UNIVERSIDAD CATOLICA DE SANTA MARIA

FACULTAD DE CIENCIAS E INGENIERIAS FISICAS Y FORMALES

ESCUELA PROFESIONAL DE INGENIERIA DE SITEMAS

METODOLOGIA PARA EL DISEÑO DE UNA RED LAN INALAMBRICA 802.11 n/ac CON SERVIDOR RADIUS PARA LA GERENCIA REGIONAL DE SALUD-AREQUIPA

Tesis presentada por el Bachiller:

- **Martín Fernández Rivera**

Para optar el Título Profesional de:

INGENIERO DE SISTEMAS

Asesor:

Ing. Jose Sulla Torres

AREQUIPA - PERÚ, 2016

PRESENTACION

Sra. Directora de la Escuela Profesional de Ingeniería de Sistema

Sres. Miembros del Jurado

De conformidad con las dispociones del reglamento de Grados y Titulos de la Escuela Profesional de Ingeniería de Sistemas, pongo a vuestra consideración el presente trabajo de investigación titulado: "METODOLOGIA PARA EL DISEÑO DE UNA RED LAN INALAMBRICA 802.11 n/ac CON SERVIDOR RADIUS PARA LA GERENCIA REGIONAL DE SALUD-AREQUIPA", el mismo que de ser aprobado me permitirá optar por el Título Profesional de Ingeniería de Sistemas.

Fernández Rivera, Martín

AGRADECIMIENTOS

Todos lo conseguido hasta este momento y lo que se me avecinan en el futuro tendrán como responsable a la universidad Católica de Santa María por haberme aceptado a ser parte de ella para poder estudiar mi carrera, así como a los diferentes docentes que me brindaron sus conocimientos y su apoyo para seguir adelante día a día.

Agradezco especialmente a mi Asesor de Tesis al Ing. Jose Sulla por haberme brindado la oportunidad de recurrir a su capacidad, conocimiento y experiencia, además de haberme tenido la paciencia de guiarme durante todo el desarrollo de la tesis.

Mi agradecimiento también va dirigido a la Gerencia Regional de Salud Arequipa GERESA, especialmente al Dr. Omar Huarachi por haber aceptado que realizar mis prácticas profesionales y posteriormente mi tesis sobre esta institución.

DEDICATORIA

Dedico este pequeño triunfo en mi vida a mis padres Daniel Fernández y Andrea Rivera quienes con todo su esfuerzo han logrado que culmine esta etapa de mi vida y sobre todo darle las gracias desde el fondo de mi corazón por haberme apoyado en los diferentes momentos de mi vida desde mis logros hasta mis fracasos y por siempre estar ahí junto a mí.

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

Ante la problemática de falta de espacio físico, el hacinamiento y alto índice de rotación del personal que sufre la Gerencia Regional de Salud Arequipa, se propone una metodología para el diseño de una red de área local inalámbrica que incorpore los protocolos de comunicación 802.11 n/ac y el protocolo de autenticación, autorización y contabilización Radius, con el fin de suplir las necesidades que presenta la institución, todo esto bajo un diseño de investigación documental.

Identificando los recursos de hardware y software que posee la institución lo cual es base para diseñar la nueva red inalámbrica. Se procede a listar los equipos necesarios a ser adquiridos los cuales tienen que tener compatibilidad con los diferentes protocolos en cuestión, también se hace uso del Windows Server 2012 R2 que ya está incorporado en la institución para habilitar el protocolo Radius en dicho servidor además de usar el Directorio Activo para ser adaptado al nuevo diseño de la red una vez se tenga todos estos requerimientos se procede a diseñar y configurar la nueva red, se optó por la simulación para demostrar cómo tienen que ser configurados los diferentes equipos de comunicación que va ser parte de la red y finalmente se establece en la investigación una simulación del uso metodología para realizar el diseño de la red inalámbrica, el cual fue probado mediante el uso del Cisco Packet Tracer, con lo cual se permitió analizar, implementar y probar la aplicabilidad de la metodología. Los resultados de esta metodología se lograron medir mediante la valoración que le dio un grupo del personal de la institución y toda el área de soporte, llegando a obtener un grado de aceptación por arriba del 70%. Con lo que se comprobó que la metodología puede ser aplicada en otros entornos similares.

ABSTRACT

The problems of lack of physical space, overcrowding and high rate of staff turnover experienced by the "Gerencia Regional de Salud Arequipa", it proposes develop a methodology for the design of a wireless local area network that incorporates the communication protocols 802.11 n/ac and the protocol of authentication, authorization and accounting Radius, in order to supply the needs that have the institution, all under a design documentary research.

By identifying the hardware and software resources that the institution owns, which is the base for designing the new wireless network. It proceeds to list the necessary equipment to be acquired, which must have compatibility with different protocols in question, in addition it uses the Windows Server 2012 R2 that is already incorporated into the institution to enable the Radius protocol on that server, besides using the Active Directory to be adapted to the new network. Once it accomplishes all these requirements, it proceeds to design and configure the new network. It chose the simulation to show how it must be set the different computers in the network. This was achieved by using different software. Finally, it sets in the research a simulation by using a methodology for the design of the wireless network, which it was tested using the Cisco Packet Tracer, which was allowed to analyze, implement and test the applicability of the methodology. The results of this methodology were achieved by assessing measure that gave a group of staff of the institution and all technical support area, obtaining an acceptance degree above 70%. So it found that the methodology can be applied in other similar environments.

INTRODUCCIÓN

Es indiscutible que estamos inmersos en un mundo dominado por las tecnologías de comunicación lo cual se debe al desarrollo de la Internet. Por tal motivo, se ha vuelto esencial el incremento de la infraestructura tecnológica en el ámbito empresarial, ya sea para las redes convencionales como para las redes inalámbricas. Sin embargo, una gran parte de las empresas no toman en cuenta que estas infraestructuras precisan de un mantenimiento constante para que no sufran vulnerabilidades o queden obsoletas ante las nuevas tecnologías emergentes, para lo cual se precisa implementar un sistema de control de acceso a la red que permita proteger la información como también tratar de tener lo último en tecnología lo cual va representar una ventaja competitiva y un mejor desempeño de las actividades de la empresa.

La motivación para llevar a cabo este proyecto es la problemática actual que adolece la red de la Gerencia Regional de Salud Arequipa, para lo cual es necesario mencionar las causas. Una de ella es que la red que no cumple con ningún estándar de cableado estructurado, llegando al punto de considerarla una red subestándar con serias deficiencias desde todos los puntos de vista del cual se quiera analizar. Otras de las causas a esta problemática son el hacinamiento de personal existente y el alto índice de rotación de personal temporal, lo cual repercute directamente en la red originando que esta ya no pueda ser escalable por la alta demanda de puntos de red por parte de los usuarios, así como falta de control del correcto uso de la red lo que da como resultado que existan serios problemas en la seguridad de información, además un inconveniente que existe es el no correcto uso de Directorio Activo lo cual trae como consecuencia que las diferentes direcciones que conforman la institución se manejen de manera independiente.

La presente tesis busca diseñar una red inalámbrica que cuente con los protocolos de comunicación 802.11n y 802.11ac, el primero de estos es el más comercial actualmente mientras que el otro es el nuevo protocolo de comunicación inalámbrica. Para poder manejar esta red inalámbrica se recurrirá al protocolo Radius para proporcionar autenticación centralizada, autorización y contabilidad de la red inalámbrica, para tal propósito esta metodología se va adecuar a la realidad de la Gerencia Regional de Salud Arequipa y suplir todas las deficiencias que presenta su red alámbrica.

El presente trabajo está estructurado de acuerdo a la siguiente alineación: En el capítulo I se detalla las problemáticas que presenta la red y la urgencia de cambiar a una red inalámbrica que cumpla con todos los requerimientos de la Institución. En el capítulo II se presentan trabajos relacionados los cuales se toman como muestra para esta tesis y la base teórica necesaria para llevar acabo la misma. En el capítulo III abarca el marco metodológico. Así como los lineamientos generales para realización de la tesis. En el capítulo IV es el desarrollo del diseño de WLAN para la Gerencia Regional de Salud Arequipa, para lo cual se presentan diferentes tipos equipos que posean los protocolos 802.11n/ac, para que seguidamente se segmente la red en VLANs y con eso poder realizar la planificación de la ubicación de los puntos de acceso mediante un simulador, finalmente realizar la simulación de la integración del protocolo Radius con la red inalámbrica.

CAPITULO 1

METODOLOGIA PARA EL DISEÑO DE UNA RED LAN INALAMBRICA 802.11 n/ac CON SERVIDOR RADIUS PARA LA GERENCIA REGIONAL DE SALUD-AREQUIPA

1.1. Caracterización del Problema

Es innegable que hoy en día todas las organizaciones fuera el que sea su rubro posean equipos informáticos y medios de comunicación que son usados para facilitar el desarrollo de los diferentes procesos, actividades internas, compartir información, recursos y ofrecer servicios con lo cual se permite a los usuarios desarrollar sus actividades diarias. Con el transcurrir del tiempo toda organización tiende a volverse más compleja, para lo cual es indispensable que las organizaciones sean más eficientes y efectivas en el manejo de los diferentes recursos que posean, facilitando la integración del personal en grupos de trabajo, siendo esencial de una comunicación continua entre los responsables y los ejecutores de las actividades, de esta forma de realizar el diseño constituye un estilo de realizar las cosas. Pero siendo más exigentes este simple estilo tiene que formalizarse agregando un adecuado control y reglas para la ejecución. Obteniendo como resultado de todas estas etapas una metodología concreta en el diseño de una red.

El uso de metodologías abarca mucho más que la simple ejecución en estudios, brinda a las diferentes áreas tecnológicas la posibilidad de garantizar que los objetivos se cumplan de manera correcta además de permitir organizar adecuadamente las diferentes fases de un proyecto, indicando cuales son las herramientas que se va emplear, facilitando el uso de lista de revisión, mediante estas se pude verificar si la información con la que se cuenta es la

necesaria para poder dar por concluida una fase del proyecto y avanzar a la siguiente. Específicamente en redes informáticas, el uso de metodologías ha permitido constituir de una forma planificada y sistemática las diferentes etapas para diseñar una red, comenzando con el diseño físico y lógico de la red, teniendo en consideración los criterios respecto a la distancia que va abarcar la red, el tipo de arquitectura que se va emplear, el tráfico de datos al cual va ser expuesta la red, la administración de hardware y software, el tipo de enlaces de datos, la capacidad de escalabilidad de la red, entre otros factores.

De acuerdo a todo lo anteriormente mencionado es que surge la idea de proponer una metodología para diseñar una red inalámbrica que se ajuste solucionar la problemática de la red alámbrica de la Gerencia Regional de Salud Arequipa, donde se realizó prácticas profesionales ya que se observa que no existe una metodología que integre soluciones al momento de diseñar una red, por tal motivo esta metodología va consistir en diseñar una red inalámbrica que integre los protocolos de comunicación 802.11 n/ac y el protocolo Radius, lo que también va servir para medir el funcionamiento de esta metodología para solucionar una problemática existente.

1.2. Objetivos de la Investigación

1.2.1. Objetivo General

Proponer una metodología para el diseño de una red inalámbrica para la Gerencia Regional de Salud Arequipa que cuente con los protocolos de comunicación 802.11n/ac y con el protocolo de autenticación, autorización y contabilización Radius.

1.2.2. Objetivos Específicos

1. Diseñar la estructura de la metodología (fases, procesos y tareas) basándose en suplir las deficiencias de la red actual de la GERESA.

2. Analizar las diferentes necesidades de los usuarios respecto al uso de la red recolectado información para su posterior uso.

3. A partir de la información obtenida de las necesidades de los usuarios diseñar una red que mejore la infraestructura actual de la red.

4. Desarrollar cada fase de la metodología propuesta, documentando la configuración total de los equipos.

5. Demostrar la aplicabilidad de la metodología mediante simulación de la red.

1.3 Preguntas de Investigación

Teniendo en cuenta el problema anteriormente planteado surge las preguntas que da inicio al desarrollo y ejecución de este proyecto las cuales son:

- ¿Cuáles son las necesidades de los usuarios de la red de la GERESA?
- ¿Qué tipo de tecnologias son las que son necesarias incorporar al diseño de la red?
- ¿Cómo soluciona el nuevo diseño las deficiencias de la red?

1.4. Línea de Investigación.

Redes y Telemática.

1.4.1 Sub-líneas de Investigación

1. Redes inalámbricas.
2. Metodologías y Técnicas para el desarrollo de servicios en Red.

1.5 Solución Propuesta

1.5.1 Justificación del estudio

La importancia de contar con una red de computadoras que comparta información, recursos y ofrezca servicios es un tema muy importante para aumentar la productividad de los usuarios dentro de una organización en el que se han dedicado grandes esfuerzos. A pesar de que este trabajo es un tema conocido, no es muy común las redes de computadoras totalmente inalámbricas, estableciendo un mejor manejo y control de los equipos que están dentro de la red. Los beneficios que se obtiene son:

1. Eliminación de las barreras físicas para la empresa.
2. Reducción de paros por problemas en la red.
3. Reducción del tiempo de respuesta para los usuarios del seguro integral de salud.
4. Mejora del servicio a los usuarios e incrementar la confianza en el SIS.

Esta son las razones principales para que se lleve a realizar el presente proyecto.

1.5.2. Descripción de la Solución

Lo que se desea es implementar una metodología para diseñar una red LAN inalámbrica con los protocolos 802.11 n/ac y que a su vez sea administrada mediante un servidor Radius que va correr en una plataforma Windows server 2012 r2, lo que se pretende es dar a conocer los equipos de hardware que cumplan con ambos requerimientos y se da a conocer las ventajas y desventajas de ambos, siendo los representantes de la gerencia regional de salud decidan cual es el que se ajusta más a sus necesidades actuales y futuras motivo por el cual se está realizando la presente tesis y a su vez demostrar mediante simulación que la propuesta es viable para llevarse a cabo a gran escala configurando un servidor Radius para que administre la conexión de los diferentes usuarios a red institucional mediante un wireless LAN Controller. Para lograr este objetivo se realiza una recopilación de las tecnologías que van hacer usadas:

TECNOLOGIA	USO
Directorio Activo	Identificación y Control de Cuentas
Radius Server	Políticas de control de acceso a la Red
Switches y Access Point	Asignación dinámica a VLAN(802.1X)

Tabla 1.1 Requisitos Tecnológicos.

Fuente: "Elaboración propia"

CAPITULO 2

FUNDAMENTOS TEÓRICOS

2.1. Estado del arte

2.1.1 Diseño e implementación de una red LAN Y WAN con sistema de control de acceso Mediante Servidores AAA. (2012)

- **Autores:**
  - Nuttsy Aurora Lazo García.

- **Objetivos:**
  - Diseño e implementación de una red LAN (Local Área Network) y WLAN (Wireless Local Área Network) con sistema de control de acceso AAA (Authentication, Authorization and Accounting).
  - Implementar el servidor IAS de Windows para lo que concierne a WLAN, luego verificar que el punto de acceso inalámbrico (Access Point - AP) cumpla con el estándar de autenticación IEEE 802.1x

- **Conclusiones:**
  - Se comprobó que los protocolos AAA RADIUS y TACACS+ tienen diferentes características en el manejo de autenticación y autorización. El protocolo RADIUS maneja ambos servicios de manera combinada, mientras que el protocolo TACACS+ los ofrece como servicios independientes. A pesar de ello fueron implementados en una misma red y coexisten para brindar una red con sistema de control de acceso robusto.

- Al culminar con la implementación del presente proyecto se pudo concluir que, gracias al servidor RADIUS, un usuario inalámbrico puede autenticarse e ingresar a la red; asimismo, el servidor TACACS+, teniendo como base el nivel de privilegio del usuario, permite a este ingresar o no a los equipos de red para realizar configuraciones en los equipos. [1]

- **Análisis:**

  La información obtenida nos muestra una gran robustez y escalabilidad en el uso de Radius Server para tecnología inalámbrica, no obstante, esta fue un diseño general, lo que lleva hacer un análisis más profundo en temas de uso para el caso de organización del estado.

2.1.2 Diseño e implantación de una red inalámbrica unificada en el colegio nuestra señora de Fátima de Valencia. (2015)

- **Autores:**

  José María Murillo Safont.

- **Objetivos:**

  - Dar cobertura a toda aquella zona del centro utilizada por el alumnado, personal docente y de administración, con fines académicos y laborales, respectivamente.
  - Gestionar de forma centralizada todos los puntos de acceso, usuarios, cortafuegos, niveles de acceso, filtros, etc.

- **Conclusiones:**

  - Se consigue dar cobertura Wifi a gran parte del centro, utilizada en su mayor medida por alumnado, personal docente y de administración. Se garantiza una velocidad de conexión de calidad y lo que es más importante, ofrece una alta seguridad y fiabilidad.

  - Se puede gestionar de forma centralizada todos los puntos de acceso, usuarios, cortafuegos, perfiles de usuarios, filtros, etc., por lo que supone un ahorro considerable de tiempo para las personas encargadas en esas tareas de administración de la red o de solución de incidencias técnicas. [2]

- **Análisis:**

La experiencia recolectada nos indica que una red wifi puede ser muy útil para una pequeña y mediana empresa brindado todas las mismas competencias que una red cableada y con la ventaja de la movilidad, también que es un tipo de red fácilmente administrable y que brinda todo tipo de personalización de acuerdo a las necesidades de cada entorno donde va ser implementada.

2.1.3 Metodología ágil para el diseño y desarrollo de redes de Área Local (LAN). (2014)

- **Autores:**

  - Guía Adriana.

- **Objetivos:**
  - Proponer una metodología ágil para el diseño y desarrollo de redes de área local (LAN) tomando en consideración, las necesidades de la organización, el hardware y el software existente, el área de cobertura, las políticas de uso y la seguridad de la red.
  - Establecer las limitaciones y deficiencias presentes en las metodologías convencionales para el desarrollo de redes LAN mediante la contratación de datos.

- **Conclusiones:**

  - La utilización de metodologías permite en campos tecnológicos asegurar la obtención de resultados satisfactorios en la ejecución de diferentes tipos de proyectos, pudiéndose con ellas: administrar las fases del proyecto, propone las herramientas a utilizar, verificar si se dispone de la información necesaria, establece las funciones, las responsabilidades y las tareas encomendadas a cada miembro del equipo de trabajo. Su aplicación para diseñar y/o desarrollar redes informáticas, permiten establecer un marco de trabajo a través de una serie planificada de pasos para la realización del diseño lógico y físico de la red, tomando en consideración las distancias que son posible cubrir, el medio de transmisión y la topología que se utilizará, el tráfico al que la red será expuesta, la calidad de los enlaces, la administración de los equipos, y sobre todo su funcionalidad y capacidad para poder crecer con el tiempo, alcanzándose así la optimización de los recursos disponibles, junto a la obtención de un diseño eficiente y confiable.

- En tal sentido el proceso de selección de la metodología de diseño no es algo fácil o que puede tomarse a la ligera ya que se debe encontrar una metodología adecuada a la cual adaptar su proyecto , sin embargo, por sencillo que esto parezca, no es algo fácil de realizar debido a que existe poca documentación sobre las metodología que pueden ser implementadas, además se debe tomar en consideración que algunas de estas metodologías están diseñadas para proyectos de redes de gran envergadura lo cual hace que sea muy difícil adaptar las fases planteadas en estas metodologías con la características del proyecto que se desea desarrollar, inclusive en algunos casos se tienen fases o actividades que retrasan con el proceso de diseño debido a que están dirigidas. [3]

- **Análisis:**

El conocimiento adquirido es que para el diseño de una Metodología Ágil para Construcción de Redes de Área Local no es algo sencillo o que pueda tomarse muy a la ligera ya que se debe buscar la metodología correcta la cual adaptar dependiendo el escenario, además, se debe tener en cuenta algunas consideraciones ya que estas metodologías están diseñadas para proyectos de redes de gran envergadura lo que hace más compleja adaptarlas a las etapas establecidas en estas metodologías con las características del proyecto que se pretende desarrollar.

2.1.4 The IEEE 802.11 Universe. (2010)

- **Autores:**
  - Guido R. Hiertz
  - Dee Denteneer, Philips

- Lothar Stibor and Yunpeng Zang
- Xavier Pérez Costa
- Bernhard Walke

Como el primer proyecto que tiene como objetivo la tasa de datos se mide en la parte superior de la capa MAC, 802.11n proporciona una experiencia de usuario comparables a la conocida Fast Ethernet (802.3u). Mucho más allá de los requisitos mínimos que se derivaron de velocidad de datos máxima del modelo con cable de 100 Mb/s, 802.11n proporciona hasta 600 Mb/s. Su característica más destacada es la capacidad de múltiples entradas y múltiples salidas (MIMO). Un concepto MIMO flexible permite para a las matrices de hasta cuatro antenas la multiplexación espacial o de formación de haz. Su innovación más debatida es el uso de canales de 40 MHz opcionales. Aunque esta característica ya estaba siendo utilizado como una extensión propietaria de las tarjetas inalámbricas con los protocolos 802.11a y 802.11g, que provocó un amplio debate sobre el solapamiento de sus vecinos. Especialmente para la banda de 2,4 GHz, se expresaron preocupaciones de que la operación de 40 MHz afectaría severamente el rendimiento del existente 802.11 con Bluetooth (802.15.1), ZigBee (802.15.4), y otros dispositivos. El desarrollo de un compromiso, que no permite la canalización de 40 MHz para dispositivos que no pueden detectar 20 MHz, impidió la ratificación de 802.11n hasta septiembre de 2009. Como consecuencia de la operación de 20/40 MHz y diversas configuraciones de antena, 802.11n define un total de 76 diferentes MCS. Dado que varios de ellos ofrecen velocidades de datos similares, 802.11n son compatibles con las mejoras de acceso al medio que introducimos en la sección MAC. [4]

- **Conclusión:**

El estándar 802.11-2007 y sus modificaciones proporcionan un amplio conjunto de funciones para la comunicación inalámbrica. 5, 10, 20, y 40 MHz de ancho de banda de canal en los 2,4, 3,65, y 4.9-5 bandas de frecuencia GHz soporta una amplia gama de dominios reguladores. Además, el 802.11 MAC ha demostrado ser lo suficientemente flexible para expandirse desde sus segmentos de mercado ancestrales. Mientras que las redes 802.11n y malla extienden aplicaciones conocidas, gama amplia (802.11y) y la comunicación vehicular (802.11p) se abren nuevos escenarios para la WLAN. Pero la cantidad cada vez mayor de modificaciones también hace que sea más y más difícil de mantener un nivel de cohesión. El trabajo sobre las últimas modificaciones tiende a tomar más tiempo que los que están en el pasado. Sin embargo, no hay alternativa a la popular, barato y flexible de la tecnología 802.11 es visible todavía. Muy por el contrario, impulsado por las múltiples necesidades de los clientes, el universo 802.11 continúa expandiéndose.

- **Análisis:**

Conociendo más sobre la evolución del protocolo 802.11 que es el usado para la comunicación inalámbrica, el cual usaremos para la implementación de la red inalámbrica mediante dos versiones de este protocolo las cuales son la que actualmente está en apogeo que es el 802.11 n y dejando la posibilidad que se pueda migrar a una tecnología que de aquí unos años será el nuevo estándar usado para las comunicaciones inalámbricas el cual es 802.11 ac, adicionalmente los equipos que se pretende implementar trabajan con ambos formatos lo cual queda para decisión de la GERESA cuál de los dos protocolos se ajusta a la necesidades requeridas.

2.1.5 IEEE 802.11ac. (2013)

- **Autores:**
    - Javier Meden Peralta

La primera de las novedades es que la velocidad de transmisión es mucho mayor, alcanzando los 1.3 Gbps gracias al movimiento de información vía tres flujos de 433Mbps cada uno. Por su velocidad, el estándar también se conoce como Wi-Fi 5G o Wi-Fi Gigabit. El radio de cobertura es más amplio, hasta un máximo de 90-100 metros, que es lo que el consumidor reclama con más frecuencia de este tipo de conexiones. 802.11ac funciona en la banda de 5 GHz, que ofrece más canales sin interferencias, y esta menos poblada", por lo tanto, aporta una mayor estabilidad a la conexión, y un mayor radio de funcionamiento. Junto a la nueva banda llega también el uso del beamforming, tecnología que permite a los Routers y Puntos de Acceso dirigir las ondas de radio de una forma más precisa, mejorando la recepción. Otras mejoras consisten en la ampliación del ancho de banda hasta 160 MHz (40 MHz en las redes 802.11n), hasta 8 flujos MIMO (4 en 802.11n) y modulación de alta densidad, 256-QAM (64-QAM en 802.11n). En el campo de las redes multimedia, esto nos asegura que podríamos reproducir en streaming dentro del hogar cualquier archivo de alta definición sin compresión, cualquiera que sea su bit Rate, como las resoluciones 4K que requieren un ancho de banda bastante más alto. También se podrían transferir películas calidad HD en un tiempo inferior a los cuatro minutos. Su uso también está recomendado para juegos en red y aplicaciones y servicios de audio bajo demanda o VozIP. A continuación, se verán los detalles de esta nueva versión del protocolo 802.11 y su comparación con los demás estándares. [5]

- **Conclusión:**

Hemos visto que el estándar IEEE 802.11ac trae consigo varias novedades y mejoras. Lo más destacable es su velocidad de transmisión, que supera los 1 Gigabit por segundo. Estamos hablando de una conexión inalámbrica más rápida que por cables, comparando con el estándar Ethernet. Con esta tecnología Wi-Fi, es posible reproducir en streaming videos de alta definición y transferir películas en un instante. Además de su excelente performance para juegos en red y aplicaciones que requieran un alto ancho de banda. También aumenta el radio de alcance de hasta los 100 metros, lo suficiente como para cubrir toda una casa. Gracias a la utilización de la banda menos saturada de 5 GHz, la tecnología Beamforming que dirige las ondas de radio de manera más precisa, y la utilización de varias antenas de transmisión con la técnica MIMO, es que la nueva versión 802.11ac logra sus objetivos, brindando una mejor calidad de conexión a los usuarios. Creo que esta tecnología va por un muy buen camino, ya que los nuevos productos que la implementan son compatibles también con las versiones anteriores de 802.11 que aún están siendo utilizadas.

- **Análisis:**

El protocolo 802.11 ac que es el protocolo que es el próximo a implementarse en el mercado, cuando vean por conveniente pondrán cambiar la configuración de los equipos para que trabajaren bajo ese estándar o también por un tema de evitar la saturación que existe en el canal de 2.4 GHz que se ve en nuestra realidad y de esa manera evitando el solapamiento al usar los 5 GHz del estándar 802.11 ac, teniendo una mejor señal y menos interferencia lo cual tiene ciertas ventajas competitiva por la velocidad que ofrece para la trasmisión de datos, los cuales son una cantidad considerable que la red actual suple con cierta deficiencia.

2.1.6 Integración red wired – Wireless. (2012)

- **Autores:**
    - Francisco García Moreno

Una de las definiciones que encontramos para la palabra integración es: "acción y efecto de incorporar algo en un todo". En nuestro caso, asimilamos "el todo" a nuestro concepto de Red empresarial, y nos centramos en solventar los problemas que nos plantearán las distintas formas de acceso a la misma. Esta palabra, Red, engloba a su vez infinidad de conceptos: segmentación en redes virtuales (las llamadas VLANs), tipos de acceso (p.e mediante cableado estructurado o medios aéreos –Wifi-) o distintos perfiles de usuarios y sus dispositivos. Todo esto hace que el concepto de Red no sea único, ni independiente en cada situación, y que, por lo tanto, genere en muchas ocasiones confusión entre los usuarios y los propios responsables de los departamentos de Tecnologías de la Información (TI).El caso más habitual, hoy en día, se produce cuando un trabajador solicita trabajar con la aplicación empresarial mediante su propio portátil o dispositivo personal... Cubrir esta y otras situaciones es, para el departamento de TI, un gran reto ya que siempre debe adaptar y garantizar los servicios de la Red y adoptar como propios dispositivos ajenos a la empresa, en ocasiones tecnológicamente más avanzados que los que la propia compañía puede ofrecer. Bring Your Own Device (BYOD) es el nombre que define este fenómeno y al que infinidad de compañías están tratando de dar respuesta. [6]

- **Conclusión:**

Se realizó un análisis previo de qué tecnologías había disponibles para desarrollar una solución de este tipo. Localizando muchas empresas que están ofreciendo soluciones propias que,

aunque algunas pueden estar basadas en un estándar abierto, finalmente se ve la imperiosa necesidad de tener que instalar programas y sistemas propietarios tanto en el apartado servidor como en el lado del cliente. Sin embargo, este tipo de soluciones propietarias también nos ofrecen una gran ventaja, y es el valor de ser instalaciones "llave en mano", es decir, ofrecen una puesta en marcha del sistema muy rápida, y un control de todos los mecanismos de seguridad implicados mediante un único punto de gestión. Aun con este valor añadido, también se encontró que las soluciones de este tipo limitan el escalado o integración con otros dispositivos o tecnologías que no estén aceptados por dichas compañías, por ejemplo, algunas de ellas usan un sistema propio de cuentas de usuarios basado en una base de datos propia. Estos inconvenientes decantaron por buscar una solución que estuviera basada en estándares y protocolos abiertos, eligiendo 802.1X como piedra angular de todo el proyecto.

- **Análisis:**

El presente trabajo es una base para la creación de una metodología para diseñar una red inalámbrica con dos diferentes tipos de protocolos y a su vez que este administrada mediante un servidor Radius, ya que podemos ver como es la implementación de una red en la cual debe cableada e inalámbrica a su vez, en el entorno de una empresa multidisciplinar que brinda acceso, a sus sistemas, de una cantidad indeterminado de usuarios que, además, deben poseer una clasificación por distintos niveles de seguridad en ese acceso. Este proyecto cubrirá la integración de ambas redes y, sobre todo, el control de dichos diferentes accesos con políticas aplicables en todos los posibles escenarios. Como modelo se usó una red empresarial, que abarca distintos departamentos, centros y edificios. La situación de partida será una segmentación a nivel de VLAN, y una configuración de los clientes y equipos, en las distintas redes.

2.1.7 Implementación del control de acceso a la red mediante los protocolos de autenticación, autorización y auditoría. (2013)

- **Autores:**
    - José R. Arana
    - Leandro A. Villa
    - Oscar Polanco

Este artículo presenta el diseño e implementación de un sistema de control de acceso a la red que proporciona el servicio de Autenticación, Autorización y Auditoría (AAA) usando software libre, empleando los protocolos estándar IEEE 802.1x y RADIUS, con base en una infraestructura de clave pública, un servicio de directorio centralizado que almacena las políticas de seguridad para cada usuario y una base de datos MySQL en donde se registran los eventos del servicio AAA; todo esto se probó en un ambiente corporativo con 300 estaciones de trabajo. En el sistema se logró: tres métodos de autenticación mediante el uso de EAP-TLS, PEAP y EAP TTLS; la administración segura de la información, concerniente a los usuarios que pueden acceder la red y los permisos que cada uno de ellos posee; el uso de certificados digitales para demostrar la identidad de un usuario o de un equipo que ejecute cualquiera de los sistemas operativos más populares. También se ha configurado un servidor RADIUS para que use dos puntos de información de políticas; un servidor de directorio OpenLDAP y el Directorio Activo de Microsoft. [7]

- **Conclusión:**

Fue posible configurar tres tipos de autenticación en el servidor de autenticación, usando en uno de estos, la infraestructura de clave pública completa (EAP-TLS) y, en los otros dos, un

esquema de credenciales basado en el nombre de usuario y la contraseña (EAP-PEAP, EAP-TTLS), con certificados de identificación personal en los servidores de autenticación, lo que permite realizar autenticación mutua, haciendo muy seguro el acceso a la red. Al tener una infraestructura de clave pública implementada, fue posible revocar los certificados de identificación personal de usuarios que no se desea que ingresen a la red, ya sea porque han dejado de formar parte de la empresa o porque sus certificados han sido robados o comprometidos. Se demostró que, si un usuario presenta un certificado de identificación personal revocado, el acceso a la red le será denegado. El acceso de los usuarios a la red con sistema AAA se probó con los sistemas operativos más populares disponibles; estos fueron: Windows en las versiones XP, Vista y 7, MAC OSX versiones 10.5 a 10.6 y Ubuntu en la versión 10.4.

- **Análisis:**

Se rescata de este proyecto que para diseñar e implementar el prototipo de una red TCP/IP que tenga como objetivo principal brindar el servicio AAA de manera escalable permitiendo: poseer múltiples métodos de autenticación según las políticas de red que se desea incorporar, mediante el uso de EAP-TLS, PEAP y EAP TTLS; pudiendo consultar información, en una base de datos central, acerca del tipo de usuarios que pueden acceder la red y el permiso que posee; Así mismo el uso de certificados digitales para demostrar la identidad del usuario o de un equipo. Este diseño considera un aislamiento robusto entre los equipos a ser autenticados para poder ingresar a la red y los servidores que proveen el servicio AAA, para que la red sea tolerante a fallas de conectividad, principalmente los equipos que tienen el Directorio de usuarios y el Servidor RADIUS lo cual va ser un modelo para la implementación del sistema de seguridad del Servidor Radius mediante el servicio AAA que se pretende implementar.

2.1.8 Autenticación de usuarios en el Active Directory utilizando servidor Radius a través de servicio de autenticación de internet. (2007)

- **Autores:**
    - Fabiano Marcelino Souza

Este documento presenta los conceptos de estructurar un entorno inalámbrico seguro a través del protocolo RADIUS, la integración de la autenticación con Active Directory, implementado por el Servicio de autenticación de Internet (IAS). Se trata de integrar el acceso Wifi a través de una red corporativa segura. Entre los conceptos presentados hay una introducción a los protocolos inalámbricos de acceso y autenticación y, las ventajas de cada protocolo. También se presenta información sobre el Active Directory, el dominio del Servicio de autenticación de Internet, RADIUS y Wifi. Además, todavía, explica el funcionamiento de todo el proceso de autenticación utilizando una manera conceptual, demostrando cada tecnología presentada. El documento incluye, además de la teoría, la forma de implementar, así como también describe cada herramienta incluida en el proceso, que termina con las pruebas para idealización de este trabajo. Hay varias posibilidades para el proceso de autenticación segura, pero en la mayoría de casos, la protección hace que sea difícil el acceso y la gestión. La más eficiente que la mayoría de las empresas hoy en día usan es una autenticación única, integrada, que proporciona acceso a diversos servicios y con la seguridad necesaria, evitando así que la intercepción o robo de información. [8]

- **Conclusión:**

En este trabajo presento inicialmente el concepto de protocolos de red, que detalla el modelo de capas, con la finalidad de conseguir el conocimiento necesario para comprensión e implementación, posibilitando una posterior administración centralizada y segura. Siguiendo

esta línea fueron presentados los términos, conceptos y los distintos tipos de protocolos de autenticación de los protocolos inalámbricos, detallando el acceso a través de Wifi, los tipos de transmisión, una noción de las redes inalámbricas de área local, metropolitana e incluso Bluetooth. También se demostró las ventajas de la autenticación de las redes inalámbricas, como la movilidad, el bajo coste de la infraestructura de red, rapidez de instalación, los factores que han llevado a las empresas a adoptar esta tecnología. Se abordan los diferentes tipos de tecnologías utilizadas, la conceptualización de ellas a fin de aclarar la función de cada tecnología en el proceso, ya que se utilizarán varias herramientas, pero con diferentes propósitos para el proyecto.

- **Análisis:**

La relación que existe entre este proyecto con el que se desea realizar es como la función del Servicio de autenticación de Internet, que es la implementación de Microsoft de un servidor RADIUS, frente a los conceptos de protocolo para redes inalámbricas, como el del proceso de autenticación, centrándose esta manera de trabajar, también se describe en la fidelidad inalámbrica (Wi-Fi), ya que este será el medio de comunicación y de acceso utilizado. Con conceptos adecuadamente definidos, se analizaron, se aplica y herramientas que permiten la autenticación de usuarios en Active Directory, utilizando el servidor Radius a través del Servicio de autenticación de Internet y lo más importante a rescatar es que todo esto describe y aclara de una forma que es posible implementar a un administrador de red.

2.1.9 Control de Acceso en segmentos de red para los usuarios autorizados en un entorno corporativo. (2011)

- **Autores:**
    - Luciano Antonio Wolf

En este artículo describe el uso del protocolo 802.1X para garantizar que sólo los usuarios debidamente registrados tienen acceso a una red corporativa. Sólo los usuarios que poseen los ajustes locales de acuerdo con las reglas pre-establecidas y configurados usando el protocolo 802.1X tendrán acceso a la red autorizada. El protocolo se basa en la autorización de acceso en el nivel físico, asegurando que ningún atacante puede obtener una dirección IP y así unirse al segmento de red y por lo tanto puede tener acceso a los servicios disponibles en el entorno. Uno de los principales problemas que se plantean en la tecnología de la información es el factor de seguridad, que debe reportar como uno de los factores más críticos es la información sensible ya que se puede ser obtenida por los intrusos. Hay varias herramientas y tecnologías para prevenir que este tipo de datos no sean obtenidos de manera ilegal a través accesos externos, sin embargo, un error frecuente es el descuido de los accesos interno por los segmentos de red lógicas que pueden comprometer los niveles de seguridad implementados. Una forma eficiente para garantizar el acceso físico a los segmentos lógicos dentro de una red corporativa, es la implementación del protocolo IEEE 802.1X para los usuarios autorizados. La misma garantía de dicho acceso mediante la validación entre elementos de red y estaciones de trabajo de los usuarios. Estos enfoques pueden ser a través del switch para las conexiones cableadas y para el acceso inalámbrico atreves de los access point (AP). [9]

- **Conclusión:**

Con la implementación del protocolo 802.1x en el entorno simulado, fue posible resolver el problema del acceso físico no autorizado a un segmento de red corporativa. Las pruebas simuladas acceso a este entorno son similares a un entorno real. Con la restricción de acceso no autorizado, siempre desde el segmento de red local, puede asegurarse de que un atacante no puede conectarse físicamente a los segmentos disponibles para este ambiente, protegiendo los diferentes servicios. La función de protocolo 802.1X es asegurar que todos los puertos físicos disponibles para el acceso a la red de manera alámbrica o inalámbrica, son supervisados por el servidor RADIUS, lo que obliga a todos los usuarios del que van usar la red a tener sus estaciones de trabajo pre configurados para garantizar que se cumple su solicitud de acceso a la red.

- **Análisis:**

Se puede usar este paper para poder aplicar la autenticación y autorización de acceso estén bajo la responsabilidad del servidor RADIUS, el cual se encarga de que todas las solicitudes de acceso a la red enviadas por los usuarios sean evaluadas para su posterior validación. El servidor tiene políticas de acceso que determinan los métodos de autenticación que se requieren para las estaciones de trabajo, tanto de manera cableado como inalámbrica. Otra función muy conveniente que puede resultar muy útil para este proyecto es que el servidor RADIUS es todavía capaz de auditar el uso de ancho de banda, los tiempos de conexión y otra información a través de cuentas. Otra cosa que aporta al proyecto es el uso de políticas de seguridad como exigir que los usuarios que quieran ingresar a la red tengan instalado un antivirus en su estación de trabajo, así como las actualizaciones automáticas de seguridad de Windows estén programadas de manera automática.

2.1.10 Guía de diseño de un WLAN para entornos de cliente de alta densidad en un ambiente de educación superior. (2013)

- **Autores:**
    - Jim Florwick
    - Jim Whiteaker
    - Alan Cuellar Amrod
    - Jake Woodhams

Esta guía de diseño proporciona directrices de ingeniería y técnicas prácticas para el diseño, la planificación y la implementación de una LAN inalámbrica (WLAN) dentro de un entorno de alta densidad en un campus universitario o la universidad. De alta densidad se define como cualquier entorno con una gran concentración de usuarios, tales como una sala de clase, sala de conferencias o auditorio donde los usuarios se conectan de forma inalámbrica, compartir aplicaciones y el uso de otros servicios de la red de forma individual. Este documento está dirigido a ingenieros de diseño de redes inalámbricas responsables del diseño, implementación y mantenimiento de redes Wi-Fi de hoy en día. Las demandas en las WLAN para la funcionalidad y su capacidad de ampliación están creciendo debido a la rápida proliferación de nuevos dispositivos y aplicaciones de red. El número de dispositivos y conexiones por usuario es cada vez mayor. Es común que la mayoría de los usuarios hoy en día, no sólo posea un dispositivo informático principal, sino también al menos otro dispositivo inteligente. Los operadores inalámbricos han trabajado duro para dar cabida a la creciente demanda de servicios de datos a través de redes inalámbricas. Se han visto obligados a considerar estrategias alternativas de procesamiento autónomo, incluyendo de forma inalámbrica la conexión de dispositivos electrónicos (Wi-Fi). Por desgracia, la mayoría de los teléfonos inteligentes está introduciendo en el mercado sólo son compatibles con Wi-Fi a 2,4 gigahercios (GHz), que está

aumentando rápidamente la presión sobre los diseñadores y administradores de Wi-Fi para diseñar productos para el segmento más pequeño del ancho de banda. [10]

- **Conclusión:**

El rendimiento de una WLAN de alta densidad dentro de un entorno de educación superior depende de lo bien que se entienden los requisitos de la red antes de que se despliegue la misma. Una buena comprensión de estos conceptos permitirá al diseñador poder modificar el diseño para dar cabida a lo imprevisto. Es importante contar con opciones de alternativas disponibles, basados en factores de cambio, y para mantener su flexibilidad en el enfoque, se presentan nuevas exigencias y desafíos. Por ejemplo, en la mayoría de los lugares, la estética será de vital importancia, y anticipar una respuesta a una crítica del diseño estético de antemano es útil. La comprensión de las diferencias de rendimiento entre una solución óptima y la solución menos intrusiva (o más estéticamente aceptables, con puntos de acceso ocultos) dejará el diseñador preparado para volver a ajustar las expectativas de ser necesario.

- **Análisis:**

En este trabajo es muy relevante debido a que presenta varias áreas del diseño como conceptos. Los valores recomendados se han ofrecido a modo de ejemplo, con base en la experiencia con las soluciones del pasado. Los valores recomendados deben ser tratados como un punto de partida y proporcionará una ventana de un rendimiento sólido. El rendimiento puede variar según las condiciones que están fuera del control del diseñador, pero la comprensión de estos conceptos y los controles permitirá que el diseñador para diseñar y comunicar una expectativa realista de los resultados.

2.2. Bases Teóricas de la Investigación

2.2.1. Redes Inalámbricas

Una red inalámbrica es un tipo de red informática que utiliza conexiones de ondas electromagnéticas para enlazar nodos de una red, mediante estas redes de telecomunicaciones las empresas evitan el costoso proceso de cableado en construcciones o una conexión entre distintos equipos en diferentes ubicaciones. Las tecnologías de comunicación inalámbrica en sus diferentes formas poseen una gran cantidad normas para su uso e implementación, las cuales nacen en consecuencia a los estándares regularizados por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Indudablemente una importante aplicación del denominado Wi-Fi es en el hogar, en las empresas, centros de esparcimiento, donde puede establecerse fácilmente una red inalámbrica de bajo costo; mediante la cual se puede compartir los diferentes recursos de red o el acceso a internet desde cualquier ubicación sin tener que romper paredes o desplegar cables. [11]

Si no se implementan medidas de seguridad adecuadas, al desplegar redes inalámbricas como en cualquier red, es factible que se vulnere la privacidad de la información. Al instalar una red inalámbrica, preocúpese de activar las protecciones de acceso que la tecnología también le ofrece. Ahora existen muchas maneras de implementar redes inalámbricas y distintos estándares existen organizaciones internacionales que ya formalizaron estándares para el uso de redes inalámbricas la IEEE (Instituto De Ingenieros Eléctricos Y Electrónicos), UIT (Unión Internacional De Telecomunicaciones) y la IETF (Internet Engineering Task Force) y que dicta normas llamadas RFC que son las normas que rigen el tráfico de internet , por recomendación de la UIT actualmente para redes inalámbricas de corto alcance y de largo alcance todas están normalizadas .[12]

2.2.2. Clasificación de redes inalámbricas según cobertura

Las redes inalámbricas se clasifican teniendo en cuenta como parámetro principal el rango que cubren a continuación, se muestra la clasificación de las redes inalámbricas según la cobertura.

