Resumen

Título:

"*Propuesta de diseño de una solución de videovigilancia soportada en cámaras IP con tecnología IEEE 802.11 para el Edificio el Rectorado, la Plaza Cubierta y el Complejo Cultural Aula Magna de la UCV* ".

Autores: Gabriela E. Millán V.
Fredis A. Alfonzo V.

Tutora Académica: Prof. Ana Morales (*M.Sc.*).

Resumen:

Debido a los diversos ataques en los que se ha visto involucrada la Universidad Central de Venezuela, surgió la necesidad de una propuesta de diseño de una solución de videovigilancia soportada en cámaras IP, con la finalidad de incrementar los niveles de vigilancia en el Edificio el Rectorado, la Plaza Cubierta y el Complejo Cultural Aula Magna de la UCV. Esta fue la propuesta de la Dirección de Tecnología de Información y Comunicaciones (DTIC), con el objetivo de reforzar los niveles de seguridad y de esta manera brindar tranquilidad a la comunidad universitaria.

En este Trabajo Especial de Grado se presenta el diseño, los dispositivos inalámbricos usados y unas pruebas de funcionamiento, que dan soporte al diseño de la solución. Los dispositivos inalámbricos involucrados en el diseño están basados en el fabricante Cisco Systems. La propuesta de diseño de la solución de videovigilancia se basa en el estándar IEEE 802.11 y así mismo se propone la implementación de QoS (*Quality of Service*), específicamente del mecanismo de DiffServ (*Differentiated Services*), con la finalidad de evitar la congestión del tráfico que transita por la red. A su vez para validar esta propuesta de diseño, se realizaron diversas pruebas. El resultado final, es una solución de videovigilancia soportada en una WLAN completamente funcional, que cumple con los requisitos exigidos por la DTIC y por la Dirección de Seguridad de la UCV.

Palabras clave:

WLAN, IEEE 802.11, Quality of Service, QoS, Differentiated Services, DiffServ, cámaras IP.

Dedicatoria

A mi madre,
por su incondicional apoyo todos estos años,
por brindarme su infinito amor,
por su comprensión y amistad,
por acompañarme en los buenos y malos momentos,
por ayudarme a hacer realidad este sueño,
por ser única… Te amo

Gabriela E. Millan V.

Dedicatoria

Por toda tu confianza y apoyo incondicional,
por creer siempre en mí,
por estar ahí todos y cada uno de mis días,
por todos tus sacrificios,
por tu gran y único amor,
te dedico este logro tan importante para mí,
a ti MADRE...

Alberto Alfonzo

Agradecimientos

A Dios, por brindarme la dicha de la salud y permitirme alcanzar mis metas.

A mis abuelos (Carlos y Maruja), que aunque ya no están entre nosotros, aun siguen vivos en mis pensamientos, les doy las gracias por formarme y hacerme una mujer de bien, por enseñarme a luchar en la vida y por tener fe en mi… gracias por darle a mi vida un toque diferente fueron y son los mejores padres que he tenido.

A mi madre, por tener esa confianza ciega en mí, por animarme todos los días a seguir adelante, por ser esa mujer luchadora que eres me siento orgullosa de ti, por eso este logro mío también es un logro tuyo, te adoro.

A mi tía y mi primo, por ser pilares fundamentales y fuertes en mi vida, aunque no se los diga con frecuencia, los amo.

A ti Ennio, por tener confianza en mí, por motivarme a luchar, por todos los consejos que me has dado, por toda la paciencia que me has tenido antes, durante y después de la culminación de este Trabajo, por amarme como lo haces, por ser parte de mi vida y por ayudarme a llevar a cabo este Trabajo, te quiero, te adoro y te amo.

A los profesores y amigos, Antonio Machado y Pablo Poskal, por ser pieza fundamental en este Trabajo, por poner su granito de arena para que la culminación de este Trabajo haya sido exitosa, nuevamente muchísimas gracias.

A mi tutora Ana Morales, por guiarnos durante el desarrollo de este trabajo.

A la gente de la DTIC (Milagros, Neudith, Roberto, Reina, Ana Belén, Prof. Alberto y Mariangela), por darme la oportunidad de desarrollar este proyecto, por ayudarnos y apoyarnos en todo lo que necesitamos, gracias.

A mis compañeros de trabajo (Jose ”Chucky”, Reily, Robert y Carlos), por hacernos reír cada vez que se presentaba la oportunidad, por hacer más amenas nuestras tardes de trabajo, gracias por ser esas personas especiales en mi vida.

A mi compañero de tesis, Alberto, por haber trabajado día a día, por apoyarme, por tenerme paciencia, sin ti este trabajo no habría sido el mismo, gracias.

Finalmente, a todos mis amigos, gracias por apoyarme, por creer en mí, cada uno de ustedes hizo un aporte en mi vida, son únicos los quiero…

A todos, Muchas Gracias!!!!!

Gabriela E. Millan V.

Agradecimientos

Doy gracias principalmente a Dios, por estar conmigo en todo momento, por haberme dado la salud, sabiduría y fortaleza para permitirme alcanzar este triunfo tan importante en mi vida.

A mi madre, tu bien sabes que sin tu ayuda nada de lo que he logrado hubiera sido posible, gracias por tu apoyo, tu paciencia, por hacerme un hombre con valores y principios, sencillamente por todo lo que eres te mereces cada uno de mis logros en la vida. Te Amo.

A María Carolina, por creer en mí en todo momento, por darme tu apoyo sincero e incondicional, tus consejos, tu confianza, tu amistad, tu amor, por estar a mi lado todo este tiempo te doy muchísimas gracias. Te Amo.

A mi tutora Ana Morales, por su orientación, sugerencias y buena disposición, muchas gracias.

A los profesores Antonio Machado y Pablo Poskal, por su gran colaboración y apoyo a lo largo de la realización de este Trabajo Especial de Grado, muchas gracias.

Al personal de la DTIC (Reina, Milagros, Neudith, Mariangela, Ennio, el Prof. Alberto), por la oportunidad que me brindaron de compartir con ustedes para llevar a cabo este proyecto, gracias.

A mi compañera de tesis, Gabriela Millán, especialmente por haberme dado la oportunidad de poder trabajar contigo en este proyecto, por tu colaboración y trabajo continuo, muchísimas gracias.

A mis compañeros de la UCV y amigos de La Parada, por haber compartido conmigo muchos momentos de mi carrera.

Y por ultimo pero no menos importante, doy gracias a la Universidad Central de Venezuela, *"La casa que vence las sombras"*, por permitirme estar entre tus espacios y formarme como un profesional de éxito, puedes tener la seguridad que mantendré tu nombre muy en alto y seré un digno representante tuyo.

