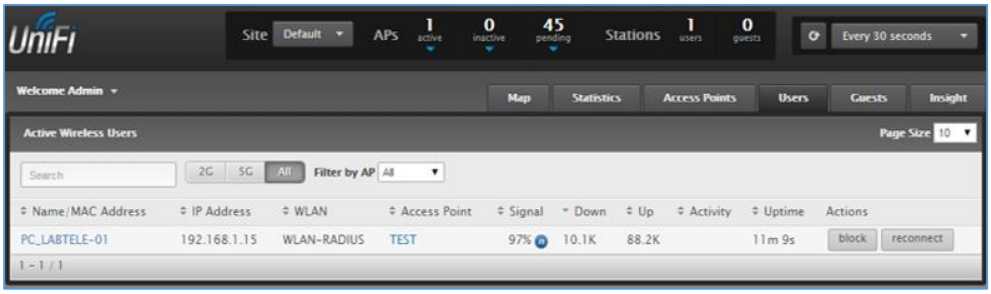


Figura No. 143: Registro de usuario activo en la consola del AP

Fuente: (UNIFI, User Guide)



- Nuevo ingreso desde terminales móviles a la red inalámbrica con el usuario de prueba a01.

Figura No. 144: Usuario de terminal móvil autenticado y conectado

Fuente: (UNIFI, User Guide)

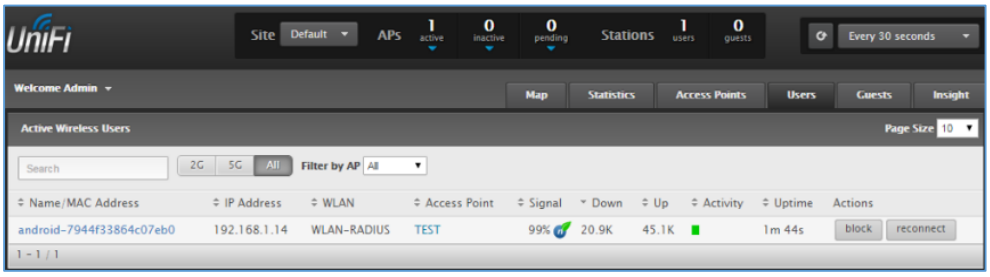


Figura No. 145: Características del nuevo usuario conectado

Fuente: (UNIFI, User Guide)

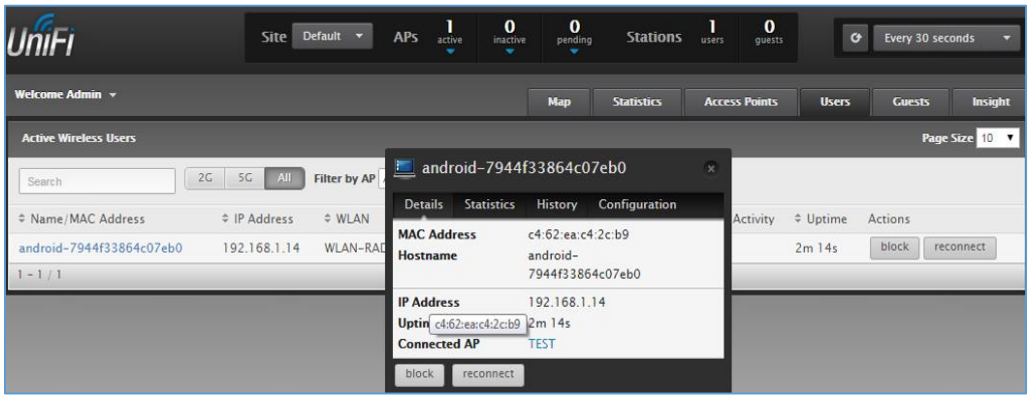
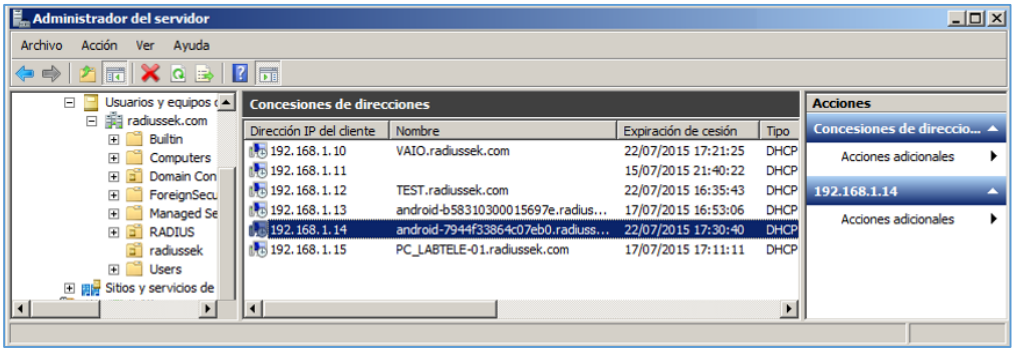


Figura No. 146: Dirección IP asignado a terminal móvil por DHCP

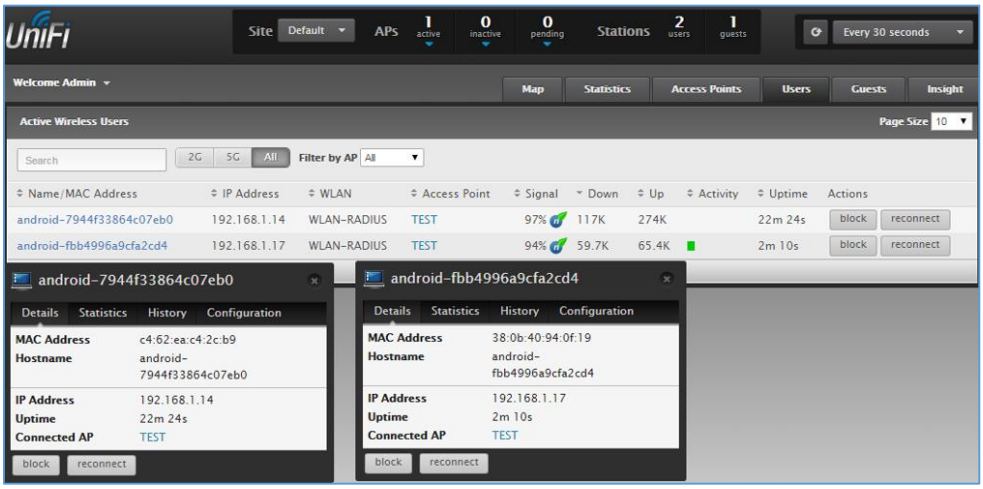
Fuente: (Microsoft)



- Conexión de otro dispositivo móvil autenticado con el usuario de prueba a01 en la red inalámbrica. Todos los usuarios autenticados que ingresen a la red inalámbrica serán visualizados en la consola de administración de los puntos de acceso.

Figura No. 147: Usuarios conectados a la red inalámbrica

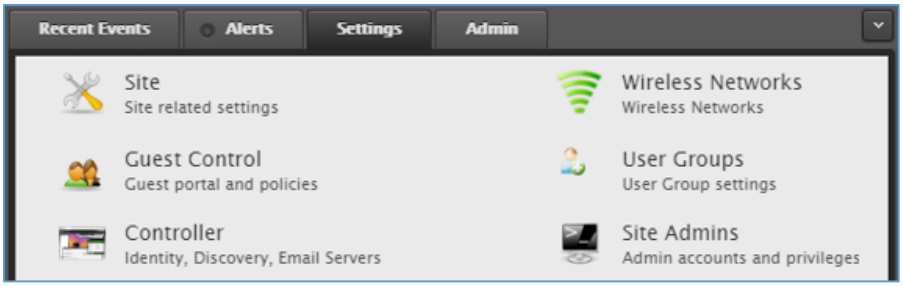
Fuente: (UNIFI, User Guide)



- Tomar en cuenta la configuración en la consola de administración de los puntos de acceso. Ubicar la pestaña ‘Settings’ y elegir la opción ‘Wireless Networks’.

Figura No. 148: Menú de opciones administrativas de la consola de AP

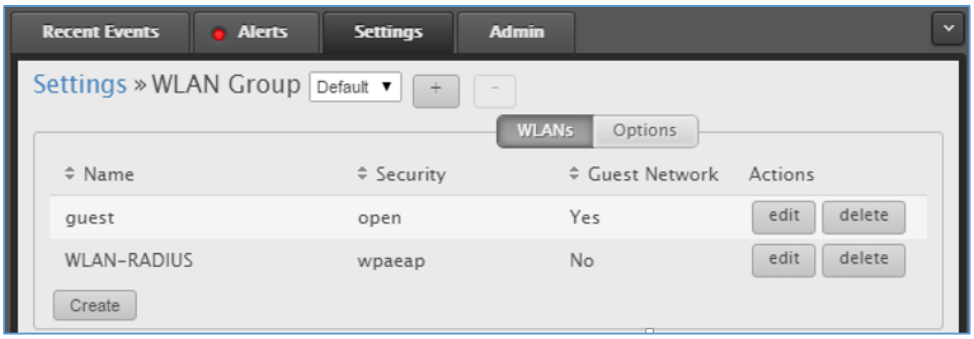
Fuente: (UNIFI, User Guide)



- Dentro de la opción de redes inalámbricas se visualizarán las que fueron creadas en un principio al momento de la instalación de la consola de administración.