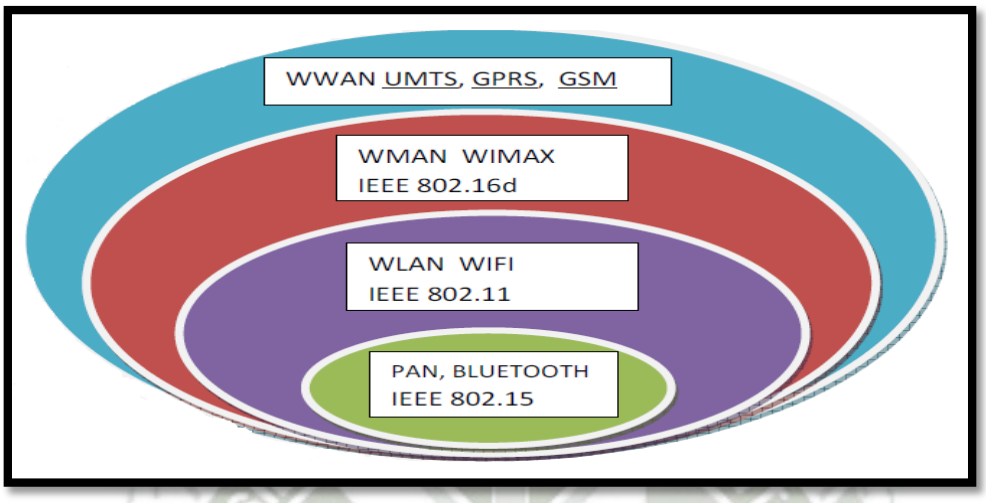

Figura 2.1 Clasificación de las tecnologías inalámbricas

Fuente: "Imagen tomada de Diseño de una Red LAN Inalámbrica para una Empresa de Lima (2011), p. 19."

2.2.2.1. Redes inalámbricas de área personal (WPAN)

Una red de área personal inalámbrica (WPAN) es una red de dispositivos de interconexión inalámbrica centrados en espacio de trabajo personal. Las PAN inalámbricas se basan en el estándar IEEE 802.15. Los dos tipos de tecnologías inalámbricas utilizadas para WPAN son Bluetooth y asociación de datos por infrarrojo. Un concepto clave en la tecnología WPAN se conoce como "plugging in". En el escenario ideal, cuando dos dispositivos WPAN están en estrecha proximidad (dentro de varios metros el uno del otro) o dentro de un par de kilómetros de un servidor central, pueden comunicarse como si está conectado por un cable. Cada dispositivo en una WPAN podrá conectar a cualquier otro dispositivo en el mismo WPAN, siempre y cuando estén dentro del alcance físico de los unos a los otros. Además, WPAN todo el mundo está interconectado.

2.2.2.2. Redes inalámbricas de área local (WLAN)

Una red inalámbrica de área local WLAN (Wireless LAN) es una red informática inalámbrica que conecta dos o más dispositivos que utilizan un método de distribución inalámbrico (de espectro extendido o de radio OFDM) dentro de un área limitada, como una casa, escuela, laboratorio de computación, o edificios. Esto ofrece a los usuarios la capacidad de moverse dentro de un área de cobertura local y todavía ser conectados a la red, y puede proporcionar una conexión a Internet más amplio. La mayoría de las WLAN modernas se basan en el estándar IEEE 802.11. Las redes locales inalámbricas más que una sustitución de las LANS convencionales son una extensión de las mismas, ya que permite el intercambio de información entre los distintos medios en una forma transparente al usuario. En este sentido el objetivo fundamental de las redes WLAN es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde puedan coexistir ambas redes, el atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado. [13]

2.2.2.3. Redes inalámbricas de área extensa (WWAN)

Una red de área amplia inalámbrica (WWAN). Es una red inalámbrica de gran tamaño mayor a una red de área amplia, en comparación con una red de área local requiere diferentes tecnologías. Este tipo de redes entregan los datos en forma de llamadas telefónicas, páginas web, y el vídeo streaming. La diferencia entre una WWAN y una WLAN es el uso de tecnologías de redes celulares de telecomunicaciones móviles, tales como LTE, WiMAX, UMTS, CDMA2000, GSM, paquetes de datos digitales celulares (CDPD) y Mobitex para transferir datos. También puede utilizar el servicio de distribución multipunto local (LMDS) o

Wi-Fi para proporcionar acceso a Internet. Estas tecnologías brindan servicios a nivel nacional o incluso a nivel mundial y son proporcionados por un proveedor de servicios de Internet (ISP). Conectividad WWAN permite a un usuario con un ordenador portátil y una tarjeta WWAN para navegar por Internet, consultar el correo electrónico, o conectarse a una red privada virtual (VPN) desde cualquier lugar dentro de los límites regionales de servicio celular.

2.2.3 WI-FI (Wireless Fidelity)

Wi-Fi es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica, principalmente mediante las bandas 2.4 y 5 GHz de bandas de radio SHF ISM. Como cualquier red de área local inalámbrica (WLAN) es un producto basado en el estándar IEEE 802.11. Sin embargo, el término Wi-Fi es utilizado en general como sinónimo de WLAN, ya que la mayoría de las redes WLAN modernas se basan en este estándar. El certificado Wi-Fi sólo puede ser utilizado por los productos Wi-Fi que cumplan con éxito las pruebas de certificación de interoperabilidad Wi-Fi Alliance. Muchos dispositivos pueden utilizar Wi-Fi, por ejemplo, laptops, smartphones, tablets, etc. Estos pueden conectarse a un recurso de red, tal como Internet a través de un punto de acceso de red inalámbrica. Tal punto de acceso tiene un alcance de unos 20 metros en interiores y un rango mayor al aire libre. La cobertura puede variar desde una habitación limitada por las paredes que bloquean las ondas de radio hasta muchos kilómetros cuadrados obtenidos mediante el uso de múltiples puntos de acceso superpuestos.

2.2.4 CSMA/CD

Carrier Sense Multiple Access con detección de colisiones (CSMA / CD) es un método de control de acceso al medio utilizado sobre todo en la creación de redes de área local utilizando

la tecnología Ethernet. Se utiliza un esquema de detección de portadora en el que una estación de datos de transmisión detecta otras señales durante la transmisión de un marco, deja de transmitir ese marco para transmitir una señal de atasco, y espera un intervalo de tiempo aleatorio antes de intentar volver a enviar la trama. CSMA / CD se utiliza para mejorar el rendimiento del CSMA por terminación de la transmisión tan pronto como se detecta una colisión, acortando así el tiempo necesario antes de un reintento. [14]

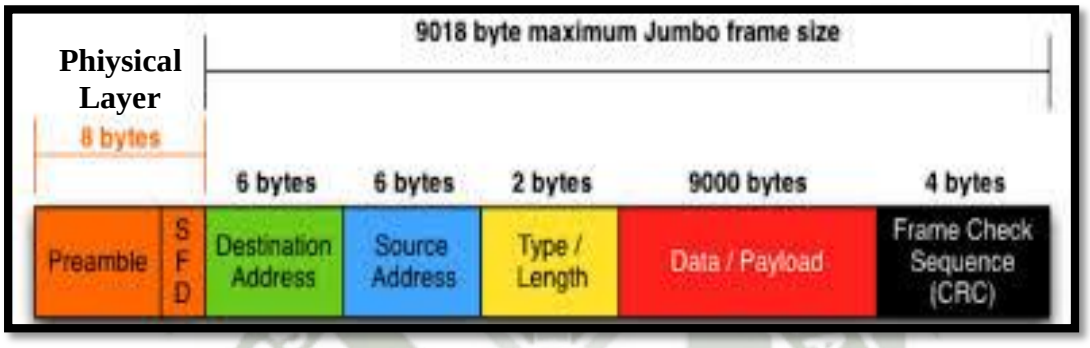

Figura 2.2 Trama usado protocolo Ethernet

Fuente: "Trama de ethernet [Figura]. (2010). Recuperado de https://sites.google.com/site/cursosciscoccna/cisco-3/2-conceptos-basicos-y-configuracion-de-switch"

2.2.5 CSMA/CA

CSMA / CA es un protocolo que opera en la capa de enlace de datos (Capa 2) del modelo OSI, es un protocolo de control de redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión. Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos (comúnmente en redes inalámbricas, ya que estas no cuentan con un modo práctico para transmitir y recibir simultáneamente). De esta forma, el resto de equipos de la red sabrán cuando hay colisiones y en lugar de transmitir la trama en cuanto el medio está libre, se espera un tiempo aleatorio adicional corto y solamente si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal. Básicamente, este proceso se puede dividir en tres fases en las que el emisor puede:

- Escuchar para ver si la red está libre.
- Transmitir el dato.
- Esperar un reconocimiento por parte del receptor.

Mediante este método se tiene la certeza que el mensaje se recibió correctamente. Debido a las transmisiones, el del mensaje original y la del reconocimiento del receptor, pierde un poco de eficiencia. Este ocasiona incremento en el volumen de tráfico y reduce las prestaciones de la red, motivo por el que se usa poco. [14]

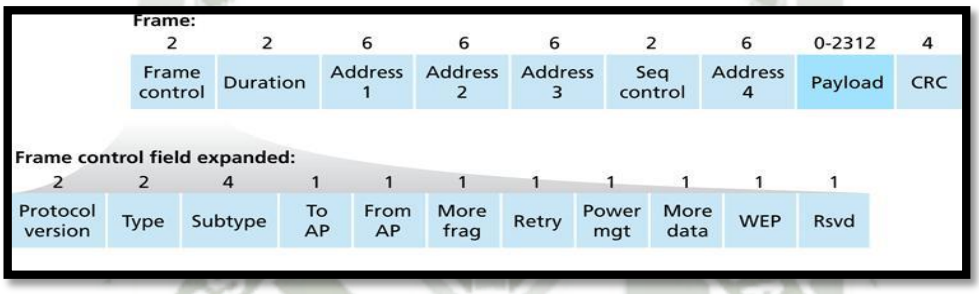

Figura 2.3 Trama usado por Wireless IEEE802.11.

Fuente: "Trama 802.11 [Figura]. (2012). Recuperado de http://wiki.inf.utfsm.cl/index.php?title=EEE_802.11_wireless_LANs_("wi-fi")"

2.2.6 Modulación espectro ensanchado

La tecnología de Espectro Ensanchado (SS) es una técnica cada vez más popular, que maximiza el uso del ancho de banda del canal permitiendo a múltiples señales utilizar el mismo canal sin colisiones, siendo altamente resistente a la interferencia y el bloqueo. Esta tecnología se puede emplear para elaborar redes inalámbricas, seguras y robustas, cuando se combina con un sistema de encriptación compleja, para lo cual se multiplica la señal digital que se quiere transmitir por una secuencia pseudoaleatoria o de pseudo-noise (PN). Esta modulación expande la información sobre un ancho de banda mayor de tal forma que se minimizan las interferencias y se dificulta su interceptación. En el receptor se desmodula la señal de espectro ensanchado empleando el mismo código PN generado en el emisor [15].

2.2.7 Modulación OFDM

OFDM es una técnica utilizada en sistemas de comunicaciones inalámbricas modernos de banda ancha. Para mitigar el efecto de distorsión del canal dispersivo en sistemas OFDM de alta velocidad de datos, prefijo cíclico se introduce para eliminar la interferencia entre símbolos (ISI). Se copia la sección del extremo de un paquete de IFFT para el comienzo de un símbolo OFDM. Típicamente, la longitud del prefijo cíclico debe ser más largo que la longitud del canal dispersivo para eliminar completamente ISI. Modulación OFDM en un transmisor incluye transformada rápida de Fourier (IFFT) operación inversa y la inserción de prefijo cíclico. En un receptor OFDM, el prefijo cíclico se elimina antes de que el paquete de datos es enviado a FFT para la demodulación. Sistemas inalámbricos de próxima generación cuentan con configuraciones muy dinámicos, donde los cambios en la longitud del prefijo cíclico de acuerdo con el modo de transmisión, estructura de la trama, y el protocolo de nivel superior. Algunos sistemas donde es usado la modulación OFDM [16]:

- El protocolo de enlace ADSL.
- El protocolo de red de área local IEEE 802.11n/ac
- El sistema de transmisión inalámbrica de datos WiMAX.
- El sistema de transmisión de datos basados en PLC.

2.2.8 Protocolos de red inalámbrica de área local

IEEE 802.11 es un conjunto de control de acceso al medio (MAC) y la capa física (PHY) es especificaciones para la implementación de la red de área local (WLAN) de comunicación del ordenador inalámbrico en las bandas de frecuencia de 2.4 GHz, 3.6, 5 y 60. Son creados y

mantenidos por el Comité LAN / MAN Normas IEEE 802. El estándar y las enmiendas constituyen la base de los productos de red inalámbricos que utilizan la marca Wi-Fi gratuita. Mientras que cada enmienda se revoque oficialmente cuando se incorpora en la última versión de la norma, el mundo empresarial tiende a poner a las revisiones, ya que de forma concisa denotan capacidades de sus productos. Como resultado, en el mercado, cada revisión tiende a convertirse en su propio protocolo [17].

Estándar 802.11																
Protocolo	Frecuencia		Ancho de Banda				Flujo de Datos				Rango Promedio	
											Interior	Exterior
	(GHz)		(MHz)				(Mbit/s)				(m)	(m)
802.11	2.4		22				2				20	100
802.11a	3.7	5	20				54				35	120
802.11b	2.4		22				11				35	140
802.11g	2.4		20				54				38	140
802.11n	2.4	5	20	40			72.2	150			70	250
802.11ac	5		20	40	80	160	96.3	200	433.3	866.7	35	100
802.11ad	60		2160				6.75 (Gbit/s)				60	
802.11ah	0.9											
802.11aj	45	60										
802.11ax	2.4	5										
802.11ay	60		8000				100 (Gbit/s)				60	

Tabla 2.1 Protocolos del estándar IEEE802.11

Fuente: "Elaboración propia"

2.2.8.1 IEEE 802.11n

Es un estándar de red inalámbrica que utiliza múltiples antenas para aumentar la tasa de transferencia. Es una enmienda al estándar de red inalámbrica IEEE 802.11a Su propósito es mejorar el rendimiento de la red en los dos anteriores protocolos 802.11a y 802.11g, con un

aumento significativo en la velocidad datos de la red de 54 Mbit/s hasta 600 Mbit/s con el uso de cuatro flujos espaciales en una anchura de canal de 40 MHz. 802.11n tiene soporte estandarizado para múltiples entradas, múltiples salidas, agregación de tramas y mejoras de seguridad, entre otras características. Puede ser utilizado en las bandas de frecuencia de 2,4 GHz o 5 GHz. Ellos son comúnmente utilizados hoy en día en otros estándares como son 802.11a, 802.11b, 802.11g, 802.11n, y las versiones 802.11ac para proporcionar conectividad inalámbrica en los hogares y las empresas. [17]

2.2.8.2 IEEE802.11ac

IEEE 802.11ac es un protocolo de red inalámbrico de la familia 802.11, desarrollado en el proceso de estándares IEEE, proporcionar redes de alto rendimiento de área local inalámbricas (WLAN) en la banda de 5 GHz. Esta especificación ha esperado por varias estaciones WLAN para un rendimiento de al menos 1Gb/s y un solo enlace rendimiento de al menos 500 Mbit/s. Las mejoras de 802.11ac son el aumento de la velocidad de datos incluyen la expansión de ancho de banda de canal de 80 y 160 MHz. Además, una nueva característica de 802.11ac es el uso de canales no contiguos, por los que dos no adyacentes 80 canales MHz puede utilizarse para formar una transmisión de 160 MHz. Esto permite la asignación de canal más flexible con el mayor ancho de banda para evitar en gran medida los canales ocupados o incluso para evitar los radares, al permitir transmisiones simultáneas a múltiples dispositivos, mejora la capacidad de la red. [17]

2.2.9 Bandas ISM

Las bandas de radio industriales, científicas y médicas (ISM) son porciones del espectro radioeléctrico reservadas a nivel internacional para el uso de radiofrecuencia (RF), estas bandas

son usadas para las comunicaciones como WLAN (Wi-Fi) o WPAN (Bluetooth), el uso de las bandas designadas en los diferentes países pueden ser diferentes debido a las variaciones en las regulaciones de radio nacionales, en nuestro país esto esta normado de acuerdo al PNAF (PLAN NACIONAL DE ATRIBUCIÓN DE FRECUENCIAS) en este documento se detalla la asignación de las bandas ISM en el cual también se designan las frecuencias de uso libre. Los teléfonos inalámbricos, dispositivos Bluetooth, comunicación de campo cercano (NFC) dispositivos y redes informáticas inalámbricas todas las frecuencias de uso asignados a las comunicaciones de baja potencia, aunque estos emisores de baja potencia no se consideran ISM. En la figura se puede apreciar frecuencias de las diferentes bandas ISM que no tienen restricción.

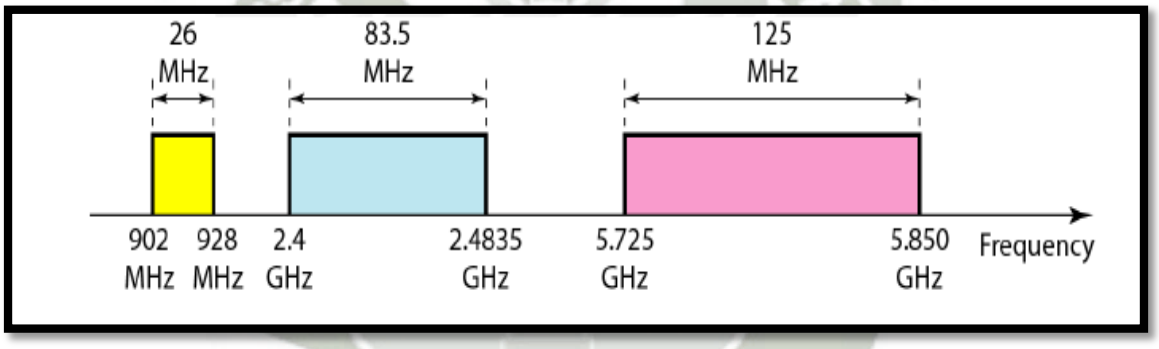

Figura 2.4 Frecuencias usadas para ISM.

Fuente: "Imagen tomada de Diseño de una Red LAN Inalámbrica para una Empresa de Lima (2011), p. 30."

2.2.10 Capa física del Estándar IEEE 802.11

La capa física (PHY) de cualquier red define la modulación y la señalización, esta es la interfaz entre el MAC y el medio inalámbrico, ofreciendo tres niveles de funcionalidad: intercambiar tramas entre PHY y MAC, utilizar portador de señal y modulación de espectro ensanchado para transmitir tramas a través del medio y proveer al MAC de un indicador de detección de portadora para señalizar actividad en el medio. La capa física se divide en dos subcapas: PMD

y PLCP. La subcapa PMD (Physical Medium Dependant) se ocupa de la modulación y de la aplicación de técnicas de espectro ensanchado de la señal y la subcapa PLCP (Physical Layer Convergent Procedure) se encarga de acondicionar las tramas que provienen de la capa MAC para su envío a través del medio radio, añadiéndoles un preámbulo y una cabecera. Todas las tramas que utilizan los PHY descritos incluyen una cabecera y un preámbulo PLCP. El preámbulo se utiliza por el receptor para adquirir la señal entrante y sincronizar con el demodulador. La cabecera PLCP contiene información acerca del paquete MAC transmitido, tal como la duración o la velocidad de transmisión utilizada. [18]

2.2.11 Capa de enlace (MAC) del Estándar IEEE 802.11

La capa de enlace se divide en dos subcapas, una de control de acceso al medio (MAC) y una de control del enlace lógico (LLC) que es común para todos los estándares 802.X. La capa MAC define tres modos de acceso:

- DCF CSMA/CA (Distributed Coordination Function CSMA/CA): Es un protocolo de acceso múltiple basado en CSMA/CA (Carrier Sense Multiple Access with Colision Avoidance). Intenta resolver problemas como la movilidad de las estaciones, la variación de la calidad del enlace radio y la aparición de terminales ocultos.
- DCF con RTS/CTS: Es una extensión de CSMA/CA, empleada para resolver el problema de los terminales ocultos, para evitar este tipo de problemas, se emplea RTS/CTS (Request to Send- Clear to Send). Cuando una estación necesita transmitir, envía primero un paquete de reserva RTS. Cuando el medio está libre, el punto de acceso responde a este paquete con un CTS que indica que la estación puede transmitir.
- PCF (Point Coordination Function): Protocolo de acceso para redes 802.11 operando en modo infraestructura. Garantiza la provisión de servicios sin contención, mediante

un control de acceso centralizado, en el que se definen dos periodos, uno libre de contenciones (CFP) y uno sujeto a contención (CP) que se alternan con el tiempo [18].

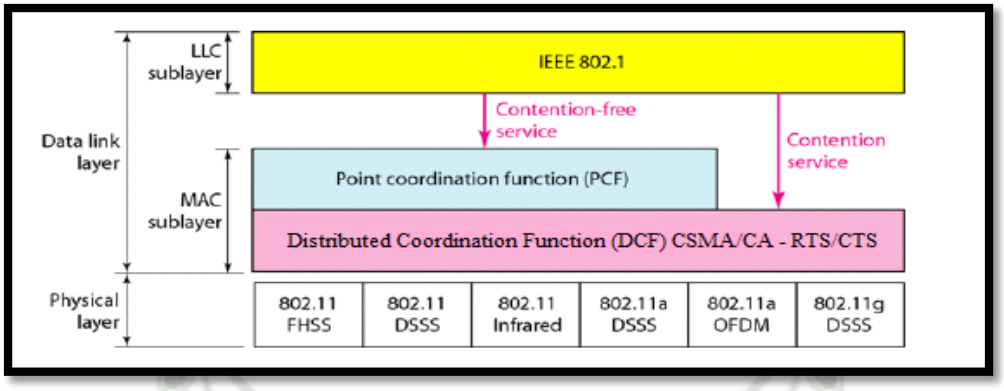

Figura 2.5 Muestra las subcapas de la capa de enlace de datos.

Fuente: "Imagen tomada de Diseño de una Red LAN Inalámbrica para una Empresa de Lima (2011), p. 32."

2.2.12 Configuración de redes inalámbricas

Las redes inalámbricas son altamente complejas este debido a la maleabilidad y variabilidad que poseen debido a esto una LAN implementada con este tipo de tecnología se hace tremendamente variable y sofisticada. La gran gama de configuraciones que nos ofrece ayuda a que este tipo de redes puedan suplir cualquier necesidad que se presente. Estas configuraciones se dividen en redes que usan Puntos de Acceso y redes peer to peer.

2.2.12.1. Peer to peer

Las tecnologías "peer to peer" (P2P) hacen referencia a un tipo de arquitectura para la comunicación entre aplicaciones que permite a individuos comunicarse y compartir información con otros individuos sin necesidad de un servidor central que facilite la comunicación. Este tipo de arquitectura de red solo precisa de un rango de cobertura para la señal, ya que los terminales móviles que estén ubicados dentro de este rango van a poder

comunicarse entre sí. Una de las ventajas de esta arquitectura es que la configuración requerida es muy sencilla para implementar y no precisa una administración de la red. Otra ventaja de la tecnología P2P es que no existe una autoridad central única que se pueda eliminar o bloquear y colapsar toda la red P2P. Esto dota a la red de la capacidad de sobrevivir por sí misma y de una gran robustez [19].

Figura 2.6 Conexión peer to peer.

Fuente: "Imagen tomada de Redes Inalámbricas IEEE 802.11, Equipos y Sistemas de Transmisión (2011), p. 8."

2.2.12.2 Punto de Acceso BSS

Este tipo de infraestructura emplean el concepto de celda, que existe para las comunicaciones inalámbricas. Una celda es la el área de cobertura de una señal radioeléctrica, en el caso de redes inalámbricas las celdas poseen un tamaño establecido, para poder subsanar esto es que se emplea múltiples fuentes para la emisión de la señal combinando celdas para cubrir de forma casi total un área más extensa.

La estrategia que se usa para aumentar el número de celdas y por consecuente aumentar el área de la red es colocar los puntos de acceso en alto, situados estratégicamente de una manera que

puedan dar una cobertura necesaria. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango variable de treinta a cien metros. Además del evidente aumento del alcance de la red por la utilización de varios puntos de acceso, y por lo tanto del empleo de varias celdas que colapsen el lugar donde se encuentre la red, permite lo que se conoce como "Roaming", es decir que los terminales puedan moverse sin perder la cobertura y sin sufrir cortes en la comunicación. En la figura 2.10 se muestra la utilización de varios puntos de acceso. [13]

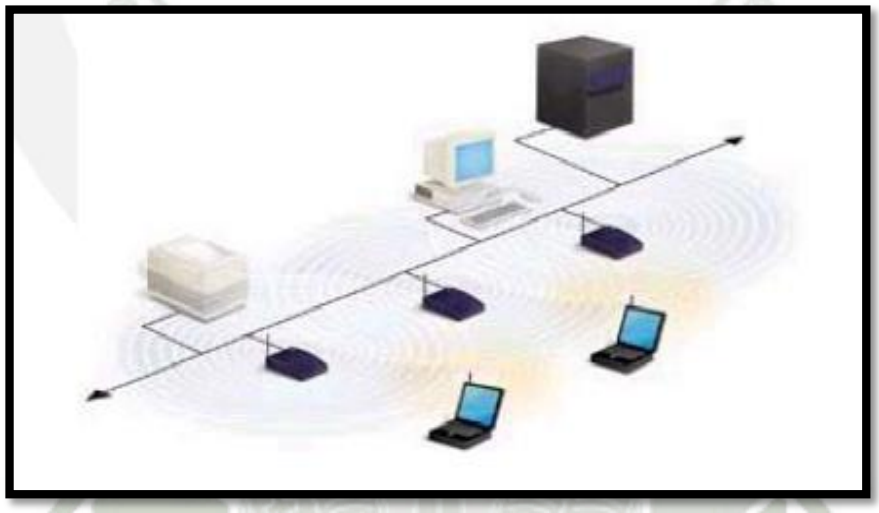

Figura 2.7 Utilización de varios Puntos de acceso con capacidad de Roaming

Fuente: "Imagen tomada de Redes Inalámbricas IEEE 802.11, Equipos y Sistemas de Transmisión (2011), p. 10."

2.2.13 Tipo de canales de IEEE 802.11n/ac

El estándar IEEE 802.11 es sus protocolos 802.11n y 802.11ac establece que estos deben usar las bandas de 2.4 GHz y 5 GHz. Para la primera banda se determinaron que debe haber 11 canales para las respectivas frecuencias que son utilizables para equipos WLAN. Sin embargo, los 11 canales de 22 MHz separados solo por 5 MHz cada uno de los cuales no son

completamente independientes (superposición de canales) en el uso diario sólo es posible la utilización de 3 de los 11 canales de manera paralela (1, 6 y 11) lo cual es válido en América mientras que en Europa poseen 13 canales y de los cuales se puede usar 4 canales no-adyacentes de forma simultanea (1, 5, 9 y 13). La asignación de canales por lo general se realiza en los access point, los usuarios de la red se conectan de manera automáticamente al canal. Mientras que en la banda de 5 GHz existen actualmente 44 canales con sus respectivas frecuencias los cuales los diferentes países aplican sus propias normas a los canales permitidos para los usuarios autorizados y los niveles máximos de potencia dentro de estos rangos de frecuencia.

2.2.14 Seguridad para redes inalámbricas

Los diferentes protocolos 802.11 de la IEEE se establece un conjunto de mecanismos los cuales tienen como función primordial brindar seguridad a la red y que esta sea similar a la que pueda brindar una red cableada. Y para lo cual es necesario conseguir la triada CIA ("Confidentiality, Integrity, Availability") en seguridad de la información:

- Confidencialidad: el objetivo es impedir la divulgación no autorizada de los datos sensibles y evitar el uso de la red por cualquier persona no autorizada, sólo debe aceptar paquetes de estaciones previamente autentificadas.
- Integridad: Garantizar que los datos y los recursos sean exactos y confiables. Y evitar que los recursos de información puedan ser modificados accidental o intencionalmente.
- Disponibilidad: El acceso oportuno y fiable a los datos y recursos por parte de los usuarios autorizados. Sin embargo, no todo el dato debe estar disponible de inmediato para los usuarios autorizados.

2.2.14.1 Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) y Wi-Fi Protected Access II (WPA2) son dos protocolos de seguridad y programas de certificación de seguridad, desarrollados por Wi-Fi Alliance para asegurar las redes inalámbricas. Se realizaron en respuesta a serias debilidades que se habían encontrado en el sistema anterior, Wired Equivalent Privacy (WEP). Wi-Fi Protected Access posee dos protocolos de cifrado, conocidos como:

- TKIP (Temporary Key Integrity Protocol). Este protocolo tiene como función principal la de intercambiar la clave compartida entre access point y cliente en intervalos tiempo continuos, con la finalidad de impedir los diferentes ataques que puedan exponer la clave.
- CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol, Counter Mode CBC-MAC Protocol). Es un mecanismo de encapsulación de cifrado de datos mejorado diseñado para la confidencialidad de los datos y con base en el modo de contador con CBC-MAC (MCP) de la norma AES.

2.2.14.2 Protocolo 802.1X

IEEE 802.1X es un estándar para el control de acceso a la red basado en puerto (PNAC). Este comprende tres partes: un suplicante, un autenticador, y un servidor de autenticación. El solicitante es un dispositivo cliente (tal como un ordenador portátil) que desea conectar a la LAN/WLAN. El autenticador es un dispositivo de red, como un conmutador Ethernet o punto de acceso inalámbrico; y el servidor de autenticación es típicamente un software que se ejecuta anfitrión soporte los protocolos RADIUS y EAP.

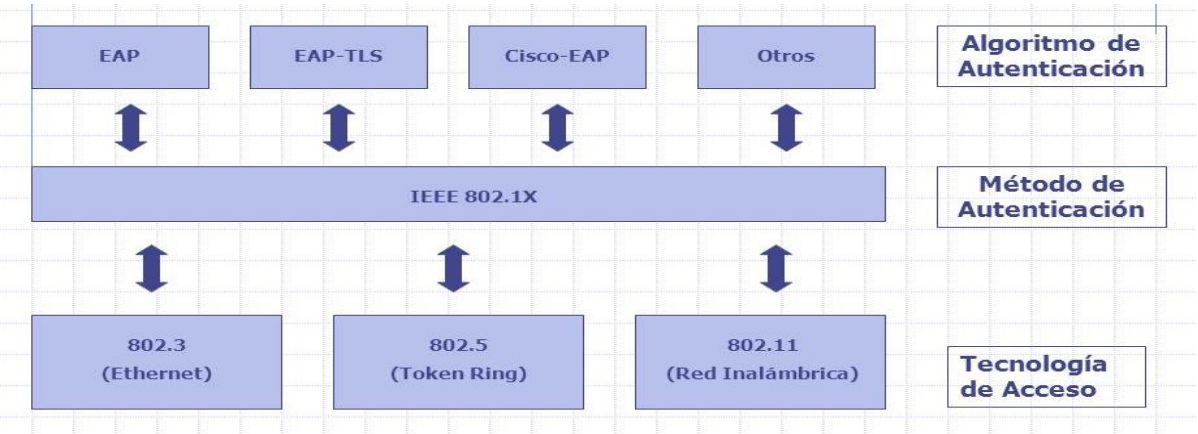

Figura 2.8 Interconexión mediante IEEE 802.1X.

Fuente: "*http://images.slideplayer.es/2/1025861/slides/slide_22.jpg*"

2.2.15 EAP

EAP (Extensible Authentication Protocol) es una extensión del protocolo PPP (Point-to-point Protocol), proporciona un mecanismo estándar para aceptar métodos de autenticación, al usar EAP se puede agregar varios esquemas de autenticación como: RADIUS, Kerberos, tarjetas de identificación, certificados entre otros. [1]

Aunque el protocolo EAP no es exclusivo de WLAN y puede ser usado para autenticación en redes cableadas, es más frecuentemente usado en redes inalámbricas. Recientemente los estándares WPA y WPA2 han adoptado cinco tipos de EAP como sus mecanismos oficiales de autenticación. EAP es una estructura de soporte, no un mecanismo específico de autenticación. El EAP provee algunas funciones comunes y negociaciones para el o los mecanismos de autenticación escogidos, de los cuales se conocen actualmente unos 40. Además de algunos específicos de proveedores comerciales, los definidos por RFC de la IETF incluyen EAP-MD5, EAP-OTP, EAP-GTC, etc. Los métodos modernos capaces de operar en ambientes inalámbricos incluyen EAP-TLS, EAP-SIM, EAP-AKA, PEAP, LEAP y EAP-TTLS. Los requerimientos para métodos EAP usados en WLAN son descritos en la RFC 4017. La

encapsulación de EAP sobre IEEE 802 se define en el estándar IEEE 802.1X, conocido como EAPOL. El cual fue diseñado originalmente para IEEE 802.3 Ethernet en 802.1X-2001, pero se adaptó para ser usado con otras tecnologías como IEEE 802.11 inalámbrica y Fiber Distributed Data Interface (ISO 9314-2) en 802.1X-2004 [21].

2.2.16 RADIUS

RADIUS (Remote Authentication Dial-In User Server) Es un protocolo que nos permite gestionar la "Autenticación, Autorización y Contabilidad" (es más conocida como AAA, al ser éste su acrónimo de su denominación original inglesa "Authentication, Authorization, and Accounting") de usuarios remotos sobre un determinado recurso.

2.2.16.1 Autenticación y Autorización ("Authentication, Authorization")

Software instalado como servicio en el sistema operativo de una computadora, es el encargado de administrar las cuentas de acceso. Recibe la autenticación y luego de realizar la comparación con sus registros envía un mensaje permitiendo o negando el acceso, además ira almacenando los eventos de dichos procesos. Para aceptar las consultas del cliente debe tener un perfil del NAS con la dirección IP del cliente y la clave de autorización. En la comunicación con el cliente, se intercambian los siguientes mensajes.

- Access - Request: Solicitud de atención para autenticación
- Access - Accept: Acepta la autenticación
- Access - Reject: No acepta la autenticación
- Accounting - Request: Registra eventos
- Accounting – Response: Confirmación de evento registrado

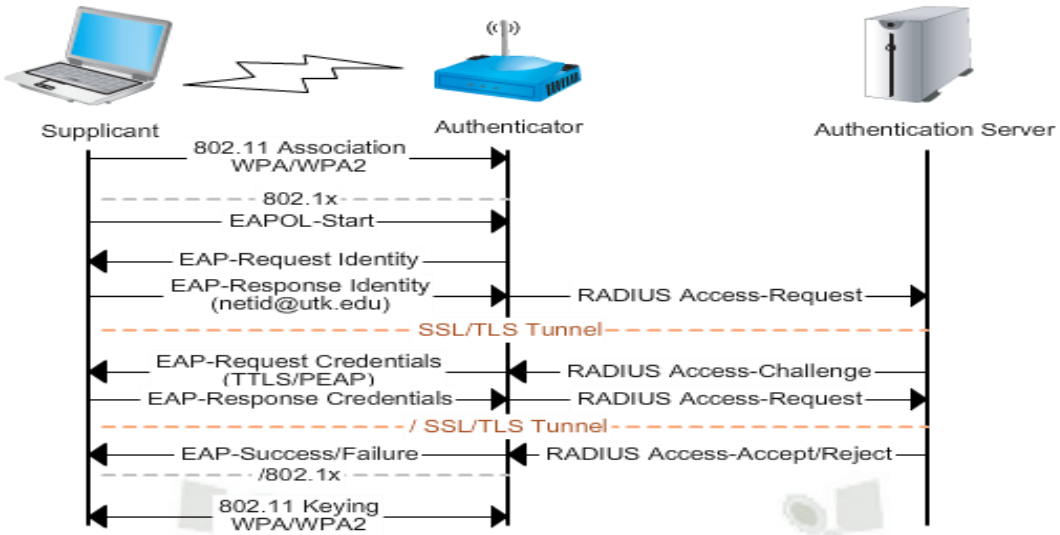

Figura 2.9 Muestra el proceso de autenticación y autorización.

Fuente: "*Authentication with 802.1x over 802.11 with EAP details* [Figura]. (2011). Recuperado de https://www.eduroam.us/node/10"

2.2.16.2 Contabilidad ("Accounting")

Cuando el acceso a la red se concede al usuario por la NAS, se inicia la contabilidad mediante un paquete de contabilidad que es enviado por Servidor de acceso a la red (NAS) al servidor RADIUS el cual contiene el paquete Acct-Status-Type que contiene el atributo "start" para señalar el comienzo del acceso a la red por parte del usuario. En el cual se encuentran los registros que contienen la identificación del usuario, dirección de red, punto de unión y un identificador de sesión único. Periódicamente, los registros de actualización provisional (un paquete de petición de cuentas RADIUS que contiene un atributo Acct-Status-Type con el valor "interim update") pueden ser enviados por el NAS al servidor RADIUS, para informar sobre el estado actual de una sesión activa. Los registros " interim" por lo general transmiten la duración de la sesión actual y la información sobre el uso actual de los datos. Por último, cuando el usuario cierra su acceso a la red, el servidor NAS emite un paquete de solicitud de contabilidad RADIUS que contiene un atributo Acct-Status-Type con el valor de "stop", que proporciona información sobre el fin de sesión esto se ve reflejado en términos de tiempo, los paquetes

transferidos, los datos transferidos, razón por la desconexión y otra información relacionada con el acceso a la red del usuario [22].

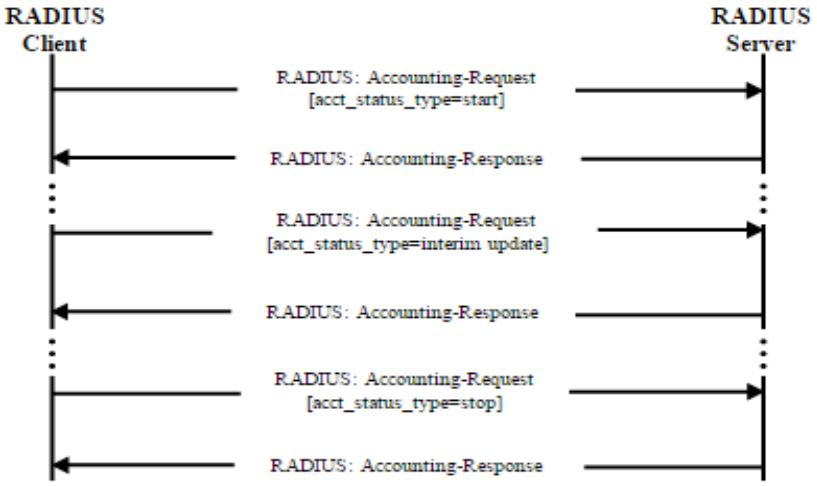

Figura 2.10 Muestra el proceso de contabilidad.

Fuente: "*https://en.wikipedia.org/wiki/RADIUS#/media/File:Drawing_RADIUS_1813.svg*"

CAPÍTULO 3

MARCO METODOLOGÍCO

3.1 Alcances y Limitaciones

3.1.1 Alcance

La propuesta de la elaboración de metodología para el diseño de red inalámbrica 802.11 n/ac con servidor Radius para la gerencia regional de salud Arequipa, pretende dar a conocer un marco de trabajo fácil de implementar y adaptable, enfocado en las necesidades actuales de la GERESA, teniendo en cuenta, las necesidades actuales que presenta, así como el hardware y el software existente, el área de cobertura, las políticas de uso y sobre toda la seguridad de la red.

La investigación estará orientada al estudio de metodologías de desarrollo de una red inalámbrica (WLAN) administrada mediante un servidor Radius. Sin aplicarse la misma a la creación de un proyecto en específico más que un modelo para una posterior implementación. Para determinar la eficiencia de la propuesta se implementarán la valoración por parte de un grupo de usuarios y la evaluación de un experto en telecomunicaciones.

3.1.2 Limitaciones

- **Limitación geográfica**

La red inalámbrica se va estar en el local de La Gerencia Regional de Salud de Arequipa ubicado en Av. De La Salud S/N - Arequipa - Arequipa.

- **Limitación temporal**

El presente trabajo se llevará a cabo durante el periodo que se realizó prácticas profesionales que fue entre abril a junio del año 2015

- **Limitación del conocimiento**

Crear una metodología para el diseño de una red inalámbrica que cumpla con los requisitos que demanda la Gerencia Regional de Salud Arequipa.

3.2 Aporte

El aporte que se pretende dar a la Gerencia Regional de Salud Arequipa es cambiar el diseño del sistema de comunicación por un sistema de red inalámbrico que va reducir los problemas de restricción física que actualmente está presente, de esta manera se benefician los trabajadores y a los invitados de la GERESA. Aumentando seguridad para acceso a la red inalámbrica, en conjunto con la asignación de VLAN en el switch y las listas de control de acceso en el router, conforman un robusto sistema de seguridad y esto a su vez administrado por un servidor Radius que brinda una correcta administración de la red, que ayudara con los problemas de fuga de información que presenta, permitiendo brindar acceso a la información de manera oportuna a los trabajadores sin ninguna restricción física.

3.3 Tipo y Nivel de investigación

3.3.1 Tipo de investigación

Por el tipo de la investigación, el presente estudio reúne las condiciones metodológicas de una investigación aplicada, en razón que se utilizaron conocimientos de las ciencias de Redes y

telemática, a fin de aplicarlas en diseño de una red inalámbrica con los protocolos 802.11 n/ac administrada por un servidor Radius

3.3.2 Nivel de investigación

De acuerdo a la naturaleza del estudio de la investigación, reúne por su nivel las características de un estudio descriptivo, explicativo y correlacionado.

3.4 Población y Muestra

3.4.1 Población.

La población de ésta investigación está constituida por 536 sujetos de estudio, a los cuales se le aplico dos cuotas para poder realizar este estudio la primera cuota es personal con acceso a la red de lo cual se redujo la poblacion a 210 y despues aplicar la segunda cuota que es la personal con conocimientos tecnicos de redes y se obtuvo una poblacion final de 10.

3.4.2 Muestra.

El tamaño de la muestra es de 10 trabajadores a quienes se aplicaran los instrumentos de investigacion, calculo de tamaño de muestra para población finita con un nivel de confianza del 95%:

$$\mathrm{n} = \frac{Z^2 * P * Q * N}{E^2(N-1) + Z^2 * P * Q}$$

Ecuación 3.1 Formula de la Muestra

Fuente: “https://es.wikipedia.org/wiki/Tama%C3%B1o_de_la_muestra”

Donde:

- n = Tamaño de la muestra
- Z = Valor critico a un determinado grado de confianza
- P = Probabilidad de éxito
- Q = Probabilidad de fracaso
- N = Población
- E = Error muestral

Dónde: Z= 1.96, P=0.50, Q=0.50, E=0.05 y N=236

$$n = \frac{1.96^2 * 0.50 * 0.50 * 10}{0.05^2(10-1) + 1.96^2 * 0.50 * 0.50}$$

n = 9.7 = 10 Trabajadores

Ecuación 3.2 Resultado de la Muestra

Fuente: Elaboración Propia

3.5 Métodos, técnicas e Instrumentos de Recolección de Datos

3.5.1 Método

El método que se va usar en la presente tesis es un método analítico con el que se pretende realizar un análisis de la situación que actualmente se presenta, desde la perspectiva técnica y considerar los requerimientos técnico que necesita la GERESA, esto asociado a las nuevas tecnologías de soluciones existentes que proponen ser la base para lograr la solución de las necesidades actuales.

3.5.2 Técnicas

Para la obtención de los datos indispensables en el desarrollo del presente proyecto, se emplearán las técnicas de:

- Observación no experimental
- Entrevistas
- Análisis documental

3.5.3 Instrumentos de Recolección de Datos

Los instrumentos que se usaran para la recolección de datos son los siguientes:

3.5.3.1 Observación directa.

Mediante las guías de observación se pretende descubrir aspectos importantes para el presente proyecto desde una perspectiva ajeno a los hechos, es decir, que mediante las guías observación se conocerá las actividades que se realizaran y que precisan de la red institucional para poder llevarse a cabo, aportando elementos esenciales para la solución del problema actual de la red. Esta técnica se empleará para elaborar un estándar del sistema base para el inicio de la solución del problema.

3.5.3.2 Entrevistas.

Se empleará entrevistas no estructuradas para conocer el diagrama detallada de la red, así como la configuración de los diferentes equipos que conforman esta. La información recolectada directamente del personal relacionado del área permitirá conocer los procesos que necesitan la red de manera indispensable, reconociendo las causas de los problemas y las condiciones actuales.

3.5.3.3 Revisión bibliográfica.

Enfocado al análisis de toda la documentación relacionada a los temas que aborda el presente proyecto, entre los que se tienen trabajos de grado, trabajos de investigación, artículos de internet, textos, manuales de equipos, etc.

3.6 Plan de Análisis estadísticos de los datos

El plan de análisis estadísticos de los datos se realizará luego de aplicar la encuesta a los usuarios.

CAPÍTULO 4

PLAN DE TRABAJO

4.1 Descripción de la Metodología.

El diseño de una red funcional que cumpla con todos los requerimientos para un correcto funcionamiento implica mucho más que solo hecho de interconectar computadoras, esta tiene satisfacer todas las necesidades por las cuales ha sido concebida, orientada para que logre un alto performance, mediante lo cual los usuarios que van hacer uso de la red puedan cumplir todas las actividades que les demanda su trabajo, con una conectividad a las diferentes aplicaciones con un tiempo de respuesta razonable. También tiene que cumplir características como escalabilidad y adaptabilidad; lo cual implica que tenga la capacidad de un continuo crecimiento y adaptación para poder incorporar nuevas tecnologías que van apareciendo y uno de los factores más críticos para el éxito de una red es la capacidad para que pueda ser administrable es decir monitorear y controlar las incidencias que puedan ocurrir en la red.