Muy agradecido con todos ustedes!

Alberto Alfonzo

Si piensas que estás vencido, lo estás.
Si piensas que no te atreves, no lo harás.
Si piensas que te gustaría ganar pero no puedes, no lo lograrás.
Si piensas que perderás, ya has perdido.
Porque en el mundo encontrarás
que el éxito comienza con el pensamiento del hombre.
Todo está en el estado mental.
Porque muchas carreras se han perdido
antes de haberse corrido,
y muchos cobardes han fracasado
antes de haber su trabajo empezado.
Piensa en grande y tus hechos crecerán.
Piensa en pequeño y quedarás atrás.
Piensa que puedes y podrás.
Todo está en el estado mental.
Si piensas que estás aventajado, lo estás.
Tienes que pensar bien para elevarte.
Tienes que estar seguro de ti mismo
antes de intentar ganar un premio.
La batalla de la vida no siempre la gana
el hombre más fuerte, o el más ligero,
porque, tarde o temprano, el hombre que gana
es el que cree poder hacerlo.

Dr. Christiaan Barnard

Tabla de Contenidos

Lista de Figuras

Lista de Tablas

Introducción

Hoy en día las WLANs (*Wireless Local Area Networks*) han llegado a ocupar un lugar importante en el mundo de las telecomunicaciones, siendo estas una extensión de las redes cableadas, ya que el intercambio de información entre estas dos redes es totalmente transparente para el usuario. Así mismo, el principal objetivo de las WLANs es el de brindar las facilidades no disponibles en los sistemas cableados.

Una WLAN puede definirse como una red local de cobertura geográfica limitada, que utiliza ondas electromagnéticas para conectar los equipos a la red, en lugar de los cables coaxiales de par trenzado o de fibra óptica, que se utilizan en las LAN convencionales cableadas. La tecnología que más penetración ha tenido en el mercado es la IEEE 802.11 (*Institute of Electrical and Electronics Engineers*), la cual se refiere a una familia de especificaciones desarrolladas por el IEEE para la tecnología de las redes inalámbricas.

Las WLANs están siendo usadas para transmisiones multimedia (video y voz), además de los datos tradicionales. Una de las implementaciones típicas donde una WLAN juega un papel importante, es en una solución de video con cámaras inalámbricas, donde se realice una transmisión constante del mismo en tiempo real. Debido a esto, surge la necesidad que este tráfico de video sea atendido de manera diferente, ese es el objetivo principal de la calidad de servicio, darle prioridad a ciertos paquetes con respecto a otros, para asegurar determinadas características de calidad en la transmisión de la información, y así poder evitar que la congestión de algunos nodos en la red afecte a las aplicaciones que requieran un menor retardo en la transmisión.

Las organizaciones actualmente utilizan esta tecnología para satisfacer sus problemas de conectividad en lugares que no es fácil instalar redes de tipo cableada, pero además, son utilizadas para funciones mas especificas como vigilancia, telefonía móvil, etc.

En la Universidad Central de Venezuela, específicamente en el Edificio el Rectorado de la UCV, se encuentra implementada una WLAN, la cual está orientada únicamente a prestar servicios de señal inalámbrica a los usuarios que allí laboran. Por consiguiente, debido a los actos delictivos que se han presentado últimamente, sería beneficioso reforzar la WLAN y ampliarla hacia la Plaza Cubierta y el Complejo Cultural Aula Magna, para que una solución de videovigilancia inalámbrica en dichas zonas pueda obtener las mejores prestaciones.

Es por ello que este Trabajo Especial de Grado tiene como objetivo principal el diseño de una solución de videovigilancia soportada en cámaras IP con tecnología IEEE 802.11. Esto permite que se incrementen los niveles de vigilancia y de esta

manera tomar decisiones concretas para velar por la seguridad de la comunidad universitaria.

El diseño de la solución de videovigilancia con cámaras inalámbricas soportado en una WLAN, se baso en una serie de requerimientos que debían tomarse en cuenta para la especificación de la red, ya que fueron propuestos por la DTIC (Dirección de Tecnología de Información y Comunicaciones). A su vez, la Dirección de Seguridad presto su colaboración en la determinación de la ubicación de las cámaras, ya que este ente tiene como misión velar por la seguridad dentro del recinto de la Universidad Central de Venezuela, la preservación de las personas, bienes y custodia de su patrimonio.

Este documento de Trabajo Especial de Grado está estructurado de la siguiente manera:

- **Capítulo 1:** describe el problema plateado, la justificación al problema, así como una serie de objetivos a cumplir. Este capítulo finaliza con la metodología a utilizar para cumplir los objetivos y el alcance, que delimita el trabajo de investigación.

- **Capítulo 2:** está dedicado a describir las WLANs, su clasificación, principales aplicaciones, requerimientos, ventajas y tecnologías asociadas. Seguidamente se define el estándar IEEE 802.11, su arquitectura, servicios, entre otros. Así mismo, en este capítulo se presenta una síntesis de QoS y los mecanismos utilizados para el marcado de paquetes.

- **Capítulo 3:** se detalla la red de datos que actualmente conforma el Edificio el Rectorado y sus adyacencias (Sala Multimedia, Edificio de Telecomunicaciones, etc.), del mismo modo, en este capítulo se presenta la propuesta de diseño de la solución de videovigilancia basado en cámaras IP con la tecnología IEEE 802.11.

- **Capítulo 4:** presenta los diferentes escenarios de pruebas, igualmente se detallan las aplicaciones que se utilizaron para realizar las pruebas.

- **Capítulo 5:** finalmente se presentan las conclusiones, limitaciones encontradas y recomendaciones obtenidas a partir de este Trabajo Especial de Grado.

Capítulo 1

Planteamiento del problema

En este capítulo se platea el problema sobre el cual se desarrolla este Trabajo Especial de Grado, el cual lleva a un planteamiento de objetivos y seguidamente a una justificación para poder dar solución al problema. Finalmente se describe el alcance y la metodología que se seguirá para alcanzar los objetivos propuestos.

1.1 Planteamiento del problema

Las redes de área local inalámbricas (WLANs) fueron diseñadas como alternativa a las redes cableadas. La tecnología predominante de las WLANs se basa en el estándar IEEE 802.11 [21], la cual ofrece conectividad inalámbrica para estaciones fijas, portátiles y móviles dentro de un área local. Una WLAN soporta una gran cantidad de aplicaciones que hacen que dicha red sea compleja, tanto de diseñar, implantar, optimizar y operar para obtener el máximo rendimiento. Es por esto, que al momento de diseñar una red inalámbrica se deben tener en cuenta ciertos factores, tales como: los requerimientos para los cuales se va a diseñar la red, el alcance del diseño, la topología a utilizar, entre otros, para que de esta forma, el diseño de la red inalámbrica alcance las mejores prestaciones.