Figura No. 149: Redes inalámbricas existentes

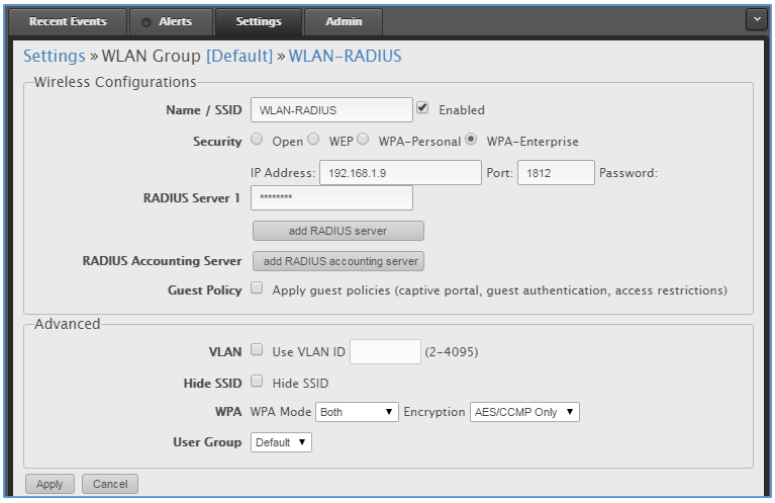
Fuente: (UNIFI, User Guide)



- Confirmar la red inalámbrica que está configurada para el proceso de autenticación seleccionando la opción ‘edit’ correspondiente a la red ‘WLAN-RADIUS’. Dentro de la ventana desplegada verificar los campos de SSID, el tipo de seguridad: WPA-Enterprise, y sobretodo que se encuentre agregado el servidor RADIUS indicando su dirección IP (192.168.1.9) y contraseña del secreto compartido cliente - servidor.

Figura No. 150: Configuración de la red inalámbrica en la consola de AP

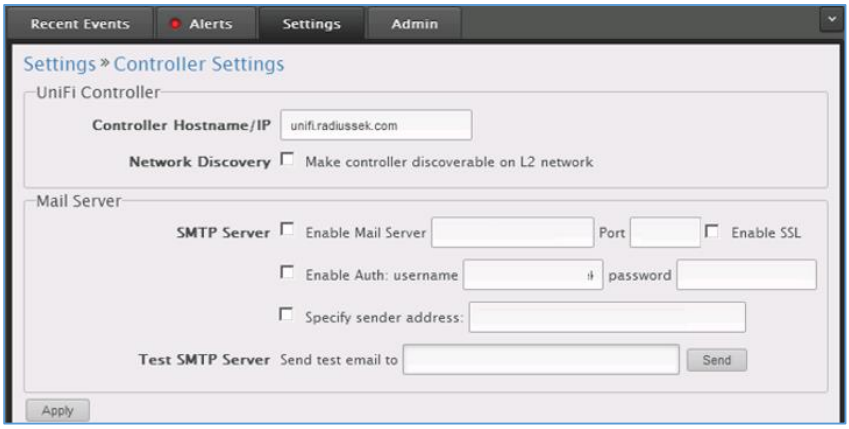
Fuente: (UNIFI, User Guide)



- Tomar en cuenta que en el controlador de la consola de gestión y administración de los AP, se debe indicar el nombre del dominio que referencia al servidor de autenticación.

Figura No. 151: Configuración de 'hostname' del controlador

Fuente: (UNIFI, User Guide)



- Todo el proceso anteriormente expuesto debe seguirse para ser implementado por completo en la red inalámbrica institucional.

CAPÍTULO IV

DISCUSIÓN

4.1 CONCLUSIONES

- Mediante el establecimiento de una arquitectura de seguridad en la red de comunicación de una organización, corporación, entidad académica, entidad financiera, empresa, etc.; que no la posea, implica tomar varias consideraciones previas y pruebas pertinentes. Dentro de estas consideraciones se examinan principalmente la infraestructura de red, detalle de equipos de la red, hardware y software utilizados en la administración y gestión de la red, arquitectura de la red, diseño de red, protocolos y estándares utilizados en la red, modelos y planes de gestión, control y seguridad en la red, presupuesto para tecnologías de información; y factores adicionales como adaptabilidad, flexibilidad, escalabilidad, Calidad de servicio (QoS) y disponibilidad de la red. Todos los aspectos analizados permitirán evidenciar la situación inicial y actual en la que se encuentra una organización en el ámbito tecnológico; lo que posibilita la implementación de nuevas soluciones tanto técnicas como logísticas en base a una toma de decisiones fundamentadas en un estudio previo.

- El análisis del estado actual de la infraestructura tecnológica general de la institución se orientó al ámbito de la red inalámbrica, proporcionando información que determinó una nueva arquitectura de seguridad a implementar. La solución se definió en base al conocimiento previo de la red inalámbrica, puesto que la institución cuenta principalmente con el hardware y software necesario y adecuado para la administración; por lo que se determinó un servidor de autenticación RADIUS de gran eficacia y adaptabilidad al estado actual de la red inalámbrica. El servidor propuesto se acopla con gran facilidad, siendo utilizado en la mayoría de redes inalámbricas modernas brindando un mejor rendimiento y seguridad.

- La arquitectura de seguridad planteada tuvo base en la aplicación de distintos escenarios mediante 2 posibles opciones de solución. El primero consistió en el uso de una solución de software libre y el segundo basado en el uso de software propietario. Los resultados al iniciar las pruebas de implementación pusieron en evidencia de que la implementación de un servidor de autenticación alternativo a la arquitectura manejada en la red inalámbrica de la institución no se adapta a las necesidades requeridas y cuya operatividad se vuelve compleja; en cambio la implementación de un servidor basado en software propietario tuvo mejor adaptabilidad haciendo flexible el manejo de las configuraciones debido a que toda la red institucional se apoya bajo software propietario.

- El manejo de gestión de los usuarios por medio de un directorio activo combinado con un servidor de autenticación RADIUS hace posible el ingreso constante de nuevos

usuarios, modificación de parámetros y atributos por cada uno de ellos, y eliminación o des habilitación de los mismos. RADIUS soporta múltiples usuarios y tareas a la vez ya que su seguridad brinda cifrado y funciones de hash para autenticación. Sin embargo, hace más robusta la comunicación en la red inalámbrica, el empleo de certificados digitales sumado a las credenciales requeridas para cada uno.

- El acoplamiento de una arquitectura de seguridad a la red institucional permitió mantener el uso de diferentes equipos de comunicación inalámbrica dedicados, no obstante el factor primordial a considerarse fue el número usuarios dentro de la red. La administración de la red inalámbrica de la institución, evidenció que el tráfico de red aumentaba por la cantidad de usuarios o clientes existentes. Por lo que el ancho de banda disminuía y el desempeño de la red bajaba, al ser una red que se encuentra abierta al público en general. Por tal motivo el empleo de los protocolos RADIUS y LDAP dentro de la arquitectura de red de la institución, permitieron solventarlo. Ambos protocolos proporcionaron una comunicación segura únicamente a los usuarios registrados en el directorio activo de la red inalámbrica, y un sistema apropiado de control de acceso de usuarios, gestión de recursos, seguridad de comunicación, y protección de información durante todo el tiempo de conexión.

4.2 RECOMENDACIONES

- Es muy importante tomar en cuenta las características de los equipos con los que opera la red de comunicación de una organización, pues proveen de un sistema de gestión que facilita la administración.

- Constatar que los equipos de comunicación inalámbrica como los puntos de acceso soporten autenticación mediante protocolos 802.1X, RADIUS y LDAP.

- Verificar que los puntos de acceso en la red inalámbrica permitan incluir conexiones con servidores de autenticación RADIUS.

- La instalación de certificados, plantillas de certificados y entidades de certificación deben ser instalados solo en el servidor local de autenticación y no por cada usuario, ya que se volvería un proceso complejo y poco eficiente.

- Llevar un registro estadístico de la cantidad de usuarios que se conectan diariamente a la red inalámbrica, lo cual dará pautas para una mejor distribución de un servicio determinado.

- Se recomienda que el secreto compartido entre el servidor de autenticación RADIUS sea complejo e igual que el configurado en el punto de acceso (AP) para una correcta comunicación entre ambos.

- Se recomienda considerar que los certificados tienen un tiempo de validez, volviéndose obsoletos al sobrepasar el tiempo pre establecido. Los certificados obsoletos son agregados como certificados revocados por la autoridad certificadora. Por lo cual se hace necesario la renovación de los mismos.

- Se recomienda la implementación del servidor de autenticación RADIUS en organizaciones con gran número de usuarios debido a la versatilidad que maneja.

- Se recomienda la utilización de puntos de acceso de nivel corporativo o empresarial ya que permiten añadir sistemas de gestión a detalle y en tiempo real.

- Se recomienda para la creación de un amplio número de usuarios, utilizar scripts de importación para evitar el ingreso por cada uno.

- Antes del inicio de la implementación total del proyecto en la institución, se recomienda socializar el nuevo proyecto con el departamento de comunicación, para que pueda ser aceptado y manejado por los usuarios.