En la presente tesis se establece como propuesta una Metodología para el diseño de una red inalámbrica que cuente con los protocolos de comunicación 802.11n/ac y con el protocolo de autenticación, autorización y contabilización Radius, la cual está enfocada en suplir las necesidades actuales de la red de la gerencia Regional de Salud Arequipa. Para elaborar se tiene en consideración las limitaciones y deficiencias encontradas actualmente en la red. Las principales características para desarrollar esta metodología son:

- Integración de los equipos de red existentes.
- Puede ser aplicada en redes que implementen medio de transmisión inalámbrico.
- Recomendar herramientas para la elaboración de la topología física y lógica de la red.
- Indicar diferentes equipos que cumplan con los estándares requeridos.
- Considerar el tipo seguridad, monitoreo y mantenimiento de la red

Fase 1: Diagnóstico de Necesidades

- Análisis de la Red
  - Análisis de la documentación existente.
  - Análisis de la infraestructura de la red.
- Determinación de las necesidades de la red
  - Identificacion de Necesidades
    - Selección de la Solución
  - Tecnología
    - Incorporación de protocolos
  - Dispositivos.
    - Access Point
    - Wireless LAN Controles
    - Tarjeta de red Inalámbrica
  - Servidores.
    - Radius Server

Fase 2: Diseño de la red

- Diseño Físico de la Red
  - ➢ Distribución de los equipos
    - Software para estudio del Sitio
    - Ubicación de los Access Point
    - Arquitectura de la red.
  - ➢ Segmentación de la Red
    - Adaptación de VLANs
    - Asignación de direcciones IP
- Diseño Lógico de la Red
  - ➢ Incorporación al Directorio Activo
  - ➢ Configuración del Directorio Activo
  - ➢ Incorporación de VLANs al Directorio Activo
    - Acceso a la red Administrativa
    - Acceso a la red Mantenimiento
    - Acceso a la red Invitados
    - Acceso a la red Sin Dominio

Fase 3: Implementación del diseño

- Protocolo Radius
  - ➢ Instalación del Servicio.
  - ➢ Autorización del uso del Directorio Activo.

- Configuración de Clientes Radius.
- Configuración De Políticas.
  - Directivas de Solicitud de Conexión
  - Directivas de Red

- Configuración de la Red
  - Red Cableada
    - Configuración general para usar autenticación en el router
    - Asignación de puertos de acceso para la configuración 802.1X
  - Red Inalámbrica
    - Configuración de los parámetros generales del Servidor Radius
    - Generación de un perfil de seguridad

Fase 4: Simulación de la Red

- Pruebas.

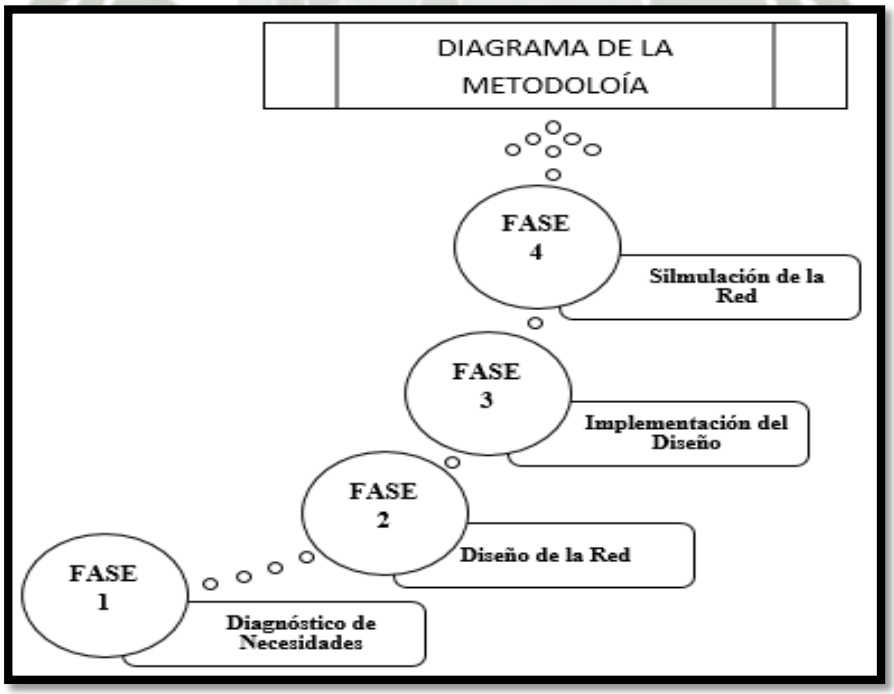

Figura 4.1 Descripción de la Metodología.

Fuente: "Elaboración propia"

4.2 Análisis de la Red

4.2.1 Análisis de la documentación existente

La red de datos de la Gerencia Regional de Salud Arequipa, posee una topología de estrella extendida siendo el nodo principal de la estrella el Data Center de la institución. Los equipos que componen la infraestructura de la red son los siguientes:

Equipo	Marca	Modelo	S.O.	Función
Servidor	Dell	Power Edge R220 E3-1220V3	Windows Server 2012 R2	Directorio Activo
Servidor	HP	ProLiant DL380p G8	Windows Server 2008	Servidor de Aplicaciones
Servidor	HP	ProLiant DL380p G8	Ubuntu Server 10.04	Múltiples
Router	Motorola	SBG901	Sistema Propio	Salida Internet
Router	Motorola	SB5101	Sistema Propio	Salida Internet
Switch	Cisco	2950	Cisco IOS	Conexión de equipos
Switch	Cisco	2950	Cisco IOS	Conexión de equipos
Switch	HP	3100	Sistema Propio	Conexión de equipos

Tabla 4.1 Descripción de los equipos de red.

Fuente: "Elaboración propia"

La distribución de la red se da mediante siete Switch cisco catalyst 2950 con 24 puertos 10/100 Mb, dos switches cisco catalyst 2950G con 24 puertos 10/100 Mb + 2 puertos GBIC y dos switches HP 3100 con 24 puertos 10/100 Mb + 2 puertos 10/100/1000 Mb. La conexión a los usuarios finales es mediante par trenzado UTP CAT 5, por necesidades propias de la direccione de Seguros Referencias y Contrarreferencias, tuvieron que contratar una línea dedicada para

dicha área que posee su propia salida a internet mediante un router Motorola SBG901 mientras que el resto de la institución posee otra salida a internet a través de un router Motorola SB4200, las cuales tiene como proveedor de internet a la compañía Star Global Com, la cual provee el servicio de internet mediante cable coaxial H500 con plan de ancho de banda de 1 Mbps para ambas líneas, de los 536 trabajadores que poseen actualmente se calcula que unos 300 son usuarios en su red con una gran diversidad de equipos, los usuarios finales es su gran mayoría utiliza Windows 7 y en una menor cantidad Windows 8.1, muy aparte de las estaciones de trabajo poseen otros equipos como impresoras de red, tablets, etc.

4.2.2 Análisis de la infraestructura de la red.

La infraestructura para la cual se va diseñar la red inalámbrica cuenta con una extensión promedio de 1800 m^2, en la cual todas las edificaciones construidas cuentan con un segundo nivel y una con hasta un quinto nivel, todos estos ambientes están hechos de material noble con paredes de 25 cm de espesor, cuentan con un alrededor de 45 oficinas de las cuales todas tienes equipos informáticos, mobiliario de oficina, cubículos de vidrio, múltiples estantes, etc., entre de todos estos obstáculos atraviesa el cableado de la red institucional para conectar a todos los equipos de la red, presentando serias deficiencias llegando a considerarla como una red substandar, en la siguiente imagen se muestra una idea general como está distribuida la red a través de la infraestructura fisca de la institución.

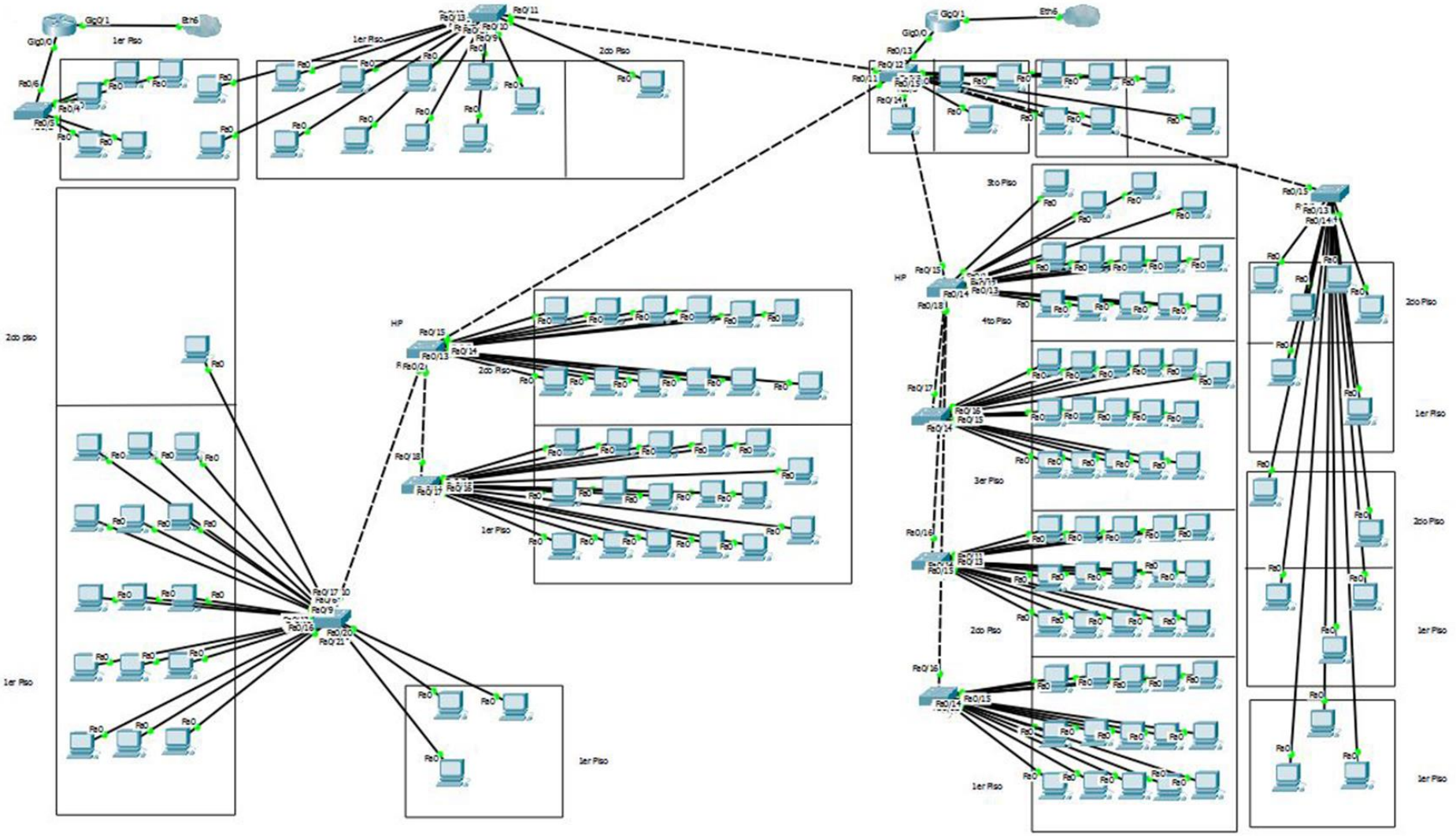

Figura 4.2 Topología de la red.

Fuente: "Elaboración propia"

4.3 Determinación de las necesidades de la red

4.3.1 Identificación de Necesidades

La actual red institucional no cumple con ningún estándar de cableado estructurado, llegando al punto de considerarla una red subestándar con serias deficiencias desde todos los puntos de vista del cual se quiera analizar, para determinar las principales deficiencias de esta red se recurrió diferentes técnicas, así como la opinión de los usuarios y sobre todo las practicas realizada en la institución para poder identificar estas necesidades que precisan ser subsanadas y las cuales son:

- Seguridad
- Velocidad
- Escalabilidad
- Control de Usuarios
- Movilidad

Estos problemas van a la par con los problemas de la institución ya que la falta de espacio físico, el hacinamiento y alto índice de rotación del personal repercuten directamente en la red para este tipo de problema la solución más idónea que se propone es una red inalámbrica ya que este tipo de red va solucionar parte la problemática principal de la red institucional y para poder solucionar las demás problemáticas se tiene que recurrir a diferentes tipos de tecnologías que integradas a la red inalámbrica va representar la solución a todos los problemas que aquejan a la red.

4.3.1.1 Selección de la Solución

Una vez conocido las necesidades de la red se realizó un análisis comparativo de las diferentes tecnologías que integradas a la red inalámbrica subsanas todas esas deficiencias teniendo en cuenta para la solución se debe contemplar visión de futuro, compatibilidad entra las distintas soluciones y sobre todo el uso de los recursos de la institución.

	Requerimiento / Protocolo	Seguridad	Velocidad		Escalabilidad	Control de Usuarios	Movilidad	Compatibilidad	
			Mínima	Máxima				Equipos	Protocolos
Recursos Existente	802.11 g	WEP	10 Mbit/s	54 Mbit/s	---	Independiente	Diferentes SSID	Si	No
	802.11 n	WPA	54 Mbit/s	600 Mbit/s	---	Independiente	Diferentes SSID	Si	Si
	Kerberos	Cliente-Servidor	---	---	Domino	Directorio Activo	Windows Server	Si	Si
	Radius	802.1X	---	---	Domino	Directorio Activo	Windows Server	Si	Si
Recursos por Adquirir	802.11 ac	WPA2	150 Mbit/s	2 Gbit/s	---	Independiente	Diferentes SSID	Si	Si
	Diameter	802.1X	---	---	Domino	Directorio Activo	Windows Server	No	No

Tabla 4.2 Comparativa de Soluciones.

Fuente: "Elaboración propia"

La solución más conveniente para subsanar las deficiencias es el uso de los protocolos de comunicación 802.11n/ac, ya que los equipos que se puede en el mercado poseen conectividad para ambos protocolos y el protocolo Radius que cumple con las características de autenticación, autorización y contabilización, el cual puede ser habilitados con los recursos que existen en la institución específicamente en el servidor Windows Server 2012 R2, la mezcla de estos protocolos dan solución a las necesidades que afronta la red actual, como también una solución para escenarios futuros.

4.3.2 Tecnología

4.3.2.1 Incorporación de protocolos

Cuando se pretende comunicar un sistema informático con otro, a través de una red inalámbrica, se requiere de la existencia de un conjunto de componentes físicos y lógicos que permitan la comunicación. Gracias a la teleinformática la cual permite la interconexión de distintos equipos y sistemas informáticos ya sea de diferente tipo o fabricante.

Para crear una metodología que sirva como guía para diseñar una red inalámbrica que va incorporar los protocolos 802.11 n/ac y Radius, los cuales dan solución a la problemática de la red y cumplen los requerimientos anteriormente mencionados para tal fin es necesario la integración de diferentes equipos que sean compatibles con estos protocolos para poder añadirlos a la red y de esa manera poder ofrecer una mayor velocidad de transmisión de datos, autenticación, autorización y contabilidad, para tal finalidad es vital definir la tecnología inalámbrica a ser utilizada, este tipo de red necesita de dispositivos como Access Point, Wireless LAN Controller, Wireless Network Interface Controller (WNIC) y Servidor de Red.

4.3.3 Dispositivos

4.3.3.1 Access Point

Los Access Point (AP) son equipos que brinda a los dispositivos que desean conectarse a la red de forma inalámbrica puedan hacerlo mediante Wi-Fi, o protocolos relacionados. Por lo general

se conecta a un Router como un dispositivo independiente o también puede conectarse a un switch para formar parte de la red y de esa manera tener una red hibrida.

- **Cisco WAP371 Wireless-AC**

Es un dispositivo que entregar alta velocidad de conectividad inalámbrica a los usuarios además brinda acceso más seguro y fiable. El Cisco WAP371 Wireless Access Point tiene doble banda 2.4/5 GHz, posee una instalación sencilla pero potente de un alto rendimiento. Ofrece funciones de clase empresarial, tales como la conectividad Gigabit Ethernet, un portal cautivo personalizable para el acceso a invitados y una seguridad robusta.

Figura 4.3 Equipo Cisco WAP371.

Fuente: "http://www.cisco.com/c/en/us/products/wireless/wap371-wireless-ac-n-dual-radio-access-point-single-point-setup/index.html"

- **Hawking HW7ACB Wireless-AC**

El HW7ACB ofrece el estándar inalámbrico más rápido y lo combina con potentes antenas de alta ganancia para mejorar su red inalámbrica en fiabilidad, alcance y cobertura. Fácil de instalar procedimientos permiten que cualquier usuario de la computadora pueda configurar.

Con capacidades integradas de Wireless-AC, este access point es compatible con el estándar IEEE 802.11 y sus protocolos 802.11 n/ac, así como con dispositivos inalámbricos compatibles a 5.0GHz para ofrecer una transferencia de hasta 750Mbps.

Figura 4.4 Equipo Hawking HW7ACB.

Fuente: http://hawkingtech.com/products/hawking_products/wireless_ac/HW7ACB.html

4.3.3.2 Wireless LAN Controller

Es un dispositivo controlador de LAN inalámbricas que se utiliza en combinación con el Protocolo de Acceso Ligero Point (LWAPP) para administrar puntos de acceso en grandes cantidades de operaciones de red. El controlador de LAN inalámbrica es parte del plano de datos en el modelo inalámbrico de Cisco. El controlador WLAN se encarga de automatizar la configuración de los puntos de acceso inalámbricos.

- **CISCO 2500 AIR-CT2504-15-K9**

Esta serie de equipos están hechos para administrar las funciones inalámbricas. Ayuda a los puntos de acceso Cisco Aironet a comunicarse en tiempo real para simplificar el despliegue y operación de redes inalámbricas. El Wireless Controller trabaja con los protocolos 802.11n/ac

los cuales proveen fiabilidad y da la flexibilidad para escalar a medida que crecen sus necesidades de la red.

Figura 4.5 Equipo cisco AIR-CT2504-5-K9.

Fuente: "http://www.cisco.com/c/en/us/products/wireless/2500-series-wireless-controllers/index.html#"

- **ZyXEL NXC2500 Wireless Controller**

El ZyXEL NXC2500 está diseñado para proporcionar a las empresas una solución que funciona como una respuesta a la planificación implementación, mantenimiento, monitoreo y al tiempo que ofrece la gestión de autenticación además el acceso para invitados. El dispositivo apoya el manejo inicial de 8 puntos de acceso y proporciona escalabilidad, con un total máximo soportado hasta 64 puntos de acceso, además ofrece tranquilidad y el futuro de las redes LAN inalámbricas centralizadas de las pequeñas y medianas-empresas.

Figura 4.6 Equipo ZyXEL NXC2500.

Fuente: "http://www4.zyxel.com/products_services/nxc2500.shtml?t=p"

4.3.3.3 Tarjetas de Red Inalámbricas

Una tarjeta de red inalámbrica (WNIC) es un controlador de interfaz de red que se conecta a una red de ordenadores basada en ondas de radio, al igual que otras tarjetas de red, funciona en la Capa 1 y Capa 2 del modelo OSI. Una WNIC es un componente esencial para que una PC de escritorio pueda integrase a la red inalámbrica.

- **Satechi® Wireless Mini Dual Band Wi-Fi USB Mini Adapter**

El Satechi Wireless Mini Adaptador USB Wifi es un adaptador para actualizar la velocidad de la red inalámbrica de una computadora. Alcanza una velocidad de hasta 433Mbps, incluso en equipos antiguos para que se unan a una red inalámbrica. Con el adaptador Wifi Satechi, todo lo que necesita para la configuración es instalar los controladores y conecte a un puerto USB.

Figura 4.7 Equipo Satechi Wireless Mini Dual Band Wi-Fi USB Mini Adapter

Fuente: "http://www.amazon.com/Satechi%C2%AE-Wireless-Adapter-Supports-Windows/dp/B00XV4EERC"

- **Sabrent Hi-Gain AC600 Dual Band Wi-Fi USB Mini Adapter**

El Sabrent Hi-Gain AC600 Dual Band Wi-Fi USB Mini Adapter es un adaptador para actualizar la velocidad de la red inalámbrica de una computadora. Alcanza una velocidad de hasta 433Mbps, incluso en equipos antiguos para que se unan a una red inalámbrica. Con el adaptador Wifi Satechi, todo lo que necesita para la configuración es para instalar los controladores y conecte a un puerto USB.

Figura 4.8 Equipo Sabrent Hi-Gain AC600 Dual Band Wi-Fi USB Mini Adapter.

Fuente: http://www.amazon.com/Sabrent-Hi-Gain-Adapter-Connection-NT-WLAC/dp/B00SJ095FO

4.3.4 Servidores

Para poder administrar todos los elementos hardware y software que van a componer la red va ser necesario un servidor de red, que es un dispositivo que proporciona funcionalidad a otros programas o equipos, llamados clientes. A este tipo de arquitectura se le denomina como un modelo cliente servidor, mediante el cual un solo cálculo global se distribuye a través de múltiples procesos o dispositivos.

4.3.4.1 Radius Server

El protocolo RADIUS cuenta con una serie de características que lo califica como un sistema de autenticación flexible y efectivo para las más diversas condiciones de una red. A continuación, se describirán las principales ventajas

- Modelo cliente/servidor
- Seguridad

- Flexibilidad y adaptabilidad
- Protocolo extensible
- Compatibilidad

Otro factor clave para escoger este protocolo es que la institución cuenta con Windows Server 2012 R2 en el cual esta implementado el Directorio Activo de la institución, esto brinda la posibilidad de habilitar un Network Policy Server (NPS) que es la implementación del protocolo Radius en ambiente Windows Server, las distintas ventajas que ofrece esta arquitectura Windows son:

- Configurable como un proxy Radius que reenvía las solicitudes de conexión a otros servidores Radius para que estos realicen su procesamiento.
- Escalable a un sistema de NPS. Sistema de protección de acceso a la Red, basado en el cumplimiento de requisitos en el cliente, antivirus, parches de seguridad, etc.
- Totalmente compatible con la base de datos de cuentas de usuario del Active Directory Domain Services (AD DS**).**

La implementación básicamente facilitara el uso de políticas de red para re direccionar el acceso a grupos específicos dentro del Directorio Activo. Para una mejor administración los usuarios no serán añadidos directamente al grupo universal; en lugar de eso se los añadirá a grupos separados que sí serán miembros del grupo universal y, seguidamente, agregar usuarios a esos grupos. Podemos ver un resumen de este procedimiento en la siguiente imagen:

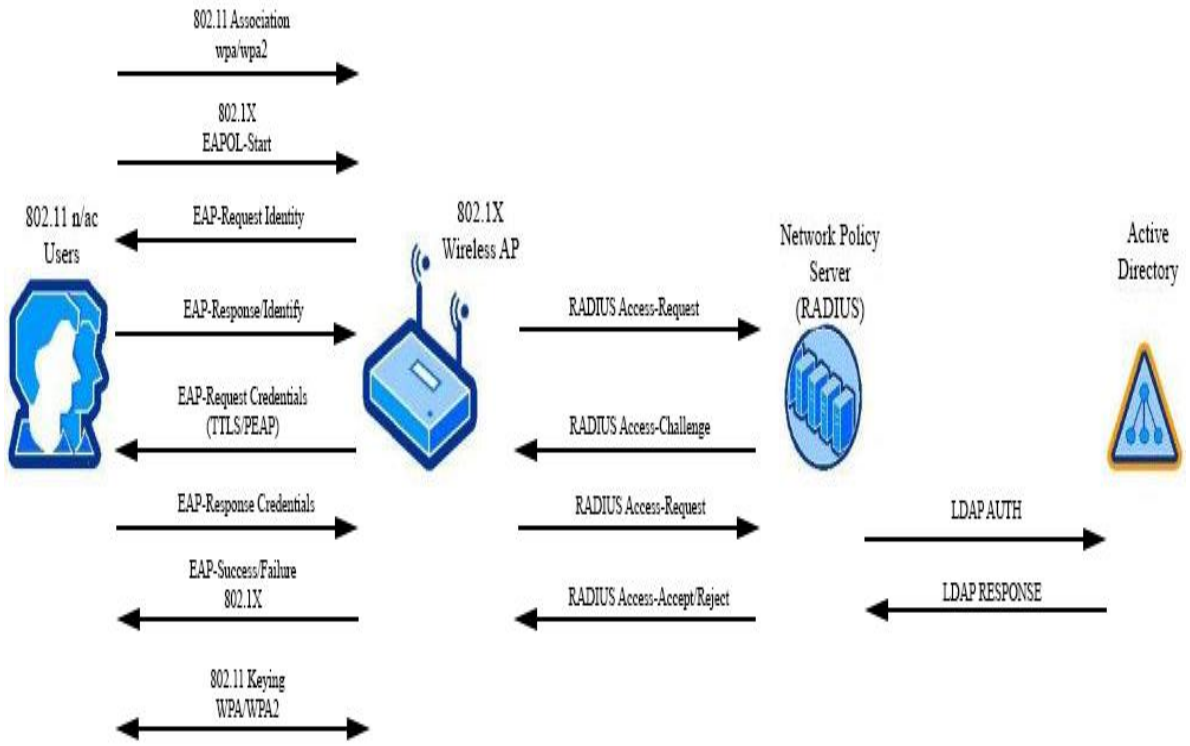

Figura 4.9 Funcionamiento NPS.

Fuente: "Elaboración Propia"

4.4. Diseño físico de la red

4.4.1 Distribución de la red

EL principal problema que se enfrenta al diseña una red inalámbrica es el tipo de infraestructura del lugar donde se desea montar la red, ya que puede ocasionar que no se reciba la señal de los puntos de acceso hacia las tarjetas inalámbricas por atenuaciones de señal, los diferentes tipos de material de acuerdo a su composición representa un obstáculo muy importante para la propagación de las ondas de radio. No todos están estructurados de la misma manera esa va varias dependiendo el lugar y los factores climáticos. Por esto hay que inspeccionar el lugar previamente. El entorno físico va ser un factor clave ya que las áreas despejadas o abiertas

proporcionan un mejor alcance de la señal de los Access Point que las áreas cerradas o congestionadas; todos estos aspectos son relevantes al momento de la distribución adecuada de los Access Point.

4.4.1.1 Software para el estudio de sitio

Para realizar el estudio del sitio se emplea el software Ekahau Site Survey de Ekahau Inc., que proporciona a los profesionales de telecomunicaciones la visión detallada de todos los requerimientos para planificar, instalar, verificar y documentar redes WLAN 802.11g/n/ac. Ekahau Site Survey es una herramienta de estudio de la instalación inalámbrica y mucho más; proporciona desde el tipo de material de las estructuras hasta los diferentes modelos de Access Point que se encuentran en el mercado, lo que simplifica considerablemente el análisis del entorno de la red WLAN y permite optimizar el rendimiento.

4.4.1.2 Ubicación de los Access Point

Mediante el software se distribuirá los access point de manera se cubra la mayor parte de las instalaciones de la Gerencia Regional de Salud Arequipa teniendo en cuenta el menor uso de access point para este fin, el software permite ingresar las dimensiones en el edificio, brinda la posibilidad de establecer los obstáculos que se van a presentar ya sea el tipo de material con que fue construido el edificio para tener en cuenta la perdida de señal de los Access Point. Las siguientes figuras son la representación de los diferentes ambientes del edificio, mostrando la distribución, cobertura e intensidad de señal inalámbrica de los equipos para cada ambiente. La figura 4.9 muestra el plano de la infraestructura del primer piso de la zona A con la distribución de los Access Point, indicando la intensidad de señal y cobertura.

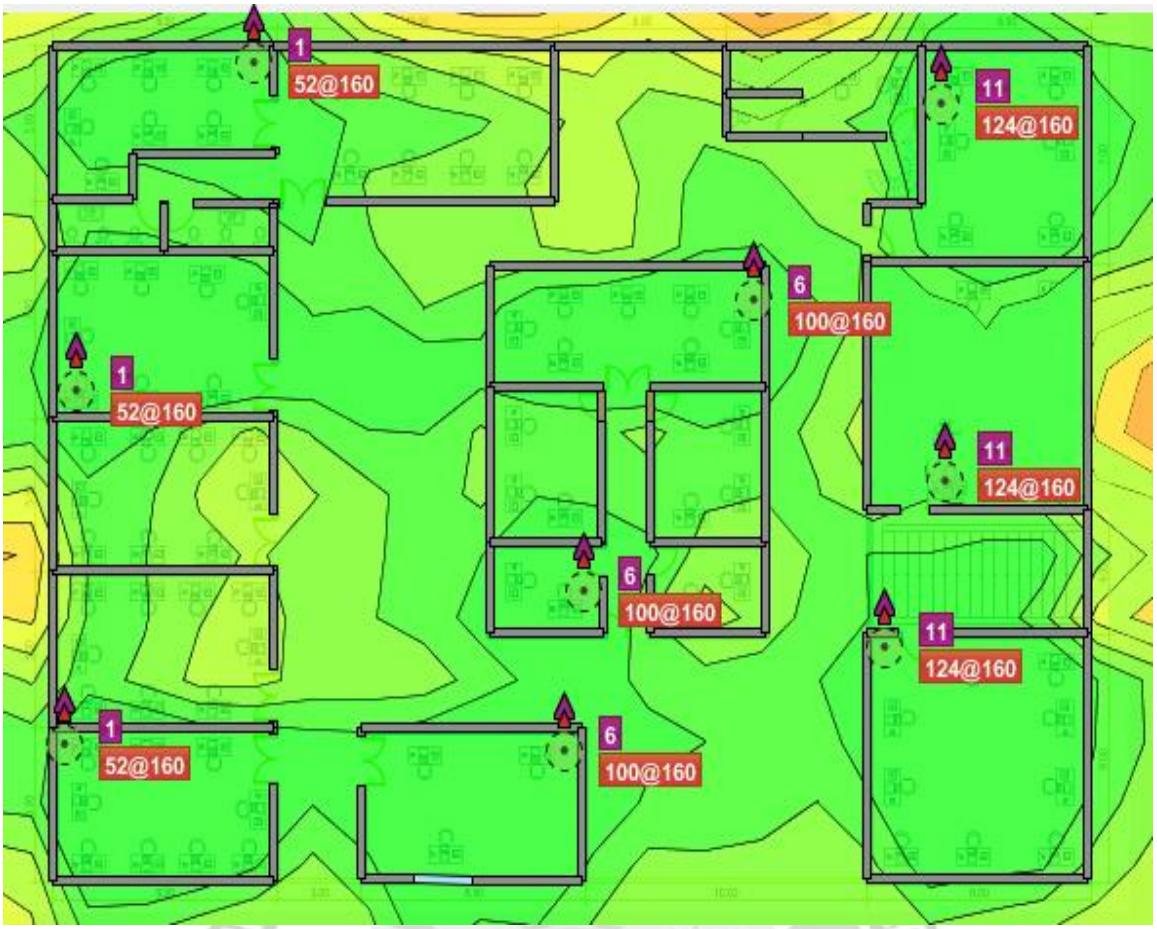

Figura 4.10 Distribución de Access Point- Primer Piso zona A.

Fuente: "Elaboración Propia"

# AP	Estándar	Canal	Banda	Cobertura	Personal
3	802.11 n	1	2.4 GHz	65 m^2 ± 5 m^2	50 aprox.
	802.11 ac	52	5 GHz	32 m^2 ± 3 m^2	
3	802.11 n	6	2.4 GHz	65 m^2 ± 5 m^2	20 aprox.
	802.11 ac	100	5 GHz	32 m^2 ± 3 m^2	
3	802.11 n	11	2.4 GHz	65 m^2 ± 5 m^2	27 aprox.
	802.11 ac	124	5 GHz	32 m^2 ± 3 m^2	

Tabla 4.3 Descripción de la Figura 4.10.

Fuente: "Elaboración propia"

La figura 4.10 muestra el plano de la infraestructura del segundo piso zona A con la distribución de los Access Point, también se indica la intensidad de señal y la cobertura tanto en m^2 como personal beneficiado.

Figura 4.11 Distribución de Access Point- Segundo Piso zona A.

Fuente: "Elaboración Propia"

# AP	Estándar	Canal	Banda	Cobertura	Personal
3	802.11 n	1	2.4 GHz	65 m^2 ± 5 m^2	10 Aprox.
	802.11 ac	52	5 GHz	32 m^2 ± 3 m^2	
2	802.11 n	6	2.4 GHz	65 m^2 ± 5 m^2	17 Aprox.
	802.11 ac	100	5 GHz	32 m^2 ± 3 m^2	
3	802.11 n	11	2.4 GHz	65 m^2 ± 5 m^2	27 Aprox.
	802.11 ac	124	5 GHz	32 m^2 ± 3 m^2	

Tabla 4.4 Descripción de la Figura 4.11.

Fuente: "Elaboración propia"

La figura 4.11 muestra el plano del tercer al quinto piso donde las estructuras de estos son iguales por eso se hace referencia en un solo mapa. Asimismo, se muestra la ubicación de los access point, la intensidad de señal y la cobertura tanto en m^2 como personal beneficiado.

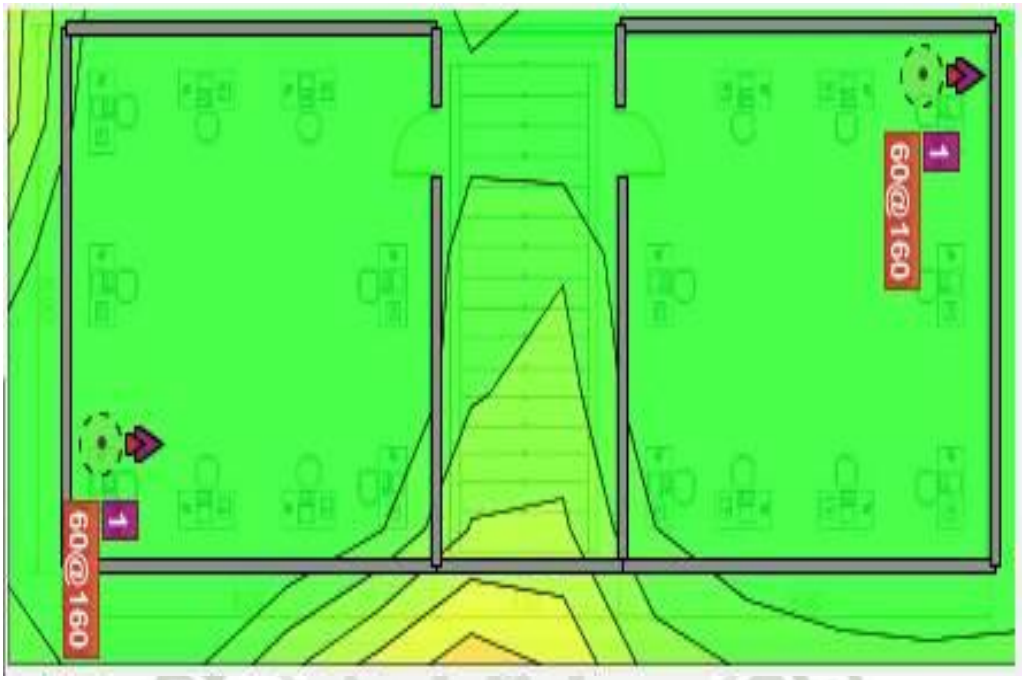

Figura 4.12 Distribución de Access Point- Tercer al Quinto Piso zona A.

Fuente: "Elaboración Propia"

# AP	Nivel	Estándar	Canal	Banda	Cobertura	Personal
2	3er Piso	802.11 n	1	2.4 GHz	65 m^2 ± 5 m^2	18 Aprox.
		802.11 ac	52	5 GHz	32 m^2 ± 3 m^2	
2	4to Piso	802.11 n	6	2.4 GHz	65 m^2 ± 5 m^2	18 Aprox.
		802.11 ac	100	5 GHz	32 m^2 ± 3 m^2	
2	5to Piso	802.11 n	11	2.4 GHz	65 m^2 ± 5 m^2	18 Aprox.
		802.11 ac	124	5 GHz	32 m^2 ± 3 m^2	

Tabla 4.5 Descripción de la Figura 4.12.

Fuente: "Elaboración propia"

La figura 4.12 muestra el plano del primer piso zona B que se encuentra al lado del local principal de la Gerencia Regional de Salud Arequipa, que actualmente es el local principal de almacén de la dirección de Medicamentos, Insumos y Drogas. Asimismo, se muestra la ubicación del AP, intensidad de señal y cobertura.

Figura 4.13 Distribución de Access Point- Primer Piso zona B.

Fuente: "Elaboración Propia"

#	Estándar	Canal	Banda	Cobertura	Personal
3	802.11 n	6	2.4 GHz	65 m^2 ± 5 m^2	8 Aprox.
	802.11 ac	60	5 GHz	32 m^2 ± 3 m^2	

Tabla 4.6 Descripción de la Figura 4.13.

Fuente: "Elaboración propia"

La figura 4.13 muestra el plano del segundo piso zona B donde se encuentra el ambiente que serán usado para mudar al personal del ambiente principal para combatir el hacinamiento. Asimismo, se muestra la ubicación de los access point, la intensidad de señal y la cobertura tanto en m^2 como personal beneficiado.

Figura 4.14 Distribución de Access Point- Segundo Piso zona B.

Fuente: "Elaboración Propia"

#	Estándar	Canal	Banda	Cobertura	Personal
2	802.11 n	11	2.4 GHz	65 m^2 ± 5 m^2	6 Aprox.
	802.11 ac	128	5 GHz	32 m^2 ± 3 m^2	

Tabla 4.7 Descripción de la Figura 4.14.

Fuente: "Elaboración propia"

4.4.1.3 Arquitectura de Red

El tipo de arquitectura que se va emplear es a una red tipo campus, ya que posee múltiples capas antes que se conecte con el dispositivo final de red. Esto brinda la oportunidad de poder

usar diferentes tipos de tecnologías en función al nivel al cual se desea configurar, contando con switches de alto rendimiento en la capa central, lo cual brindara a la capa de acceso una gran facilidad a la hora de utilizarlos switches con menor nivel de complejidad, como también el uso de un Wireless LAN Controller con el cual se va gestionar todos los access point de manera centralizada aplicando todas las configuraciones requeridas en este y no de manera individual.

Para este caso en particular la arquitectura que se va emplear va una donde los dispositivos finales se van a comunicar a través de los access point y solo los equipos que no puedan contar con una tarjeta inalámbrica se van a comunicarse de manera directa con los switches, los cuales van a conectarse a los switches centrales del Data Center.

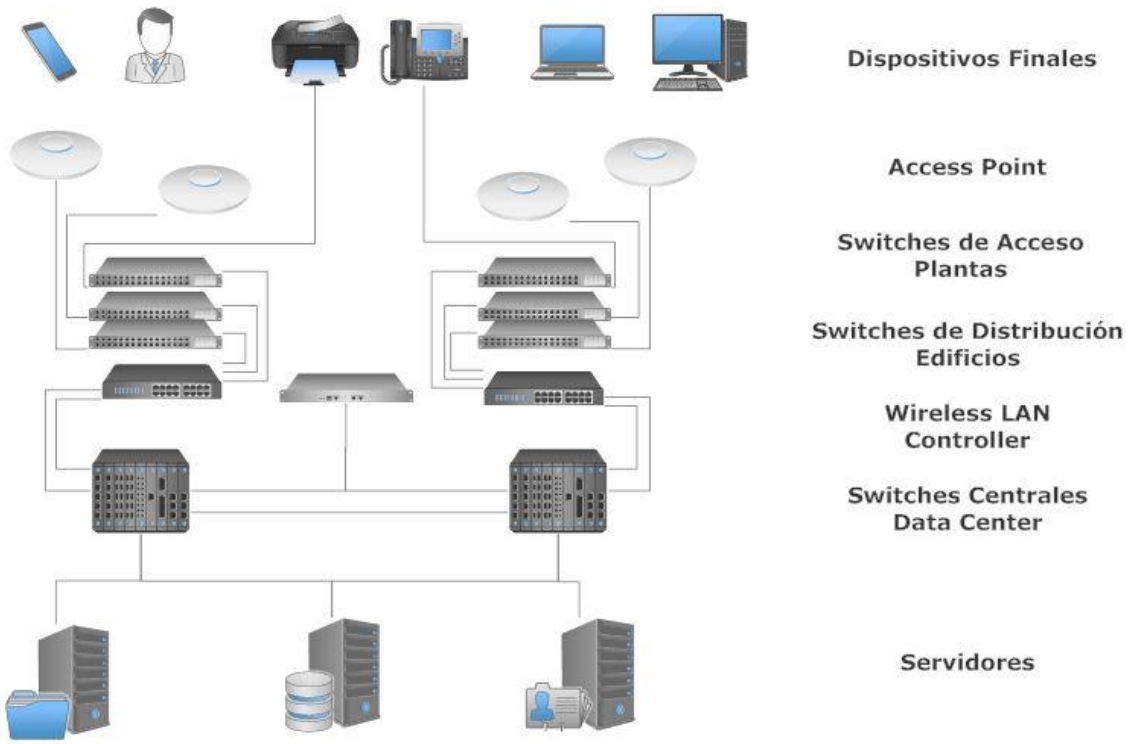

Figura 4.15 Arquitectura de Switch.

Fuente: "Elaboración Propia"

4.4.2 Análisis Financiero

La cantidad de equipos que se emplearan para la realización de este proyecto son los siguientes:

34 Access Point

1 Wireless LAN Controler

50 Tarjetas inalámbricas

Valor de Equipos		Total de Equipos	
Access Point	$ 62	Access Point	$ 2108
Wireless LAN Controler	$ 276	Wireless LAN Controler	$ 276
Tarjetas Inalámbricas	$ 17	Tarjetas Inalámbricas	$ 850
		Total	$ 3234

Tabla 4.8 Costo de equipos

Fuente: "Elaboración Propia"

El presupuesto anual que el estado le asigna a la institución para el mantenimiento de LAN es de $1500; de los cuales se emplea para las diferentes áreas.

4.4.2.1 Flujo de Caja

En el flujo de caja se va considerar principalmente el ahorro que se va tener por el costo de mantenimiento, como uno de los ingresos de valores para la implementación de este proyecto

Para el coste de mantenimiento de la nueva estructura de red WLAN se ha tomado en consideración posibles averías que pueden presentar los diferentes equipos de la red WLAN. La institución cuenta con área especializada, los cuales se tendrán que encargar de controlar el buen estado de la señal inalámbrica en los diferentes ambientes de la GEREA, así como también del mantenimiento y el posible cambio de equipos. Este beneficio va significar un ahorro sustancial a la institución respecto al costo de mano de obra elevado que se podría generar en un agente externo.

Flujo de caja	**Año 0**	**Año 1**	**Año 2**	**Año 3**	**Año 4**
Detalle de Ingresos					
Capital	4000	0	0	0	0
Presupuesto de Mantenimiento	0	1500	1500	1500	1500
Total de Ingresos	4000	1500	1500	1500	1500
Detalle de Egresos					
Costo de Implementación	3500	0	0	0	0
Costo de Mantenimiento	0	250	250	500	250
Total de Egresos	3500	250	250	500	250
Saldo Neto	500	1250	1250	1000	1250
Saldo Acumulado	500	1750	3000	4000	5250

Tabla 4.9 Flujo de Caja

Fuente: "Elaboración Propia"

4.4.2.2 Análisis Costo Beneficio

En este análisis se va indicar los beneficios que la institución puede obtener con la implementación de este proyecto, ya sea en el aspecto económico como también a nivel laboral.

En el aspecto económico el ahorro que se va experimentar por concepto de mantenimiento de la red es sustancial, pudiendo llegar a un ahorro aproximado del 600 %, teniendo como referencia que existen periodos que en los cuales el costo por concepto de mantenimiento de la red a sobrepasado el valor del presupuesto anual.

Periodo	Costo Estimado Mantenimiento Red WLAN	Costo Presupuestado Mantenimiento Red LAN
Año 1	250	1500
Año 2	250	1500
Año 3	500	1500
Año 4	250	1500

Tabla 4.10 Costo de Mantenimiento

Fuente: "Elaboración Propia"

Respecto a la parte laboral los trabajadores administrativos van a poder acceder a la red desde cualquier ubicación que se encuentren, sin tener la imperiosa necesidad de conectarse mediante un cable de red, entre otros múltiples beneficios. Esto tendrá como mayor ventaja el poder acceder a la información en tiempo real.

4.4.3 Segmentación de la Red

La segmentación de una red es la división de la misma en subredes más pequeñas las cuales estarán integradas, por una parte, de los equipos de la red principal, esto da la posibilidad de tener una escalabilidad ordenada y así aumentar el rendimiento, tomando en cuenta que existe una única topología, los mismos protocolos en un solo entorno de trabajo, para afrontar esta tarea es viable la implementación de la tecnología de VLAN que permite una administración de manera más flexible y a la vez cumple con los requerimientos de la institución, como resultado se ve una mayor productividad de los usuarios.