Las redes inalámbricas presentan ciertas ventajas frente a las redes cableadas, como son: movilidad, escalabilidad, flexibilidad y ventajas de instalación. La ventaja más importante es la flexibilidad, la cual permite cambios de topologías fácilmente y alcanzar sitios donde la tecnología cableada no podría instalarse [10].

Una de las aplicaciones donde la tecnología inalámbrica puede ser implementada, es en una solución de videovigilancia con cámaras IP basadas en la tecnología IEEE 802.11, y uno de los motivos por el cual esta solución de videovigilancia está siendo implementada por muchas organizaciones, viene dado por los crecientes problemas de inseguridad tanto pública, como privada.

Uno de los problemas a los que se enfrenta la UCV hoy en día, son los disturbios que vienen fuertemente marcados por las grandes diferencias políticas que existen dentro de la comunidad universitaria y el país. El principal foco de disturbios dentro de la UCV, es el Edificio el Rectorado y sus adyacencias (Plaza el Rectorado, Edificio del

FCU (Federación de Centros Universitarios)), el cual ha sido víctima de violentos ataques, ya que es en este lugar, donde los estudiantes quieren defender sus ideales, debido a que este edificio es el más importante de la Universidad, porque allí laboran la mayoría de las autoridades universitarias.

Debido a los incesantes problemas de inseguridad en la UCV, se han tomado diversas medidas para controlar estos hechos y garantizar la seguridad en el Campus Universitario. Dentro de estas medidas se encuentran: aumento de la cantidad de vigilantes en las áreas comunes de la UCV, un mayor control en todas las entradas, recuperación de las casetas de vigilancia y colocación de barras de seguridad, entre otras.

En la actualidad el Edificio el Rectorado cuenta con un conjunto de cámaras de circuito cerrado para incrementar la vigilancia en todas sus áreas y pasillos. Esta solución cumple con los mínimos requerimientos a nivel de seguridad, aunque no es la más eficiente, ya que implica una serie de costos adicionales asociados a la instalación de todas las cámaras, como el cableado, la reubicación y la incorporación de nuevos dispositivos. Por otra parte, la Plaza Cubierta y el Complejo Cultural Aula Magna, no poseen ninguna solución de videovigilancia, la cual es muy importante para monitorear constantemente todas sus áreas y de alguna manera brindar seguridad a la comunidad universitaria.

Los grandes avances en las tecnologías inalámbricas, la necesidad de monitorear los acontecimientos las 24 horas del día, la obligación de evitar daños y modificaciones en la estructura física del Edificio el Rectorado y la falta de una implementación de una solución de videovigilancia con cámaras IP inalámbricas basadas en la tecnología IEEE 802.11, dan la mezcla perfecta para la siguiente interrogante:

- ¿Es posible realizar una propuesta de diseño de una solución de videovigilancia soportado en cámaras IP con tecnología IEEE 802.11 para el Edificio el Rectorado, la Plaza Cubierta y el Complejo Cultural Aula Magna de la UCV?

1.2 Justificación del problema

Garantizar la seguridad de la comunidad universitaria es una necesidad. Actualmente la UCV es un foco principal de diversos ataques que ponen en riesgo tanto a estudiantes como a empleados, por esta razón, se realizará una propuesta de diseño de una solución de videovigilancia soportado en cámaras IP inalámbricas con tecnología IEEE 802.11, para incrementar el nivel de vigilancia y de esta manera, preservar las instalaciones y garantizar en amplia medida la integridad física de la comunidad universitaria.

El circuito cerrado que se encuentra implementado en el Edificio el Rectorado, presenta ciertas zonas sin cobertura (puntos ciegos), donde no es posible captar imágenes, ya que carecen de cámaras para realizar el monitoreo constante de estas zonas. La implementación de una nueva cámara al sistema de circuito cerrado que

actualmente dispone el Edificio el Rectorado implicaría un incremento en los costos relacionados al cableado, personal involucrado para la instalación, entre otras.

La implementación de una solución de videovigilancia con cámaras IP inalámbricas, propone eliminar los costos asociados a la implantación de un nuevo dispositivo cableado, ayudando a su vez a la conservación de las instalaciones de la UCV, la cual fue declarada Patrimonio Mundial, Cultural y Natural de la Humanidad por la UNESCO en el año 2000 [37].

Así mismo, una de las grandes ventajas que ofrece la solución de videovigilancia es la flexibilidad, ya que permite cambios de topología fácilmente, en el caso que nuevas zonas requieran ser monitoreadas.

En base a esto, la propuesta planteada sugiere la integración de los dispositivos implementados actualmente, como los APs (*Access Point*), con los nuevos dispositivos que se sugieren, para reforzar la WLAN ya existente en el Edificio. A su vez, la Plaza Cubierta y el Complejo Cultural Aula Magna, no poseen ningún tipo de solución de videovigilancia, lo que hace necesario la implementación de la misma, ya que al haber una vigilancia proactiva, permite tomar decisiones para mejorar la seguridad, garantizando la integridad de los estudiantes y del personal de la UCV.

1.3 Objetivos

1.3.1 Objetivo general

Diseñar una solución de videovigilancia soportada en cámaras IP con tecnología IEEE 802.11 para el Edificio el Rectorado, la Plaza Cubierta y el Complejo Cultural Aula Magna de la UCV, para incrementar la vigilancia y garantizar la integridad física de la comunidad universitaria.

1.3.2 Objetivos específicos

- Evaluar la situación actual de la red inalámbrica del Edificio el Rectorado, la Plaza Cubierta y del Complejo Cultural Aula Magna de la UCV.

- Evaluar el sistema de videovigilancia que actualmente se encuentra implementado en el Edificio el Rectorado de la UCV.

- Determinar que dispositivos inalámbricos se adaptan mejor a la solución de videovigilancia y a la WLAN, de acuerdo a las necesidades requeridas por la organización.

- Elaborar el diseño de la solución de videovigilancia y de la red inalámbrica.

- Realizar pruebas de calidad de servicio para garantizar la entrega segura de paquetes.

1.4 Metodología

La metodología a seguir para poder llevar a cabo los objetivos planteados en este Trabajo Especial de Grado se describe a continuación:

1.4.1 Estudio teórico

Es necesario realizar un profundo estudio del funcionamiento de las redes inalámbricas, así como también comprender los mecanismos de QoS que se pueden aplicar a estas redes basadas en la tecnología IEEE 802.11, y realizar una evaluación de los principales protocolos de compresión de video para comprender su funcionamiento y virtudes que posean.