BIBLIOGRAFÍA

1. Aguirre, J. R. (2006). Seguridad Informática y Criptografía.
2. Arana, J. R. (2013, 5). *http://www.scielo.org.co/.* Retrieved from Implementación del control de acceso a la red: http://www.scielo.org.co/pdf/inco/v15n1/v15n1a12.pdf
3. *Aspectos Avanzados de Seguridad en Redes.* (n.d.). UOC.
4. CISCO. (2008). *CCNA Exploration: Aspectos básicos de Networking.* ciscopress.com.
5. CISCO. (2010). *CCNA Discovery: Networking para el hogar y pequeñas empresas.* ciscopress.com.
6. CISCO. (2013). *http://www.cisco.com.* Retrieved from Configuring RADIUS Servers: http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-3_7_JA/configuration/guide/i1237sc/s37radi.pdf
7. DORDOIGNE, J. (n.d.). *Redes informáticas.* eni.
8. Forouzan, B. A. (2006). *Transmisión de datos y redes de comunicaciones.* Mc Graw Hill.
9. Hallberg, B. (2010). *Fundamentos de Redes.* Mc gRaw Hill.
10. Hansen, Y. F. (2009). *Sistemas basados en la Autenticación en Windows y Linux/GNU.* Alfaomega, Ra-Ma.
11. *http://whp-aus2.cold.extweb.hp.com/.* (n.d.). Retrieved from http://whp-aus2.cold.extweb.hp.com/pub/networking/software/Security-Oct2005-59906024-Chap05-RADIUS.pdf

12. INEI. (2005). *Redes Inalámbricas Wireless.*
13. (2010). *Internet y Redes Inalambricas.*
14. Ltd. , O. S. (2015, 07 15). *https://www.open.com.au/*. Retrieved from Radiator® RADIUS Server: https://www.open.com.au/radiator/ref.pdf
15. Matthews, M. (n.d.). *Windows Server 2008: Guía del administrador.* Mc Graw Hill.
16. NEC. (2010). *Microsoft® Windows Server® 2008 R2 Enterprise.*
17. Santos, J. (2011). *Seguridad y alta disponibildad.* RA-MA.
18. (n.d.). *Seguridad en Redes Inalámbricas 802.11*.
19. servtech. (2015, 01 10). *http://www.servtech.mx/*. Retrieved from http://www.servtech.mx/auditoria-forense/
20. Stallings, W. (2000). *Sistemas Operativos.* Madrid: Prentice Hall.
21. Stallings, W. (2010). *Comunicaciones y Redes de Computadores.* Pearson.
22. Stallings, W. (2010). *Fundamentos de seguridad en redes.* Pearson.
23. Tanembaun. (2012). *Redes de computadoras.* Pearson.
24. Tanembaun, A. (1997). *SISTEMAS OPERATIVOS diseño e implementacion.* Prentice Hall.
25. Tanembaun, A. (n.d.). *Sistemas operativos distribuidos.* Prentice Hall.
26. Taylor, P. (2005). *ZeroShell WPA Enterprise.*
27. TechNet, M. /. (2004, 11). *www.microsoft.com.* Retrieved from Arquitectura de la solución de LAN inalámbrica segura: https://www.microsoft.com/latam/technet/articulos/wireless/pgch03.mspx

28. Tuomimäki, J. (2003, 05). *http://www.tml.tkk.fi/*. Retrieved from Overview, details and analysis of Radius protocol: http://www.tml.tkk.fi/Studies/T-110.551/2003/papers/12.pdf
29. UNIFI. (n.d.). *User Guide.*
30. Zacker, M. -C. (2010). *Windows Server 2008 R2*. nSight, Inc.
31. Zeroshell. (n.d.). *Guide.*

ANEXOS

ANEXO A – CERTIFICADO PRUEBAS DE IMPLEMENTACIÓN

FACULTAD DE ARQUITECTURAS E INGENIERÍAS
ÁREA DE SISTEMAS INFORMÁTICOS

Quito, 24 de julio de 2015

CERTIFICADO

Por el presente, certifico que el Sr. **Luis Alberto Muñoz Alvarez** con C.I.: 1722945688, egresado de la Universidad Internacional SEK, efectuó el Proyecto de Investigación de fin de carrera, analizando, desarrollando, y realizando las debidas pruebas de implementación con el área de sistemas informáticos de la institución, la arquitectura de seguridad para el control de acceso de la red inalámbrica de la Universidad Internacional SEK para el campus Miguel de Cervantes.

El interesado puede hacer uso de este certificado como a bien tuviere.

Atentamente,

Ing. Edison Estrella, MBA.
Administrador

ANEXO B – ÍNDICE DE ABREVIATURAS

- **AP** Access Point, Punto de Acceso
- **AES** Advanced Encryption Standard
- **AAA** Autentificación, Autorización y Contabilidad
- **BD** Base de Datos
- **CA** Certificate Authority, Autoridad Certificadora
- **CHAP** Challenge Handshake Authentication Protocol, Protocolo de Autentificación por Desafío Mutuo
- **DES** Data Encryption Standard, Cifrado Estadarizado de Datos
- **DNS** Domain Name Service, Servicio de Nombres de Dominio
- **DHCP** Dinamic Host Configuration Protocol
- **EAP** Protocolo de autentificación extensible
- **EAP-TLS** EAP Transport Level Security
- **EAPOL** EAP OverLan
- **IEEE** Institute of Electricaland Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos
- **IDEA** International Data Encription Algorithm
- **ITU-T** International Telecommunications Union, Unión internacional de telecomunicaciones
- **IP** Protocolo de Internet
- **ISP** Internet Service Provider, Proveedor de servicios de Internet
- **IAS** Servicio de autentificación de Internet

- **LDAP** Lightweight Directory Access Protocol, Protocolo Ligero de Acceso a Directorios
- **LAN** Local Area Network, Red de Área Local
- **MD5** Message-Digest Algorithm 5
- **NAS** Network Access Server, Servidor de Acceso a la Red
- **NPS** Servidor de directivas de red
- **PEAP** Protocolo de autentificación Extensible Protegido
- **RADIUS** Remote Authentication Dial-In User Service
- **RC5** Rivest Cypher 5
- **RSA** Rivest Shamir Adleman
- **SHA** Secure Hash Algorithm
- **SSID** Service Set IDentifier
- **SMTP** Simple Mail Transfer Protocol, Protocolo Simple de Transmisión de Correo
- **SQL** Structured Query Language, Lenguaje de Consulta Estructurada.
- **SSH** Secure Shell, Intérprete de Órdenes Segura
- **TLS** Transport Layer Security, Seguridad para Nivel de Transporte
- **TCP** Transmission Control Protocol, Protocolo de Control de Transmisión
- **UID** Identificador de Usuario
- **UDP** Protocolo de Datagramas de Usuario
- **Wifi** Wireless Fidelity, Fidelidad Inalámbrica
- **WLAN** Wireless Local Areanetwork, Red de Área Local Inalámbrica

ANEXO C – IMPLEMENTACIÓN RADIUS

Implementación del servidor RADIUS en la red inalámbrica de la institución

Una vez efectuadas las pruebas, se realizó la implementación en la red institucional. La implementación de configuraciones fue relativamente menor debido a que ciertas configuraciones ya estaban pre establecidas.

Se efectuó una conexión remota al equipo que alojaría al servidor de autenticación RADIUS. Se realizaron los mismos procesos desde la asignación de una dirección IP fija hasta la creación de roles necesarios para su funcionamiento.