4.4.3.1 Adaptación de VLANs

Se precisa conocer bien los distintos perfiles de acceso que puedan existir. Para que de esa manera se pueda asignar a los diferentes perfiles una determinada red de acceso. En la mayoría de los casos su red puede estar ya creada y en algunos casos podremos definir nuevas redes para cubrir toda la casuística. Los perfiles de acceso controlados por 802.1X son:

- Equipos de la Gerencia Regional de Salud Arequipa.
    - Servidores
    - PCs de escritorio
    - Laptops.
    - Impresoras de red.
    - Equipos aislados por seguridad.
- Equipos externos.
    - Dispositivos personales de trabajadores.
    - Equipos de Invitados y Proveedores.

- Personal.

  - Trabajadores.
  - Invitados.
  - Proveedores

A partir de estos datos vamos a confeccionar la tabla matriz de asignaciones de redes.

VLANS		10 –Administrativa	20 – Mantenimiento	30 - Invitados	50 – Sin Dominio
Recursos	Servidores	✓			
	Estaciones de Trabajo	✓			
	Impresoras	✓			
	Equipos Aislados				✓
	Equipos Personales		✓	✓	
	Equipos Invitados			✓	
Perfiles	Trabajador	✓			
	Soporte	✓	✓	✓	✓
	Invitado			✓	
	Proveedor		✓		

Tabla 4.11 Perfiles de Acceso.

Fuente: "Elaboración propia"

La VLAN 10 en la cual se asignará las estaciones de trabajo que cumplan todos los requisitos para ingresar al dominio con usuarios pertenecientes al dominio y dentro del grupo de trabajadores. Así mismo, todos los dispositivos como Servidores, Impresoras de red, fotocopiadoras tienen que ser incluidos en el dominio y únicamente los equipos que pertenezcan a la Gerencia Regional de Salud Arequipa.

Para la VLAN 20 aquí se encuentran los usuarios conocidos, registrados en el dominio, pero que estén usando equipos externos (laptops, smartphones o equipos de proveedores usados para realizar tareas puntuales).

La VLAN 30 se usará para equipos que no estén registrados en el dominio, pero pensados para uso externo, por ejemplo, invitados, expositores, etc. El Usuario validado tampoco ha de estar en el dominio.

Finalmente, la VLAN 50 para equipos conocidos, y usados en la red, pero que no cumplen con los requisitos para ser registrados en el dominio y en la VLAN 10. Como vendría a ser servidores o equipos de red, adquiridos por la institución, que debido a la garantía o soporte no pueden contar con política de actualización de parches de seguridad, actualización de antivirus lo cual no permite su inclusión en el Dominio. Procederemos a realizar su registro atreves de su dirección MAC en AD. Este tipo de configuración abierta brinda la oportunidad de asumir nuevos roles y con ello nuevas redes según vaya evolucionando la complejidad del entorno de trabajo. Para verificar la versatilidad y flexibilidad, a nivel de políticas, que permite al sistema, es suficiente los 4 roles descritos anteriormente.

4.4.3.2 Asignación de direcciones IP

La asignación las direcciones IP se tienen que tomar en consideración el crecimiento y la seguridad de la Gerencia Regional de Salud por tal motivo se opta por direccionamiento VLSM teniendo en cuenta que para la VLAN administrativa requiere alrededor de 150 direcciones IP, la VLAN mantenimiento solo son necesario 10 IP, laVLAN administrativa va contar con alrededor de 100 IP y por ultimo la VLAN sin dominio solo son necesarias 25 IP, para tal

motivo se realiza la distribucion VLSM de las direcciones IP para las VLANs como también para el Data Center.

	Dirección IP	Mascara de Subred	Gateway	Interfaz
Administrativa	128.10.0.0	255.255.255.0	128.10.0.1	gigabitEthernet 0/0.10
Invitados	128.10.1.0	255.255.255.128	128.10.1.1	gigabitEthernet 0/0.20
Mantenimiento	128.10.1.128	255.255.255.224	128.10.1.129	gigabitEthernet 0/0.30
Sin Dominio	128.10.1.160	255.255.255.224	128.10.1.161	gigabitEthernet 0/0.50
Data Center	128.10.1.192	255.255.255.240	128.10.1.193	gigabitEthernet 0/1

Tabla 4.12 Asignación de IPs.

Fuente: "Elaboración propia"

4.5 Diseño lógico de la red

4.5.1 Incorporación al Directorio Activo

En el Directorio activo es donde se ubican todas las cuentas de los grupos, usuarios, equipos, etc. por tal motivo es imprescindible la integración con la red para poder accesar a la base de datos del Directorio Activo para poder administrar a todos los usuarios que van hacer uso de la red y poder aplicar políticas de red para tener una adecuada administración de los recursos de la misma.

Adaptando las distintas VLANS de acuerdo a los diferentes perfiles necesarios para el correcto desenvolvimiento de la red, se procede crear en el directorio activo los diferentes grupos de seguridad en los cuales se colocarán los objetos. Ya definidas las redes virtuales en función de los diferentes perfiles que componen la red, una buena práctica es generar los grupos de

seguridad para cada VLAN. Los nombres de los diferentes grupos existentes van de acuerdo a las funciones de los estándares usados en la Gerencia Regional de Salud, para una mejor administración se adicionará una referencia a la VLAN donde trabajaran los diferentes equipos. Así, lo grupos creados serán:

- GS_GERESA_VLAN10
- GS_GERESA_VLAN20
- GS_GERESA_VLAN30
- GS_GERESA_VLAN50

Con esto conseguiremos asignar un nuevo elemento al directorio activo, lo que sigue es asignar el grupo de seguridad de acuerdo al perfil que le corresponda. El mayor reto va ser la integración de estos grupos con los equipos que ya son parte del dominio. Para realizar esto se aplicará un esquema de implementación.

4.5.2 Configuración del Directorio Activo

Se procede a realizar la respectiva configuración de los diferentes grupos de usuarios como de las maquinas en sus respectivos perfiles de acceso previamente establecidos. Muy aparte del tipo de perfil de cada equipo o usuario todos precisan cumplir con un requisito primero antes de tener permisos conexión remota controlada por políticas de acceso. Para realizar esta configuración se procede a verificar las propiedades de los objetos, equipos y usuarios que posean permisos de acceso remoto controlado por políticas de marcado y verificar que la opción de no retornar llamada al usuario (No Callback) este seleccionada.

Esta configuración es útil principalmente por razones de seguridad, así como de otra índole correspondiente, mediante esta se puede denegar que un objeto ya sea maquina o usuario tenga acceso a cualquier red de la institución sin verse forzado a la delimitación de acceso del nivel capa 2 (switch). Se puede ver estas opciones en la siguiente imagen:

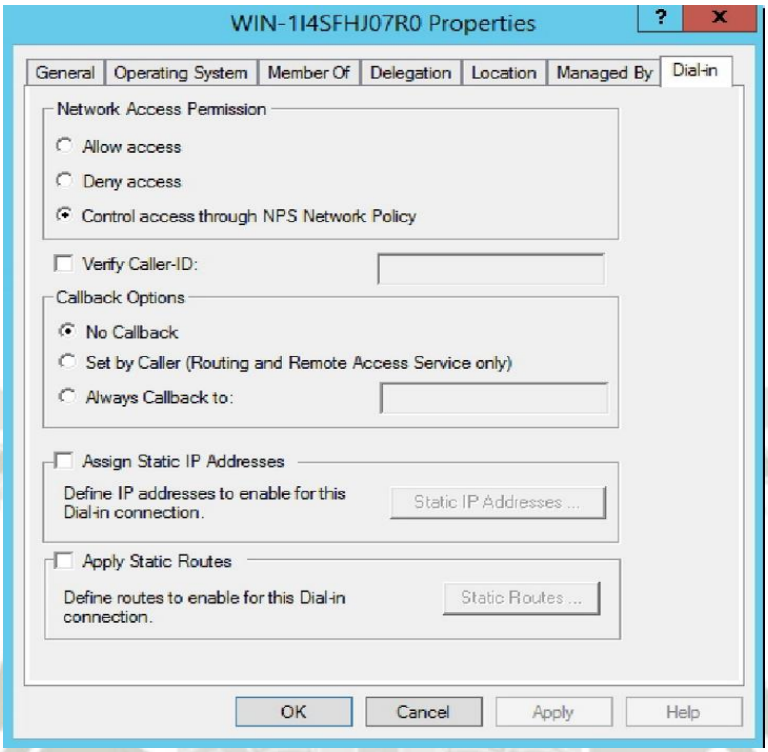

Figura 4.16 Políticas de Marcado del Directorio Activo.

Fuente: "Elaboración Propia"

4.5.3 Incorporación de VLANs al Directorio Activo

4.5.3.1 Acceso a la red Administrativa

Los equipos a los cuales se le autoriza la conexión a la red Administrativa tienen que ser propiedad de la GERESA y son:

- PCs de escritorio

- Laptops
- Impresoras de red
- Fotocopiadoras
- Escáneres

Se crea los grupos locales dentro del dominio para poder incluir ahí a todos los usuarios que correspondan con los tipos de perfil mencionados. Para adicionar un grupo, se tiene que dirigirse al administrador de usuarios y equipos del Directorio Activo una vez ahí es preciso situarse en la unidad organizativa (dominio) y se sigue los siguientes pasos:

1. Sobre "Grupos", botón derecho y se pulsa en nuevo.
2. Se introduce el nombre del grupo: ejemplo: GS_GERESA_RadiusVlan10
3. El ámbito habrá de ser: "Global".
4. Tipo de grupo se selecciona "Seguridad".

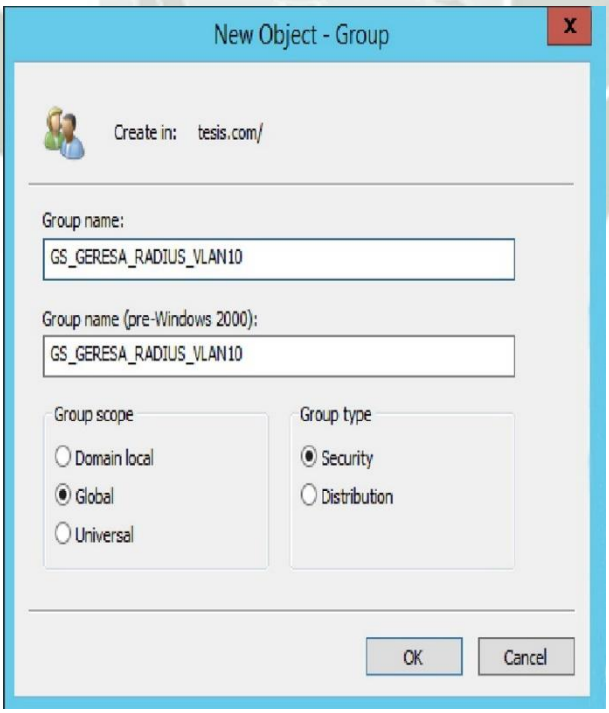

Figura 4.17 Nuevo grupo en el Directorio Activo.

Fuente: "Elaboración Propia"

Para todas las PCs de escritorio y laptops se sabe que por diseño estos equipos una vez incluidos en el directorio activo, forman parte del grupo de seguridad local llamado "Domain Computers". Que una vez validado por un servidor Radius, se delega la tarea de validación de usuarios de la red Administrativa a los controladores de dominio.

Para el resto de equipos es necesario seguir otro método ya que estos no pueden realizar un proceso de validación en el directorio activo. El cual se basa en un control de identificación a través de la dirección MAC; por tal motivo se tiene que generar una cuenta de usuario local, que posea nombre de usuarios y contraseña, que tendría que ser la misma dirección MAC del equipo. Por este tipo de características solo se usará la interfaz de red cableada. Una vez generado el grupo se procede a incluir en él los objetos creados:

- Los equipos que no pueden iniciar sesión en el servidor de dominio (por ejemplo, una impresora de red) se pueden añadir al sistema como un usuario del dominio considerando que es necesario que su nombre y contraseña (en minúsculas) tienen que ser la dirección MAC del equipo. Estos objetos son añadidos al grupo GS_GERESA_RadiusVlan10.

Vemos un ejemplo de usuarios de este tipo:

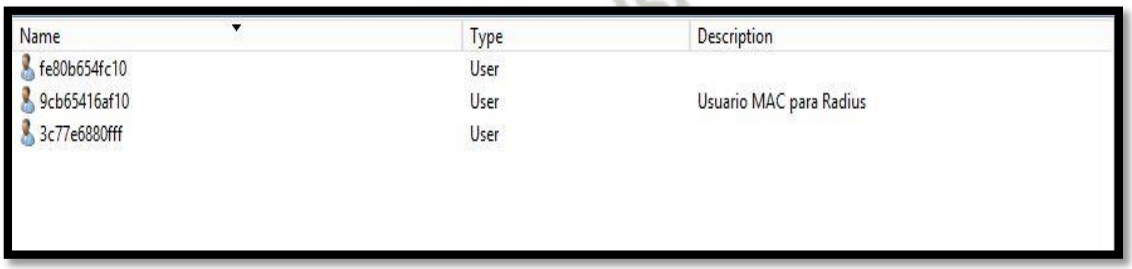

Figura 4.18 Usuarios MAC.

Fuente: "Elaboración Propia"

4.5.3.2 Acceso a la red Mantenimiento

Esta red está diseñada con el fin de ser utilizada mediante dispositivos que den mantenimiento a la red ya sea por parte del equipo de soporte o algún proveedor, teniendo en cuenta que para ambos casos es necesario que estos usuarios estén registrados en el directorio activo. Por tal motivo es preciso crear un grupo de seguridad para poder incluir en dicho perfil cualquier objeto de forma independiente. Este grupo se le asignara el formato de los otros grupos para el nombre, el cual sería GS_GERESA_RadiusVlan20. En esta red se reunirá los usuarios del área de soporte, así como también los usuarios de los diferentes proveedores que tienen que tener acceso a la red aplicando políticas de seguridad en este grupo, otro factor importante es que aquí no se tendrá en cuenta los dispositivos sino los usuarios. Para ello podemos basarnos en un grupo interno del dominio que ya los incluye:

- Domain Users.

4.5.3.3 Acceso a la red Invitados

Esta red diseñada exclusivamente para el uso invitados y los equipos destinados para el uso de personal externo, la cual está controlada por el área de soporte de la institución. En la cual se creará usuarios invitados con solo derecho de salida a internet, esta red solo estará activa en la sala de conferencias y sala de reuniones de la gerencia general. Con este criterio se crea un grupo de seguridad donde incluirlos con el nombre: GS_GERESA_RadiusVlan30.

4.5.3.4 Acceso a la red Sin Dominio

En el caso de esta red la cual ese va controlar con el servicio de NPS. En la cual se concentrarán todos los equipos que por determinadas características no pueden ingresar a la red administrativa. Por tal motivo tampoco se los puede incluir dentro del dominio, continuando con el procedimiento de alta en el directorio activo atreves de la creación de usuarios cuyos nombres y contraseñas va a ser la dirección MAC correspondiente. Todos estos usuarios creados por esta red serán incluidos en otro grupo para diferenciarlos del resto de perfiles el cual vendrá a ser SG_GERESA_RadiusVlan50. Bajo esta organización de perfiles y grupos, se puede personalizar las políticas de NPS discriminando el tipo de usuario que está solicitando el acceso.

4.6 Protocolo Radius

El protocolo Radius es usado en una amplia gama de servicios, el cual usa la norma IEEE 802.1X para el control de acceso de la red, que es utilizado en redes inalámbricas. Debido a su flexibilidad, el uso de servidores RADIUS en calidad de agentes en los dispositivos de red tales como access point les permite autenticar y gestionar el acceso de un gran número de usuarios de estos servicios.

Ya que el presente proyecto es la creación de una metodología para el diseño de una red inalámbrica, la cual estará administrada mediante el protocolo Radius, por diferentes motivos no se va llevar acabo la implementación real por esa razón se ve la imperiosa necesidad de usar un software para la simulación de cómo debe realizarse las configuraciones del protocolo Radius, en esta ocasión se va ser empleo de VMWare Workstation en el cual se va correr Windows Server 2012 R2, la misma plataforma con la que cuenta la institución en este momento.

4.6.1 Instalación del Servicio

Para recrear esta configuración se parte de un servidor Windows Server 2012 R2 instalado en una máquina virtual. Contando con el sistema operativo en línea se procede en primer lugar a la instalación del servicio NPS para luego se realice la configuración respectiva.

Para su instalación se procede con la siguiente configuración la cual indica los siguientes pasos:

1. La configuración inicial para parametrizar el servidor, es agregar funciones para iniciar el asistente de instalación del acceso y directiva de redes. En el caso que este tipo de configuración no se encuentre activa, se procede desde el menú de administración del servidor a revisar sus funciones o roles.

2. En Seleccionar funciones del servidor, se selecciona Servicios de acceso y directivas de redes y a continuación, clic en Siguiente.

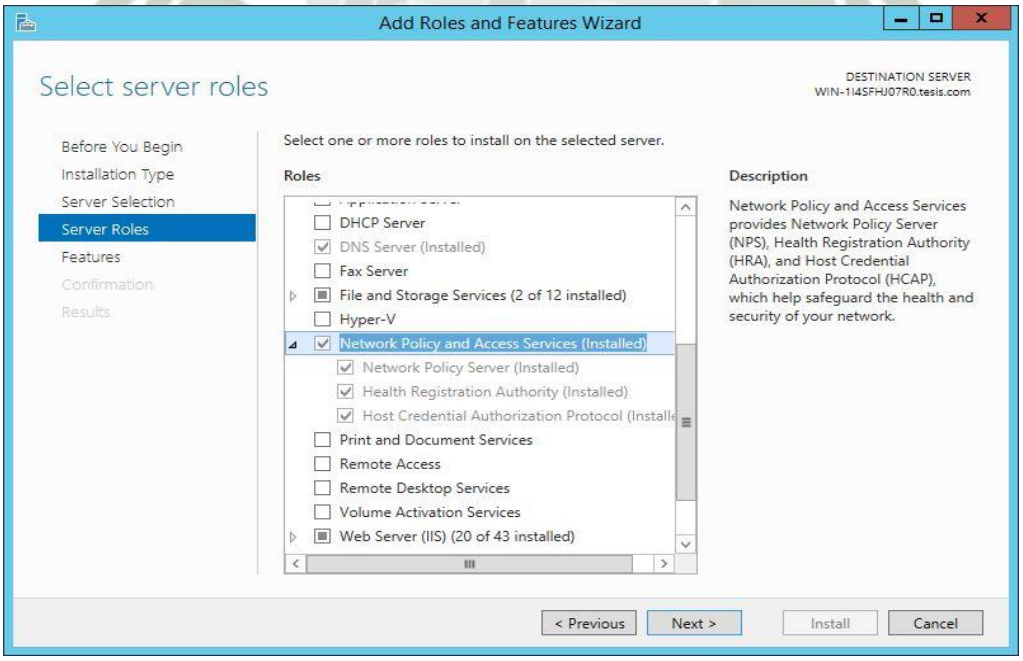

Figura 4.19 Roles del Servidor.

Fuente: "Elaboración Propia"

Este proceso se realiza en ambos servidores, sin distinción de roles a usar. Con este servidor se puede configurar 3 tipos de servicios:

- Servidor de políticas de NAP.
- Servidor RADIUS para RAS o conexiones VPN.
- Servidor RADIUS para 802.1X cableada e inalámbricas.

Para este caso en particular, se utilizará el servidor para el último tipo de servicios. Es decir, como servidor de políticas para 802.1X

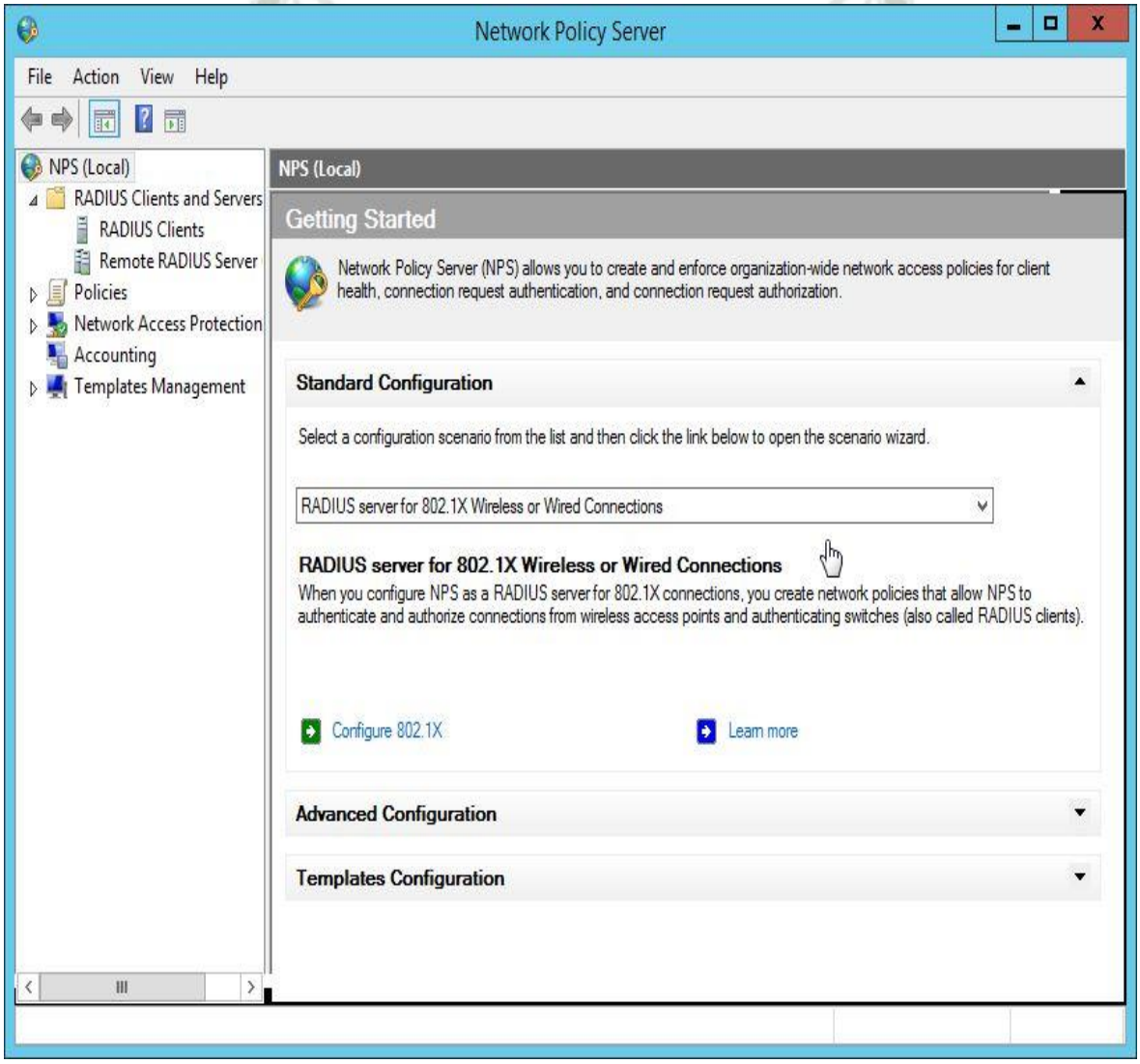

Figura 4.20 Roles del Servidor.

Fuente: "Elaboración Propia"

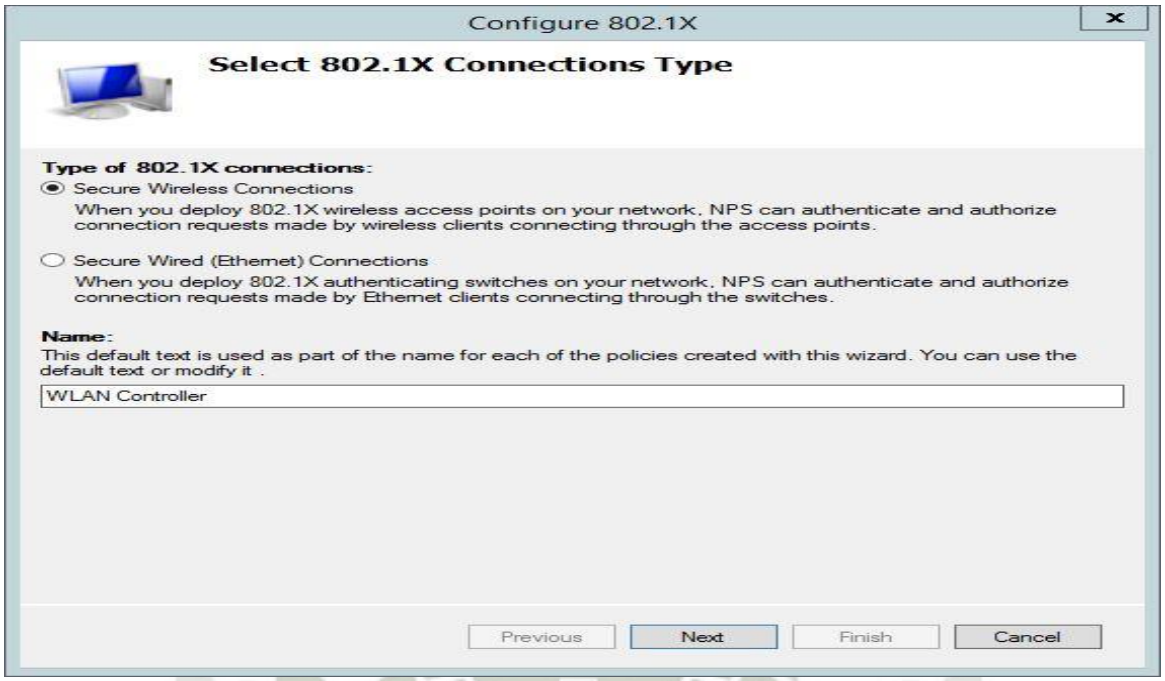

Figura 4.21 Roles del Servidor.

Fuente: "Elaboración Propia"

Figura 4.22 Roles del Servidor.

Fuente: "Elaboración Propia"

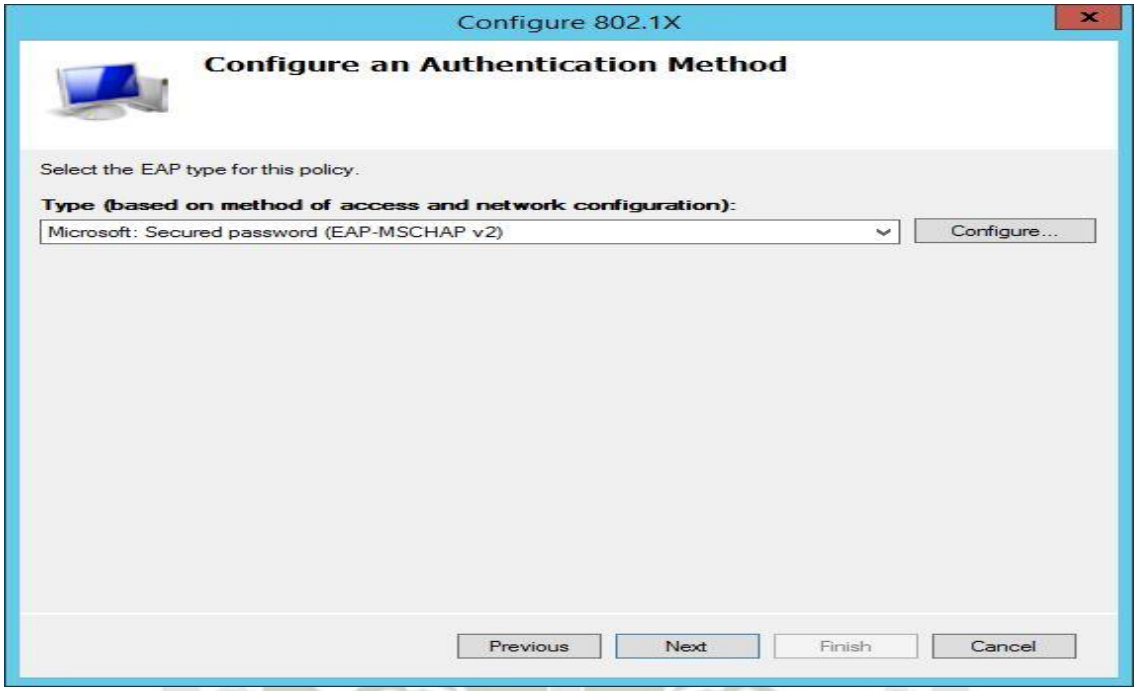

Figura 4.23 Roles del Servidor.

Fuente: "Elaboración Propia"

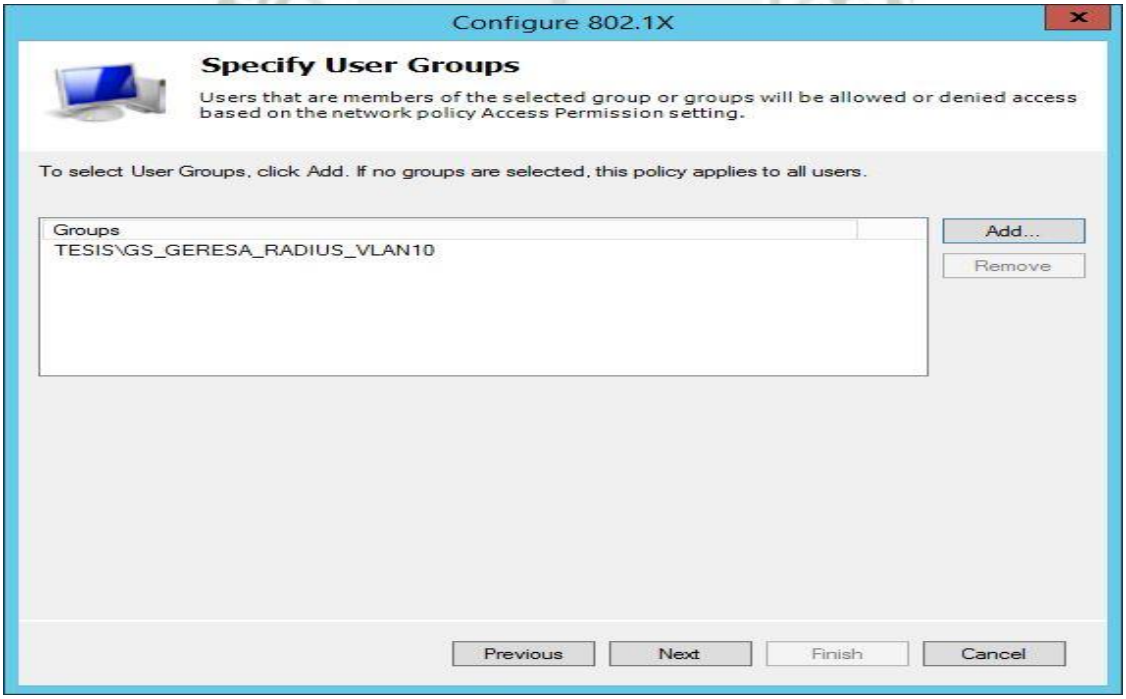

Figura 4.24 Roles del Servidor.

Fuente: "Elaboración Propia"

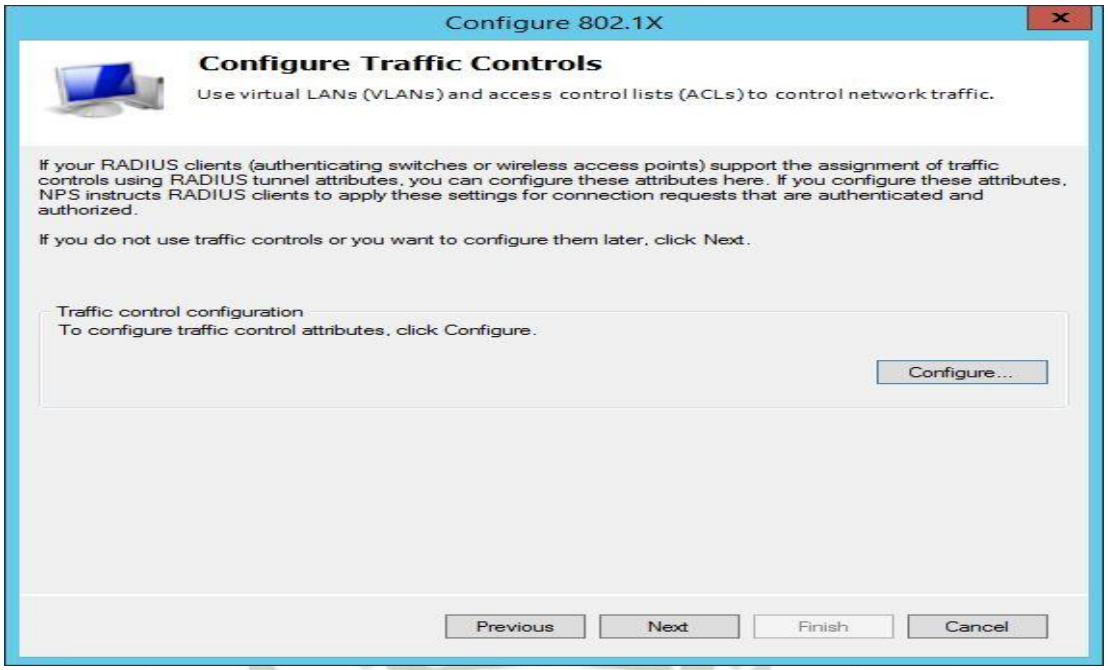

Figura 4.25 Roles del Servidor.

Fuente: "Elaboración Propia"

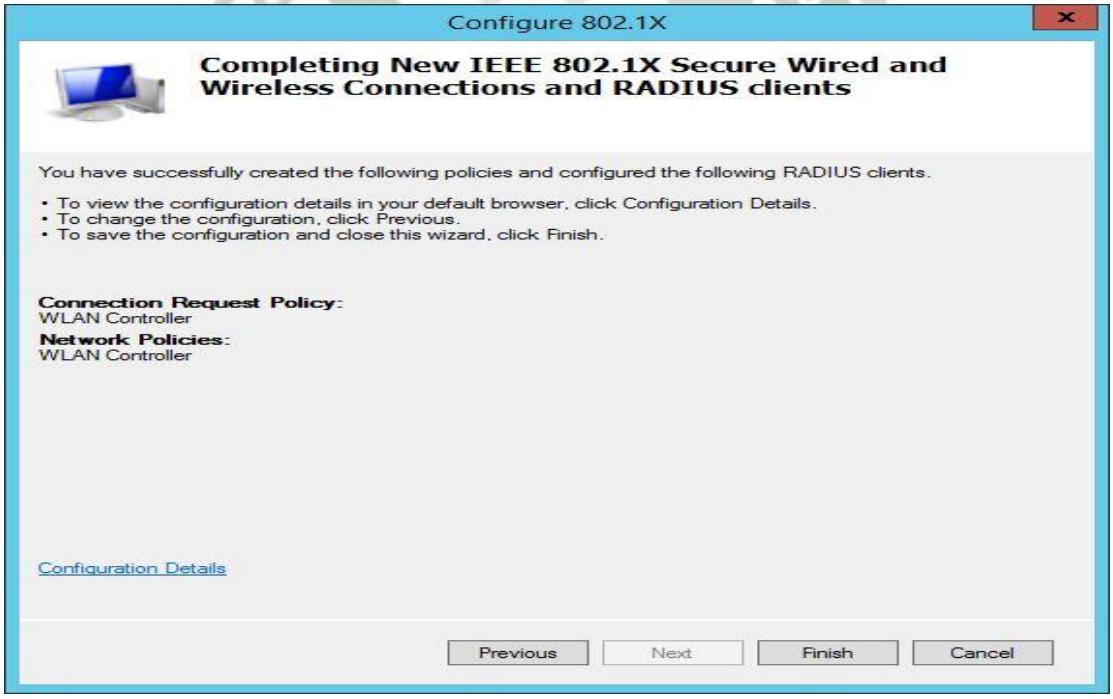

Figura 4.26 Roles del Servidor.

Fuente: "Elaboración Propia"

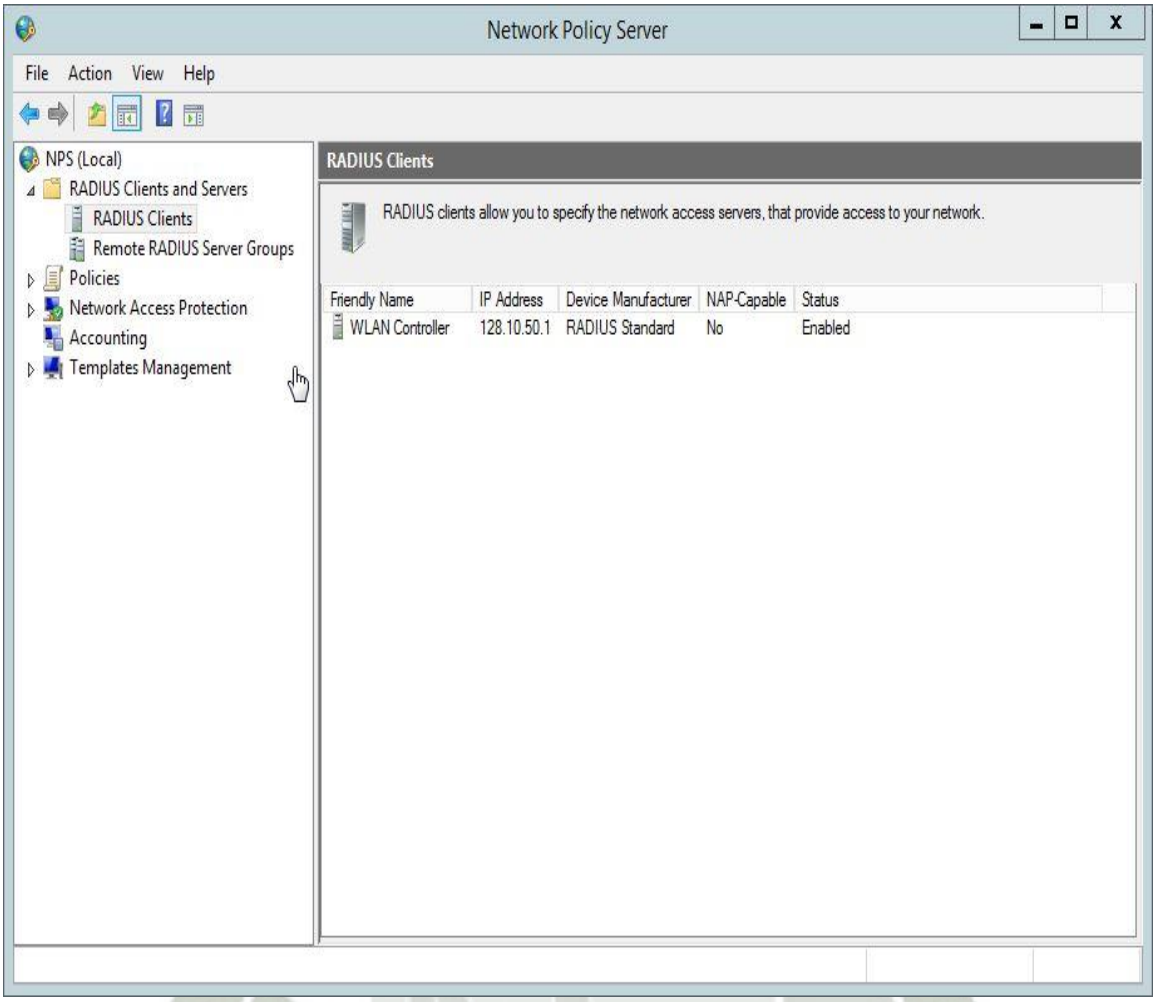

Figura 4.27 Roles del Servidor.

Fuente: "Elaboración Propia"

4.6.2 Autorización del uso del Directorio Activo.

El servidor precisa de la base de datos de cuentas de equipo y usuarios del Directorio activo, se precisa dar la autorización de este servicio a la red, para proceder con esta tarea se tiene que disponer los privilegios necesarios en el Dominio. En algún caso particular que un usuario no cumpla con estos requisitos se tendrá que realizar de manera manual por parte del departamento de TI. Los registros se pueden realizar de las siguientes maneras:

- Desde la consola de NPS.
- Usando el comando netsh.
- Mediante la consola de equipos y usuarios del Directorio Activo.

La manera más común para realizar es proceso es mediante la propia consola del NPS, y los pasos a seguir son los siguientes:

- Ingresar al Administrador del Servidor y en la sección de herramientas.
- Seleccionamos NPS (Network Policy Server).
- Dentro de este apartado se da click derecho sobre NPS (local) y a continuación, se selecciona Registrar servidor en Active Directory.
- Cuando aparezca el cuadro de diálogo Registrar servidor de directivas de redes en Active Directory se acepta dichas directivas.

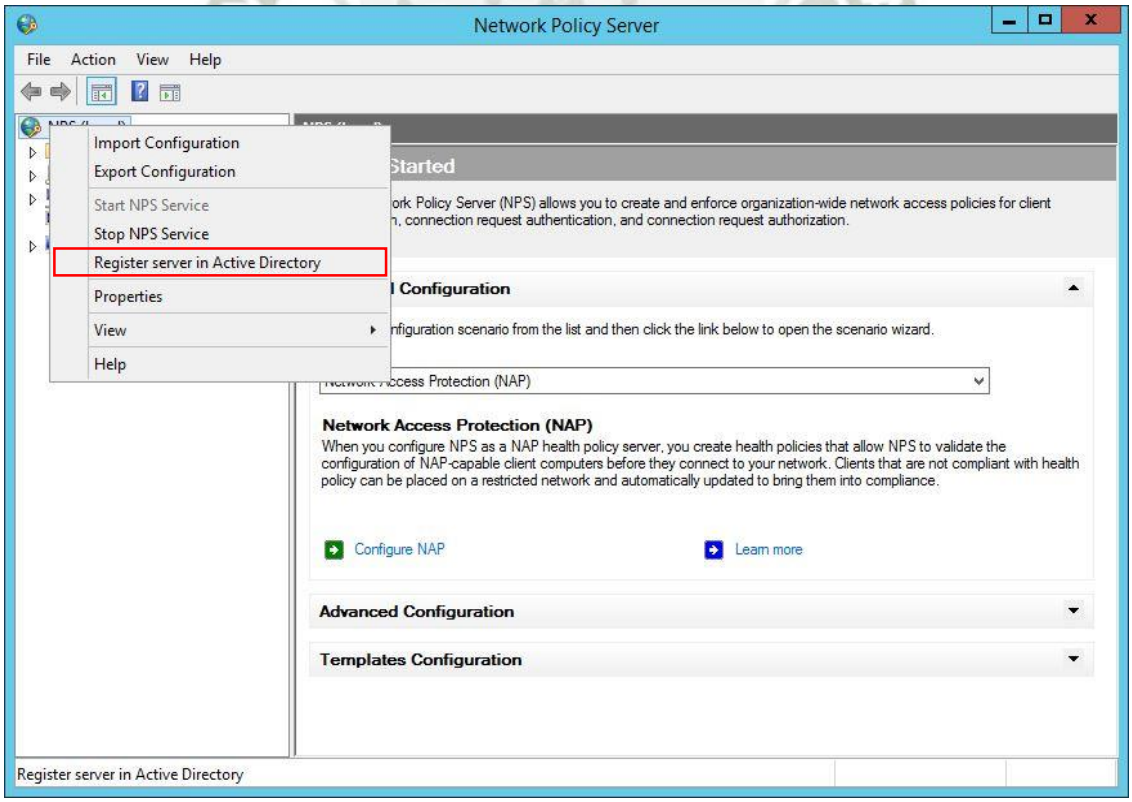

Figura 4.28 Registro del Servidor.

Fuente: "Elaboración Propia"

Una vez que se registra un servidor Radius dentro del Directorio Activo este tiene la potestad de poder ingresar a toda la información concerniente a las cuentas de usuario para que de esa manera pueda corroborar las distintas credenciales de autenticación para el acceso a la red. Una vez que las credenciales de los diferentes usuarios se autentican y se autoriza la conexión, el servidor Radius permite el acceso de los usuarios mediante condiciones específicas esto proporciona que todas las actividades de los usuarios sean registradas dentro del servidor, para una posterior auditoria. Radius permite que la red tenga el control de acceso a través de la autenticación, autorización de los usuarios por medio del registro en un punto central de los servidores Radius.

4.6.3 Configuración de Clientes Radius.

Una arquitectura de Radius, los dispositivos finales no son los clientes 802.1X, vienen a ser los equipos encargados de establecer la conexión a la red, en este proyecto son los switches y access point.