1.4.2 Evaluación

Además de un estudio de la red inalámbrica que actualmente posee el Edificio el Rectorado, la Plaza Cubierta y el Complejo Cultural Aula Magna de la UCV, es importante conocer la ubicación actual de las cámaras del edificio, áreas de cobertura y puntos ciegos. Con respecto a la Plaza Cubierta y al Complejo Cultural Aula Magna es necesario conocer que áreas son las más críticas basándose en las recomendaciones de la Dirección de Seguridad de la UCV.

1.4.3 Diseño de la solución

Diseñar la red inalámbrica, donde su área de cobertura alcance los actuales puntos ciegos, para que al momento de implementar las cámaras IP de videovigilancia basadas en la tecnología IEEE 802.11, se tenga una cobertura total del Edificio el Rectorado, sus adyacencias y las áreas no cubiertas del Complejo Cultural Aula Magna de la UCV.

1.4.4 Selección de tecnologías a utilizar

La selección de las cámaras IP, así como de los APs necesarios para el diseño de la red, estarán únicamente basados en la tecnología del fabricante Cisco Systems como requerimiento de la DTIC de la UCV.

1.4.5 Pruebas

Se realizarán diversas pruebas para verificar el correcto funcionamiento del diseño de la red y el cumplimiento de todos sus requerimientos, como lo son cobertura de RF, marcado de paquetes para asignarle prioridad a los mismos, monitoreo de áreas específicas, entre otras.

1.5 Alcance

El diseño de la solución de videovigilancia soportado con cámaras IP con tecnología IEEE 802.11, se va a llevar a cabo en el Edificio el Rectorado, específicamente en los pasillos de planta baja y los pisos 1, 2 y 3, debido a que para tener acceso a las oficinas, se debe circular por el área de los ascensores y los pasillos, ya que estas son áreas comunes. De igual forma se extenderá el diseño a la Plaza Cubierta y el Complejo Cultural Aula Magna de la UCV. Así mismo, todos los dispositivos involucrados en el diseño serán del fabricante Cisco Systems.

Capítulo 2

Marco teórico

En este capítulo se describe el estándar 802.11, sobre el cual se basan las tecnologías inalámbricas, del mismo modo se detallan las aplicaciones, requerimientos y tecnologías de transmisión de las WLANs. Adicionalmente se aborda el tema de QoS (*Quality of Service*), específicamente el marcado de paquetes, para darle una atención eficiente a los mismos cuando circulan por la red.

2.1 Redes de área local inalámbricas

La fuerte necesidad que tenían los usuarios de una red que pudiera soportar la aparición de diversos dispositivos inalámbricos en el mercado, fue lo que impulso la rápida aparición de las WLANs, esta red es la que hace posible que los dispositivos inalámbricos puedan estar en contacto con otros dispositivos de la red, es decir, las WLANs le permiten al usuario movilidad y acceso simultáneo a la red.

Las primeras tecnologías WLANs (*Wireless Local Area Network*) ofrecían velocidades de transmisión de 1 a 2 Mbps [21], a pesar de esta limitación de ofrecer tasas de transmisión tan bajas, las tecnologías inalámbricas lograron ocupar un lugar importante en el mercado, ya que ofrecían a los usuarios libertad y flexibilidad de movimiento.

Las WLANs utilizan al igual que las LAN (*Local Area Network*) cableadas un medio de transmisión, pero en lugar de utilizar cable de par trenzado o de fibra óptica, las WLANs utilizan IR (*Infrared*) ó RF (*Radio frequency*) como medio de transmisión, donde la RF es más usada debido a su mayor alcance y mayor ancho de banda [10].

La RF se define como una tecnología usada para enlazar equipos conectados a una red, en lugar de usar los medios cableados convencionales [5]. Este tipo de tecnología surge por la necesidad de tener interconectividad dentro de espacios abiertos, en los que no se podía llegar con cables tan fácilmente. Por otro lado, la IR presenta ventajas, ya que soporta tasas de datos muy elevadas y los costos de implementación son bajos, pero por otra parte se tiene que, las distancias de transmisión son muy limitadas. Inicialmente esta tecnología de transmisión tuvo un gran auge, pero la poca

confiabilidad debido a la fácil obstrucción de la señal y el corto alcance que ofrecía, hicieron que estas redes tuvieran un uso muy limitado.

Comparada con el cable, la RF tiene las siguientes características [5]:

- El medio de propagación de la RF es el espacio libre, que a diferencia del cable no requiere una conexión directa para recibir la señal. Todo el que este en el espacio de cobertura de la RF y tenga un mecanismo receptor, puede recibir la señal y recibir las tramas de datos.

- A diferencia del cable, el cual tiene una cobertura aislante, la RF está expuesta a interferencias de otras señales de RF que funcionen en la misma área geográfica y a la misma frecuencia o similar.

- Cada país tiene su regulación para las bandas de RF. El espectro disponible para las comunicaciones inalámbricas se puede dividir en dos: las bandas con licencia, donde es necesario tener autorización del regulador para poder transmitir y las bandas no reguladas, donde sólo es necesario cumplir con un mínimo de requisitos para poder hacer uso de las frecuencias.

Las WLANs utilizan las bandas de frecuencia 2,4 y 5 GHz (*Gigahertz*), que son bandas de frecuencia libre, donde se desempeñan las redes inalámbricas y la mayoría de los equipos electrónicos con algún desempeño inalámbrico [10].

La Figura 2.1, tomada de [39], muestra la estructura y topología de una red de área local inalámbrica, a su vez muestra la conexión de los dispositivos a los AP a través de ondas de RF.

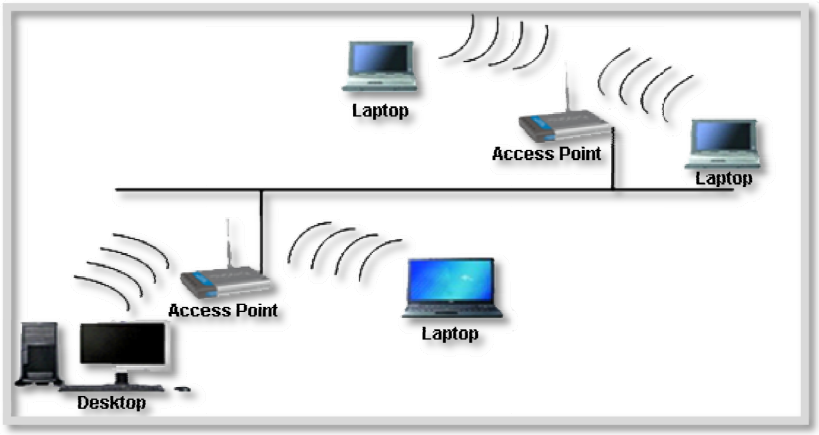


Figura 2.1: Red WLAN.