Fig. 1

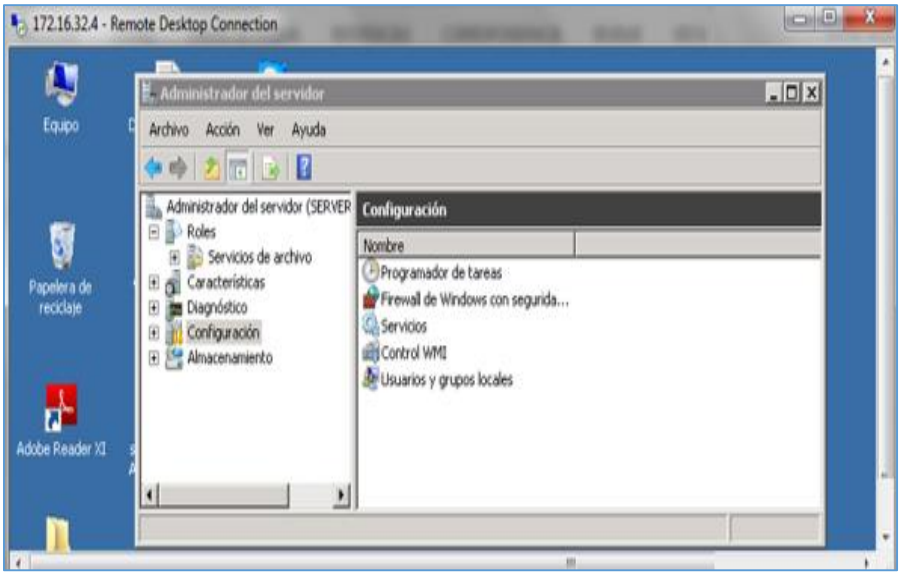
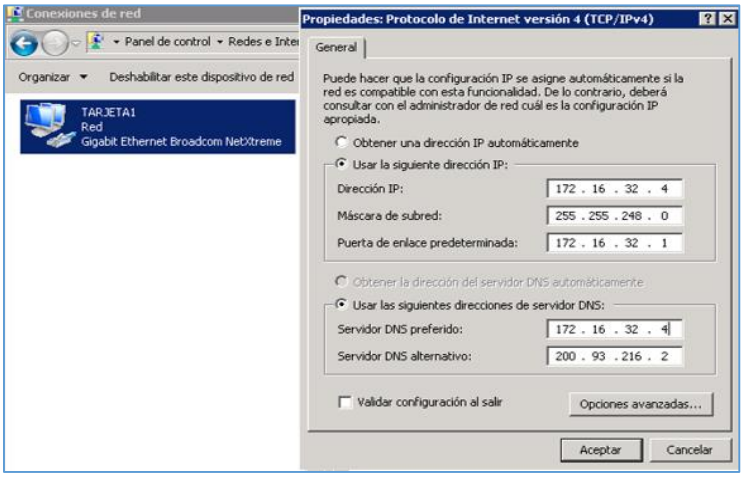
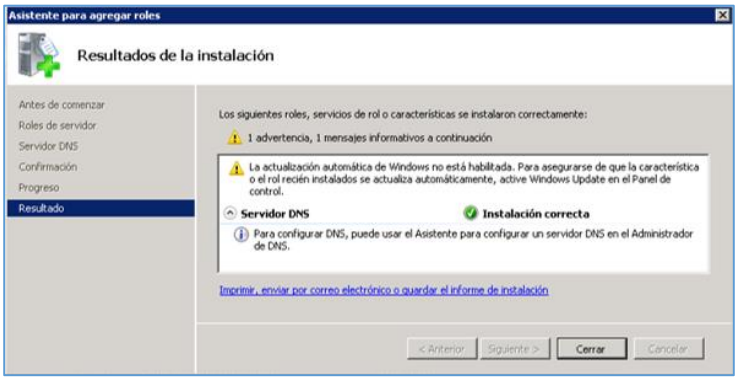


Fig. 2



La instalación del rol servidor DHCP no fue necesario instalarlo ya que en la red, existe un firewall conectado al router que toma señal del ISP para proporcionar el servicio de internet, adicionalmente posee DHCP para la asignación de las direcciones IP.

Fig. 3



En el rol de servidor DNS instalado se crearon nuevas zonas de búsqueda directa e inversa y se configuraron en base a las implementaciones de prueba realizadas anteriormente.

Fig. 4

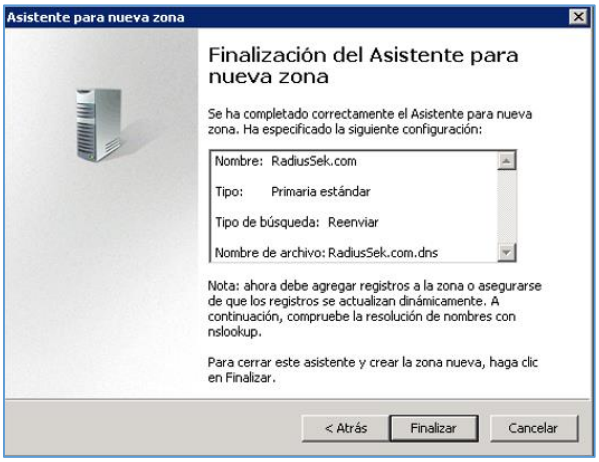


Fig. 5

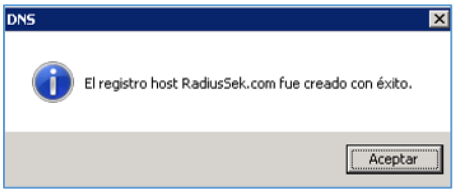
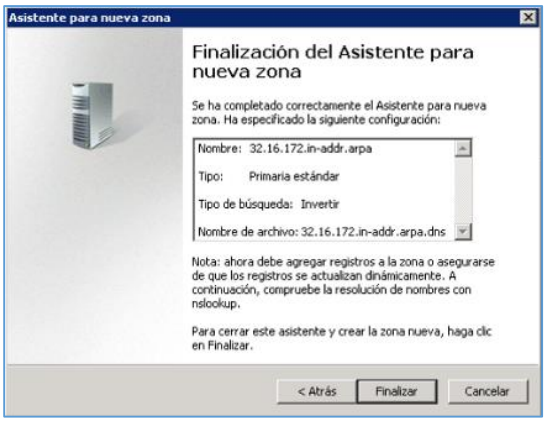


Fig. 6



Se instaló también los roles de servicios de dominio de Active Directory, servicios de certificados de AD, servicios de acceso y directivas de redes.

Fig. 7

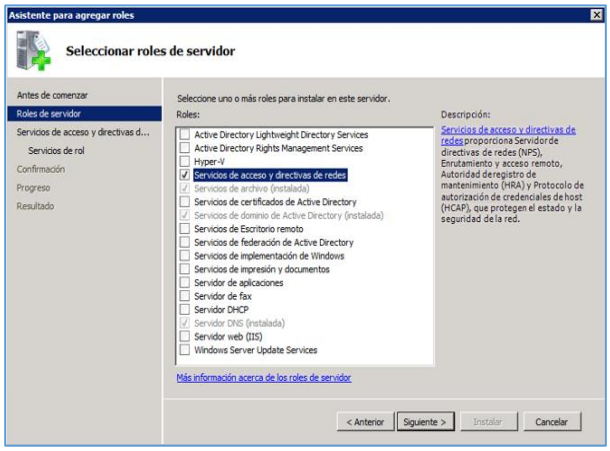


Fig. 8

Fig. 9

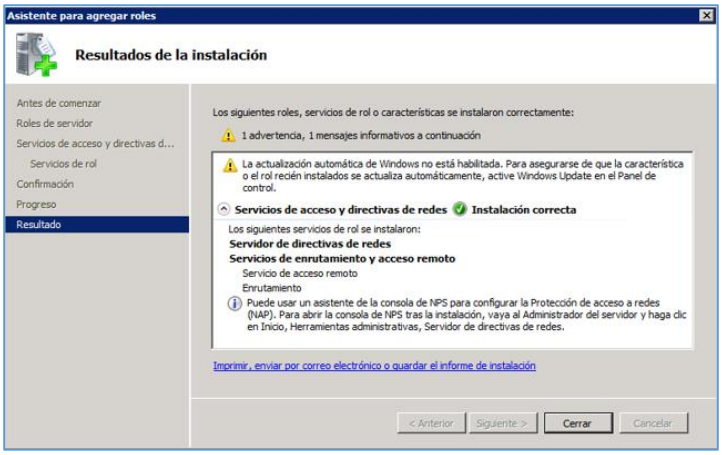


Fig. 10

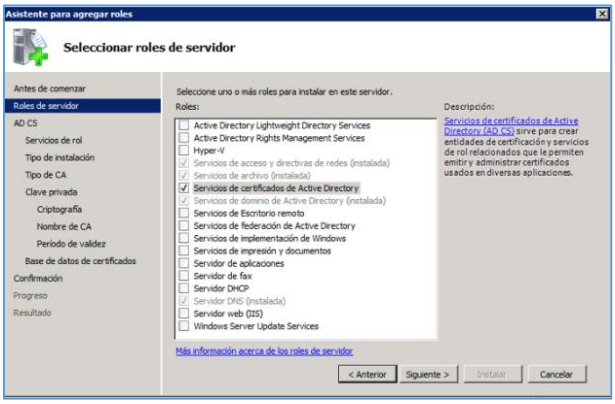
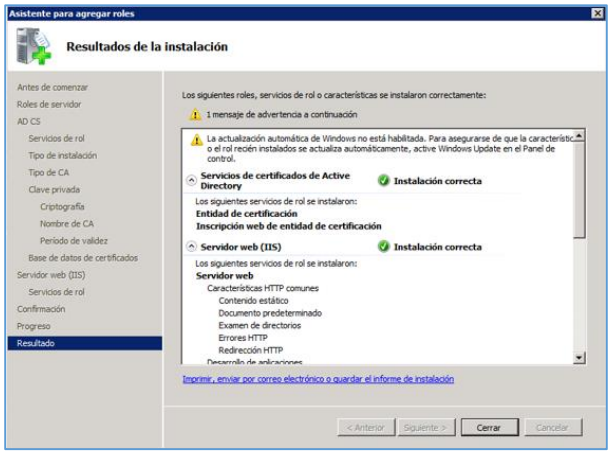


Fig. 11



Creación de usuarios de prueba en el directorio activo en la red inalámbrica

Se crearon los objetos: unidad organizativa, grupo, usuarios, equipos de prueba en base a las configuraciones realizadas en las pruebas de implementación previas.