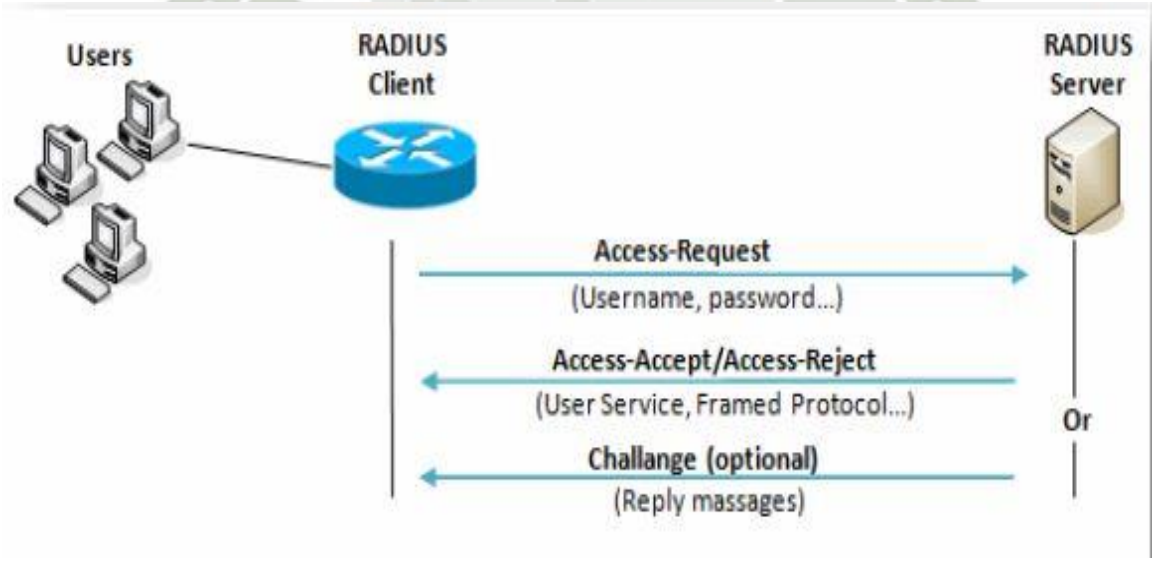

Figura 4.29 Proceso de Autenticación.

Fuente: http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

Estos equipos son los encargados de dar la autorización para ingresar a la red de acuerdo a la asignación de políticas definidas por el servidor Radius. Una forma de controlar el uso no autorizado de estas comprobaciones es establecer una palabra de paso, conocida como secreto compartido, entre los clientes del servidor Radius y el servidor NPS. La finalidad de esta clave es definir una contraseña única entre dos equipos, pudiendo establecer una comunicación de manera independiente entre cada cliente, usando siempre distintas contraseñas. Para una mejor administración se va definir una clave común para los usuarios con la finalidad de una mejor gestión de estos sistemas. Para generar el secreto compartido, se puede realizar de 2 formas:

- Manual. Se decide y se configura por medio de la consola.
- Automático. El servidor NPS genera una clave automática que tiene que ser configurada en el cliente.

Para este caso en particular se va realizar la configuración de forma manual, para poder establecer una única clave para todos los clientes. Para facilitar esta tarea se va a crear una plantilla de configuración de la clave compartida, de tal manera que cada vez que se agregue un usuario nuevo, se puedas seleccionar esta plantilla y la configuración de la clave sea de manera automática.

Dentro de la consola de NPS, se sigue los siguientes pasos:

1. Administración de plantillas.
2. Secretos compartidos, botón derecho -> Nuevo.

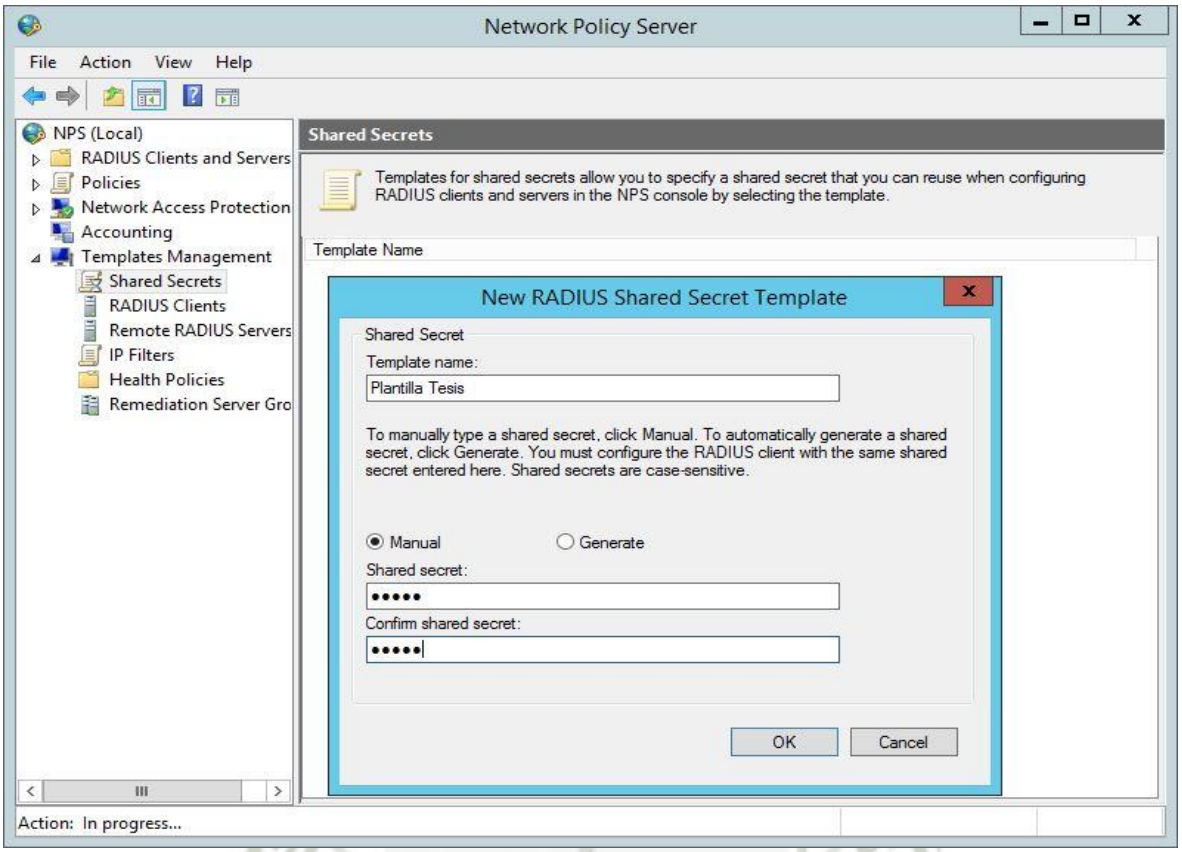

Figura 4.30 Plantilla de Secreto Compartido.

Fuente: "Elaboración Propia"

Se establece el nombre para la plantilla, y se configura manualmente el secreto compartido. Ahora procede a agregar a un cliente Radius, en el cual usara la plantilla creada anteriormente. Dentro de la consola de NPS, se sigue los siguientes pasos:

1. Clientes y servidores RADIUS
2. Clientes RADIUS, botón derecho -> Nuevo cliente
    a. Nombre y descripción: Nombre de equipo.
    b. Dirección IP: Dirección del equipo.
    c. Secreto compartido. Se selecciona la plantilla.
3. Opciones avanzadas
    a. Nombre de proveedor: RADIUS standard

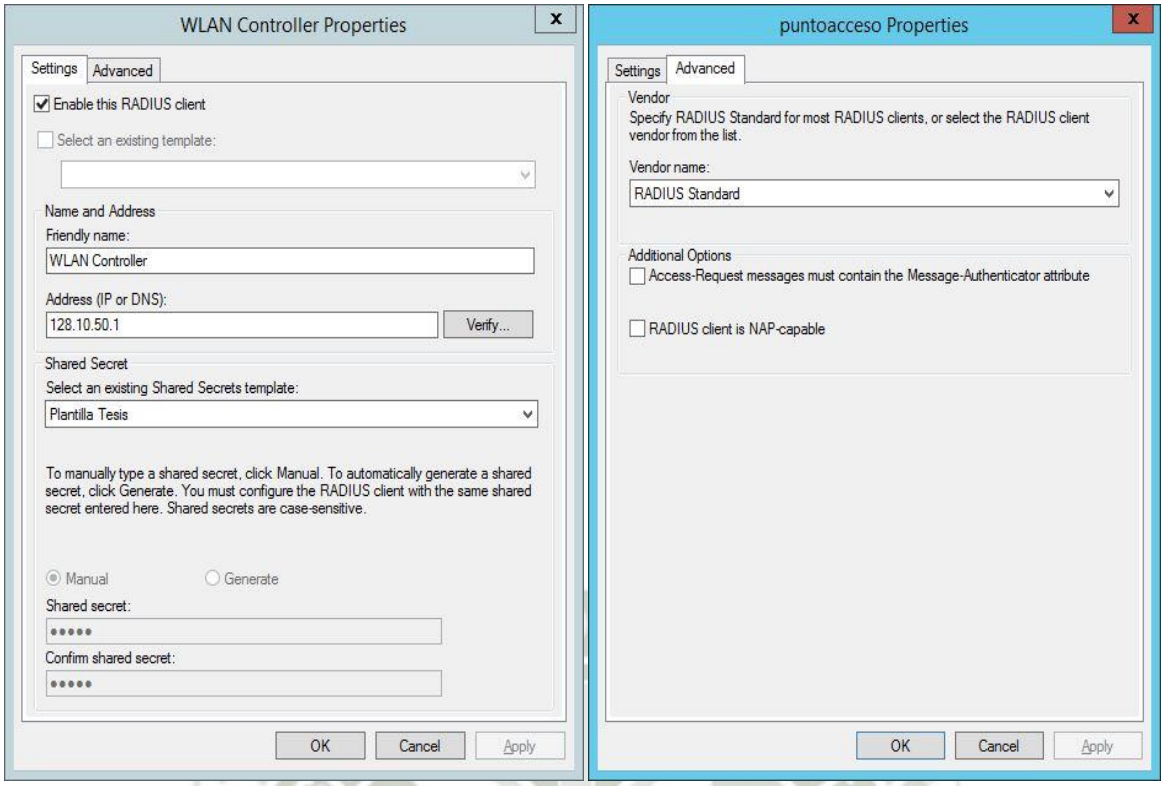

Figura 4.31 Configuración de cliente Radius.

Fuente: "Elaboración Propia"

4.6.4 Configuración De Políticas.

El funcionamiento está en relación a un sistema de colas, en la cual cada política tiene un orden, al cual se le asigna su prioridad para ejecución. Sucesivamente el sistema analiza las diferentes políticas configuradas siguiendo un orden; cuando localiza una determinada política que se va aplicar a un perfil, el sistema termina la evaluación, ejecuta la política y devuelve los resultados al cliente Radius. Al no existir ninguna política aplicable, establecer una por defecto. De las cuales se tiene varios tipos de políticas:

- Directivas de solicitud de conexión.
- Directivas de red.
- Directivas de mantenimiento.

En este caso sólo las dos primeras serán de aplicación, dado que la tercera sólo se usa en caso de añadir, al sistema, un sistema de NAP.

4.6.4.1 Directivas de Solicitud de Conexión

Con esta clase de políticas se establecerá que servidor va ser el encargado de la autenticación, autorización y administración de las solicitudes de acceso recibidas desde los clientes de NPS. Se tiene que realizar primero la definición de los tipos de conexiones que se va controlar para este proyecto va ser conexiones cableadas como inalámbricas. Por tal motivo para estos dos tipos de perfil en los que se va configurar las reglas de conexión establecidas.

Configuración de las solicitudes de conexión de la red cableada

En la consola NPS, en el subapartado de directivas de solicitud de conexión, se procede a crear una nueva política, a la cual se le asigna el nombre de "Conexiones Ethernet". En la primera ventana de configuración, se especifica "unspecified", ya que no se debe precisar el tipo de servidor de acceso a la red, ya que de lo contrario cualquier switch puede generar dichas solicitudes de acceso.

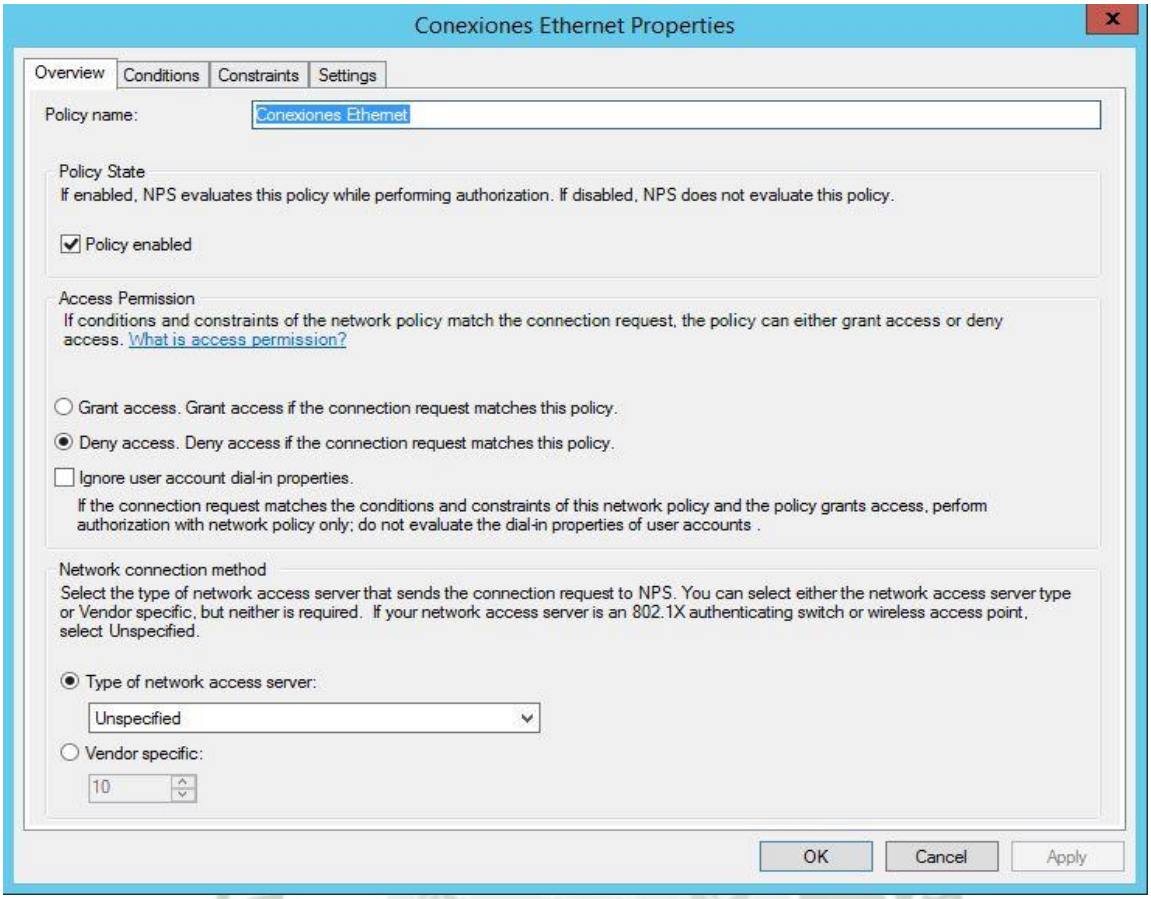

Figura 4.32 Propiedades de Conexiones Ethernet.

Fuente: "Elaboración Propia"

En el siguiente apartado: "Condiciones". Mediante el cual se va corroborar el mensaje obtenido del servidor Radius y el cual evaluara si cumple los requisitos de esta directiva. En este caso se requiere que las solicitudes de conexión en su totalidad sean reenviadas por los switches sean evaluadas por el servidor Radius. En la cual se tiene que determinar el tipo de puerto NAS, en el cual evalúa el tipo de medio utilizado por el usuario, el que se ve usar es Switches Ethernet. Agregando una nueva condición, y se elige: "Tipo de puerto NAS".

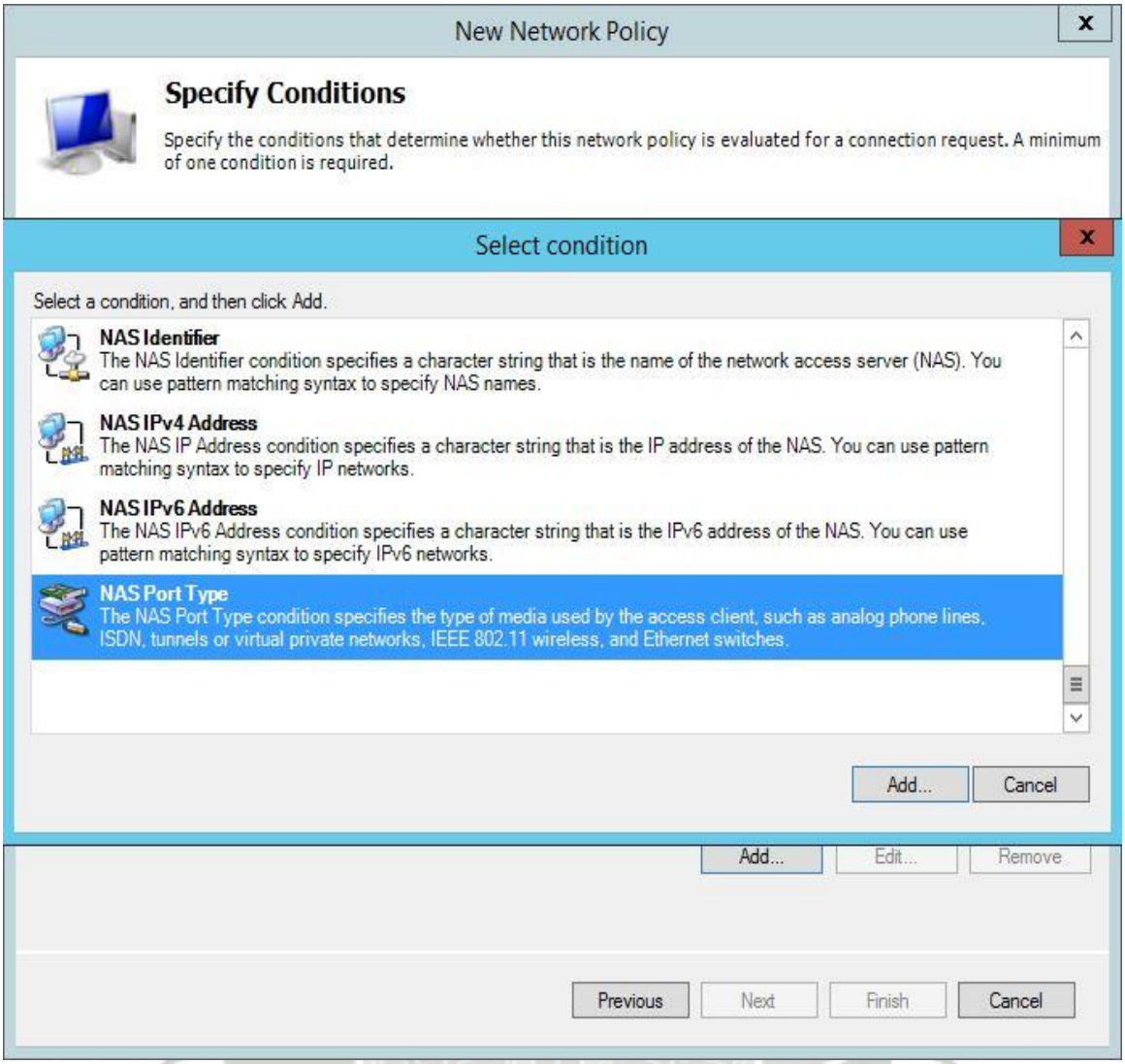

Figura 4.33 Condiciones de tipo Puerto NAS.

Fuente: "Elaboración Propia"

El tipo de conexión que llegará, desde los usuarios que no podrán realizar la autenticación va ser una conexión túnel 802.1X por Ethernet; se escoge esta alternativa. Dado que los usuarios ya han sido limitados para las diferentes VLANS, a medida que se va configurando las directivas, también se filtra los distintos niveles de comunicaciones entrantes y sus respectivas condiciones.

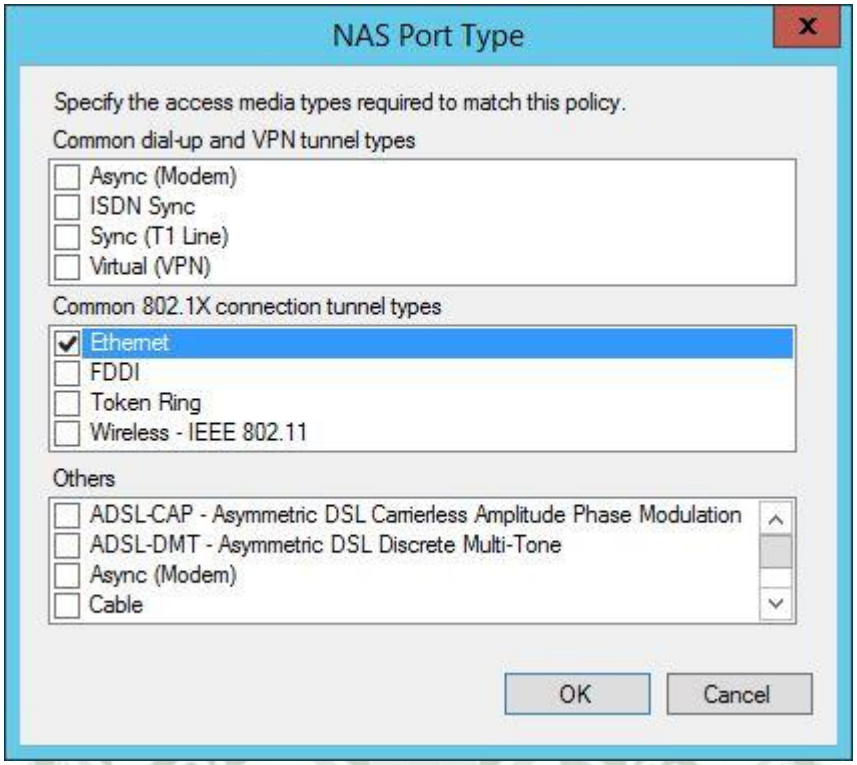

Figura 4.34 Condiciones de tipo Túnel.

Fuente: "Elaboración Propia"

La última parte de la configuración es indicar cuales son las solicitudes que se procesaran en el servidor Radius. Para lo cual en el apartado de "Configuración" hay que asegurarse que el tipo de Autenticación indicar que las solicitudes se van procesar en servidor local.

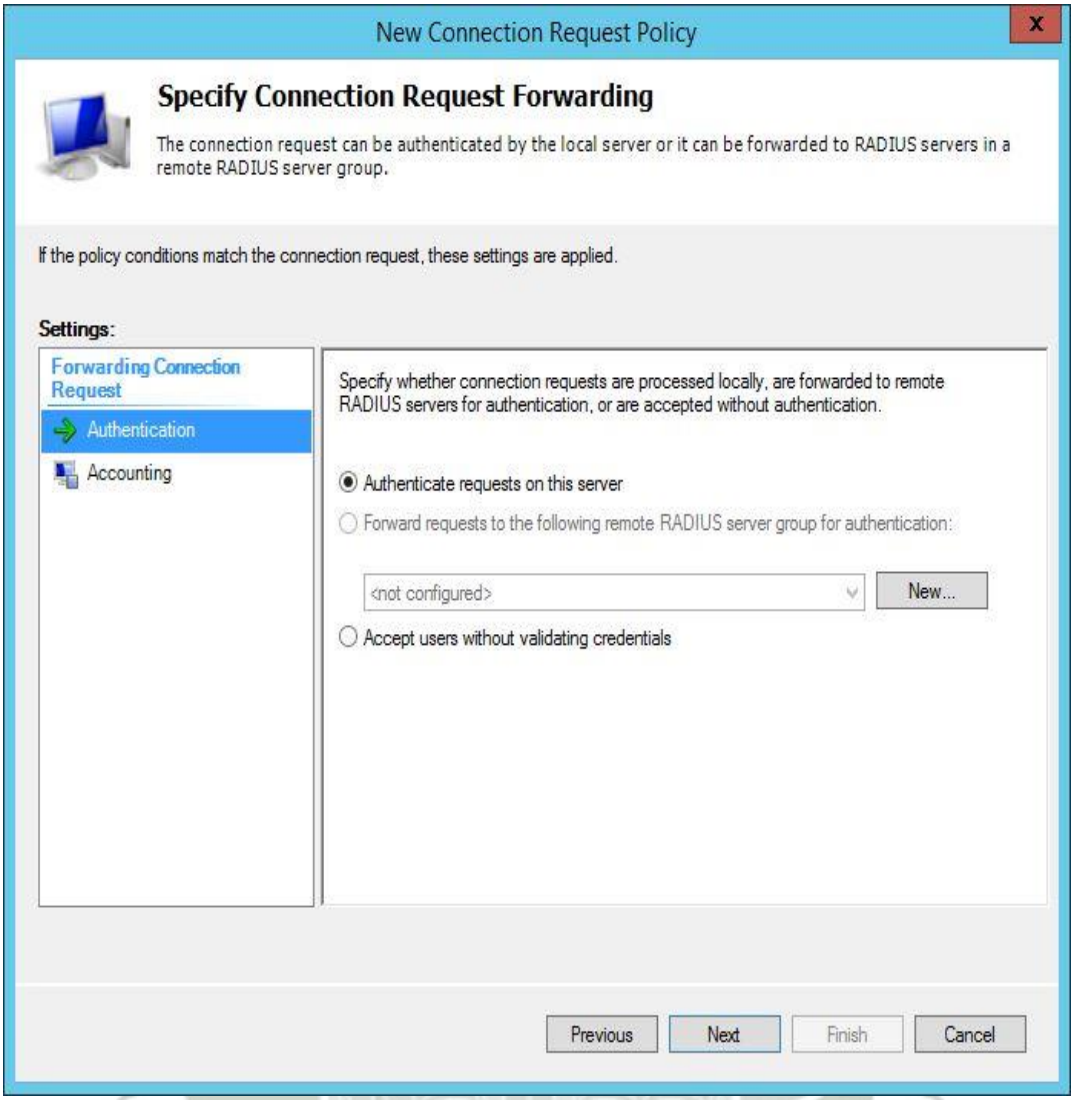

Figura 4.35 Configuración de Autenticación.

Fuente: "Elaboración Propia"

Con esto se da por finalizado la configuración de esta directiva y con lo cual se procesará en su totalidad las peticiones enviadas por los equipos que no puede realizar el proceso de autenticación, es decir todos aquellos que estén directamente conectados a lo switches configurados como clientes.

Configuración de las solicitudes de conexión de la red inalámbrica

Para configurar este tipo de conexión se tiene que la arquitectura seleccionada para este caso es un sistema que va utilizar un WLAN Controller para administrar los diferentes access point, el cual va re direccionar todo el tráfico hacia la red. Como parte de este tráfico se va incluir la validación del servidor Radius, por lo tanto, la configuración de la directiva va ser de manera centralizada sobre el WLAN Controller. Esta forma de funcionamiento la configuración se va realizar de la siguiente forma: Generando una nueva directiva de acceso, no especificando el tipo de servidor de acceso a la red.

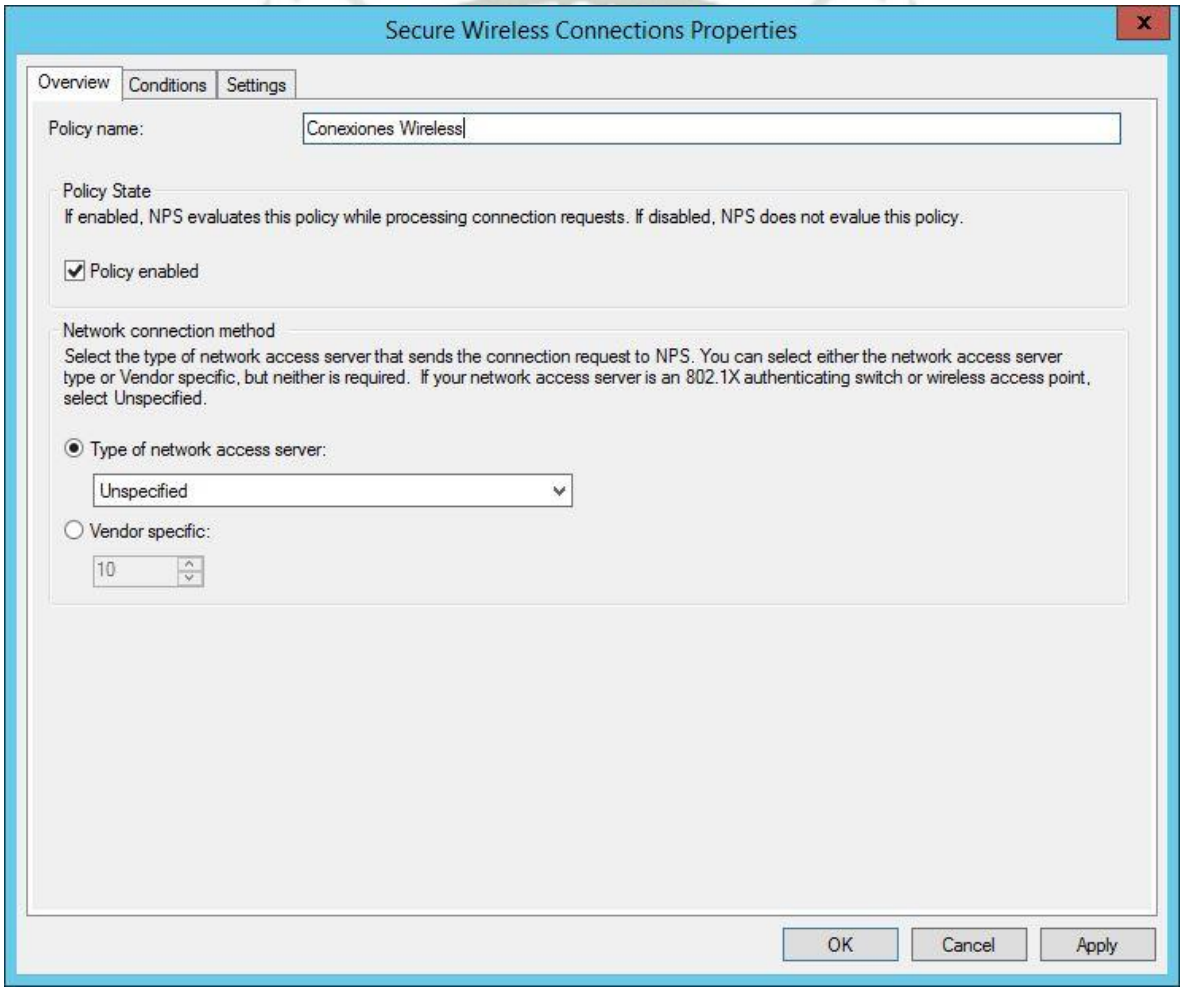

Figura 4.36 Propiedades de Conexiones Wireless.

Fuente: "Elaboración Propia"

En el apartado de "Condiciones", se define la forma de funcionar de la arquitectura inalámbrica. Agregado una nueva condición en la cual se define la dirección del cliente de acceso. Esta dirección IP va ser del WLAN Controller.

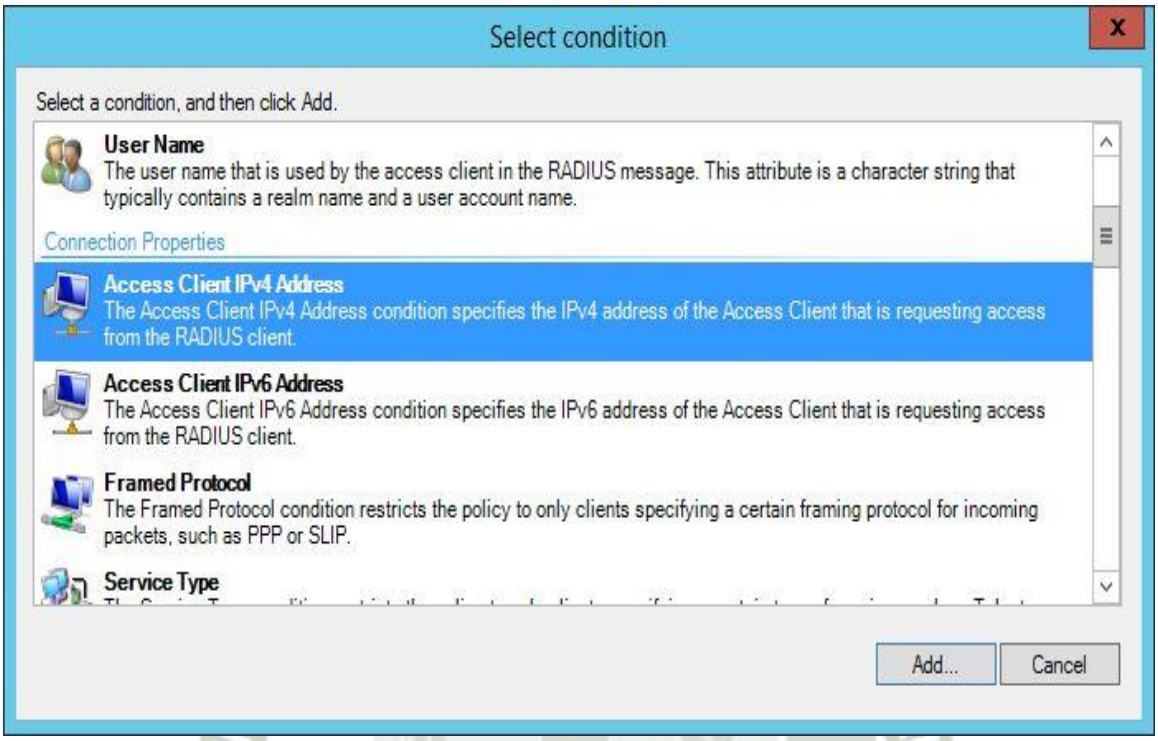

Figura 4.37 Condiciones de la conexión Wireless.

Fuente: "Elaboración Propia"

De esta manera se puede obtener un modelo escalable de múltiples WLAN Controller independientes, si se llegara a dar el caso. Finalmente, la última parte de esta configuración es indicar que las solicitudes se analicen en el servidor Radius. Para lo cual, en "Configuración", hay que cerciora de que, en "Autenticación", este seleccionado que las solicitudes se procesen en el servidor local.

De esta forma se tiene configurados las conexiones inalámbricas, provenientes del WLAN Controller, así como las peticiones de los switches de red, que serán analizadas en el servidor Radius.

4.6.4.2 Directivas de Red

Las directivas de red son la parte esencial de configuración del servidor Radius. En este apartado, se va configurar las diferentes acciones que se va realizar frente a las solicitudes de acceso reenviadas por los usuarios. Al integrar estas políticas, lo primero que se precisa es revisar si se cumple con todos los requisitos de los diferentes perfiles de acceso de la red a la cual se pretende controlar. Realizando un repaso sobre los perfiles de acceso (VLANs), se concluye que los tipos de acceso son:

- Red Administrativa.
- Red de Mantenimiento.
- Red de Invitados.
- Red sin dominio.

Toda la información necesaria de las cuentas de usuarios y/o maquina va ser proporcionada por la base de datos del Directorio Activo; por tal motivo que las políticas se van apoyar sobre las tareas de configuración de este servicio que realizamos en el apartado de configuración del Directorio Activo.

EL modo en que funciona el motor de políticas limita a la red debido a que solo ejecutara la primera política de acceso posea todos los requisitos necesarios. Por tal razón que antes de implementar la configuración de políticas, es indispensable la realización de un diagrama de flujo en el cual se va reflejar el camino que va seguir el sistema.

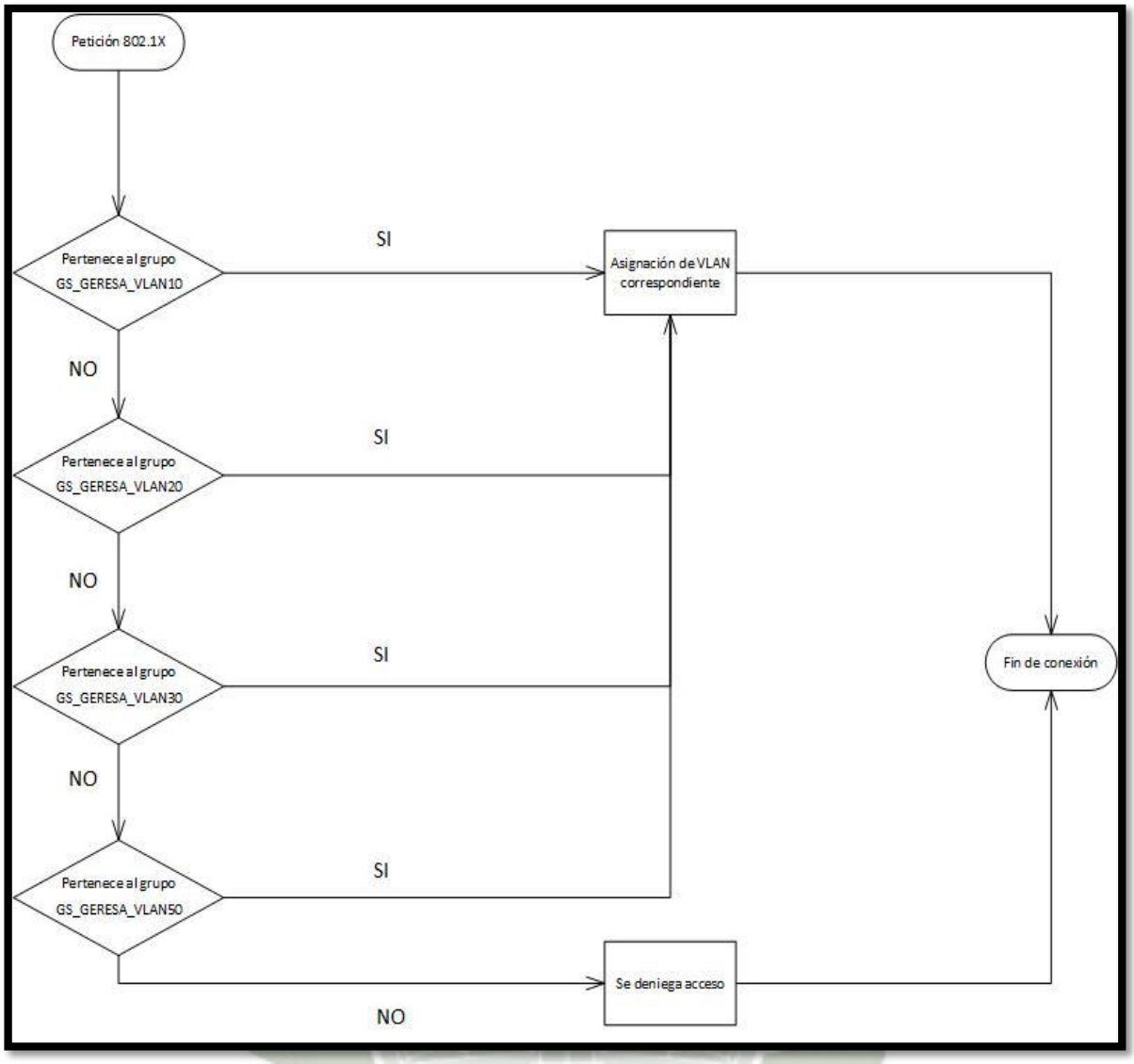

Figura 4.38 Diagrama de Políticas.

Fuente: "Elaboración Propia"

Se va realizar las configuraciones de políticas siguiendo el diagrama de flujo. Incluyendo una descripción detallada de las 2 primeras políticas, el resto seguirán el mismo procedimiento, por lo que solo será indicado:

VLAN 10

El primer perfil según el diagrama de flujo es la red "Administrativa – VLAN 10", dicha red solo requiere que el equipo pertenezca al grupo "GS_GERESA_VLAN10". Los pasos a seguir para agregar dicha política son:

1. En el administrador de NPS, sobre Directivas de Red, con el botón derecho ratón -> Nuevo. Se ingresa el nombre de la política; en este caso vendría ser: Equipos Vlan10.

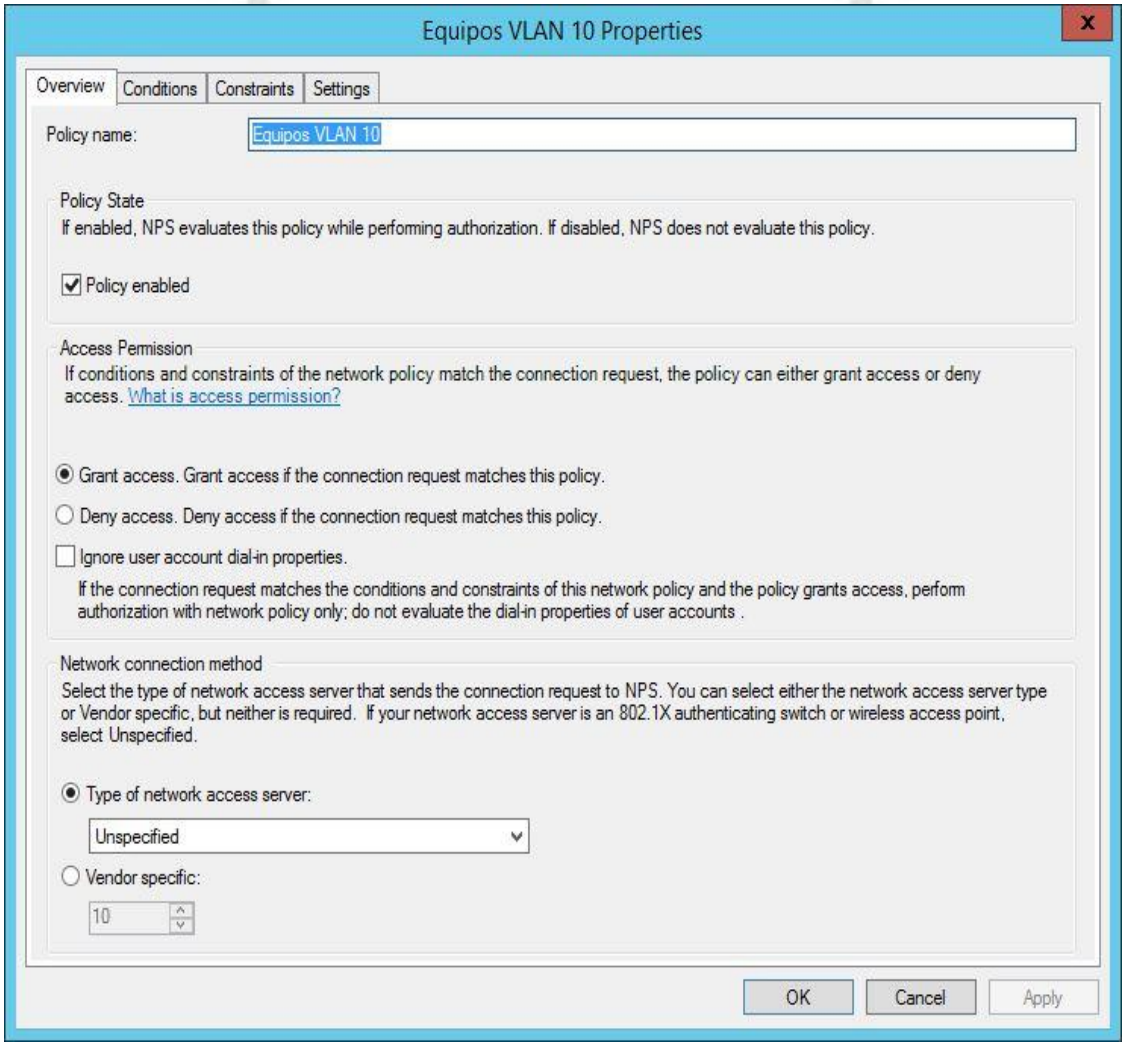

Figura 4.39 Directivas VLAN 10.

Fuente: "Elaboración Propia"

2. Lo que prosigue es llenar las condiciones que ha de tener los diferentes equipos para que cumplan esta política. Indicando que tiene que pertenecer a cualquiera de los dos siguientes grupos: GS_GERESA_RadiusVlan10 o GS_GERESA_MAC_VLAN10, para manejar esta red se tendrá que generar 2 políticas de acceso distintas: una para los equipos compatibles con la autenticación 802.1X, y la otra para los que no lo sean (impresoras, terminales, etc.) en la que va usar la dirección MAC como credenciales de acceso. Para lo cual se hace click en "Agregar" y selecciona "Grupos de Usuarios". Localizamos el grupo en cuestión y lo agregamos. De esta forma la única condición que nos debe quedar es que pertenezca al grupo que hemos seleccionado.