2.2 Clasificación de las redes de área local inalámbricas

Según el área de cobertura, las redes inalámbricas se pueden clasificar en [10]:

- **Redes de área personal inalámbricas (*Wireless Personal Area Networks, WPANs*):** alcanzan a cubrir solamente unos 10 metros. Estas redes son usadas para la conexión de dispositivos periféricos, tales como: impresoras, teléfonos móviles, electrodomésticos, PDA, etc.

- **Redes de área local inalámbricas (*Wireless Local Area Networks, WLANs*):** la cobertura de estas redes es de muy corto alcance, equivale a una cobertura no mayor a los 100 metros *indoor* y no mayor a los 300 metros *outdoor*, dependiendo de los obstáculos que se encuentren en la trayectoria de las ondas de RF.

- **Redes de área metropolitana inalámbricas (*Wireless Metropolitan Area Networks, WMANs*):** también conocidas como WLL (*Wireless Local Loop*). El área de cobertura de este tipo de redes va desde 4 a 10 Km. Un ejemplo de una WMAN, es una red WIMAX (*Worldwide Interoperability for Microwave Access*), basada en el estándar IEEE 802.16e, que puede alcanzar una velocidad aproximada de 70 Mbps.

- **Redes de área amplia inalámbricas (*Wireless Wide Area Networks, WWANs*):** este tipo de redes poseen la mayor área de cobertura, aunque poseen un ancho de banda más reducido. Generalmente las WWANs son propiedades de proveedores de servicios o de empresas de telecomunicaciones. Un ejemplo de estas redes, son las redes celulares de tercera y cuarta generación.

En la Figura 2.2, tomada de [38], se muestra la clasificación de las redes inalámbricas.

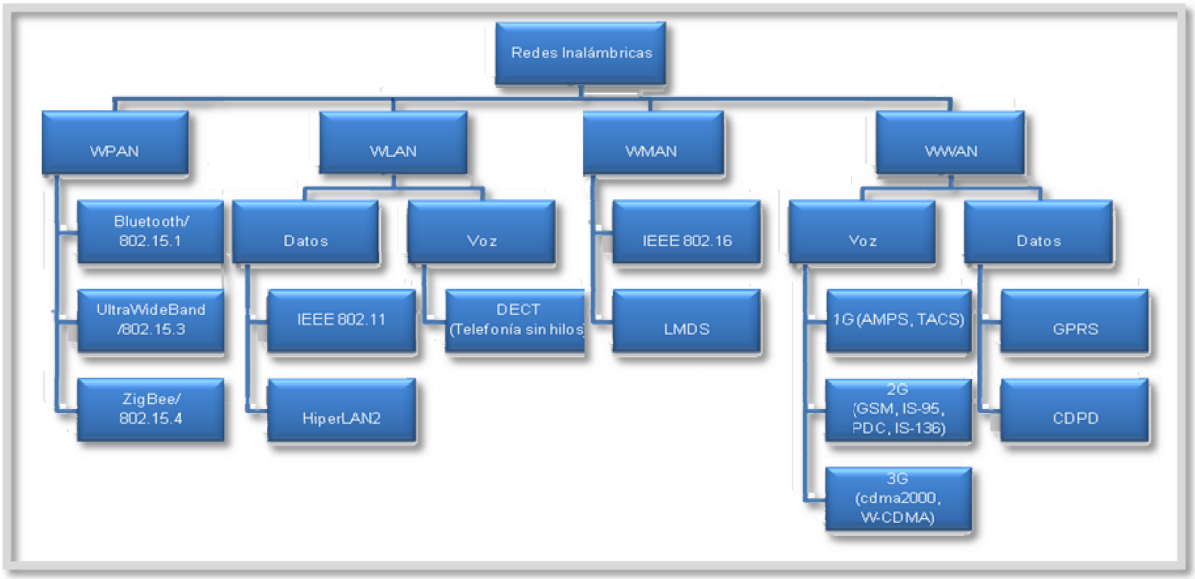


Figura 2.2: Clasificación de las redes inalámbricas.

Según su forma de conexión, las redes de área local inalámbricas están conformadas por dos topologías [10]:

- **Topología de infraestructura:** la topología de infraestructura permite la inserción de dispositivos inalámbricos controlados por un AP (*Access Point*). La función principal del AP, es coordinar la transmisión y la recepción de múltiples dispositivos inalámbricos en un área específica. Esta topología de infraestructura permite soportar varios APs, con la finalidad de cubrir un área más extensa. La Figura 2.3, tomada de [38], muestra un ejemplo de una red de infraestructura.

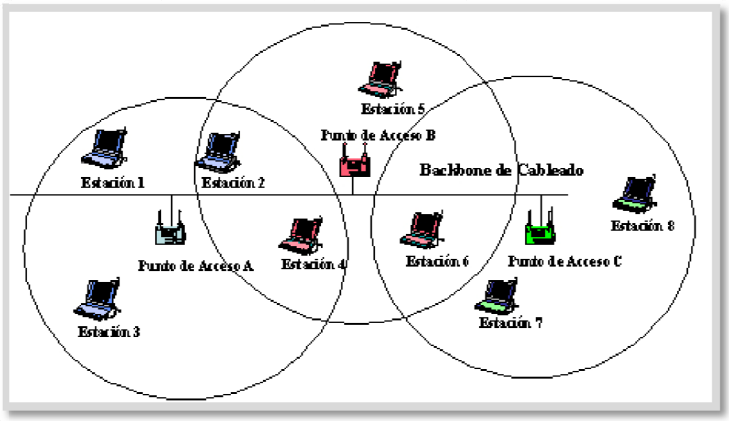


Figura 2.3: Red de infraestructura.

- **Topología Ad-hoc:** la topología Ad-hoc carece de APs o de un controlador central para establecer una conexión entre dispositivos inalámbricos, lo que permite crear una red LAN entre los mismos dispositivos. Este tipo de topología, es utilizada en pequeños espacios o áreas de tamaño reducido y cuando no se necesita acceso a otra red. La Figura 2.4, tomada de [38], muestra un ejemplo de una red Ad-hoc.