Unidad organizativa / Usuario de prueba

Fig. 12

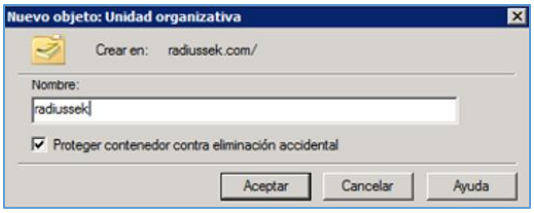
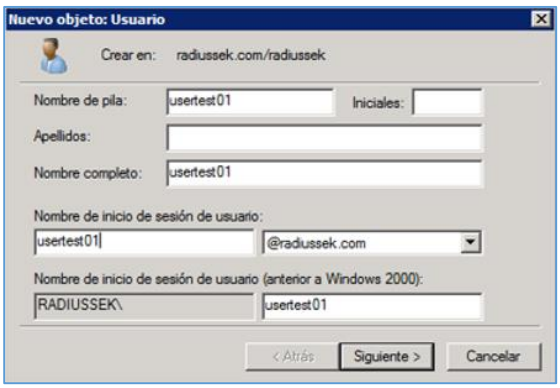


Fig. 13



Grupo / Equipo

Fig. 14

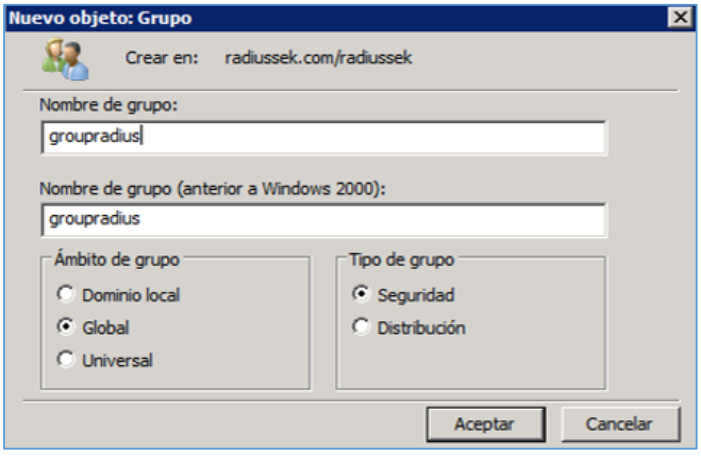
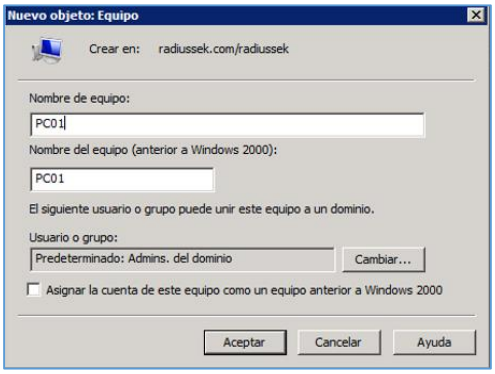


Fig. 15



Para la vinculación de un amplio número de miembros para un grupo determinado perteneciente a una unidad organizativa determinada se debe realizar mediante el uso de un script o plantilla con los datos asociados o concatenados respectivamente.

Fig. 16

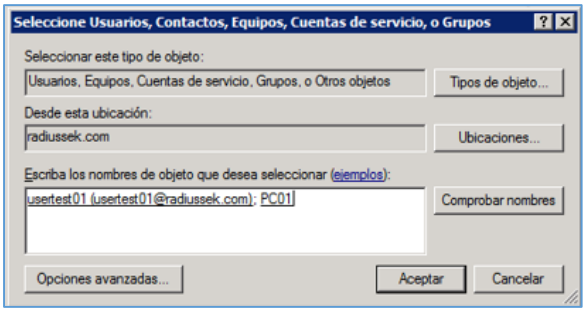
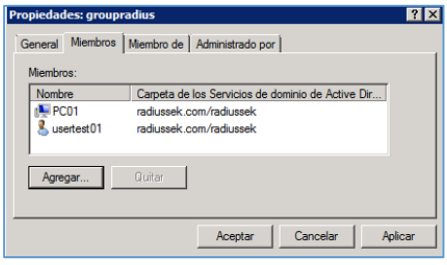


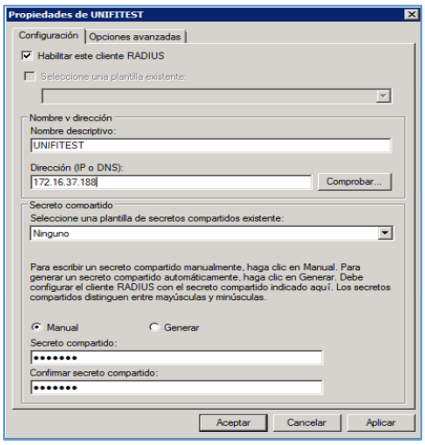
Fig. 17



Se crearon los clientes RADIUS, y se configuraron los principales parámetros.

Fig. 18

Fig. 19



Se establecieron los clientes, métodos de autenticación, grupos de usuarios correspondientes.

Fig. 20

Fig. 21

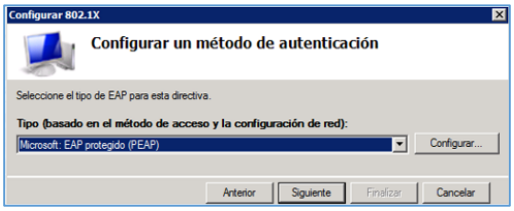
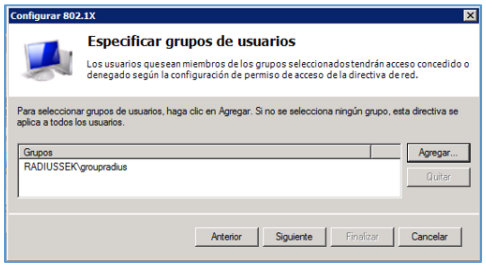


Fig. 22



Instalación de certificados

Al ingresar a la consola raíz se incluyeron los 3 complementos requeridos para el proceso de autenticación: Plantilla de certificado, Certificados, Entidad de certificación de manera local. Todos se configuraron en base a las pruebas de implementación previas. Al finalizar se guardó la configuración realizada en el servidor.

Fig. 23

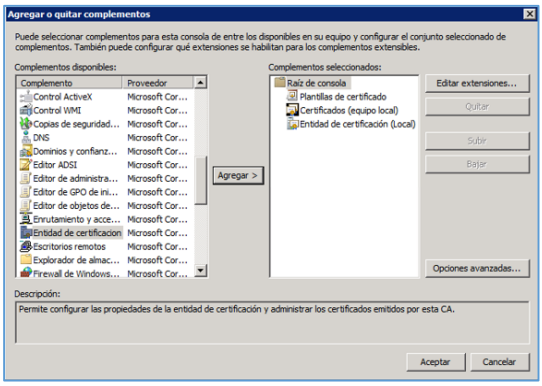


Fig. 24

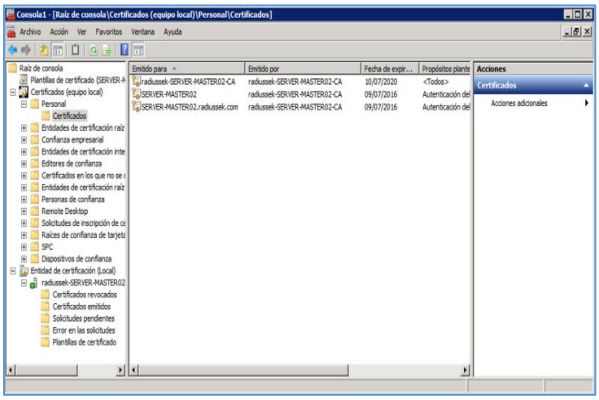
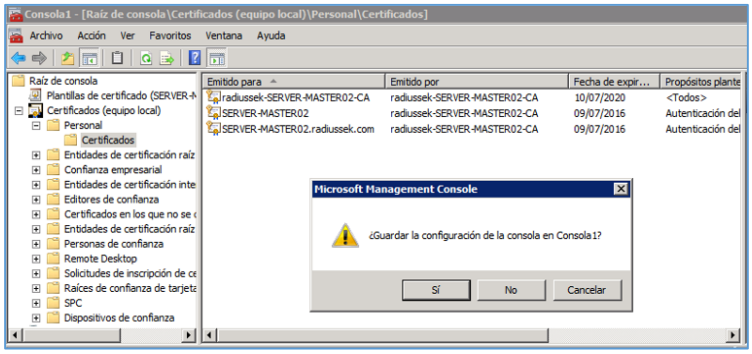