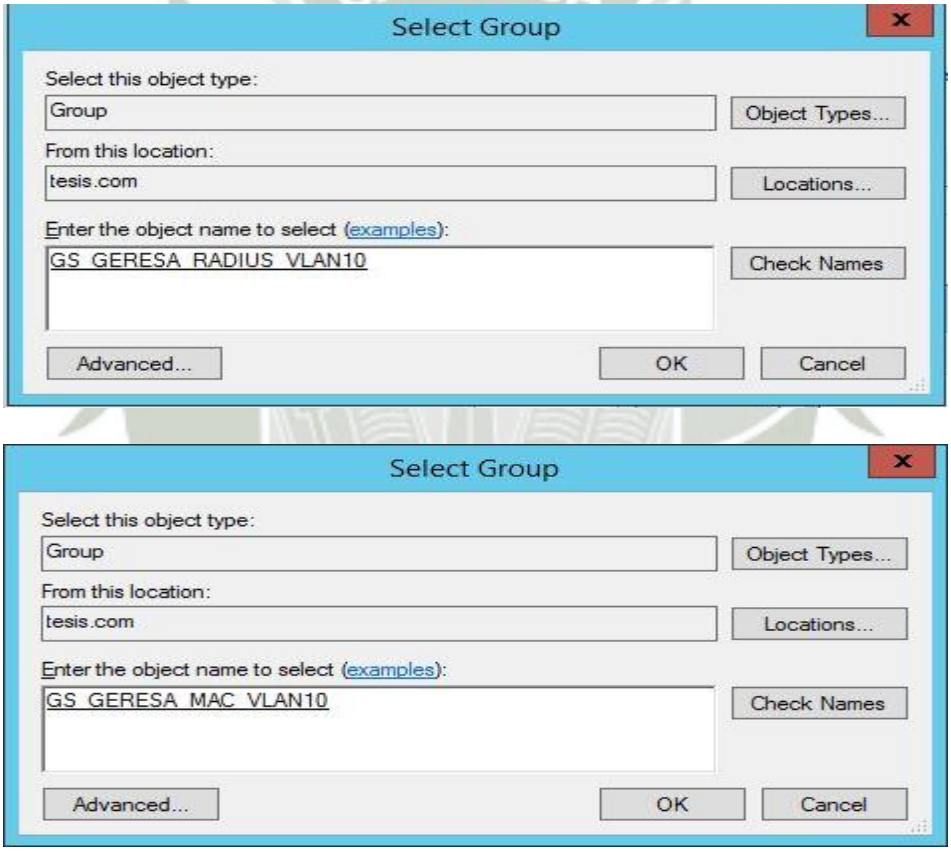

Figura 4.40 Grupos de la directiva VLAN 10.

Fuente: "Elaboración Propia"

3. A continuación, se indica que se va conceder el acceso a dicha petición.

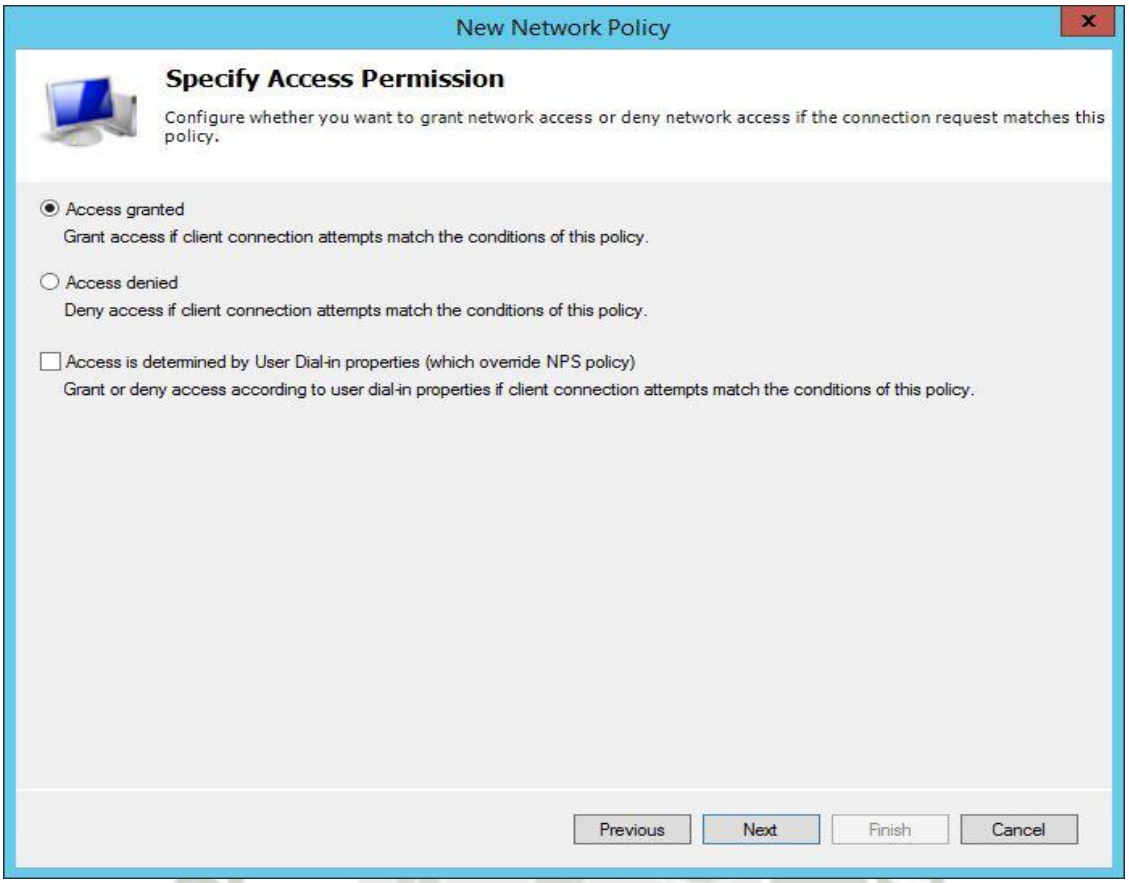

Figura 4.41 Permisos de la directiva VLAN 10.

Fuente: "Elaboración Propia"

4. Se escoge el método de encriptación. Estas máquinas están apoyadas en el servicio de los switches de MAB, el cual les brinda que tras un intento errado de autenticación por 802.1X, enviar la dirección MAC como credenciales de usuario y contraseña. Por lo cual se va usar un método de cifrado básico en el envío de dichos valores, ese método será PAP.

5. Al momento de indicar las restricciones no se establece ninguna, debido a los usuarios son los aceptarán las conexiones de los equipos que ya establecieron las políticas de "Directivas de solicitud de conexión".

6. La ultima configuración requerida va ser situar la interfaz de red correspondiente a cada VLAN.

    a) Framed protocol: PPP

    b) Service-Type: Framed

    c) Tunnel-Medium-Type: 802 (includes all 802 media plus Ethernet canonical format)

    d) Tunnel-Pvt-Group-ID: 10

    e) Tunnel-Type: Virtual LANs

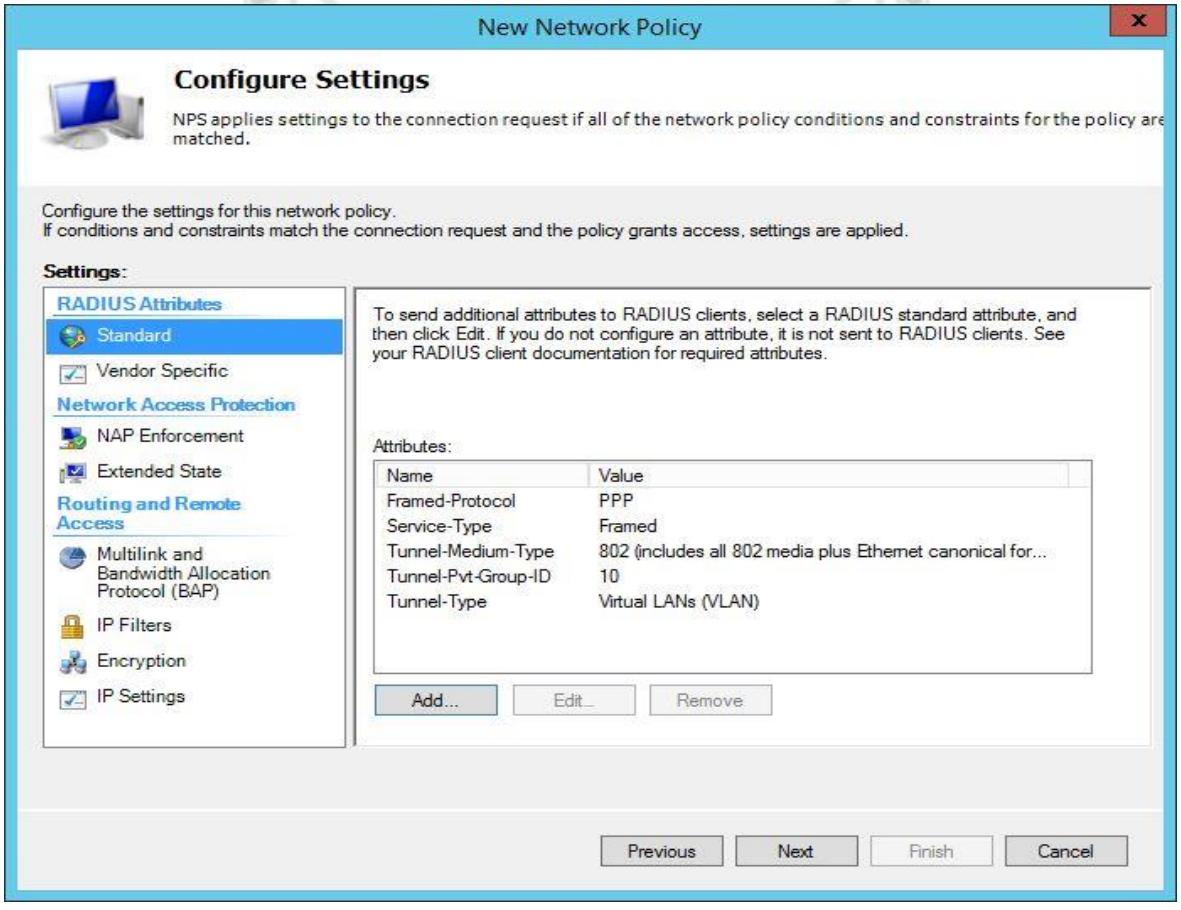

Figura 4.42 Atributos de la directiva VLAN 10.

Fuente: "Elaboración Propia"

7. Finalmente se obtiene el resumen de toda la configuración que se ha realizado, se verifica los valores y se finaliza la tarea del asistente.

VLAN 20

La política a evaluar es la Red de Mantenimiento. Esta red permitirá el acceso a usuarios del departamento de TI y a los proveedores de los diferentes servicios con los que cuenta la GERESA, para lo cual tienen que estar registrados en base de datos de usuarios, usando dispositivos externos. Este comportamiento se consigue con el grupo creado en el Directorio Activo llamado GS_GERESA_Radius_VLAN20 donde está incluido todos los usuarios registrados. Procediendo con la configuración de política según el mismo procedimiento que se ha estado realizando anteriormente.

VLAN 30

Realizamos la configuración de la siguiente VLAN de acuerdo al diagrama de flujo, la cual correspondería a la VLAN 30, que pertenece al perfil de Red de Invitados. Los pasos a seguir son similares a la configuración de la VLAN 10, los cuales son:

1. En el administrador de NPS, sobre Directivas de Red, con el botón derecho ratón -> Nuevo. Se ingresa el nombre de la política; en este caso vendría ser: Equipos Vlan30

2. El siguiente paso se precisa definir las condiciones que ha de tener el equipo para cumplir esta política. Indicando que tiene que ser parte del grupo: GS_GERESA_Radius_VLAN30. Para se procede a hacer click en “Agregar” y seleccionar “Grupos de Usuarios”. Localizado el grupo en cuestión y se procede a agregarlo. De esta forma la única condición que falta es que pertenezca al grupo que hemos seleccionado.

3. A continuación, se indica que se va conceder el acceso a dicha petición.

4. Hay que elegir el método de encriptación. Estos equipos establecen su conexión atreves de cuentas que son generadas por el Directorio Activo, encargando esto al sistema operativo del usuario invitado a enviarlas por la red. Es por ello que se usa un método seguro en el envío de sus credenciales; ese método será MS-CHAP y su segunda versión mejorada MS-CHAP-V2. El tipo de comunicación en el cual se basará es el método EAP-PEAP, que brinda la posibilidad de realizar una encriptación del tráfico con la opción de poder prescindir de una asignación de certificados digitales por cada cliente.

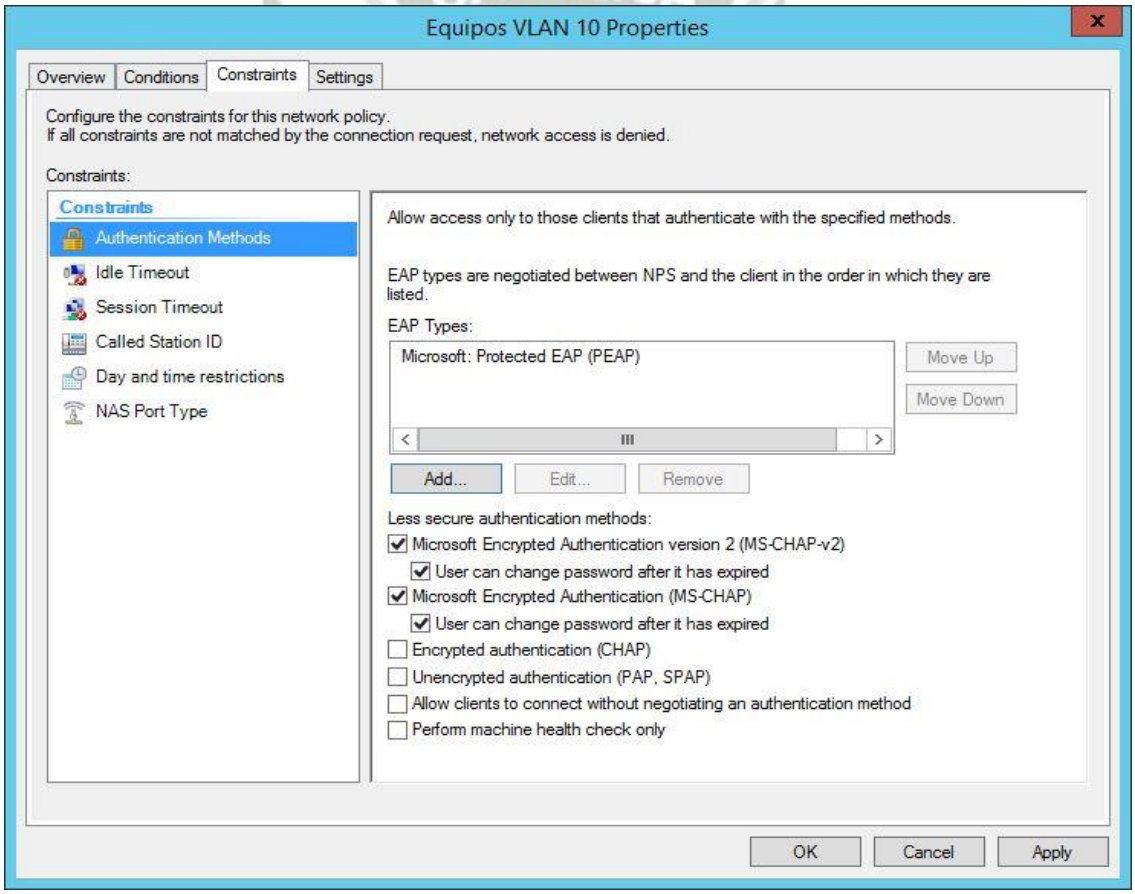

Figura 4.43 Método de Autenticación.

Fuente: "Elaboración Propia"

Para un mayor grado de seguridad se empleará un certificado de servidor. La configuración y creación del certificado no es parte del proyecto, pero para fines didácticos se creó un servidor paralelo para la emisión de certificados digitales con el nombre de tesis-WIN, ahora indicamos el certificado individual generado para este servidor.

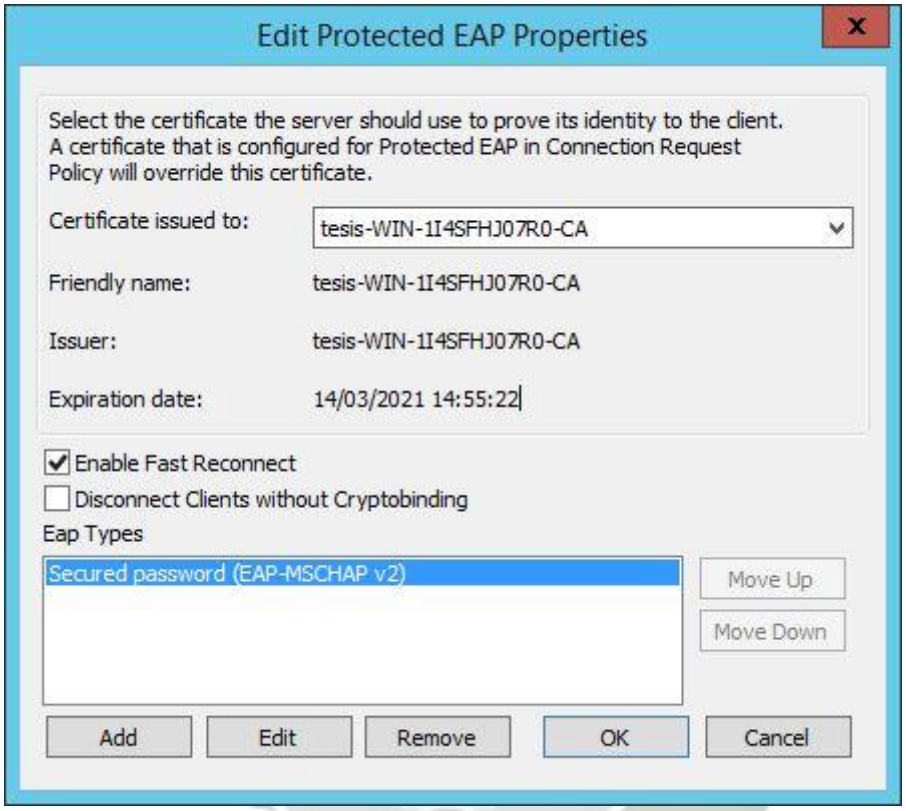

Figura 4.44 Elección de Certificado.

Fuente: "Elaboración Propia"

5. Al momento de indicar las restricciones no se establece ninguna, debido a los usuarios son los aceptarán las conexiones de los equipos que ya establecieron las políticas de "Directivas de solicitud de conexión".

6. La ultima configuración requerida va ser situar la interfaz de red correspondiente a cada VLAN.
    a. Framed protocol: PPP
    b. Service-Type: Framed
    c. Tunnel-Medium-Type: 802 (includes all 802 media plus Ethernet canonical format)
    d. Tunnel-Pvt-Group-ID: 30
    e. Tunnel-Type: Virtual LANs

7. Finalmente se obtiene el resumen de toda la configuración que se ha realizado, se verifica los valores y se finaliza la tarea del asistente.

VLAN 50

La configuración de la VLAN 50, que corresponde al perfil de Red Sin Dominio. Esta Red es la que dispone de la menor cantidad número de usuarios y equipos conocidos, y usados en la red, pero que no cumplen con los requisitos para ser registrados en el dominio Para manejar esta red se tendrá que generar 2 políticas de acceso distintas: una para los equipos compatibles con la autenticación 802.1X, y otra para los que no (servidores, impresoras, etc.) en la que se debe usar su dirección MAC como credenciales de acceso. Ambas configuraciones seguirán el mismo proceso que las anteriores políticas ya configuradas.

4.7 Configuración de Equipos de Red

Una vez realizada la habilitación del protocolo Radius en el ambiente Windows Server 2012 R2 se procede con la configuración de los diferentes equipos que son parte de la red para que puedan habilitar este protocolo, en el caso de una red inalámbrica siempre va tener una parte cableada la que va conectar los access point con el Data center y por el alto volumen de access point estos van a ser administrados de una forma centralizada mediante un Wireless LAN Controller, para recrear estas configuraciones se va emplear dos softwares:

- Cisco Packet Tracer
- NetworkSims

4.7.1 Equipos de Red Cableada

Ya que toda red inalámbrica siempre va precisar de una parte cableada ya sea para conectarse a un dispositivo como un router o switch, en tal caso se va a mantener un diseño de segmentación por capas (Core, Distribución, Acceso). Los usuarios de la red se ubican en la capa de nivel de acceso, a este nivel los dispositivos de red, que usan son router Cisco 2911. La configuración de estos dispositivos, para actuar de clientes de Radius, pasa por las siguientes medidas:

- Configuración general para usar autenticación en el router.
- Establecer el router como cliente de NPS.
- Establecer en los puertos de acceso la configuración 802.1X correcta.

4.7.1.1 Configuración general para usar autenticación en el router.

Por configuración de fábrica, los routers u otros dispositivos no tienen habilitadas todas las configuraciones que el equipo puede brindar como el caso del router que no tiene habilitado el mecanismo de autenticación, autorización y monitorización en su configuración; que es más conocido como AAA (authentication, authorization and accounting). Para poder utilizar esta función en los equipos Cisco, en este ejemplo se está usando una topología con dos routers uno para acceso a la red de la institucional de la GERESA y el otro de uso exclusivo del Data Center para realizar las configuraciones son necesarias las siguientes sentencias en cada router.

Configuración del router de salida (Router0):

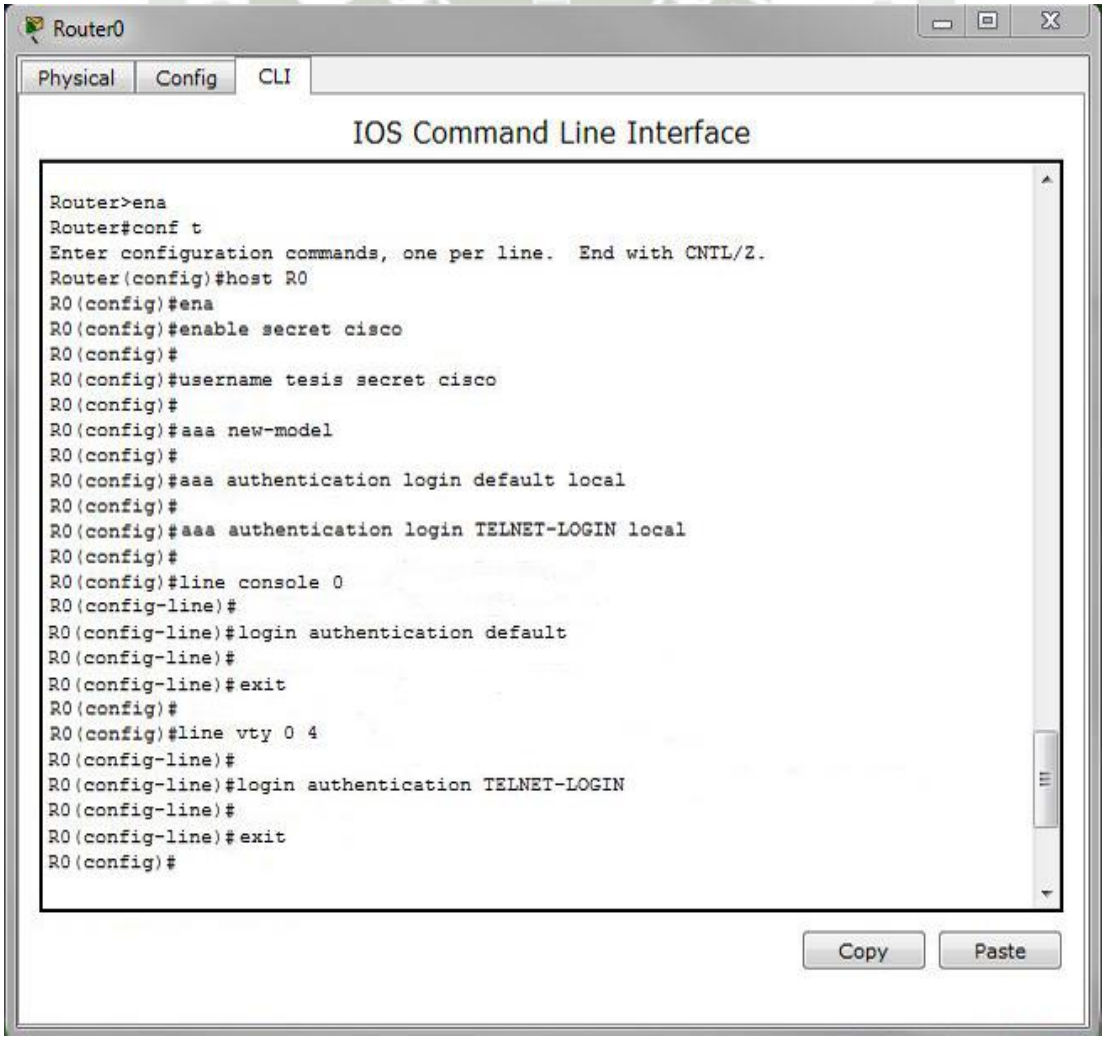

Figura 4.45 Configuración General del Router 0.

Fuente: "Elaboración Propia"

Se procede a configurar el modo de autenticación basado en 802.1X, indicado que toda la autenticación 802.1X sea realizada sobre los servidores Radius, de igual manera se procede a indicar los mecanismos de autenticación en el router, asignando el servidor de Radius que cumplirá la función de servidor de NPS, que evaluaran las políticas de acceso. La configuración final en la que se establecerá, además del servidor NPS, la clave compartida entre ambos. Esta clave vendría a ser un medio de paso, que se establece la comunicación entre cliente Radius y Servidor, para de esa manera evitar la solicitud de acceso a usuarios no autorizados, la configuración del router del Data center(Router1) es la siguiente:

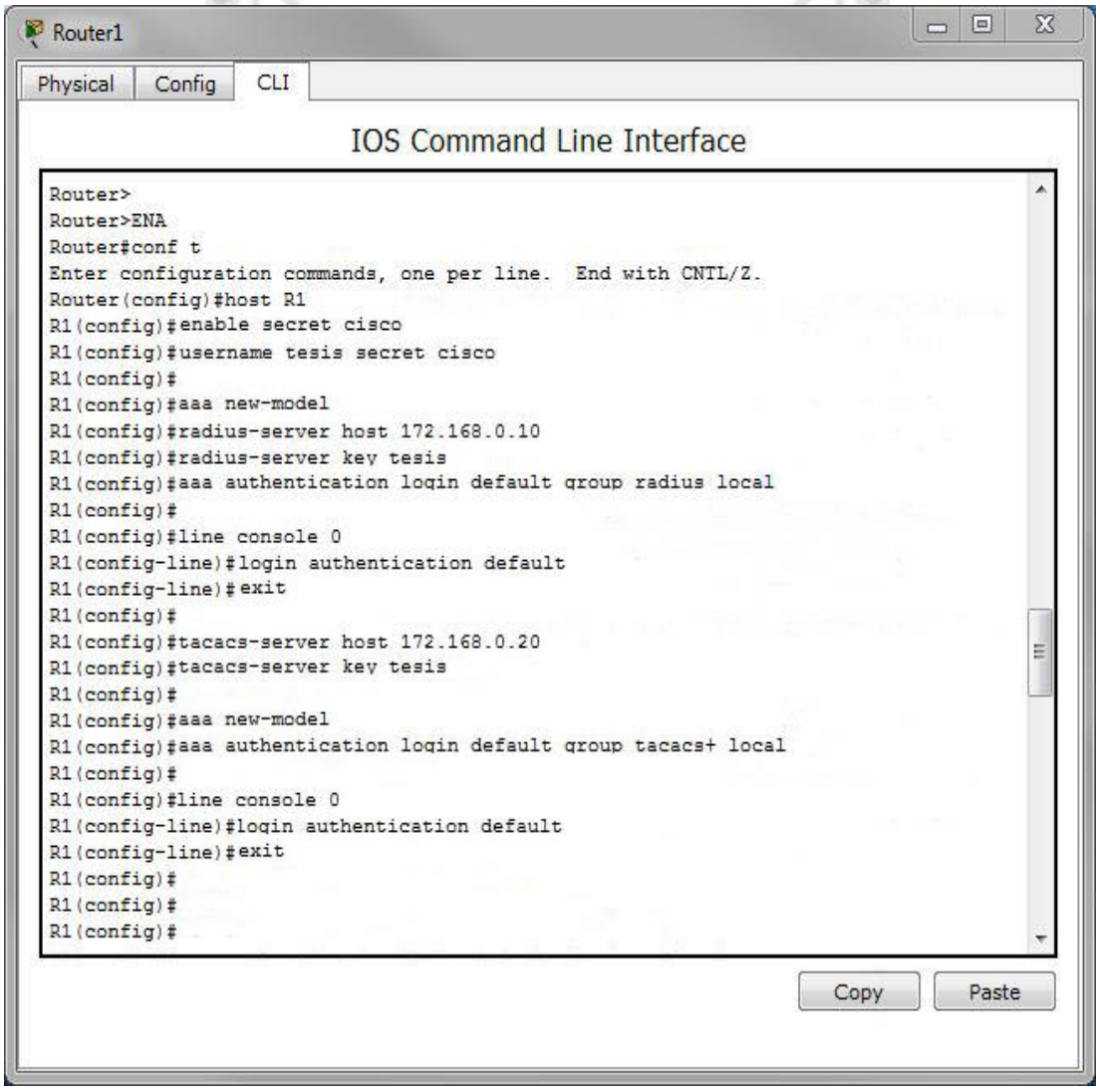

Figura 4.46 Configuración General del Router 1.

Fuente: "Elaboración Propia"

4.7.1.2 Asignación de puertos de acceso para la configuración 802.1X.

Una de las cosas útiles que brinda esta implantación es el hecho que puede realizarse de manera progresiva, lo cual perite que a cada switch se le pueda indicar si todos o algunos de los puertos de acceso para que realicen la autenticación basada en 802.1X. otro punto rescatable es que al momento de configurar los puertos se puede indicar cuales vas a ser para uso de equipos no compatibles con 802.1X, para que puedan articular otro mecanismo para iniciar sesión.

Para tal motivo, Cisco brinda un mecanismo nombrado MAB en sus equipos el cual permite realizar una autenticación 802.1X tomando la dirección MAC del equipo que solicita el acceso cuando este no puede realizarlo de manera autónoma con sus respectivas credenciales de usuario. En la siguiente figura se muestra el proceso descrito:

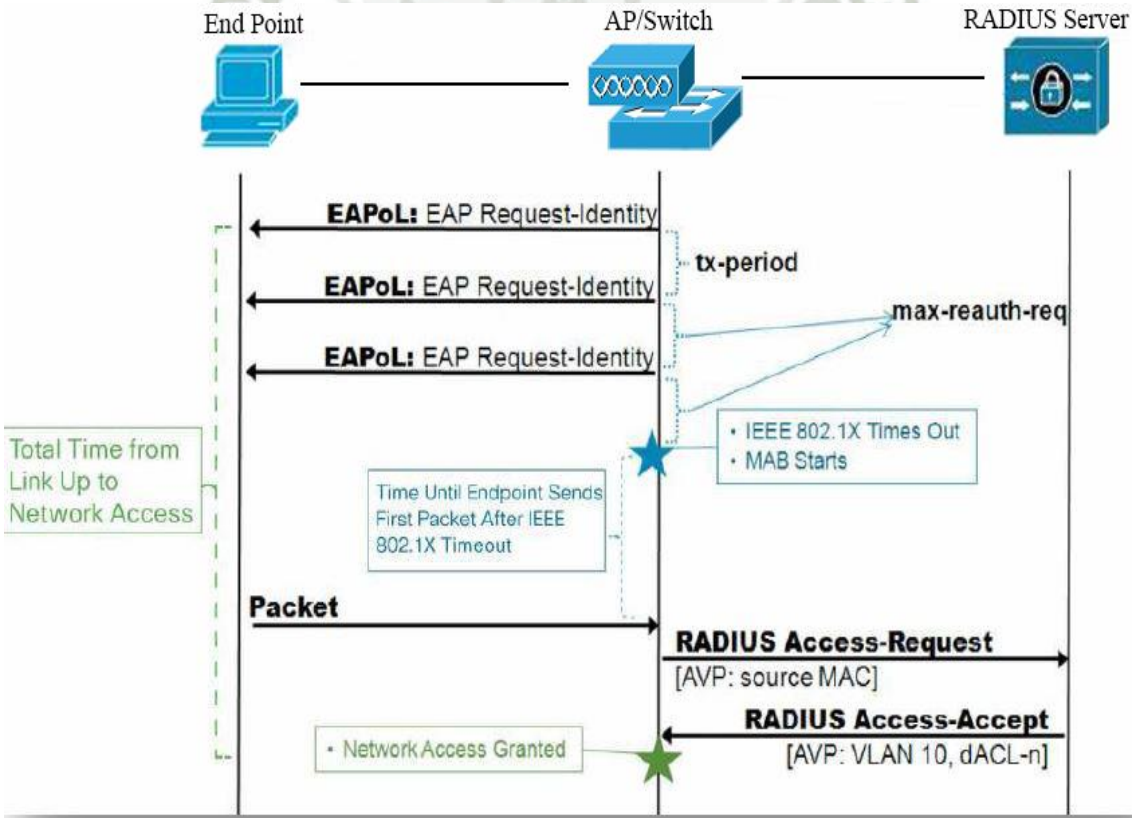

Figura 4.47 Proceso EAPOL.

Fuente: "Elaboración Propia"

4.7.2 Equipos de Red Inalámbrica

Ya que se pretende trabajar toda la red mediante access point una manera de poder centralizar y administrar fácilmente todos los equipos es mediante un Wireless LAN Controller (WLAN), como ventaja es que la configuración de la red inalámbrica se tendrá desde un único punto de configuración, todos los access point recibirán las solicitudes de conexión mediante WLAN, este equipo será el cliente del sistema Radius y en el cual se configurará todos los parámetros necesarios para la red inalámbrica como el uso de la clave compartida.

La configuración del WLAN se realizará de manera similar al de la red cableada debido a que es preciso primero configurar los parámetros iniciales del Servidor Radius, seguidamente es indispensable la configurar los SSID a los cuales el Servidor Radius aplique la validación y los cuales son:

- Configuración de los parámetros generales de Radius.
- Generación de un perfil de seguridad.
- Configuración del ESS.

4.7.2.1 Configuración de los parámetros generales del Servidor Radius

1. Se ingresa al módulo de administración del WLAN.

2. Se ubica el apartado Security.

3. En esta opción se puede configurar AAA dentro del cual se encuentra Radius.

a. Se procede a añadir el servidor mediante la opción “Add”.

b. Se asigna la dirección IP del servidor Radius y la clave compartida.

c. Se indica el número de puerto.

La configuración de este apartado quedaría como la siguiente imagen:

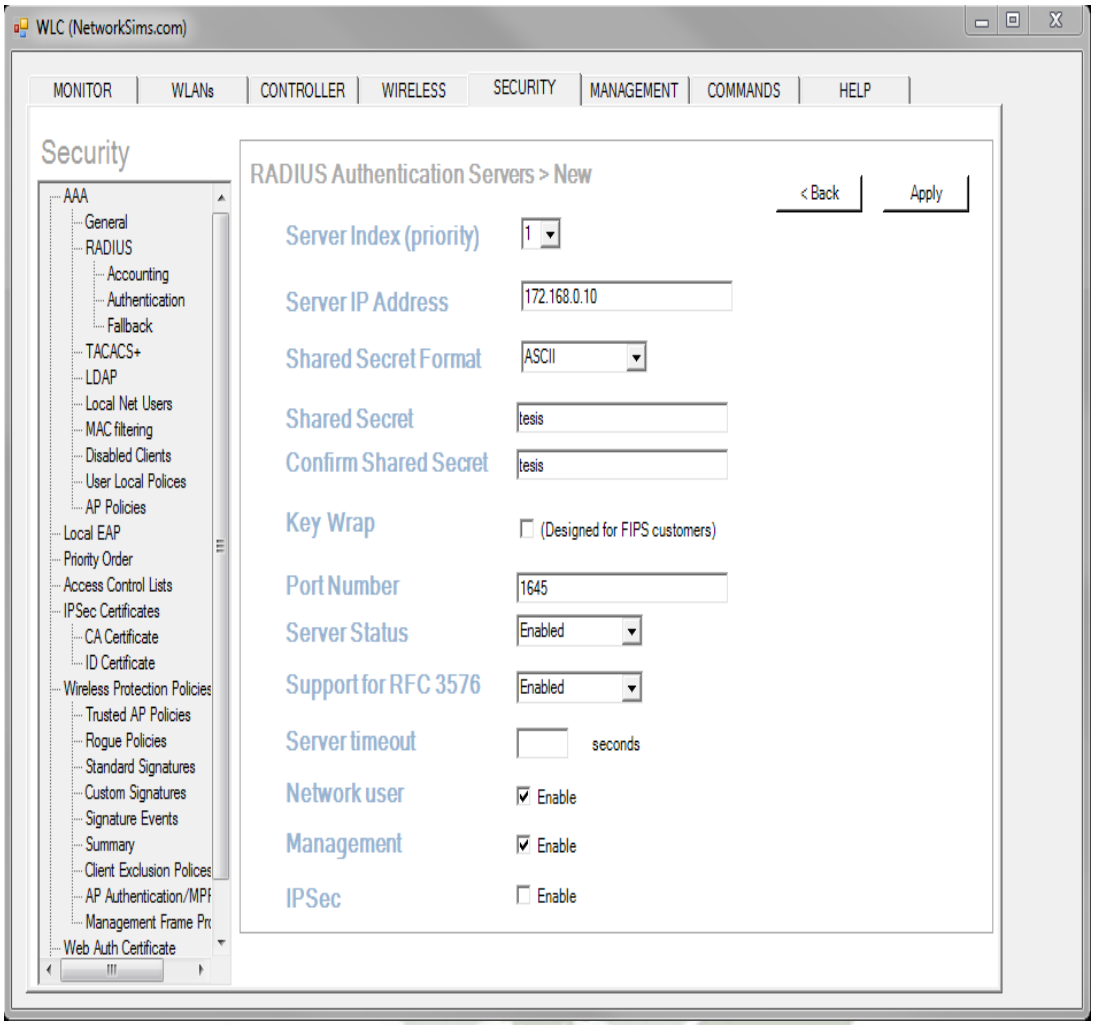

Figura 4.48 Configuración Radius en el WLAN.

Fuente: "Elaboración Propia"

Este procedimiento se realiza también para agregar el segundo controlador. Luego de haber concluido el proceso, ya se puede configurar los perfiles de seguridad que será usados para validación en el servidor NPS.

4.7.2.2 Generación de un perfil de seguridad.

Para generar un SSID es preciso realizar el siguiente proceso:

1. Se ingresa al módulo de administración del WLAN Controller.
2. Se ubica el apartado WLANs.
3. En la opción "New", generamos un perfil de acceso para acceso a NPS.
    a. En el subapartado General se indica el perfil de Seguridad y el nombre del SSID.
    b. En el subapartado Security se emplea el protocolo de cifrado WPA2 con TKIP

Mostramos la configuración de este apartado en la siguiente imagen:

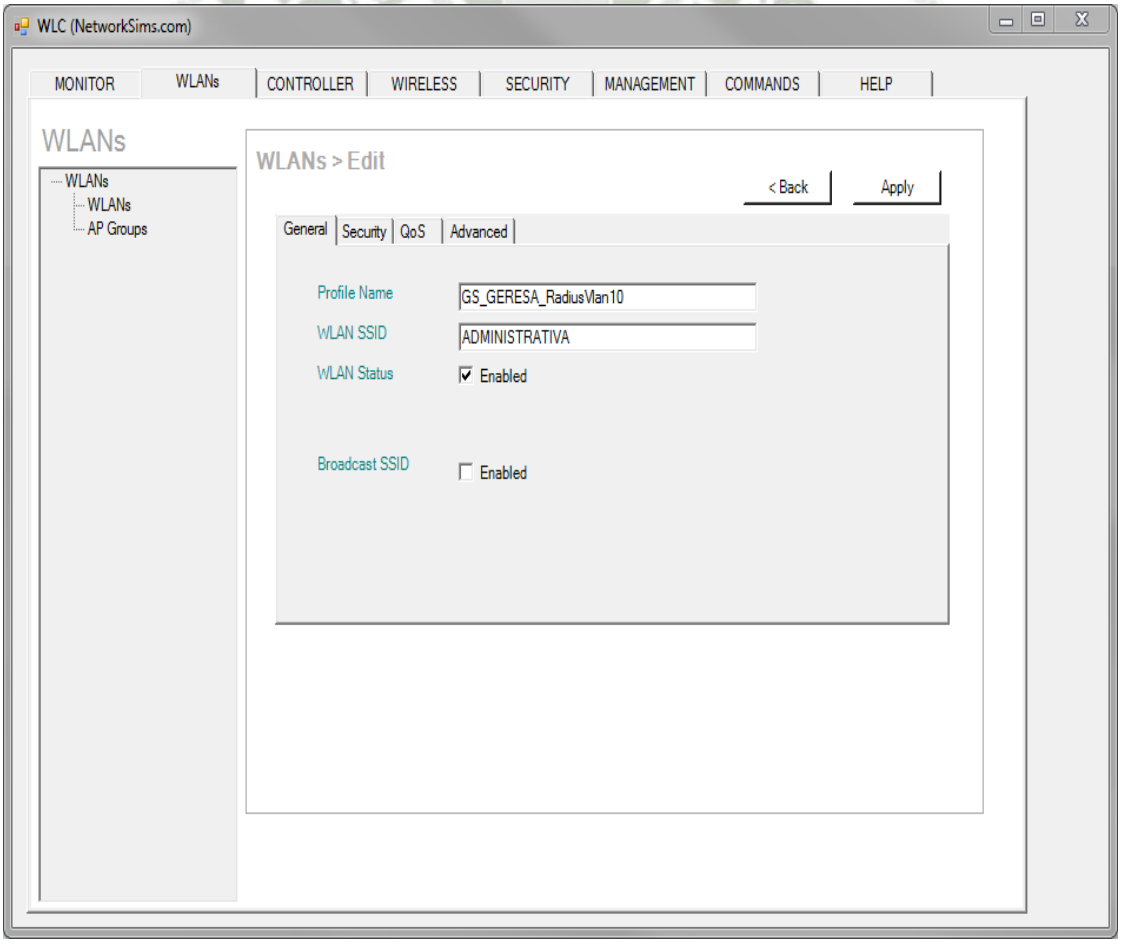

Figura 4.49 Configuración de Perfiles.

Fuente: "Elaboración Propia"

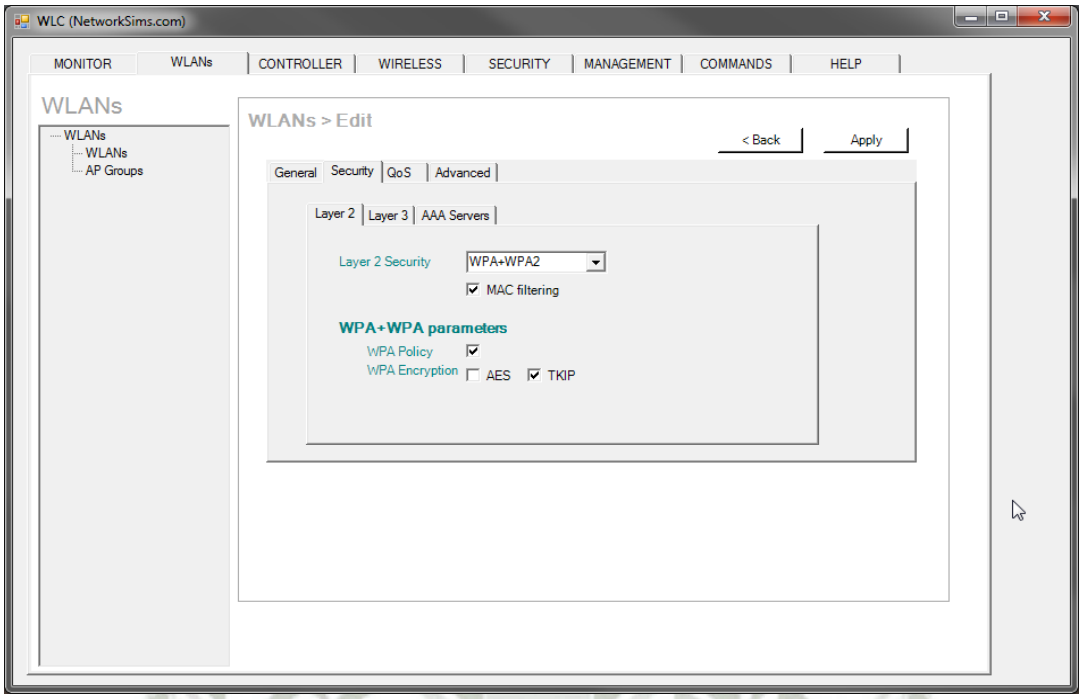

Figura 4.50 Configuración de Perfiles.