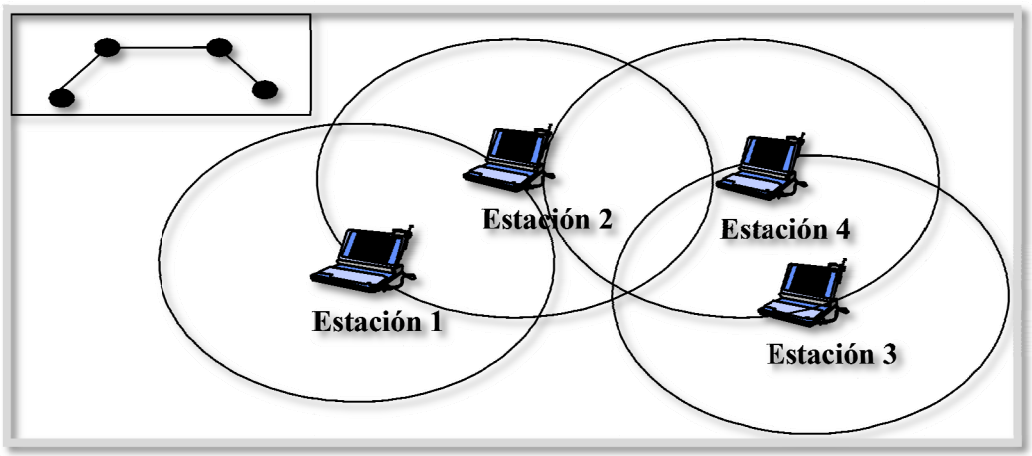


Figura 2.4: Red Ad-hoc.

2.3 Requerimientos de las redes de área local inalámbricas

Una WLAN debe cumplir los mismos requisitos de cualquier otra red LAN. Existe un conjunto de requerimientos específicos para entornos WLAN. Entre los más importantes se encuentran los siguientes [35]:

- **Rendimiento:** el protocolo de Control de Acceso al Medio, debería hacer un uso tan eficiente como fuera posible del medio inalámbrico para maximizar la capacidad.

- **Número de nodos:** una WLANs debe ser capaz de dar soporte a diferente número de nodos.

- **Conexión a la LAN troncal:** en la mayoría de los casos, es necesaria la interconexión con estaciones situadas en una LAN troncal cableada. Puede ser también necesario, dar soporte a usuarios móviles y redes inalámbricas Ad-hoc.

- **Área de servicio:** la zona de cobertura para una red WLAN tiene un diámetro no mayor a los 100 metros aproximadamente.

- **Consumo de energía:** las implementaciones típicas de WLAN poseen características propias para reducir el consumo de potencia mientras no se esté usando la red, como un modo de descanso. Por esta razón, el protocolo de Control de Acceso al Medio no requiere que los nodos móviles supervisen constantemente los puntos de acceso o realicen comunicaciones frecuentes con una estación base.

- **Robustez en la transmisión y seguridad:** una WLAN puede ser propensa a sufrir interferencias. El diseño de una WLAN debe permitir transmisiones fiables, incluso en entornos ruidosos y debe ofrecer seguridad.

- **Funcionamiento de redes adyacentes:** es probable que dos o más WLANs operen en la misma zona o en alguna en la que sea posible la interferencia entre ellas. Estas interferencias pueden repercutir negativamente en el funcionamiento normal del algoritmo MAC.

- **Funcionamiento sin licencia:** las WLANs no necesitan una licencia para la banda de frecuencias usada por la red.

- **Handoff/Roaming:** el protocolo de Control de Acceso al Medio usado en WLAN debería permitir a las estaciones móviles desplazarse de una celda[1] a otra.

- **Configuración dinámica:** se debe poder hacer la inserción, eliminación y traslado dinámico y automático de dispositivos sin afectar a otros usuarios.

1 Son usadas con el fin de cubrir diferentes áreas para proveer mejor radio de cobertura.

2.4 Características de las redes de área local inalámbricas

Algunas de las características más importantes de las WLANs se enumeran a continuación [10]:

- **Rendimiento:** una WLAN ofrece un rendimiento adecuado para las aplicaciones de oficina más comunes que trabajan en red.

- **Integridad:** las conexiones en una WLAN proveen un desempeño en la integridad de los datos, igual o mejor que en las redes cableadas.

- **Compatibilidad:** la mayoría de las WLANs proveen interconexiones estándares como Ethernet. Estas redes tratan a los nodos inalámbricos como cualquier otro componente de la red.

- **Facilidad de uso:** se simplifican muchos de los procesos de instalación y configuración, de esta manera la ausencia de cableado incide en reducir los costos.

2.5 Ventajas de las redes de área local inalámbricas

Las LAN Ethernet cableadas funcionan a velocidades superiores que la mayoría de las WLANs que operan entre 11 y 54 Mbps. Sin embargo, una razón para instalar una WLAN, es que en muchos entornos LAN pequeños las velocidades más bajas resultan adecuadas para soportar las necesidades de las aplicaciones y el usuario, lo que implica que se puede implementar una WLAN sin tener una deficiencia en las prestaciones de la comunicación entre los dispositivos [10].

Otra razón, es que durante las reconfiguraciones, las WLANs no requieren un recableado ni sus costos asociados. A continuación se presentan algunas de las ventajas proporcionadas por las WLANs [39]:

- **Movilidad:** acceso a una red en cualquier sitio donde se encuentra el usuario, sólo limitado por la cobertura de la misma.

- **Escalabilidad:** las configuraciones de la red pueden cambiarse fácilmente, ya que una red que inicialmente soportaba pocos usuarios puede extenderse, incorporando nuevos dispositivos de interconexión, sin necesidad de preocuparse por la instalación de cables.

- **Flexibilidad:** permite fácilmente cambios de topologías y alcanzar sitios donde la tecnología cableada no podría instalarse.

- **Ventajas de instalación:** eliminan la necesidad de cables a través de paredes y techos, así como también reducción del tiempo de instalación en aquellos sitios que requieran cambios de topologías frecuentes.

2.6 IEEE 802.11

El IEEE (*Institute of Electrical and Electronics Engineers*) es una asociación de profesionales con sede en EEUU, que fue fundada en 1884, y que actualmente cuenta con miembros de más de 140 países. Esta asociación investiga en campos como el aeroespacial, computacional, comunicaciones, y es un gran promotor de estándares [27].

IEEE 802.11 es un estándar de comunicaciones, oficialmente designado como *IEEE Standard for WLAN MAC and PHY Specifications*, que define la capa física y de enlace para una transmisión inalámbrica. El estándar original fue publicado por el IEEE en 1997 [27], y es conocido como IEEE 802.11-1997, dos años más tarde se actualizaría dando lugar al IEEE 802.11-1999. Este estándar, permitía unas velocidades de transferencia desde 1 hasta 2 Mbps, y trabajaba en la banda ISM a una frecuencia de 2,4 GHz, en la que no se precisa licencia [16]. Existen diferentes grupos de trabajo dentro del estándar IEEE 802.11, que trabajan en el desarrollo de subestándares del mismo.