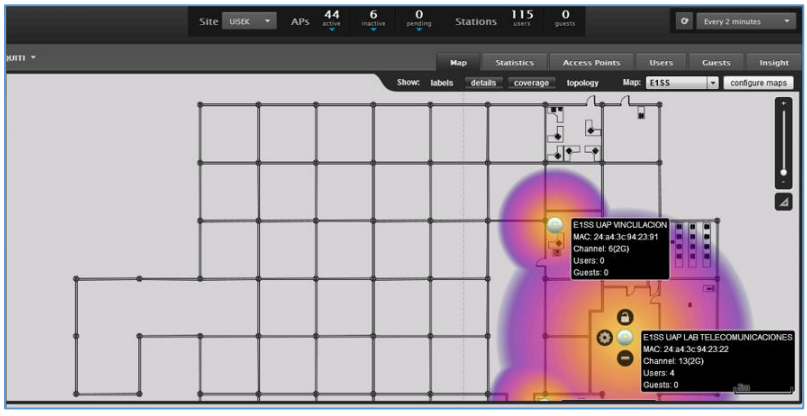
Fig. 25



Punto de Acceso

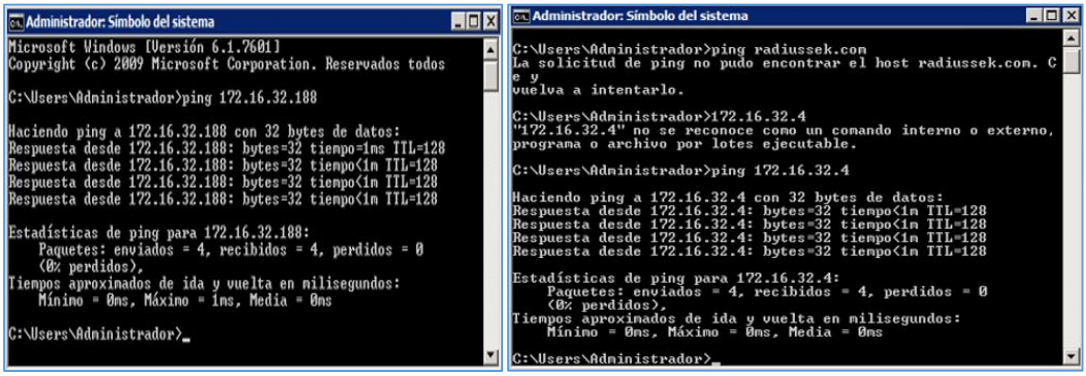
Las configuraciones para los puntos de acceso no fueron extensas ya que la consola de administración y gestión de los equipos de comunicación inalámbrica ya se encontraba instala y pre configurada.

Fig. 26



Se comprobó el estado de conexión entre un punto de acceso de prueba con el servidor de autenticación RADIUS.

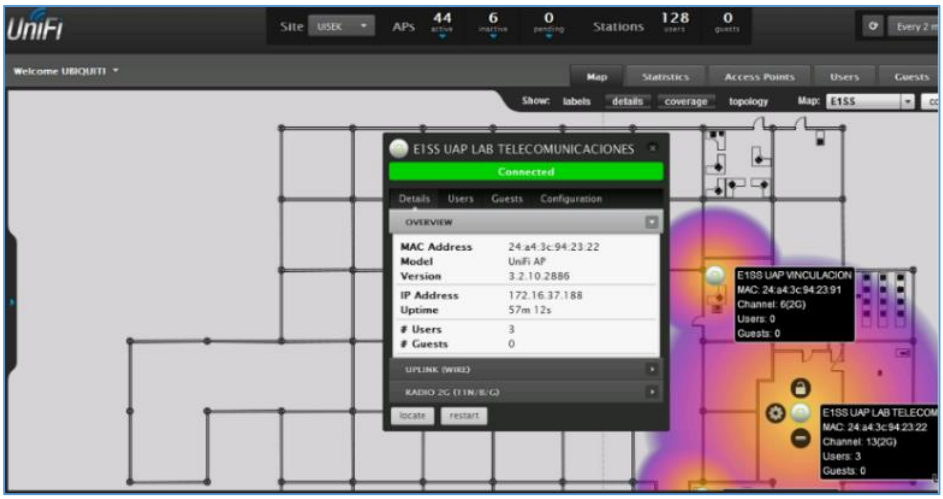
Fig. 27



Visualización de la configuración de un punto de acceso en consola de administración

Como las pruebas iniciales en la red inalámbrica de la institución fueron con respecto al punto de acceso correspondiente al laboratorio de telecomunicaciones, se presentan las configuraciones establecidas. También se muestra su funcionamiento en tiempo real.

Fig. 28



Características configuradas en el punto de acceso.

Fig. 29

Fig. 30

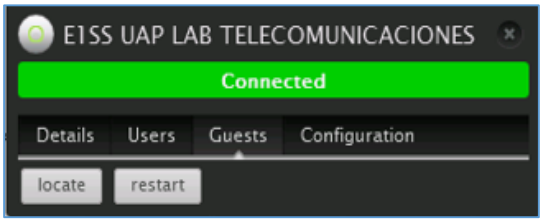


Fig. 31

Fig. 32

También es posible tener un estado estadístico de la situación en tiempo real del uso de la red inalámbrica de la Universidad. Cada AP es identificable por un color determinado, adicionalmente fue posible visualizar el número de usuarios conectados a la red inalámbrica.

Fig. 33

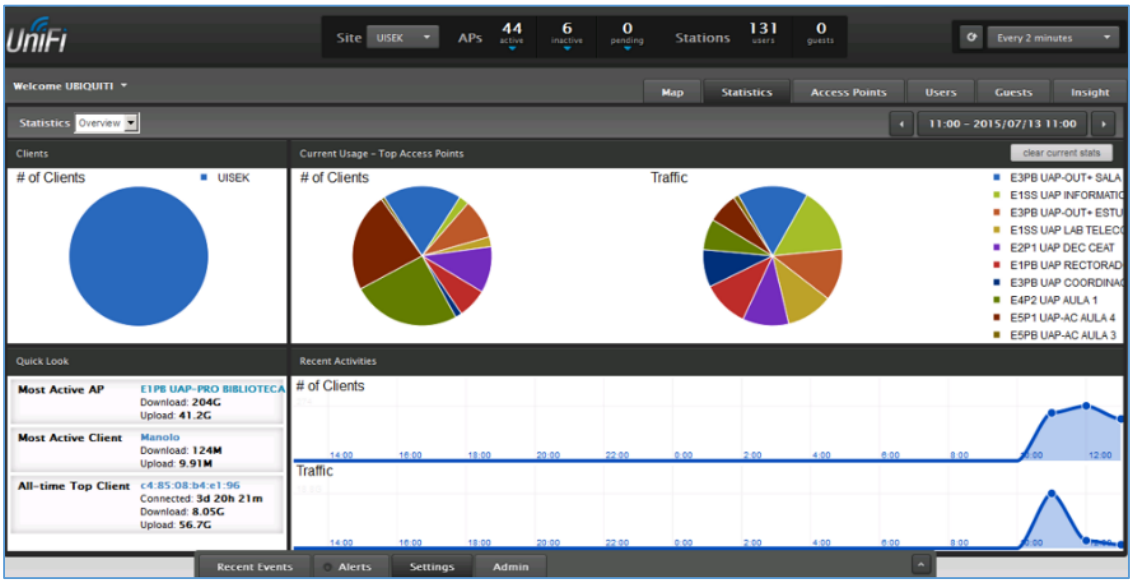
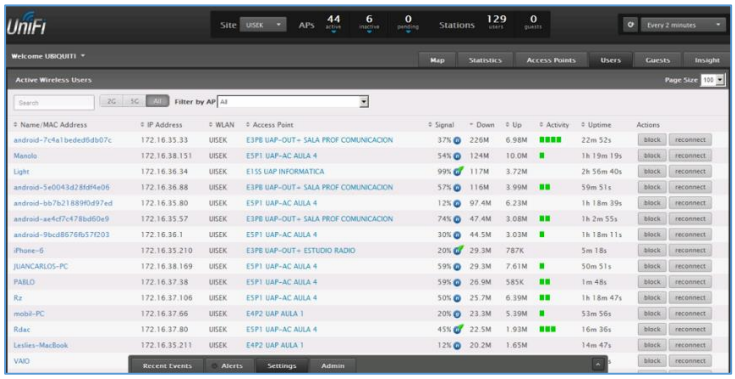


Fig. 34



Inclusive al haber posibles incidentes, la consola envía mensajes de alerta informando cualquier tipo de índole suscitado.

Fig. 35

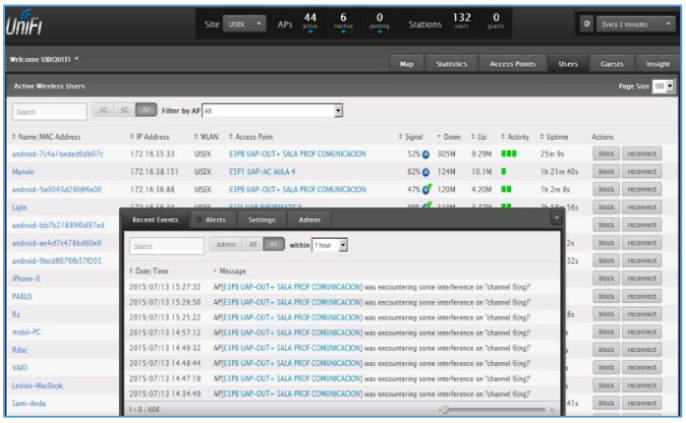
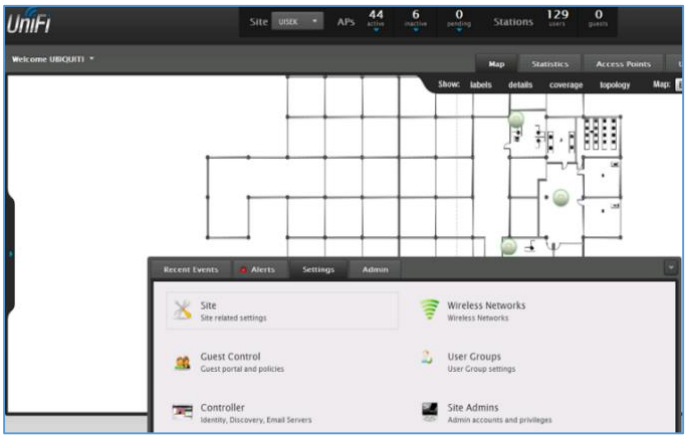
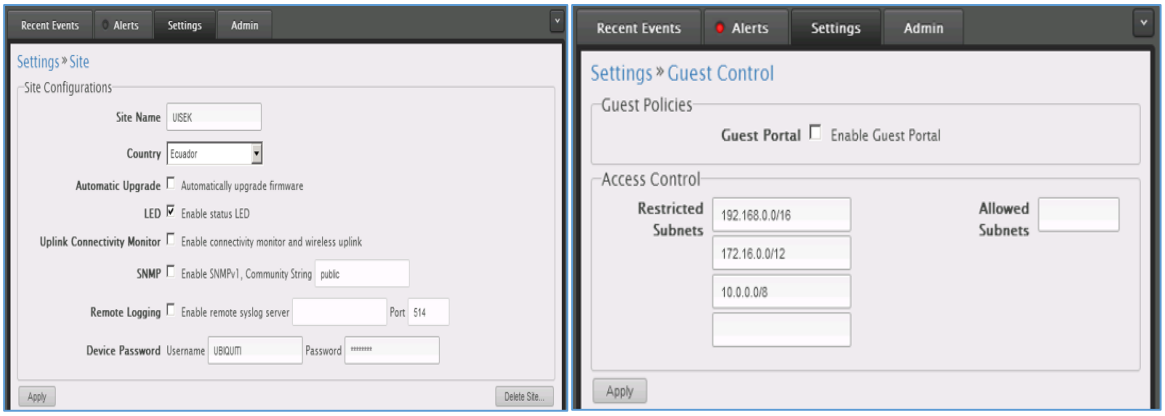