Fuente: "Elaboración Propia"

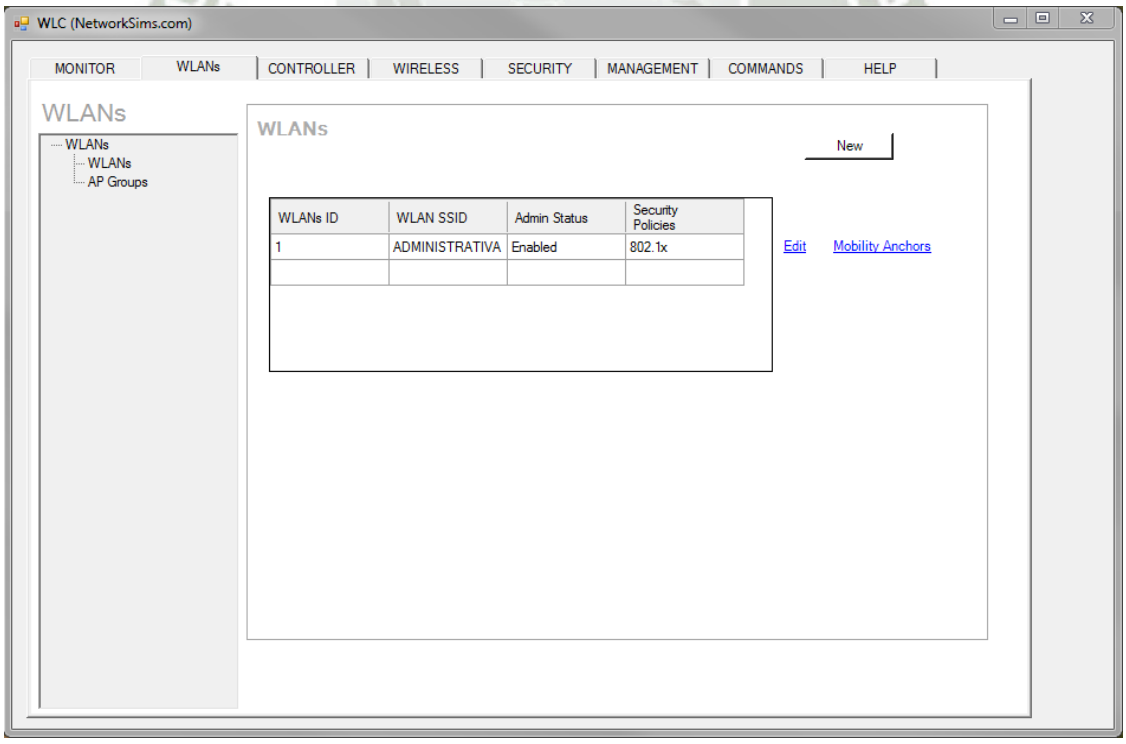

Figura 4.51 Configuración de Perfiles.

Fuente: "Elaboración Propia"

La arquitectura adecuada para este tipo de topología es Extended Service Set (ESS) mediante la cual se garantiza obtener un mismo SSID replicado por todos los access point con el mismo identificador, este se aplicará para la VLAN Administrativa, para configurar se debe realizar los siguientes pasos:

1. Se ingresa al módulo de administración del WLAN Controller.
2. Nos situamos en el apartado "Wireless", subapartado Access Point.
3. En la opción "General", se configura cada Access Point.
    a. Se les asigna un nombre.
    b. Establecer la dirección IP, la máscara de red y la dirección de Gateway.
    c. Indicar el AP ID del perfil de la VLAN y seleccionar VLAN estática.

Como se muestra la configuración de este apartado en la siguiente imagen:

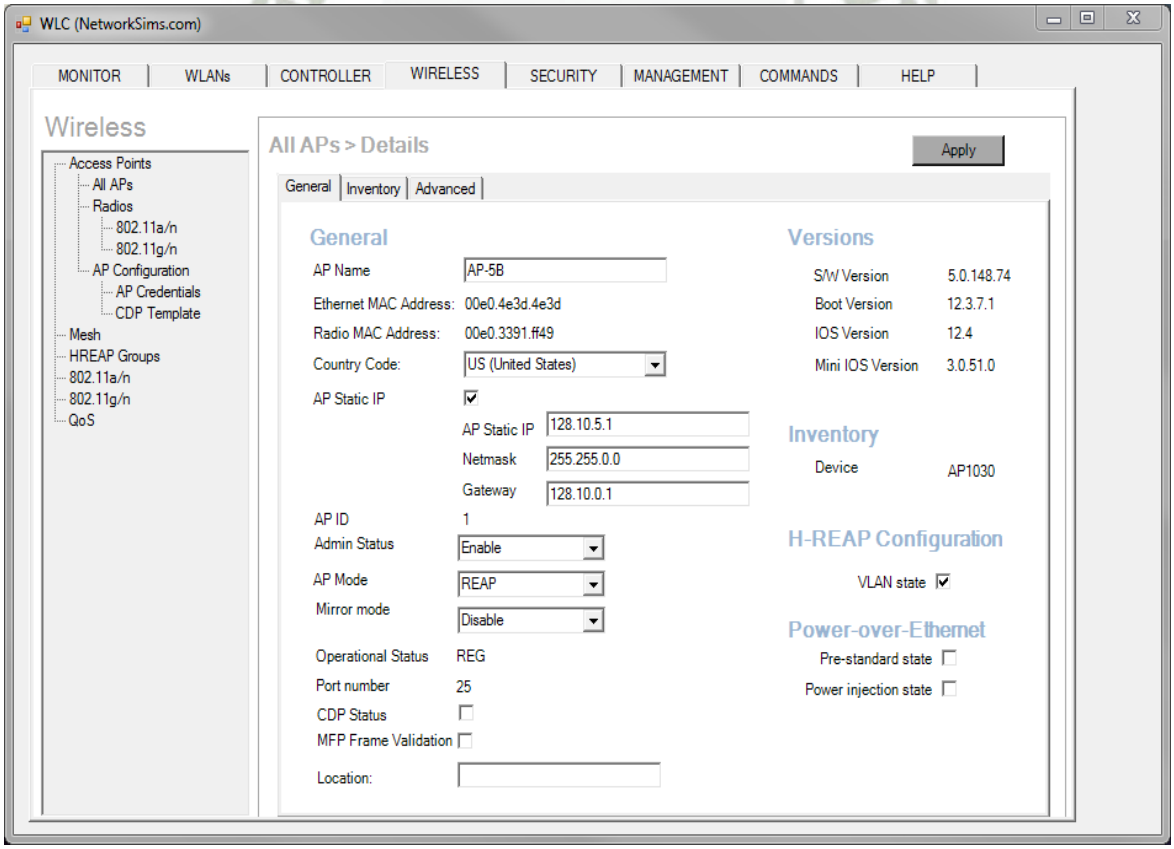

Figura 4.52 Configuración de ESS.

Fuente: "Elaboración Propia"

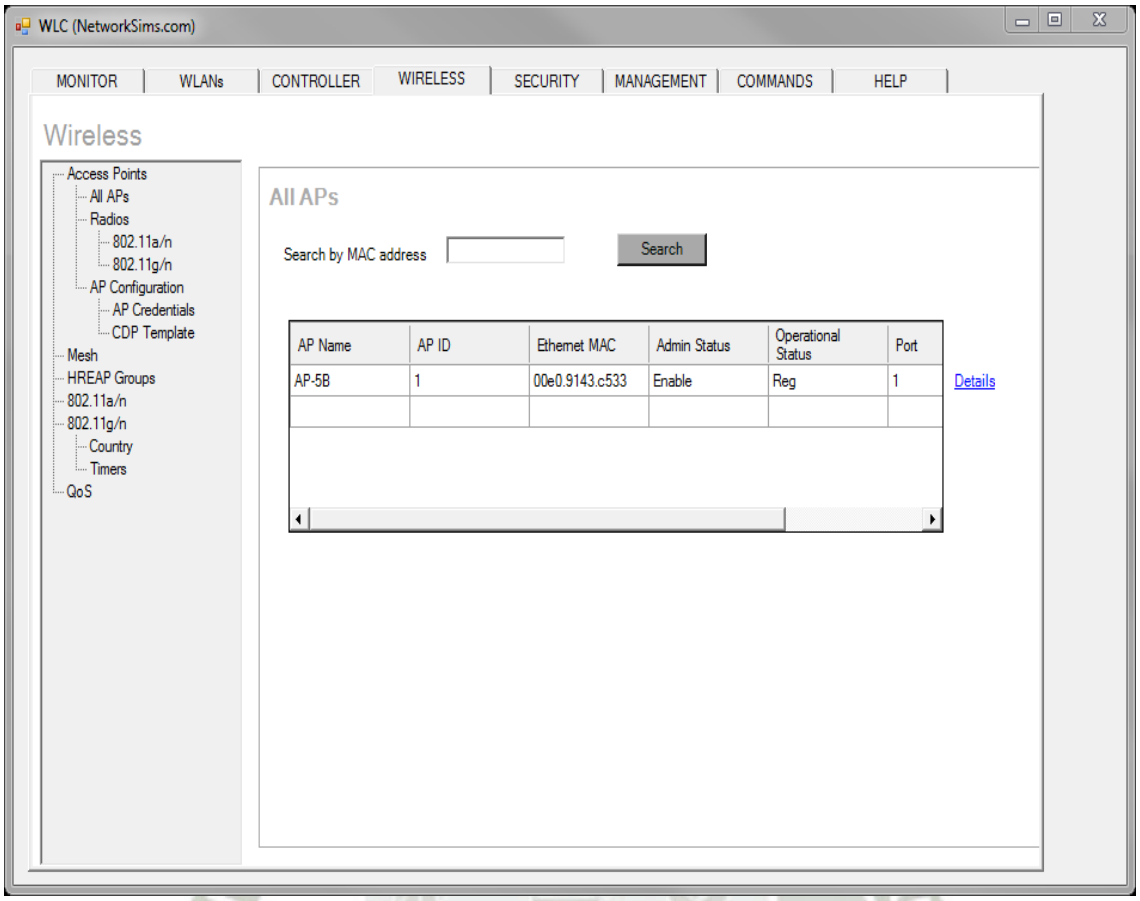

Figura 4.53 Configuración de ESS.

Fuente: "Elaboración Propia"

Una vez realizada la configuración de los diferentes parámetros en el WLAN Controller, la forma de funcionamiento de los access point se verá subordinado al servidor NPS. De manera que se vincule los usuarios con el SSID, el WLAN reenviara las credenciales al servidor NPS y los cuales, a través de las políticas de seguridad, darán o no autorización para el ingreso a la VLAN correspondiente. Cuando los usuarios estén conectados a la VLAN que les corresponde tendrán todos los servicios de red de la VLAN.

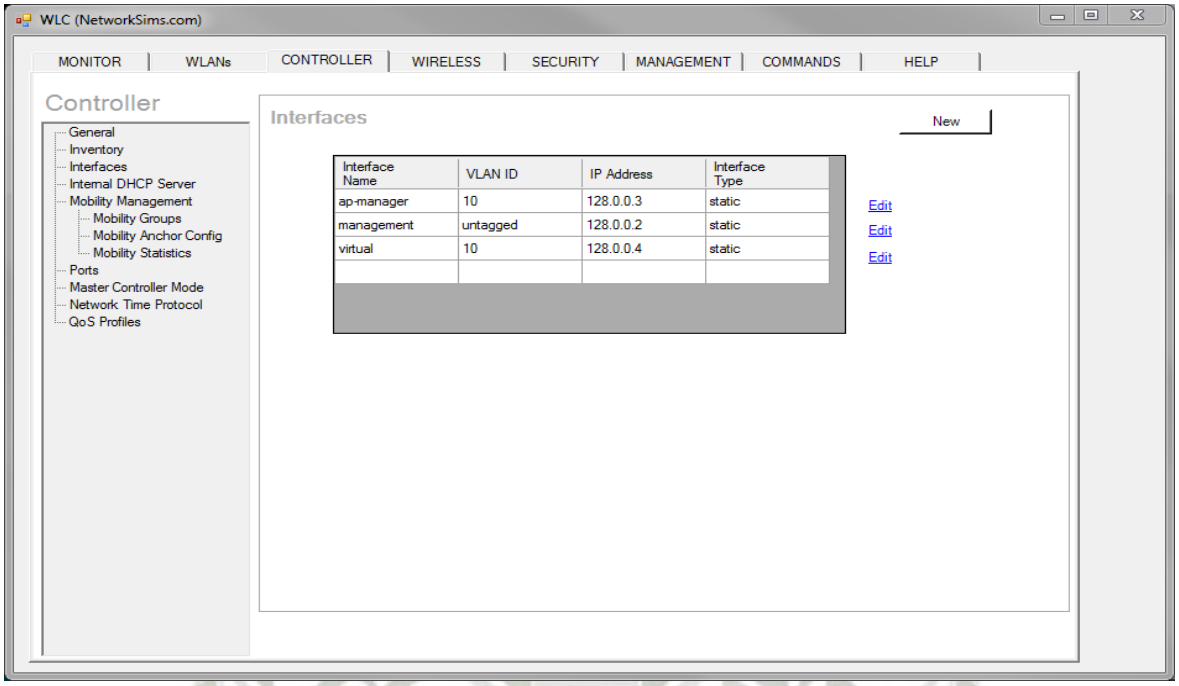

Figura 4.54 Configuración final del WLAN.

Fuente: "Elaboración Propia"

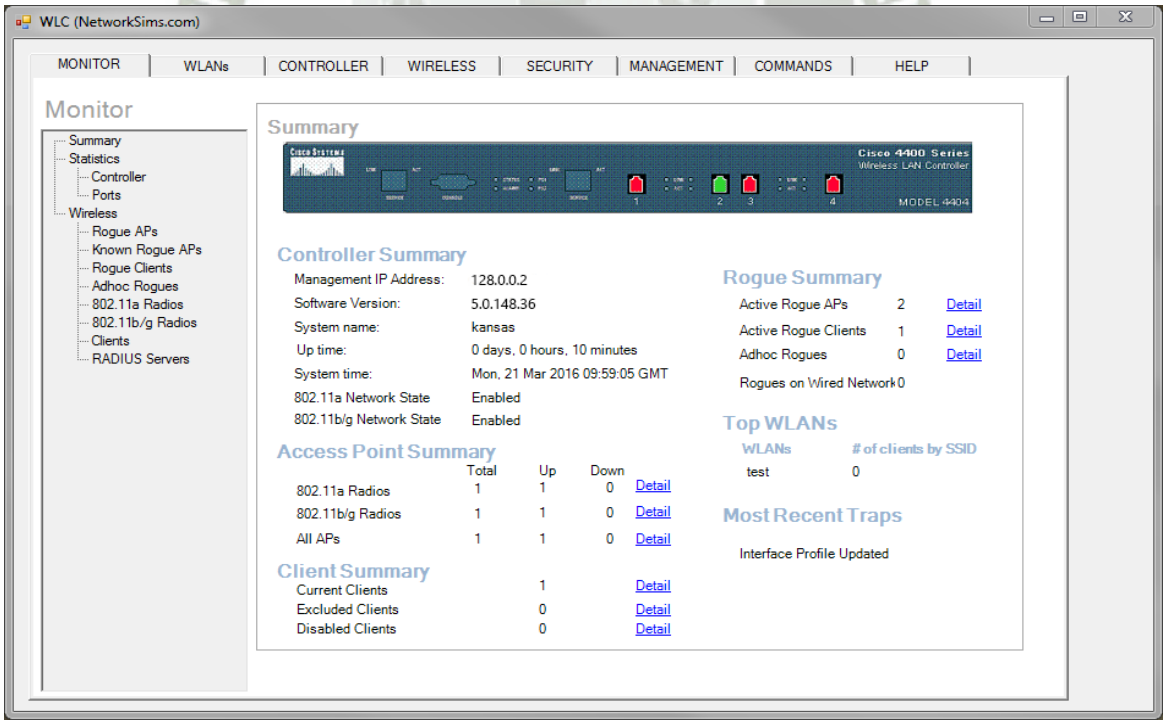

Figura 4.55 Configuración final del WLAN.

Fuente: "Elaboración Propia"

4.8 Plan de Contingencia

Como parte del diseño de la red inalámbrica se contempla la creación de un plan de contingencia ante algún problema que pudiera surgir y afecte directamente a la red, el cual permitirá mantener la contigencia operativa frente a cualquier evento que perjudique a los usuarios y de esa manera minimizar el impcato negativo hacia la red, el cual comprende la siguiente estructura.

El proceso de contigencia comienza cuando un usuario reporta un requerimiento al aqrea de soorte por algun porblema en la conexión de la red, para lo cual el personal encargado se dirige a la maquina de usuario para proceder a verificar si el problema es con la conectividad hacia access point, caso sea este el problema se prueba cambiando de banda o conectando a la red alámbrica, caso contrario con el desperfecto no es del access point se procede a revisar la tarjeta inalámbrica, si ese el el inconveniente se procede a cambiar la la tarjeta inalámbrica, si el problema persite se revisa el access point o el cableado hacia el switch y por ultimo se revisa el swtich si el inconveniente es sobre estos equipos se procede a cambiar los equipos que presentan algun desperfecto por ultimo sino el problema no es de hardware seprocede a reconfigurar o formatiar el equipo, concluiendo el plan de contingencia cuando el usuario tenga accesso nuevamente a la red, el siguiente diagrama muestra como se debe realizar el proceso de contingencia.

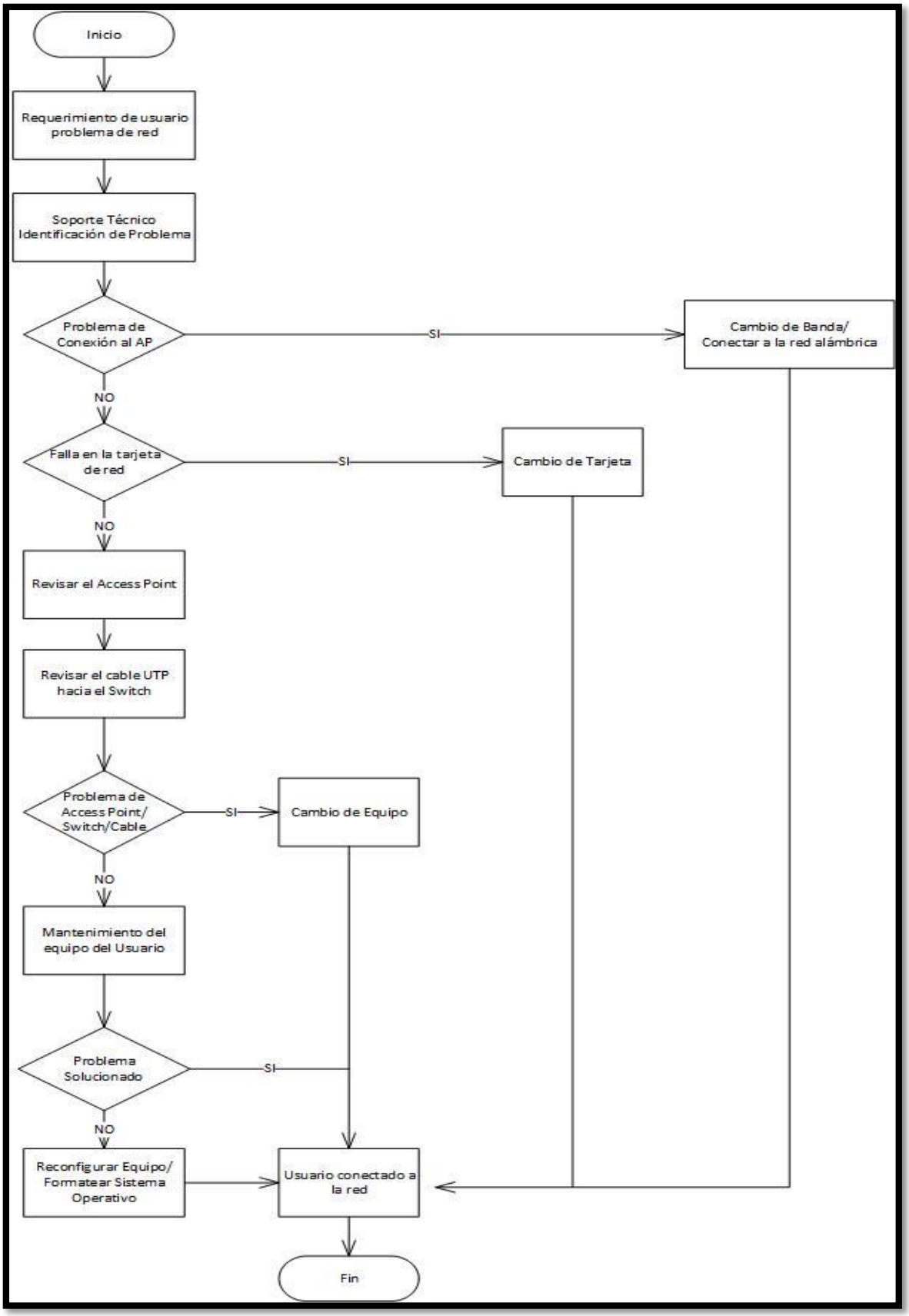

Figura 4.56 Diagrama de Contingencia.

Fuente: "Elaboración Propia"

4.9 Pruebas

El diseño de una red de una forma correcta es un reto que implica algo más que realizar una interconexión de computadores, en este caso la red inalámbrica diseñada requirió cumplir múltiples características que le permitan lograr los objetivos para la cual ha sido creada; estos objetivos fueron cumplidos de manera progresiva. Con la presentación de los equipos los cuales nos brindan la posibilidad de poder usar ambos estándares dejando esta última decisión de acuerdo a las exigencias actuales que precisa la gerencia regional de salud, para lo cual se tiene como referencia la simulación de la distribución de los access point en las instalaciones físicas de la GERESA.

La red tiene diferentes clases de usuarios por lo cual fue necesario la segmentación de la misma en VLANs para una mejor administración e una integración con el Directorio Activo, para tener una administración de todos los grupos, usuarios y equipos que conforman la red y poder adecuar cada uno de ellos en las VLANs según el perfil que desenvuelven dentro de la red. Todo lo previamente indicado es necesario para llevar acabo la integración de la red con los diferentes protocolos que son establecidos en esta tesis, pada poder probar todo esto se recurrí a la simulación mediante el software Cisco Packet Tracer.

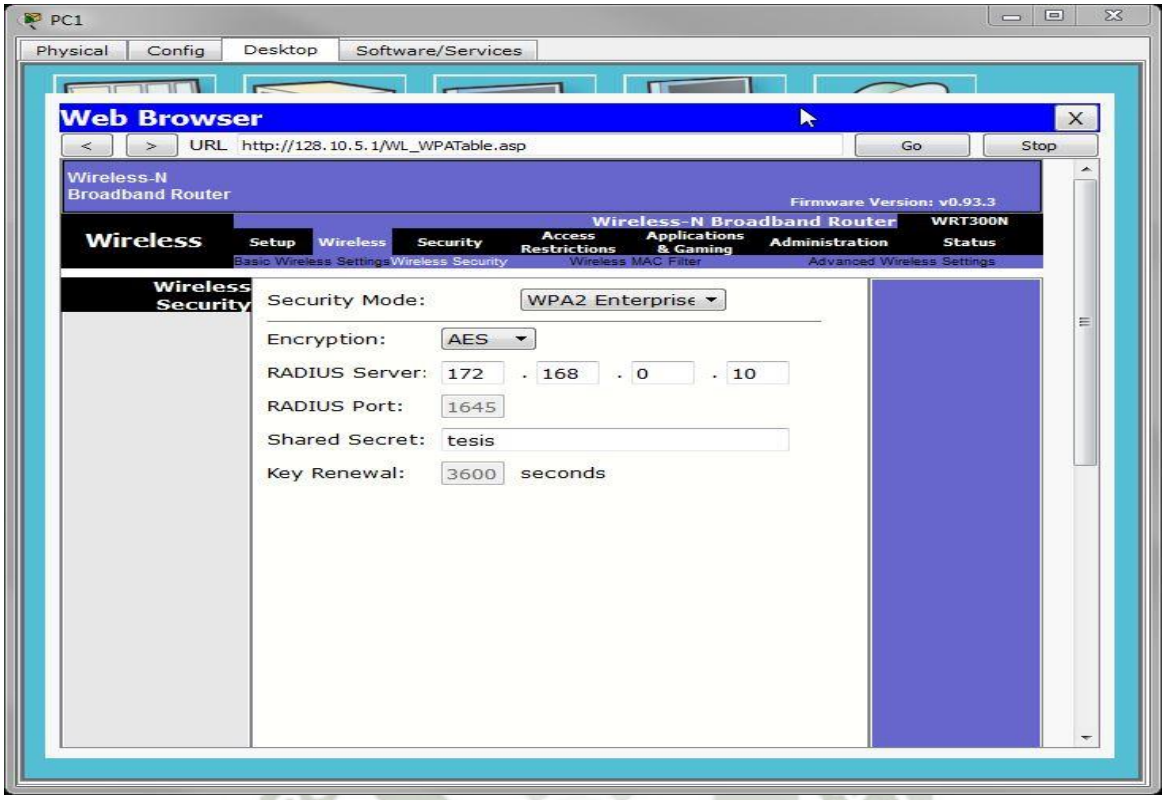

Figura 4.57 Elección de Certificado.

Fuente: "Elaboración Propia

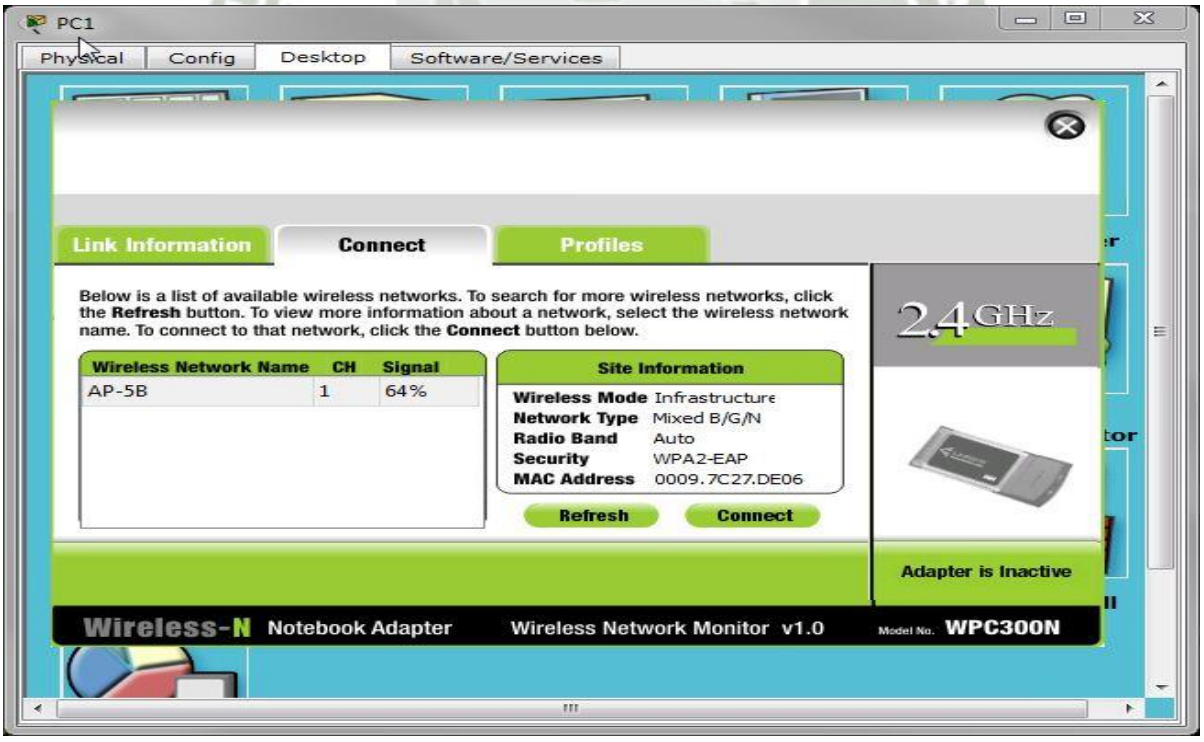

Figura 4.58 Elección de Certificado.

Fuente: "Elaboración Propia"

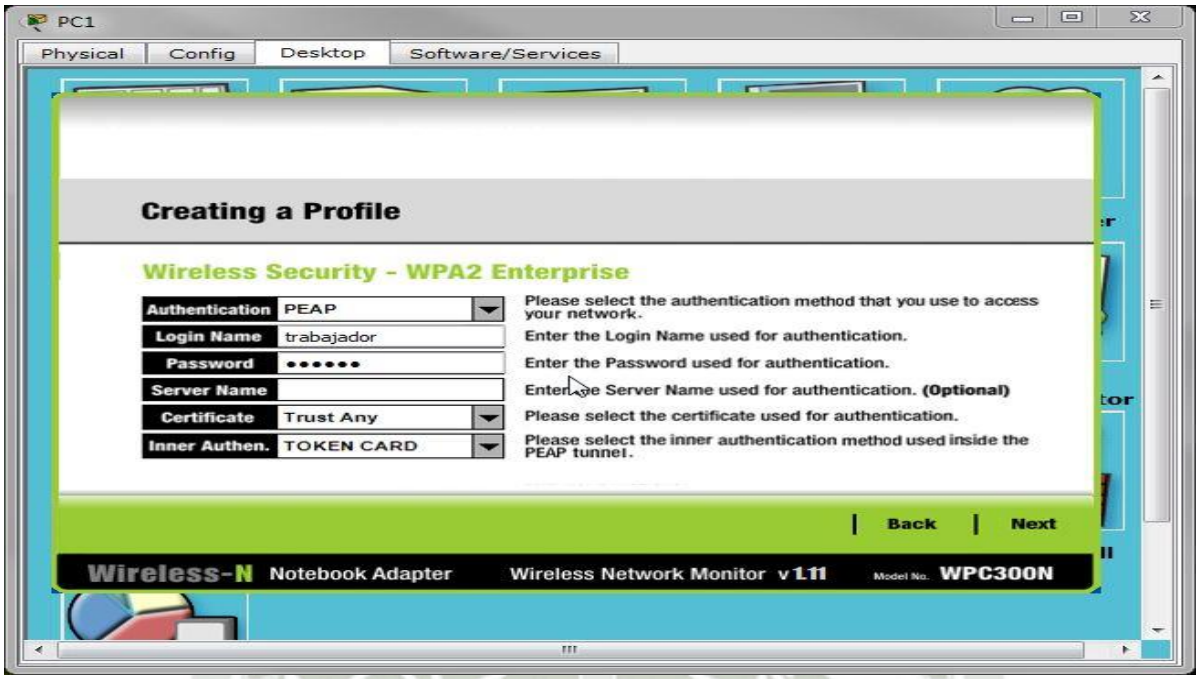

Figura 4.59 Elección de Certificado.

Fuente: "Elaboración Propia"

Figura 4.60 Elección de Certificado.

Fuente: "Elaboración Propia"

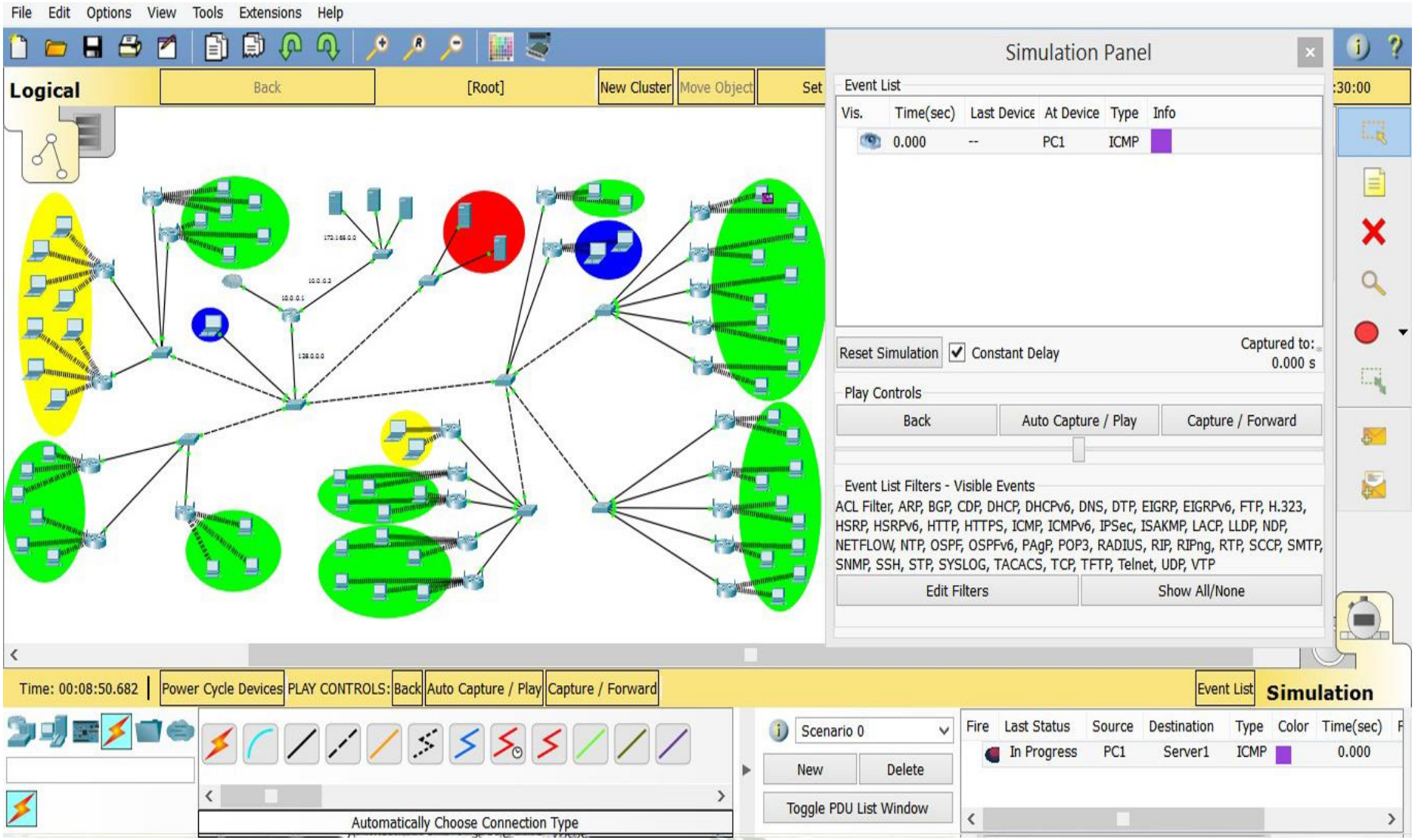

Figura 4.61 Simulación PC - Servidores de la VLAN Administrativa.

Fuente: "Elaboración Propia"

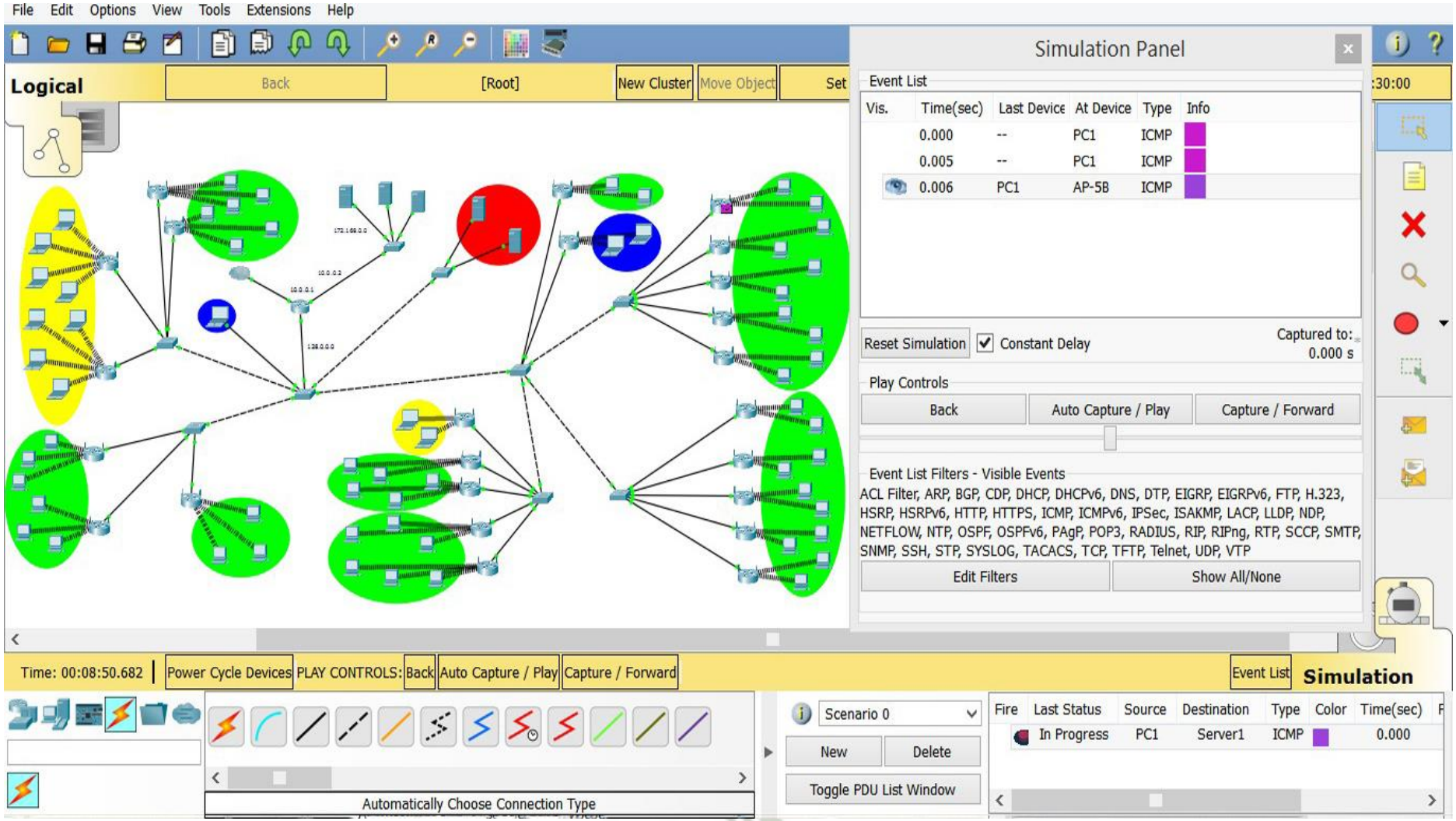

Figura 4.62 Simulación PC - Servidores de la VLAN Administrativa.

Fuente: "Elaboración Propia"

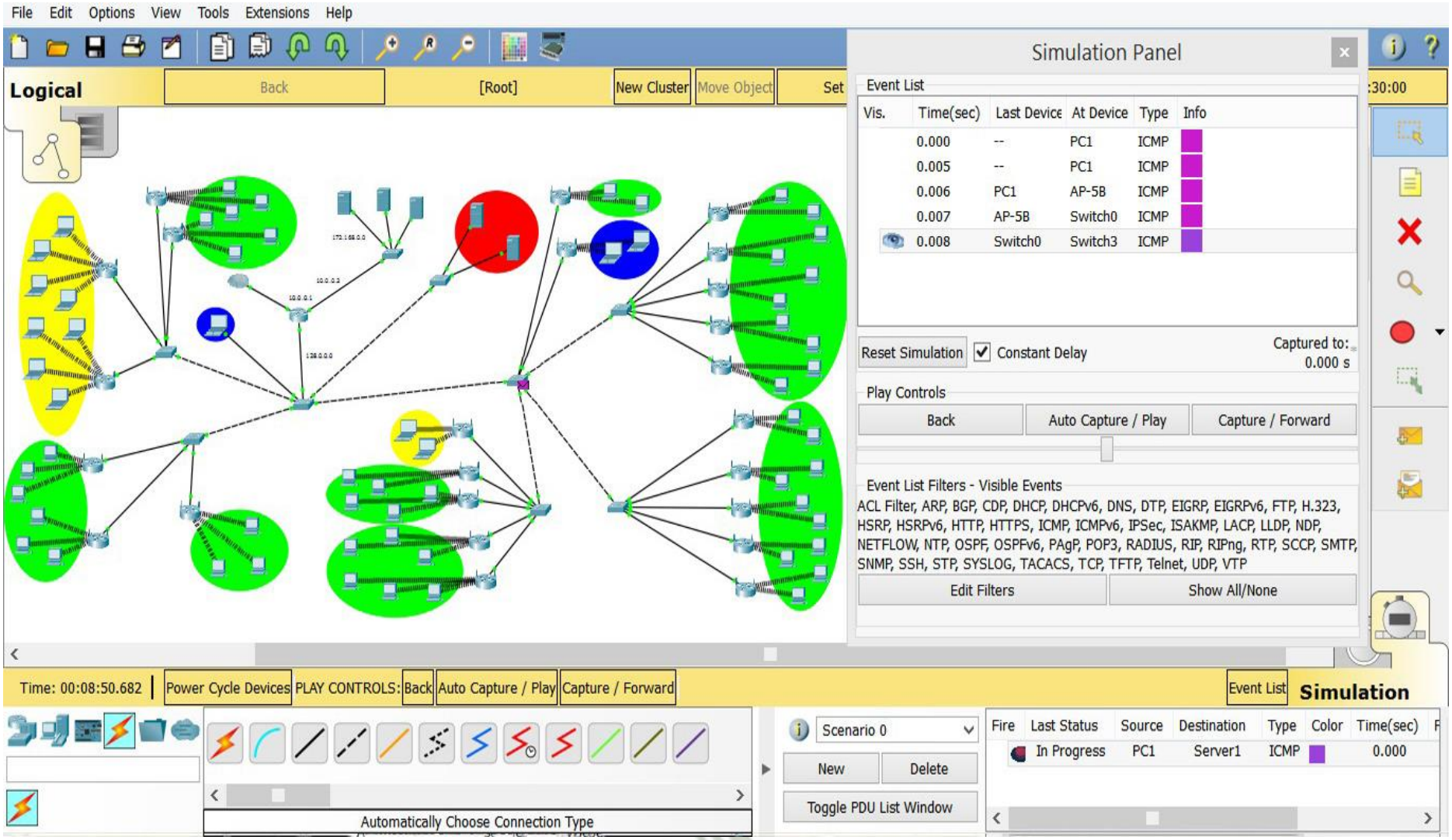

Figura 4.63 Simulación PC - Servidores de la VLAN Administrativa.

Fuente: "Elaboración Propia"

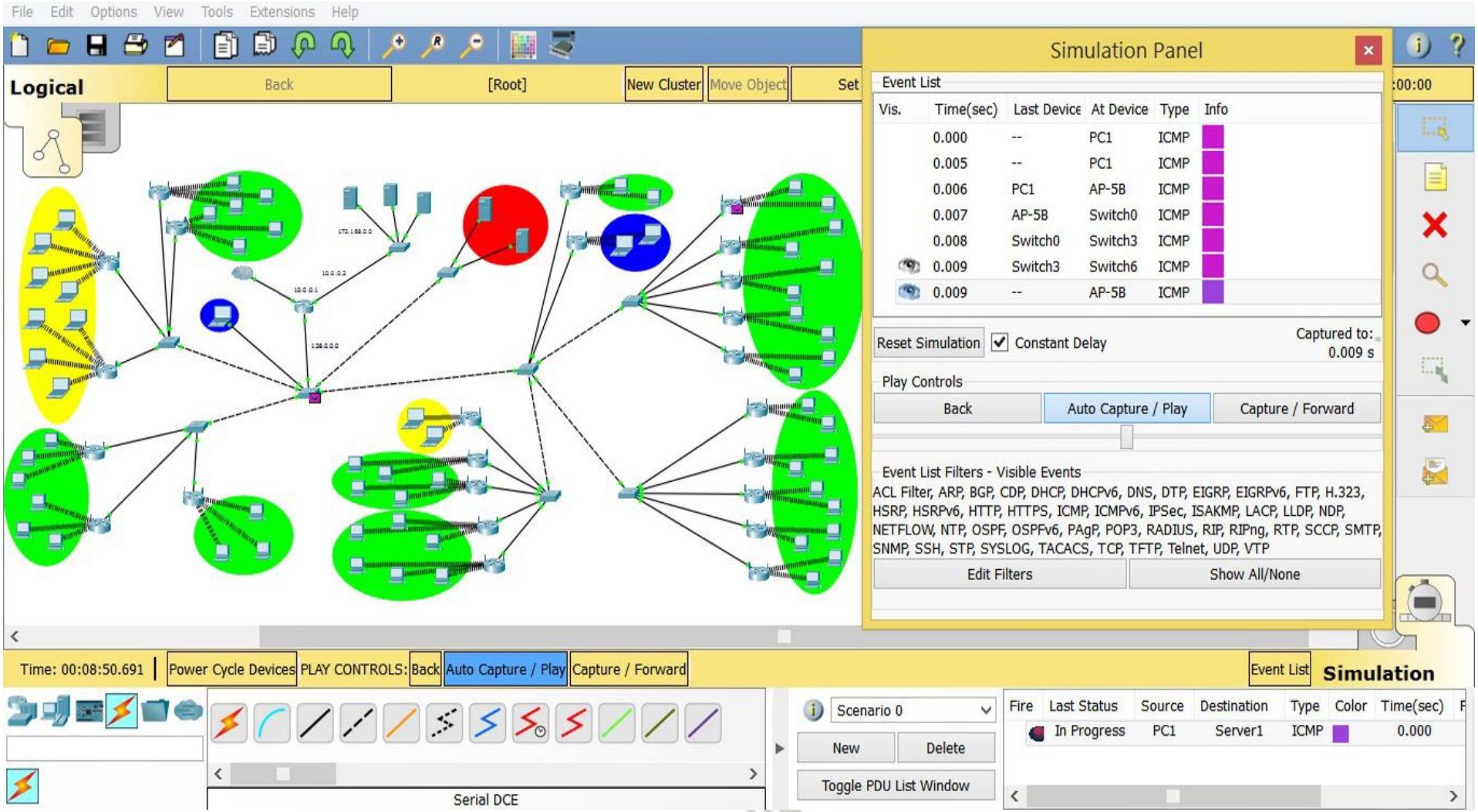

Figura 4.64 Simulación PC - Servidores de la VLAN Administrativa.