En la Tabla 2.1, tomada de [35], se muestra el grupo de trabajo de IEEE 802.11.

Grupo de Trabajo	Características
IEEE 802.11	Estándar original con tasas de 1 y 2 Mbps trabajando a 2.4 GHz.
IEEE 802.11a	Tasas de hasta 54 Mbps en 5 GHz.
IEEE 802.11b	Mejoras sobre la norma 802.11 para tasas de hasta 11 Mbps.
IEEE 802.11d	Itinerancia internacional.
IEEE 802.11e	Mejoras para el soporte de calidad de servicio.
IEEE 802.11f	Comunicación entre puntos de acceso.
IEEE 802.11g	Tasas de hasta 54 Mbps en 2.4 GHz (compatible con 802.11b).
IEEE 802.11h	Trabaja en 5 GHz y propone extensiones para la compatibilidad con Europa.
IEEE 802.11i	Mejoras en seguridad.
IEEE 802.11j	Extensiones para Japón.
IEEE 802.11k	Medidas en los recursos radio.
IEEE 802.11n	Mejoras mayores en la tasa de transmisión.
IEEE 802.11p	Uso de 802.11 en vehículos.
IEEE 802.11r	Itinerancia rápida.
IEEE 802.11s	Redes GRID inalámbricas.

Tabla 2.1: Grupo de trabajo de IEEE 802.11.

2.6.1 Protocolos derivados de IEEE 802.11

Desde sus comienzos, el estándar IEEE 802.11 ha tenido una serie de evoluciones y modificaciones, de las cuales se han derivado varias especificaciones, que se explican a continuación [35]:

- **IEEE 802.11:** este protocolo proporciona una velocidad de transmisión de 1 a 2 Mbps utilizando el rango de frecuencia de 2,4 GHz, usando FHSS (*Frequency Hopping Spread Spectrum*) o DSSS (*Direct Sequence Spread Spectrum*).

- **IEEE 802.11a**: revisión del protocolo IEEE 802.11, que opera en la banda de frecuencia de 5 GHz y proporciona una velocidad máxima de 54 Mbps. IEEE 802.11a tiene 12 canales no solapados, 8 para redes inalámbricas y 4 para conexiones punto a punto. No puede interoperar con equipos del estándar IEEE 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

- **IEEE 802.11b**: también llamado IEEE 802.11 Wi-Fi[2] (*Wireless Fidelity*), es una revisión del protocolo IEEE 802.11 y utiliza CCK[3] (*Complementary Code Keying*) para llegar a velocidades de 5,5 y 11 Mbps en el rango de frecuencia 2.4 GHz usando DSSS.

- **IEEE 802.11c**: especifica métodos para conectar diferentes tipos de redes mediante redes inalámbricas.

- **IEEE 802.11d**: permite que distintos dispositivos intercambien información en rangos de frecuencia, según lo que se permite en el país de origen del dispositivo.

- **IEEE 802.11e**: define el uso de QoS (*Quality of Service*).

- **IEEE 802.11f**: utiliza el protocolo IAPP (*Inter Access Point Protocol*), que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento, sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como itinerancia.

- **IEEE 802.11g**: proporciona 54 Mbps en el rango de frecuencia 2,4 GHz, manteniendo la compatibilidad con el protocolo IEEE 802.11b. Puede trabajar con el protocolo IEEE 802.11a, cambiando la configuración del dispositivo.

- **IEEE 802.11h**: proporciona a las redes IEEE 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión.

2 Es un sistema de envío de datos sobre redes, que utiliza ondas de radio en lugar de cables.
3 Esquema de modulación usado por las WLANs.

- **IEEE 802.11i**: estándar que define el cifrado y la autentificación para complementar y mejorar el WEP (*Wired Equivalent Privacy*). Se implementa en WPA2 (*Wi-Fi Protected Access 2*).

- **IEEE 802.11n**: puede trabajar en dos bandas de frecuencias: 2,4 GHz y 5 GHz, y alcanzar una taza de transmisión de hasta 100 Mbps, a su vez hace uso de la tecnología MIMO[4] (*Multiple Input Múltiple Output*). Gracias a ello, IEEE 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi y permite alcanzar un mayor rendimiento. Así mismo, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada.

2.7 Arquitectura IEEE 802.11

La arquitectura del IEEE 802.11, está formada por una serie de elementos que interaccionan para proveer movilidad a las estaciones. El elemento básico de la arquitectura definido en el estándar, es la STA (*Station*), que puede ser cualquier elemento que contenga una capa MAC y una capa Física. Las estaciones pueden ser móviles, portátiles o estacionarias [21].

En la Figura 2.5, tomada de [21], se muestra la arquitectura IEEE 802.11.

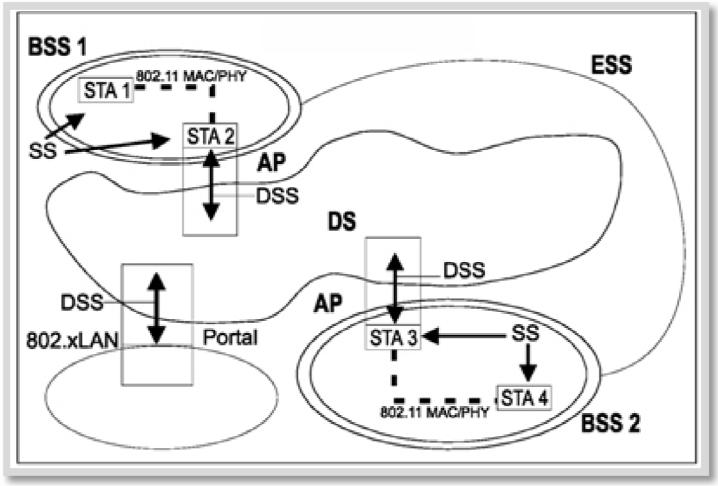


Figura 2.5: Arquitectura IEEE 802.11.

Los componentes de la arquitectura, que se pueden utilizar en una implantación WLAN son [21]:

- **BSS (*Basic Service Set*):** un conjunto de estaciones que han utilizado el servicio de asociación y se han sincronizado correctamente. La pertenencia a un BSS no implica que la comunicación inalámbrica con todos los demás miembros de la BSS sea posible.

4 Se refiere específicamente a la forma como son manejadas las ondas de transmisión y recepción en antenas para dispositivos inalámbricos.

- **DS (*Distribution System*):** sistema usado para interconectar un conjunto BSSs para crear un ESS (*Extended Service Set*). El DS puede ser una red cableada o inalámbrica, ya que el estándar especifica tal restricción.