Fig. 36



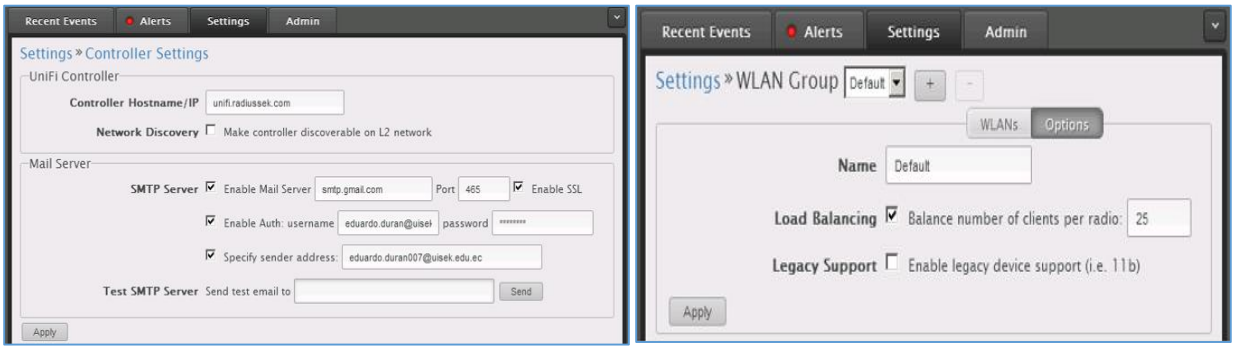
Configuraciones del menú de opciones de la consola administrativa de AP

Fig. 37



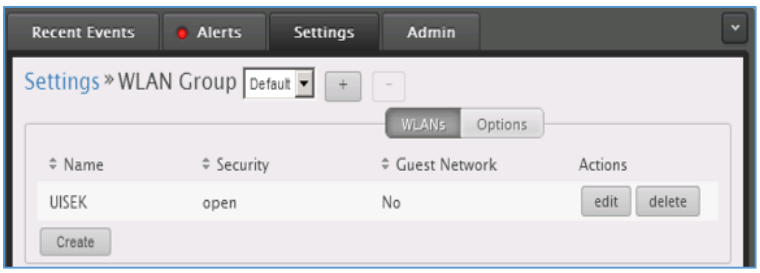
Dominio referenciado al del servidor DNS alojado en el servidor de autenticación RADIUS.

Fig. 38



Red inalambrica existentes SSID: UISEK.

Fig. 39



Importación de mapas de ubicación para gestión de red

La consola de administración permite importar mapas para ubicar los equipos inalámbricos (AP) en la red y proporcionar una mejor administración.

Fig. 40

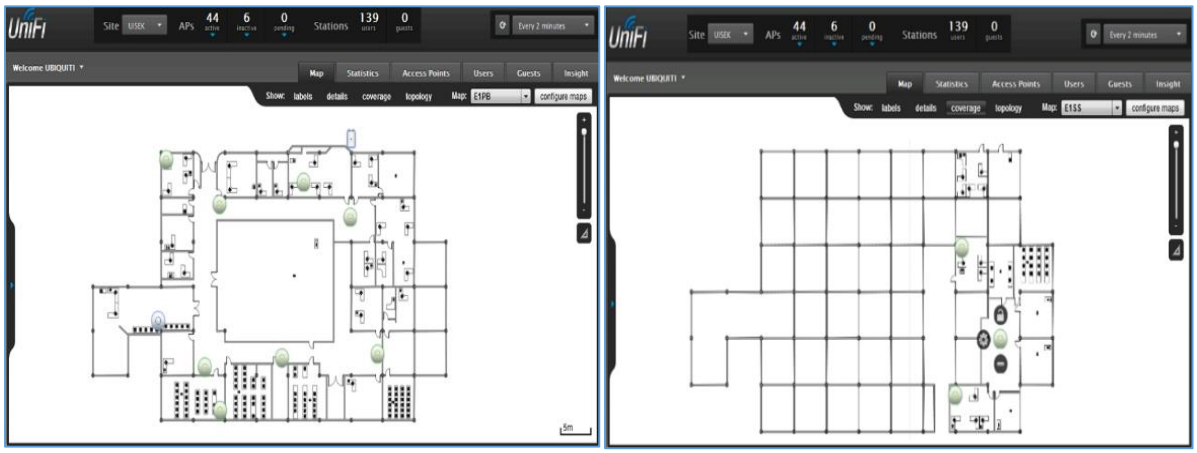


Fig. 41

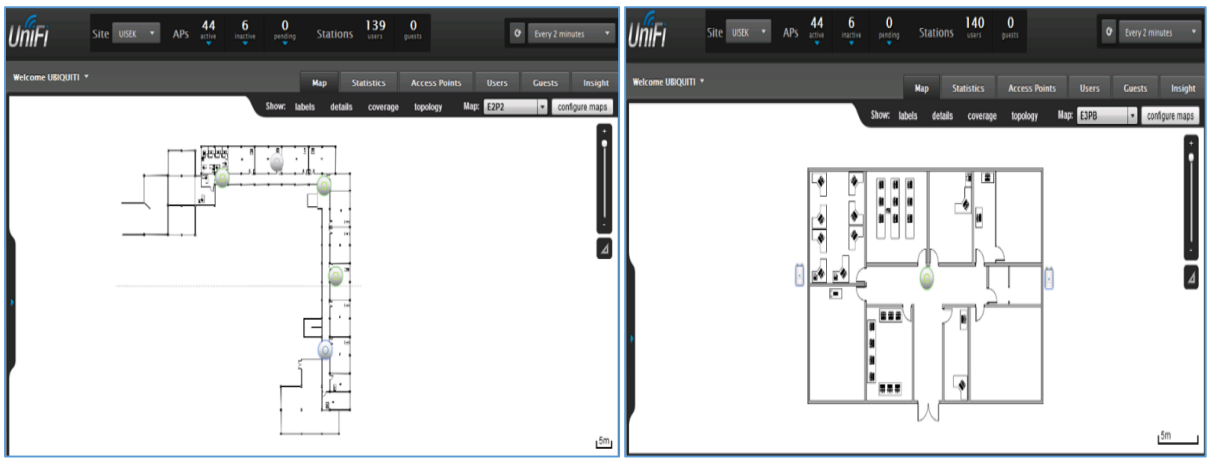
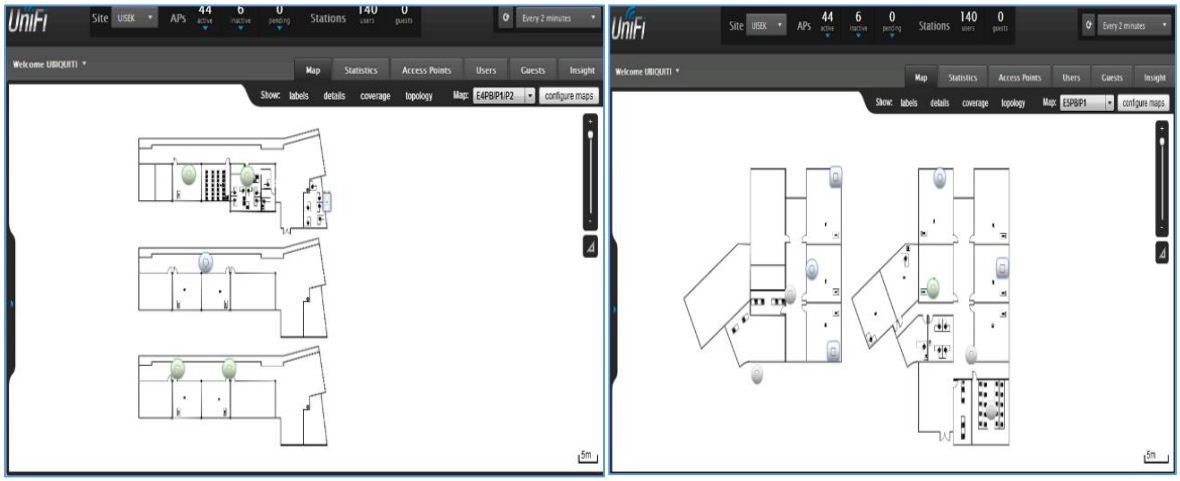