Fuente: "Elaboración Propia"

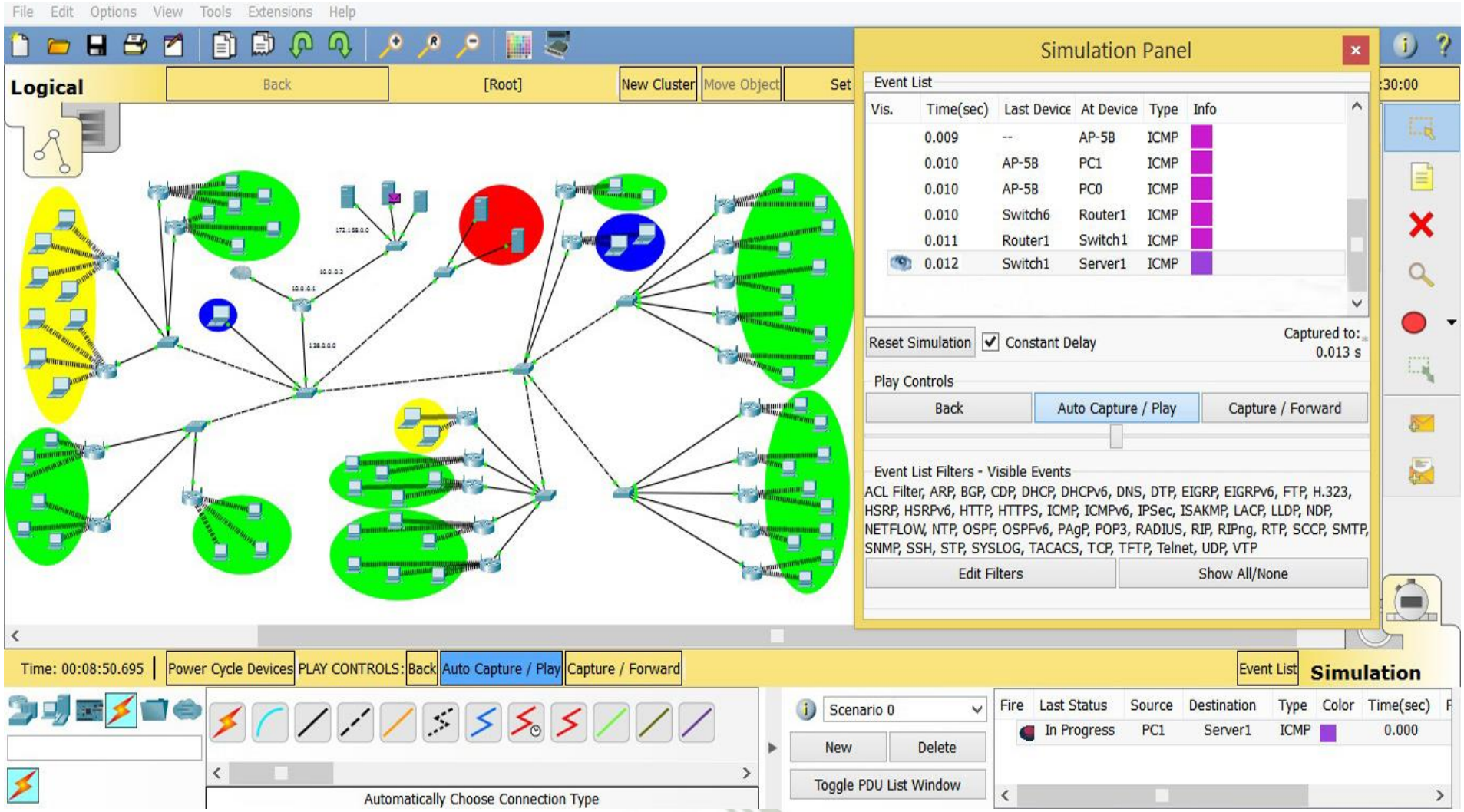

Figura 4.65 Simulación PC - Servidores de la VLAN Administrativa.

Fuente: "Elaboración Propia"

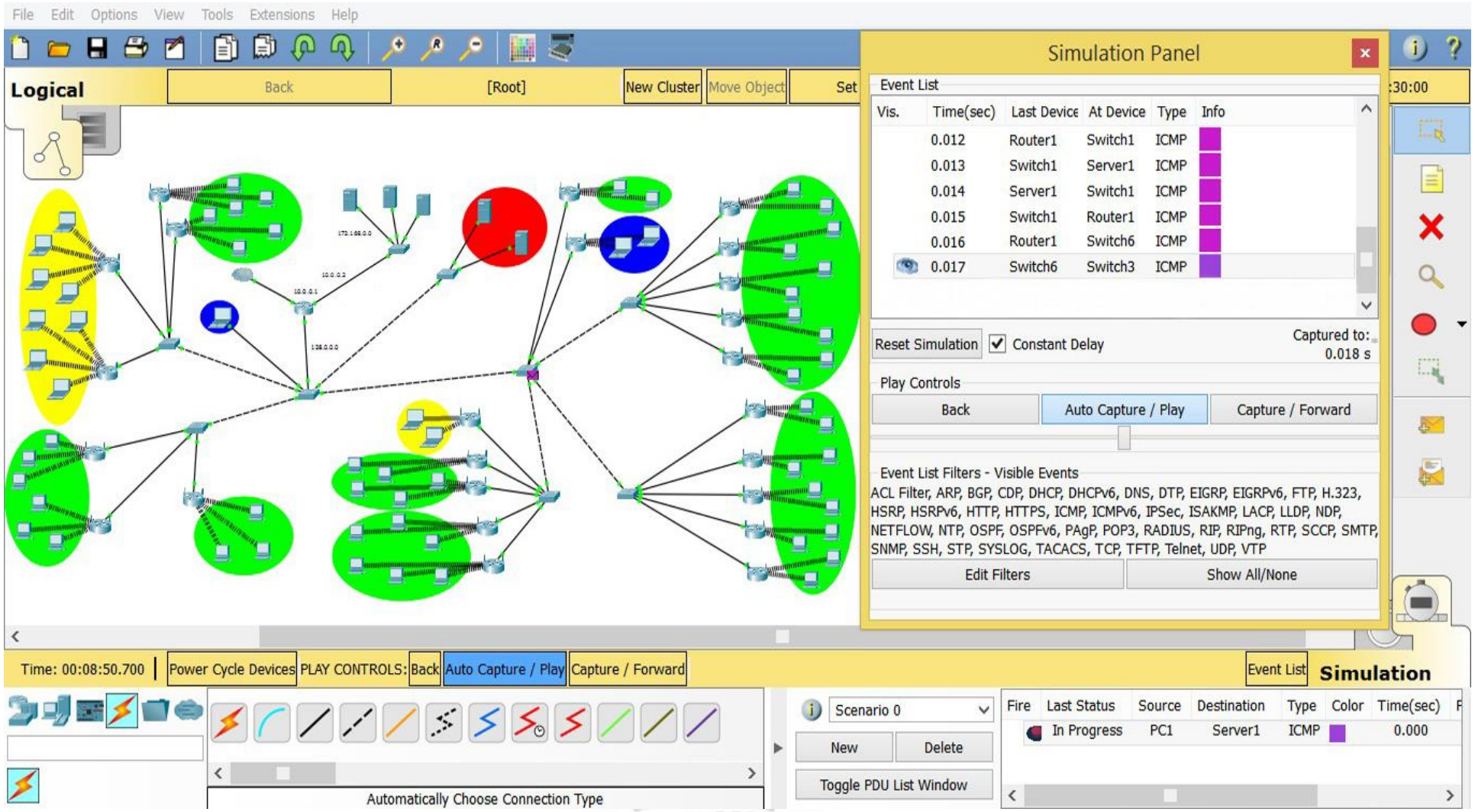

Figura 4.66 Simulación PC - Servidores de la VLAN Administrativa.

Fuente: "Elaboración Propia"

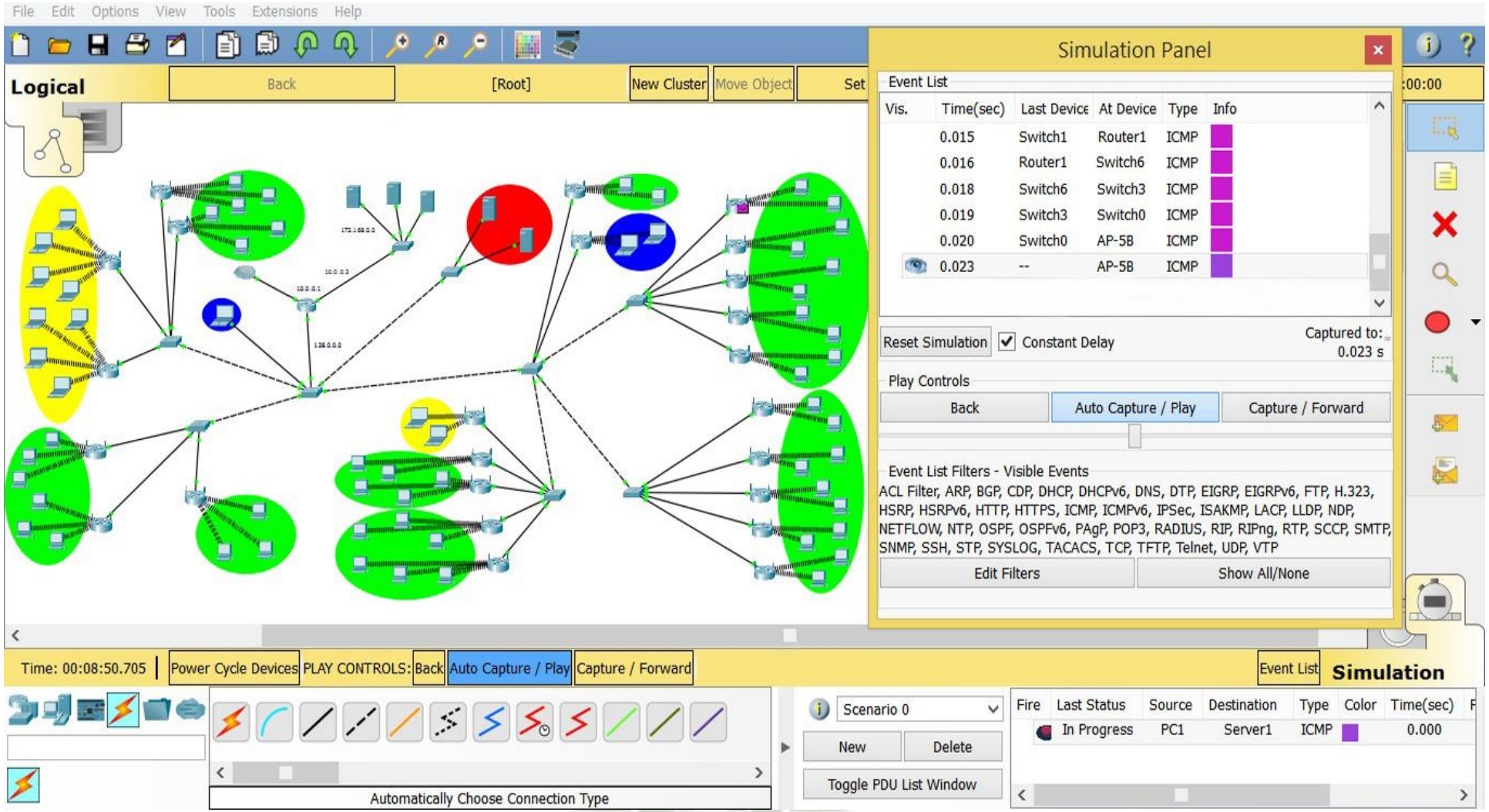

Figura 4.67 Simulación PC - Servidores de la VLAN Administrativa.

Fuente: "Elaboración Propia"

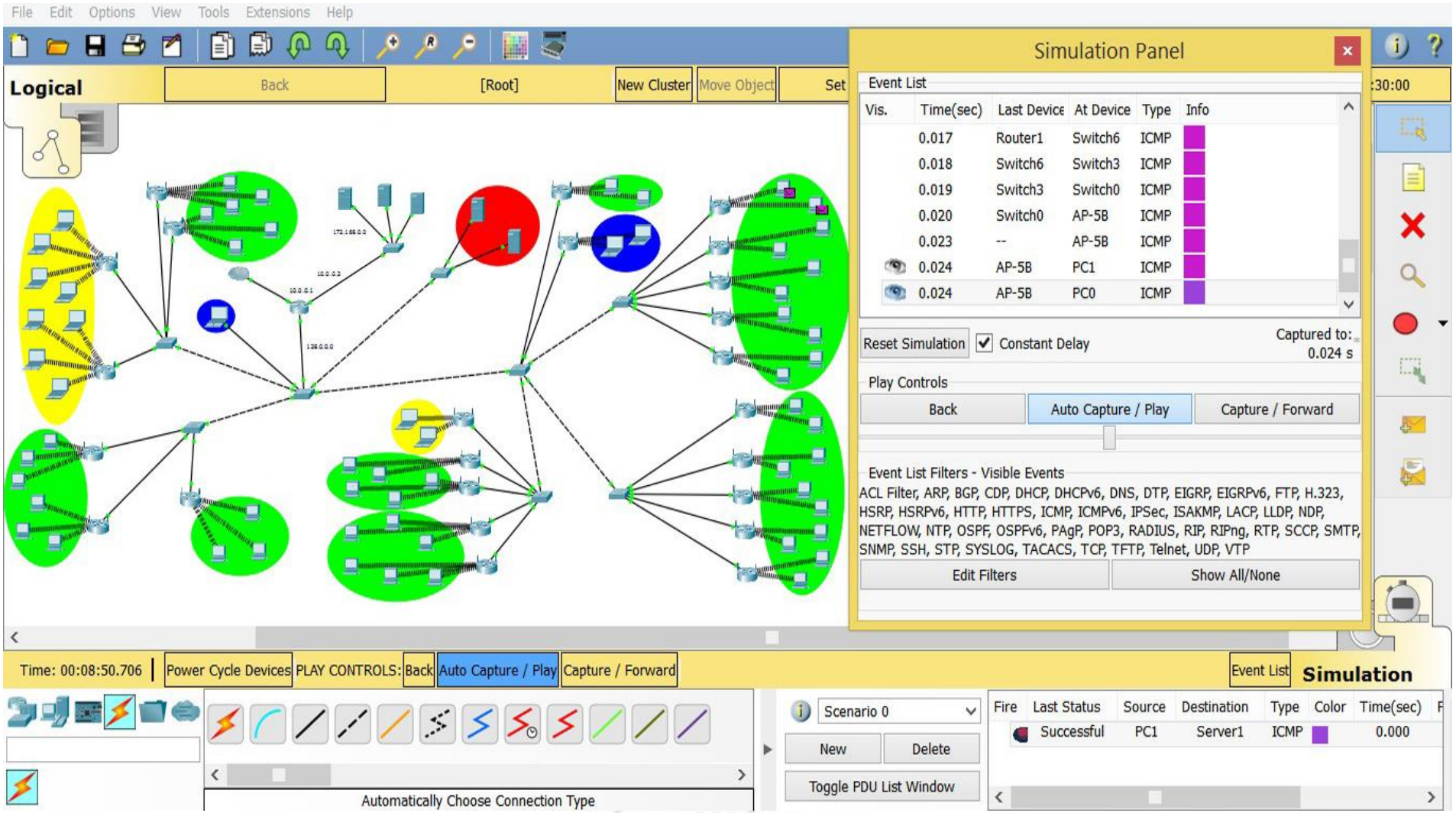

Figura 4.68 Simulación PC - Servidores de la VLAN Administrativa.

Fuente: "Elaboración Propia"

4.10 Análisis de la valoración de la metodología

A continuación, se presentan el análisis de los resultados sobre la valoración de la aplicabilidad de la metodología en la institución, para este análisis participaron el área de soporte conjuntamente con el área de estadistica e informatica, los cuales respondieron las siguientes preguntas:

Item 1 ¿Considera la metodología lo suficientemente detallada para poder implementarla?

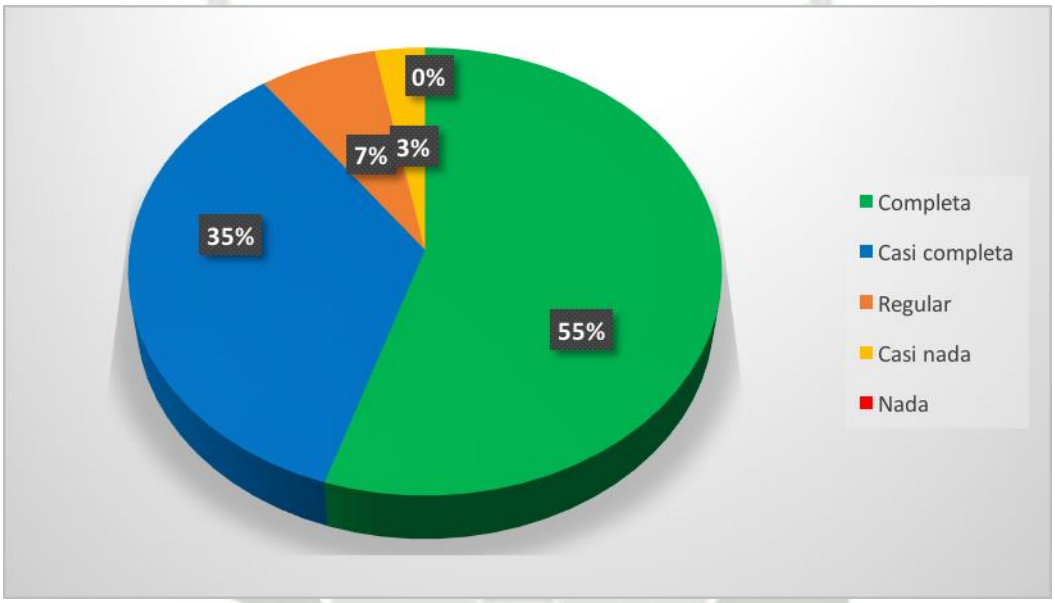

Figura 4.69 Nivel de detalle de la metodología.

Fuente: "Elaboración Propia"

Análisis: a partir de la valoración del personal involucrado, se obtuvo que un 55% que la metodología es completa mientras que un 35% considera que esta casi completa, por lo que se llega a la conclusión que si se detallan claramente las diferentes fases y actividades a realizar la metodología propuesta.

Item 2 ¿De que manera abarca la metodología las necesidades de la red?

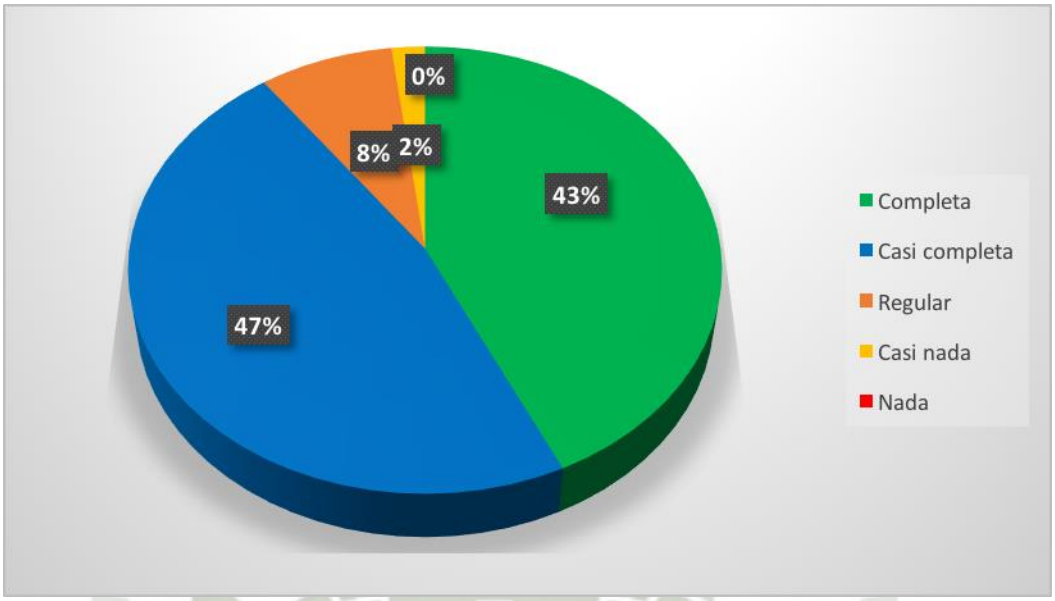

Figura 4.70 Grado de efectividad de la metodología.

Fuente: "Elaboración Propia"

Análisis: a partir de la valoración del personal involucrado, se obtuvo que un 43% que la metodología va solucionar las necesidades de la red mientras que un 47% considera que esta casi completa, por lo que se llega a la conclusión que la metodología planteada puede solucionar las diferentes necesidades presentes en la red.

Item 3 ¿Para su criterio como estima que la incorporación del protocolo de comunicación 802.11 n/ac va subsanar la velocidad de transmisión de datos?

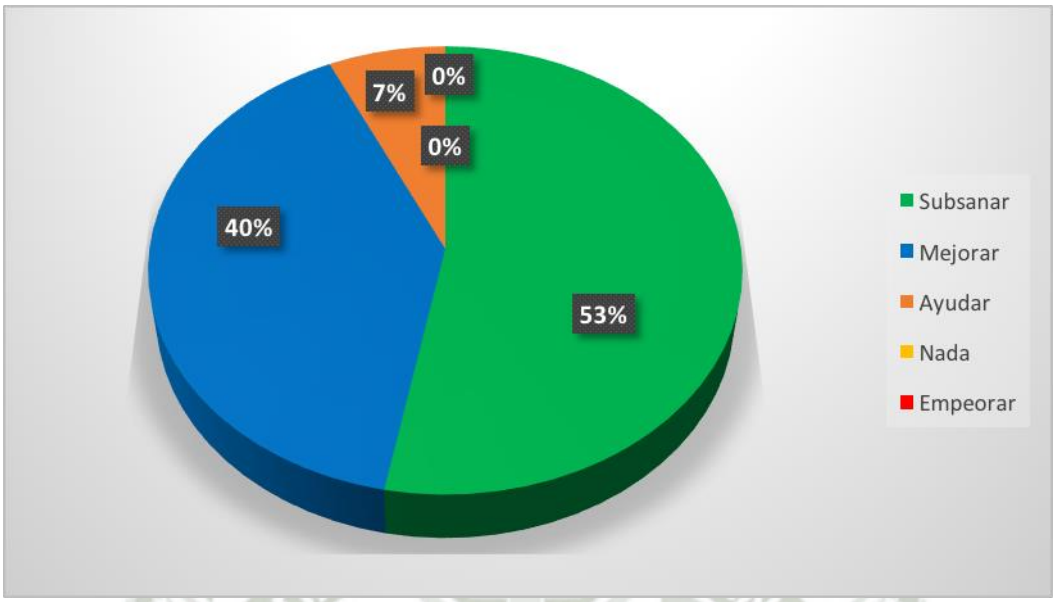

Figura 4.71 Criterio para la subsanación del problema

Fuente: "Elaboración Propia"

Análisis: a partir de la valoración del personal involucrado, se obtuvo que un 53% que va subsanar el problema existente mientras que un 40% considera que la velocidad va mejorar, por lo que se llega a la conclusión que mediante la incorporación de los protocolos de comunicación pueden resolver el problema de la velocidad de transmisión de datos que sufren los trabajadores de la institución.

Item 4 ¿Para su criterio como ve la incorporación del protocolo de de autenticación, autorización y contabilización Radius va subsanar el problema de seguridad y control de la red?

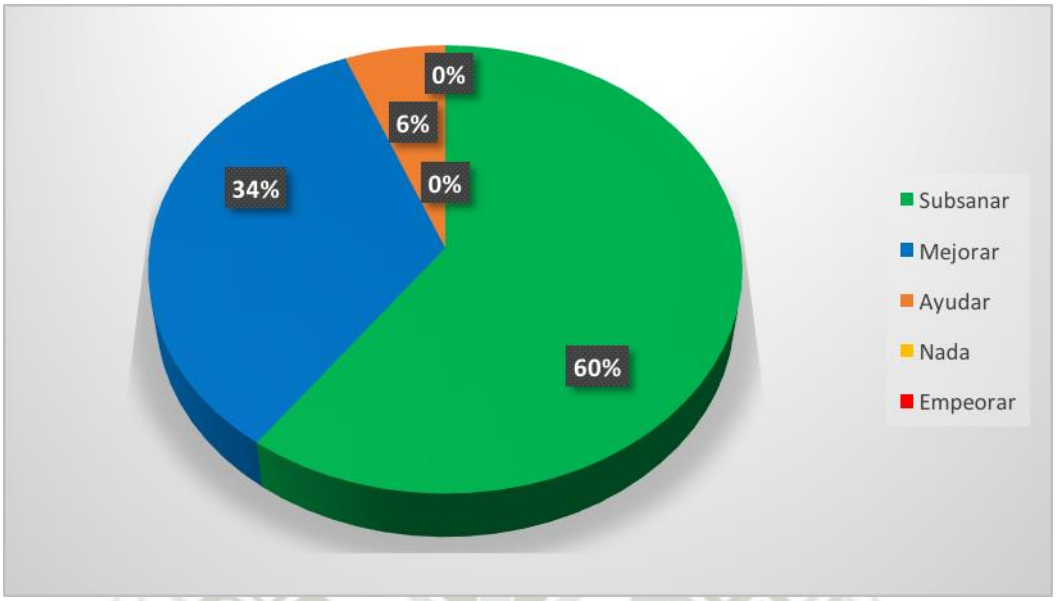

Figura 4.72 Criterio para la subsanación del problema.

Fuente: "Elaboración Propia"

Análisis: a partir de la valoración del personal involucado, se obtuvo que un 60% que va subsanar el problema existente mientras que un 34% considera que la seguridad va mejorar, por lo que se llega a la conclusión que mediante la incorporación del protocolo Radius puede resolver la seria problemática de la seguridad adicionalmente también lograr tener una correcta administración del uso de la red.

Ítem 5 Comparativa del nivel de satisfacción de los usuarios respecto a la red actual y al nuevo diseño de la red de la GERESA

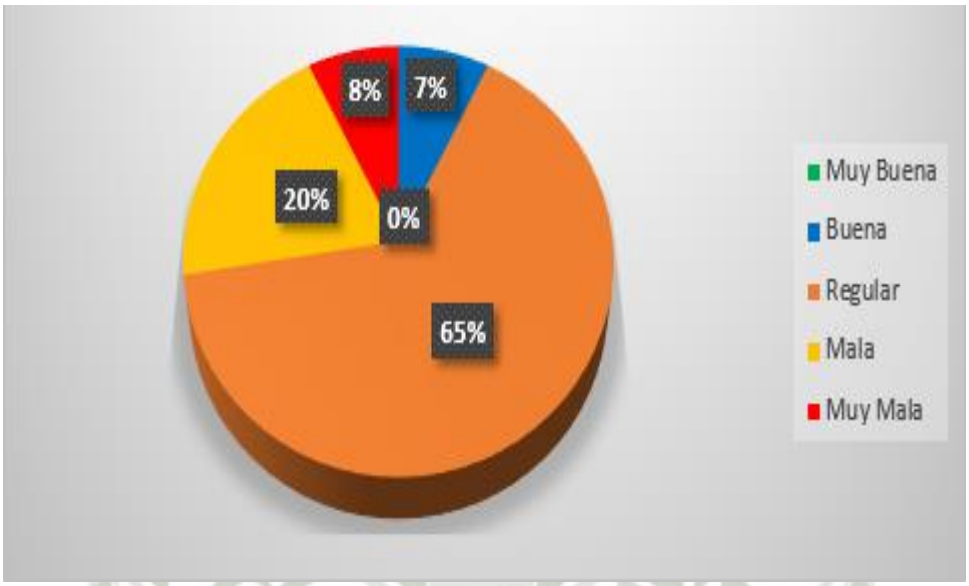

Figura 4.73 Nivel de Satisfacción ante la actual red de la GERESA.

Fuente: "Elaboración Propia"

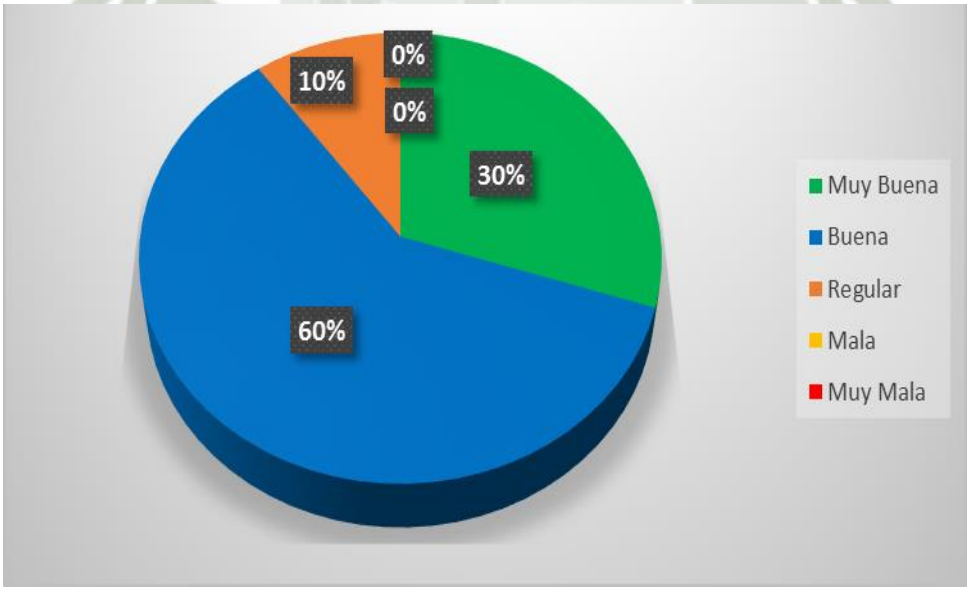

Figura 4.74 Nivel de Satisfacción para el nuevo diseño de la red inalámbrica.

Fuente: "Elaboración Propia"

Mediante esta comparativa se demuestra la actual insatisfacción que tiene el personal de la GERESA hacia la red institucional siendo superior al 85% el grado de desaprobación de la actual red, además de una alta tasa de aceptación al cambio del nuevo diseño propuesto con una valoración del personal y el área de soporte, se obtuvo que un 60% opina que es una buena opción mientras que un 30% considera que es muy buena opción, por lo que se llega a la conclusión que los usuarios están de acuerdo con el nuevo diseño de la red para solucionar los problemas que presente la red.

CONCLUSIONES

1. Mediante esta presente tesis se propuso una metodología con la cual se diseñó una red inalámbrica que suple las deficiencias que presenta la red de la GERESA con equipos que cuentan con conectividad y administración de los protocolos 802.11n/ac y el protocolo de autenticación, autorización y contabilización Radius.
2. Se establecieron las fases, procesos y actividades que componen la metodología tomando en consideración para esta las necesidades y limitaciones que presenta la institución.
3. Con el análisis de la documentación existente, la infraestructura de la red y sobre todo con las practicas realizadas en la institución se logro identificar las principales deficiencias que presenta esta red y que ocasiona múltiples problemas a los usuarios al momento de desarrollar sus actividades.
4. Con la información obtenidad de las necesidades de la red se determinó que la mejor opción para solucionar los problemas de red de la GERESA es una red inalámbrica que integre los protocolos de comunicación 802.11n/ac y el protocolo de autenticación, autorización y contabilización Radius.
5. Se detalló cada fase de la metodología haciendo hincapié en la configuración de todos los equipos que deben integran la red para que de esa manera se pueda lograr una adecuada incorporación de los protocolos a la red inalámbrica.
6. Con el fin de corroborar el funcionamiento de la metodología se ha recurrido a simulación de la topología de la red con los protocolos integrados, con lo cual se prueba que la metodología puede ser adaptada a otros entornos similares.

RECOMENDACIONES

1. Para alteraciones posteriores a la implantación de la red se debe tener en cuenta las características de los equipos a incorporar, ya que tienen que ser compatibles con los protocolos integrados a la red para que no afecte la escalabilidad de la red.

2. Realizar actualizaciones de los planos de la ubicación de los access point y cualquier tipo de modificación que se realice a cualquier otro equipo que integre la red para tener una adecuada administración de la red.

3. Ejecutar un mantenimiento preventivo, periódico y continuo de los recursos de hardware y software, para evitar cualquier tipo de daño físico y/o lógico a la red.

4. Realizar capacitaciones a los diferentes usuarios sobre el uso de la red inalámbrica, así como de políticas de seguridad, con el fin de fomentar una "cultura informática" de tal manera minimizar riesgos y explotar los beneficios de la tecnología en las diferentes actividades laborales.

5. Mantener una copia de seguridad de la configuración de los diversos equipos de la red como también de los sistemas operativos, los cuales se deben encontrarse en lugares seguros con el fin evitar cualquier tipo de problema y poder garantizar una reinstalación en caso de algún daño lógico a los equipos o sistemas.

REFERENCIAS

[1] Lazo, N.A. (2012). Diseño e Implementación de una Red LAN y WLAN con Sistema de control de acceso mediante servidores AAA. (Tesis de Pregrado). Pontificia Universidad Católica del Perú, Lima, Perú.

[2] Murillo, J.M. (2015). Diseño e implantación de una red inalámbrica unificada en el Colegio Nuestra Señora de Fátima de Valencia. (Tesis de Pregrado). Universidad Politécnica de Valencia, Gandía, España.

[3] Guía, A. (2014). Metodología ágil para el diseño y desarrollo de redes de área local (LAN). (Tesis de Pregrado). Universidad Nacional Experimental De los Llanos Occidentales Ezequiel Zamora, Barinas, Venezuela.

[4] Guido, R., Denteneer, D., Stibor, L., Yunpeng, Z., Pérez, X., y Bernhard, W. (2010). The IEEE 802.11 Universe. IEEE Communications Magazine, *48*(1), 62-70.

[5] Meden, J. (2013). IEEE 802.11ac (Tesis de Pregrado). Universidad Católica Nuestra Señora de la Asunción, Asunción, Paraguay.

[6] García, F. (2012). Integración Red Wired – Wireless (Tesis de Pregrado). Universidad Oberta de Catalunya, Catalunya, España.

[7] Arana, J., Villa, L., y Polanco O. (2013). Implementación del control de acceso a la red mediante los protocolos de autenticación, autorización y auditoría. Ingeniería y Competitividad, *15*(1), 127-137.

[8] Souza, F. (2007). Autenticação de usuarios no active directory utilizando Radius através do serviçio de autenticação da internet (Tesis de Pregrado). Sociedade educacional de Santa Catarina – SOCIESC, Santa Catarina, Brasil.

[9] Wolf, L. (2011). Controle de acesso em segmentos de rede para usuários autorizados en um ambiente corporativo (Trabajo Final de Curso). Universidade Luterana de Brasil, Rio Grande do Sul, Brasil.

[10] Florwick, J., Whitearker, J., Cuellar, A., y Woodhams J. (2013). Wireless LAN Design guide for high density client environments in higher education. Cisco Design Guides, *11*(13), 1-41.

[11] Sebastián. (11 de enero del 2011). Conozca las redes inalámbricas [Mensaje en un blog]. Recuperado de http://zebas-redemax.blogspot.com.br/2011/05/conosca-las-redes-inalambricas.html

[12] Barrenechea, T. (2012). Diseño de una red Inalámbrica para una empresa de Lima (Tesis de Pregrado). Pontificia Universidad Católica del Perú, Lima, Perú.

[13] Ponce, M., Molina, E., y Mompó, V. (2011). Redes inalámbricas: 802.11 (Trabajo de Investigación). Universidad Politécnica de Valencia, España.

[14] Prado, C. (2010). Ethernet Industrial: Modelos y conectividad en el ámbito de procesos industriales (Tesis de Maestría). Universidad Nacional de la Plata, Buenos Aires, Argentina.

[15] Chávez, P., y Reinoso A. (2004). Diseño de una red móvil de comunicación utilizando tecnología de espectro ensanchado (SS) en la ciudad de Guayaquil en la banda de frecuencia ICM (2.4 – 2.4835) GHz ≡ (2400 – 2483.5) MHz (Tesis de Pregrado). Escuela Superior Politécnica del Litoral, Guayaquil, Ecuador.

[16] Uribe, J. (2007). Desarrollo e Implementación de una Interfaz sobre Esquemas de Modulación y Demodulación OFDM (Tesis de Pregrado). Universidad Austral de Chile, Valdivia, Chile.

[17] Perahia, E., y Stacey, R. (2013). *Next Generation Wireless LANs 80211n and 802.11ac.* Cambridge, Reino Unido: Cambridge University Press.

[18] Milagro, F., y Los Santos, A. (2009). Comparativa de IEEE 802.11 e IEEE 802.16: capa física y de enlace (Tesis de Doctorado). Universidad de Vigo, Vigo, España.

[19] Panda Security. (2010). ¿Qué es Peer – to Peer (P2P) ?. Panda Cloud Internet Protection Simply… Evolution, *1*(1), 1-6.

[20] Giraldo, W. (2015). *Taller-Sistemas1*. Recuperado de http://myslide.es/documents/taller-sistemas1.html

[21] Extensible Authentication Protocol, (s.f.). En *Wikipedia*. Recuperado el 29 de marzo del 2016 de https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

[22] Radius, (s.f.). En *Wikipedia*. Recuperado el 29 de marzo de 2016 de https://en.wikipedia.org/wiki/RADIUS

ANEXOS

Anexo I

Glosario de terminos

Medio: se pueden definir dos, la radiofrecuencia y los infrarrojos.

Access Point (AP): es un dispositivo de red que interconecta equipos de comunicación alámbrica para formar una red inalámbrica.

La asignación de canales: permite tener access point de manera continua sin que ellos se solapen o interfieran entre sus señales.

Sistema de distribución: es un sistema que permite la interconexión inalámbrica de puntos de acceso en una red IEEE 802.11.

Conjunto de servicio básico (BSS): grupo de estaciones que se intercomunican entre ellas. Se define dos tipos:

- Independientes: cuando las estaciones, se intercomunican directamente.
- Infraestructura: cuando se comunican todas a través de un punto de acceso.

Área de servicio Básico (BSA): es la zona donde se comunica las estaciones de una misma BSS, se define dependiendo el medio

Conjunto de servicio Extendido (ESS): es la unión de varios BSS.

Metodologia: Conjunto de métodos que se siguen en una investigación científica, un estudio o una exposición doctrinal.

Servidor Radius: es un protocolo de red que proporciona autenticación centralizada, autorización y contabilidad del uso de la red.

IEEE 802.11n/ac: Protocolos de comunicación que se derivan del estándar IEEE 802.11

Windows Server 2012 R2: Sistemas operativo desarrollado por Microsoft para su uso en servidores.

Directorio Activo: Servicio de directorio de Windows para dominio de redes.

Switch: Dispositivo lógico digital de interconexión de redes de computadoras

OFDM: Orthogonal Frequency Division Multiplexing, método de modulación de redes inalámbricas

MAC: Media Access Control es un identificador único de un dispositivo de red

Mbit/s: Megabit por segundo es una unidad que se usa para cuantificar un caudal de datos

ISM: Industrial, Scientific and Medical son bandas de comunicación reservadas internacionalmente para un uso no comercial

NFC: Near Field Communication es un tipo de tecnología de comunicación inalámbrica

Roaming: Capacidad de un dispositivo inalámbrico para moverse dentro de un área de cobertura

VLAN: Virtual LAN es una red de área que agrupa equipos de una manera lógica no física

Escalabilidad: Propiedad de un sistema o una red para adaptarse al crecimiento sin perder calidad

Router: Dispositivo de red que permite el enrutamiento de paquetes entre redes independientes

IP: Protocolo de Internet es un estándar que se emplea para el envio y recepción de información

SSID: Service Set Identifier es un nombre incluido en todas las redes inalambricas

Anexo II

Encuesta

Metodología para el diseño de una red LAN inalámbrica 802.11 n/ac con servidor Radius para la Gerencia Regional de Salud-Arequipa

A continuación encontrará una serie de preguntas destinadas a conocer su opinión técnica sobre diversos aspectos de la Metodología para el diseño de una red LAN inalámbrica 802.11 n/ac con servidor Radius para la Gerencia Regional de Salud-Arequipa. Mediante esto queremos conocer lo que piensa usted sobre esta temática.

Por favor lea las instrucciones al inicio de cada sección y conteste la alternativa que más se acerca a lo que usted piensa. Sus respuestas son confidenciales y serán reunidas junto a las respuestas de muchas personas que están contestando este cuestionario.

PREGUNTAS

Por favor marque con una X la alternativa que más se parece a lo que usted piensa.

1. ¿Considera la metodología lo suficientemente detallada para poder implementarla? Para esta pregunta se anexo la metodología para que usted pueda leer y a partir de ahí responder esta pregunta.

Completa	Casi Completa	Regular	Casi nada	Nada

2. ¿ De que manera abarca la metodología las necesidades de la red?

Completa	Casi Completa	Regular	Casi nada	Nada

3. ¿ Para su criterio como estima que la incorporación del protocolo de comunicación 802.11 n/ac va subsanar la velocidad de transmisión de datos?

Subsanar	Mejorar	Ayudar	Nada	Empeorar

4. ¿ Para su criterio como ve la incorporación del protocolo de de autenticación, autorización y contabilización Radius va subsanar la seguridad y control de la red?

Subsanar	Mejorar	Ayudar	Nada	Empeorar

5. ¿Cuál es su nivel de satisfacción respecto a la red actual?

Muy Buena	Buena	Regular	Mala	Muy Mala

6. ¿Cuál piensa que va ser su nivel de satisfacción respecto a la nueva red?

Muy Buena	Buena	Regular	Mala	Muy Mala

Muchas Gracias

Anexo III

Instrumentos

Metodología para el diseño de una red LAN inalámbrica 802.11 n/ac con servidor Radius para la Gerencia Regional de Salud Arequipa

Fase 1: Diagnóstico de Necesidades

- Análisis de la Red
  - Análisis de la documentación existente.
  - Análisis de la infraestructura de la red.
- Determinación de las necesidades de la red
  - Identificacion de Necesidades
    - Selección de la Solución
  - Tecnología
    - Incorporación de protocolos
  - Dispositivos.
    - Access Point
    - Wireless LAN Controles
    - Tarjeta de red Inalámbrica
  - Servidores.
    - Radius Server

Fase 2: Diseño de la red

- Diseño Físico de la Red
  - Distribución de los equipos
    - Software para estudio del Sitio
    - Ubicación de los Access Point

- Arquitectura de la red.

➢ Segmentación de la Red

- Adaptación de VLANs
- Asignación de direcciones IP

- Diseño Lógico de la Red

➢ Incorporación al Directorio Activo

➢ Configuración del Directorio Activo

➢ Incorporación de VLANs al Directorio Activo

- Acceso a la red Administrativa
- Acceso a la red Mantenimiento
- Acceso a la red Invitados
- Acceso a la red Sin Dominio

Fase 3: Implementación del diseño

- Protocolo Radius

➢ Instalación del Servicio.

➢ Autorización del uso del Directorio Activo.

➢ Configuración de Clientes Radius.

➢ Configuración De Políticas.

- Directivas de Solicitud de Conexión
- Directivas de Red

- Configuración de la Red

➢ Red Cableada

- Configuración general para usar autenticación en el router
- Asignación de puertos de acceso para la configuración 802.1X

- Red Inalámbrica
    - Configuración de los parámetros generales del Servidor Radius
    - Generación de un perfil de seguridad

Fase 4: Simulación de la Red

- Pruebas.