Fig. 42



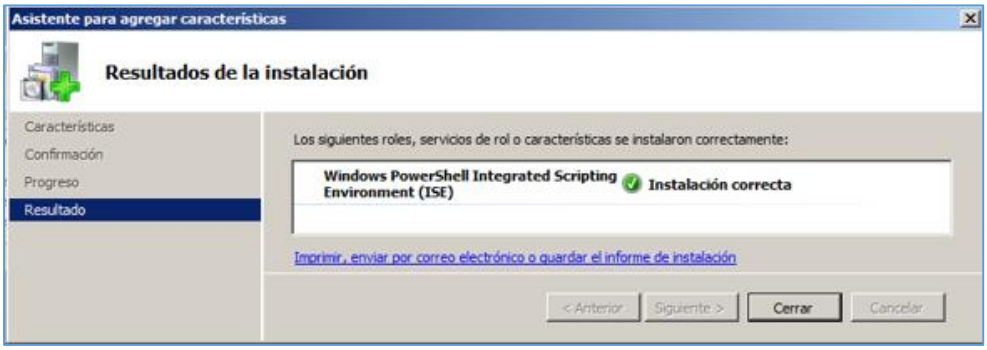
Ubicación del AP de prueba ubicado en el laboratorio de telecomunicaciones.

Fig. 43

Importación de usuarios

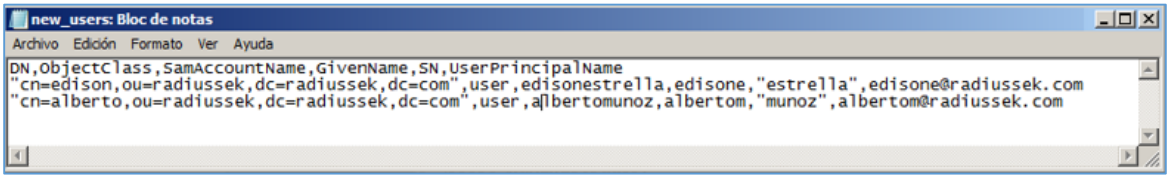
Hay diversos métodos de importación para un número extendido de usuarios, que deben ser ejecutados desde una consola de comandos o powershell.

Fig. 44



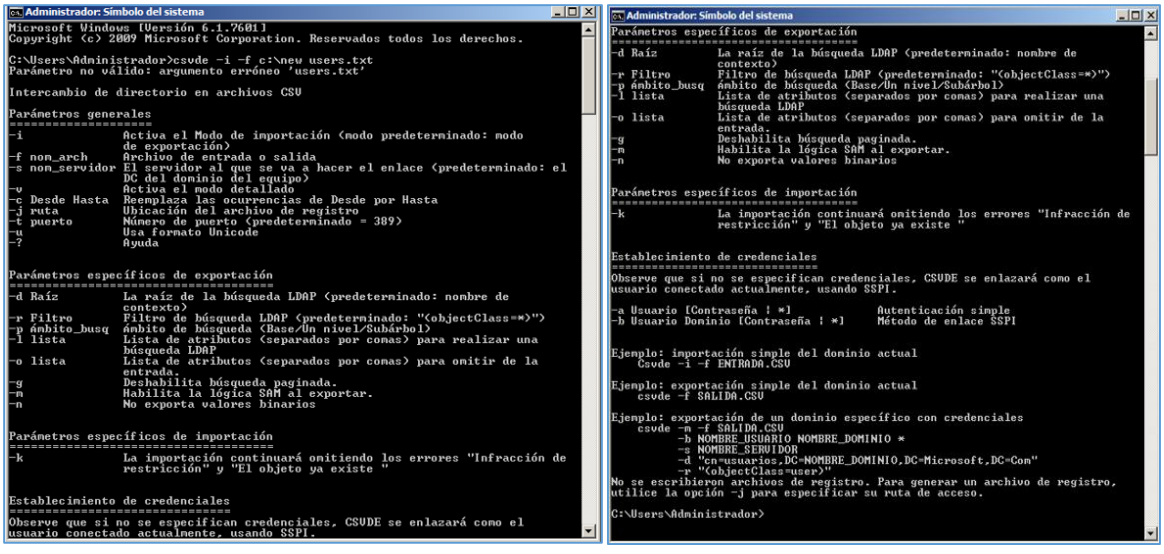
Script de importación:

Fig. 45



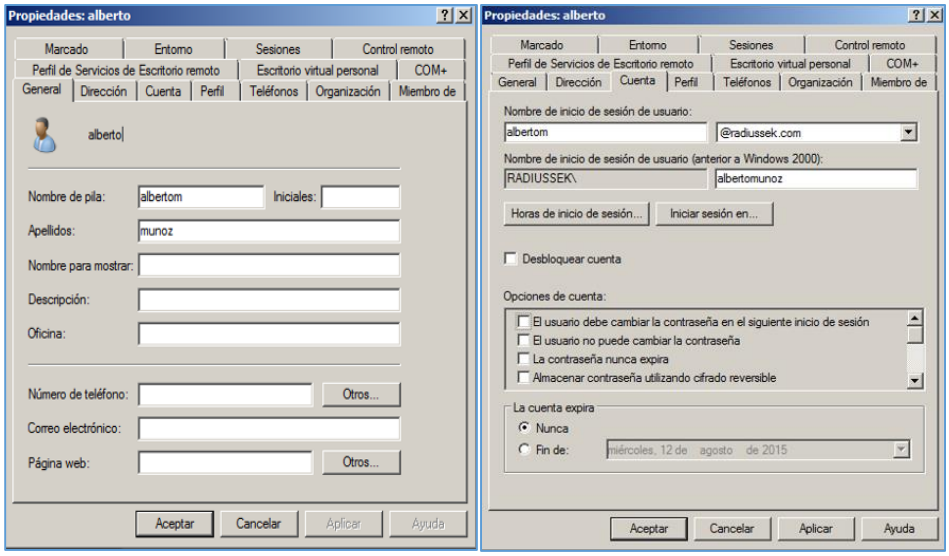
Ejecución del script:

Fig. 46



Comprobacion del usuario creado:

Fig. 47



Herramientas de importación como: CSVDE, no permiten la importación del atributo de contraseña para un usuario, de modo que se haría tedioso configurar una contraseña por cada usuario considerando que pueden ser múltiples. La contraseña tendrá que reestablecerse manualmente.

Fig. 48

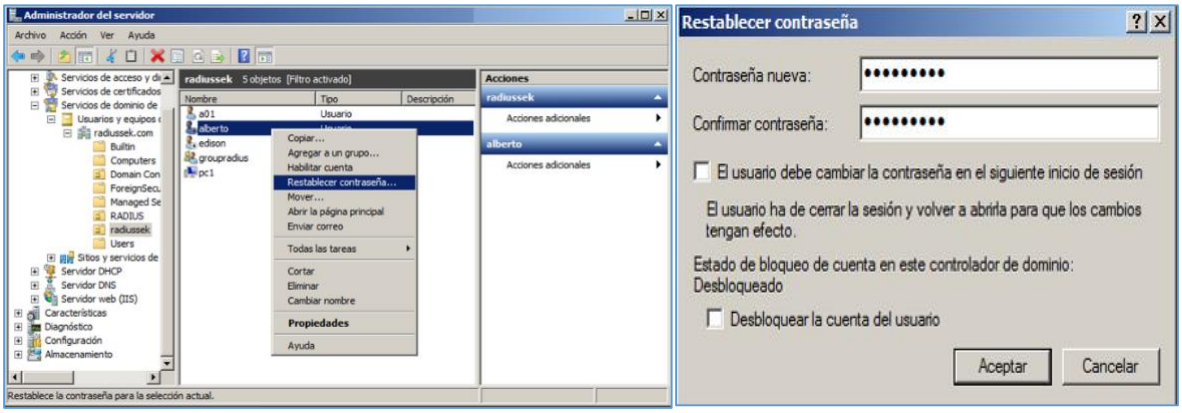
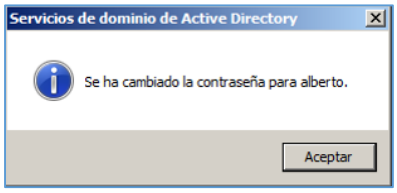


Fig. 49



Como la institución requiere registrar todos los usuarios existentes, se recurre a un proceso de carga masiva mediante un script que contenga los atributos básicos. La información del total de usuarios existentes se tomara de la base de datos en SQL Server. El script puede incluir todos los usuarios requeridos y ser ejecutado mediante un proceso de ejecución por lotes (batch).

Script alternativo para ser ejecutado desde una consola de comandos.

Fig. 50