- **IBSS (*Independent Basic Service Set*):** el BSS está formado por su propia red, y no tiene acceso a ningún DS. Como un IBSS consta de estaciones que están directamente conectadas, también recibe el nombre de red de igual a igual. Un IBSS puede tener un número aleatorio de miembros.

- **ESS (*Extended Service Set*):** el DS y el BSSs permiten crear una WLAN con un tamaño y complejidad como se quiera. IEEE 802.11 se refiere a estas redes como ESS. ESS es la unión de varios BSS conectados mediante un DS común.

- **Portal:** se usa para integrar una red 802.11 con una red 802.X. Un portal es el punto lógico donde se integra un red 802.11 con una red no IEEE 802.11.

2.8 Servicios IEEE 802.11

IEEE 802.11 ofrece 9 tipos de servicios, 5 a nivel de distribución, y 4 a nivel de estación, los cuales se definen a continuación:

2.8.1 Servicios a nivel de distribución

A nivel de distribución, IEEE 802.11 ofrece una serie de servicios, entre los cuales se encuentran [19]:

- **Asociación:** establece la asociación inicial entre una estación y un AP en un determinado BSS para que pueda haber comunicación.

- **Disociación:** elimina la asociación. En este punto, un AP o una estación, notifica que una asociación ha terminado.

- **Reasociación:** permite transferir una asociación existente de un AP a otro, permitiendo también que una estación se mueva de un BSS a otro.

- **Distribución:** permite el ingreso al DS, estableciendo la comunicación entre estaciones de diferentes BSS conectados al mismo DS.

- **Integración:** intercambio de información entre una red Wi-Fi y otras redes conectadas a ella.

2.8.2 Servicios a nivel de estación

Los siguientes servicios, los ofrece IEEE 802.11 a nivel de estación [19]:

- **Autenticación:** establece la identidad de las estaciones y autoriza la asociación. Previo a la asociación entre una estación y un AP, se requiere que la autenticación sea mutuamente aceptable y exitosa.

- **Desautenticación:** se utiliza cuando una autenticación existente debe terminarse. Es una notificación que no se puede rechazar.

- **Privacidad:** asegura la confidencialidad de los datos transmitidos, protegiendo la lectura del contenido de las tramas a quien no sea el destinatario previsto. El uso de encriptación es opcional.

- **Entrega de datos:** fragmenta y ensambla los paquetes de la subcapa LLC para su paso a la capa física.

2.9 IEEE 802.11 control de acceso al medio

El grupo de trabajo IEEE 802.11, considera dos tipos de propuesta para el algoritmo MAC: protocolo de acceso distribuido, el cual distribuye la decisión de transmitir sobre todos los nodos, usando el mecanismo de detección de portadora, éste protocolo tiene sentido para las redes Ad-hoc y también es efectivo para la configuración de otras WLANs. El uso de protocolos de acceso centralizado, es natural cuando se tienen un número de estaciones inalámbricas conectadas entre sí y con un tipo de estaciones base. Este protocolo es especialmente útil cuando los datos son de gran prioridad.

Todas las WLANs usan IEEE 802.11, para garantizar de alguna manera la entrega confiable de datos en la capa física y la capa MAC. El ruido, las interferencias y otros efectos de propagación, son el resultado de la perdida de grandes números de tramas. Esta situación puede ser tratada con mecanismos fiables, usados en capas superiores como TCP (*Transmission Control Protocol*), sin embargo, el tiempo usado para la retransmisión en las capas superiores es típicamente tratado en segundos. En la capa MAC se manejan dos tipos de funciones, la DCF (*Distributed Coordination Function*) y la PCF (*Point Coordination Function*) las cuales se explican a continuación [35]:

2.9.1 DCF (*Distributed Coordination Function*)

En esta función ningún dispositivo tiene prioridad. Si una estación quiere transmitir, escucha el medio, si el medio esta libre, la estación quizás transmita, de lo contrario la estación debe esperar a que el medio sea liberado para poder comenzar a transmitir y evitar una colisión. También, utiliza el mecanismo de CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*). Los paquetes enviados son confirmados mediante un ACK, en caso de no recibir la confirmación el paquete es reenviado [35]. Utilizando IFS (*Interframe Space*) las reglas de acceso CSMA/CA son las siguientes:

- Si la estación detecta inicialmente que el canal esta libre, espera un periodo de tiempo igual al SIFS (*Short Interframe Space*), si el canal luego de este tiempo continúa libre, la estación puede transmitir inmediatamente.

- Si el medio está ocupado, puede ser porque la estación inicialmente encontró el medio ocupado o porque durante el tiempo de espera SIFS otra estación comenzó a transmitir, en este caso la estación difiere la transmisión y continua escuchando el medio hasta que el mismo este libre.

- Una vez que la transmisión haya terminado, la estación espera otro tiempo SIFS. Si durante este periodo el medio continúa libre, la estación espera un periodo de tiempo denominado *backoff*[5] y de nuevo escucha el medio. Si el medio continua libre la estación puede transmitir. Si durante el tiempo *backoff*, el medio es ocupado por otra estación, dicho tiempo se detiene y se reanuda cuando el medio esta libre.

- Si la transmisión es fallida, la cual es determinada por la ausencia de un ACK, entonces se asume que ocurrió una colisión.

- Si se recibe el ACK, la estación que transmite sabe que la trama se ha recibido correctamente en la estación destino. Si la estación tiene otra trama que enviar, comienza el protocolo CSMA/CA en el paso dos. Si el ACK no se recibe, la estación que transmite entra en la fase *backoff* de nuevo en el paso dos, con el valor al azar elegido de un intervalo más grande [35].

En el diseño de una red, se puede presentar un problema conocido como el nodo oculto, el cual consiste en que una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo que no lo puede escuchar. Para solucionar este problema, se utiliza el protocolo RTS/CTS (*Request to Send/Clear to Send*), que consiste en: cuando la estación esta lista para transmitir, no envía la información sino un paquete de petición del medio RTS, si la estación receptora considera que el medio puede ser utilizado, envía un paquete concediéndole permiso CTS, adicionalmente informa al resto de las estaciones que el medio está siendo utilizado por un determinado lapso de tiempo, esto lo realiza NAV[6] (*Network Allocation Vector*). Cuando el nodo receptor recibe el paquete satisfactoriamente envía un ACK, lo cual da por concluido el intercambio de información [27].

En la Figura 2.6, tomada de [27], muestra un esquema de DCF.

5 Es un tiempo aleatorio exponencial.
6 Es un campo de la trama MAC y representa un timer que indica el tiempo de reserva del medio.

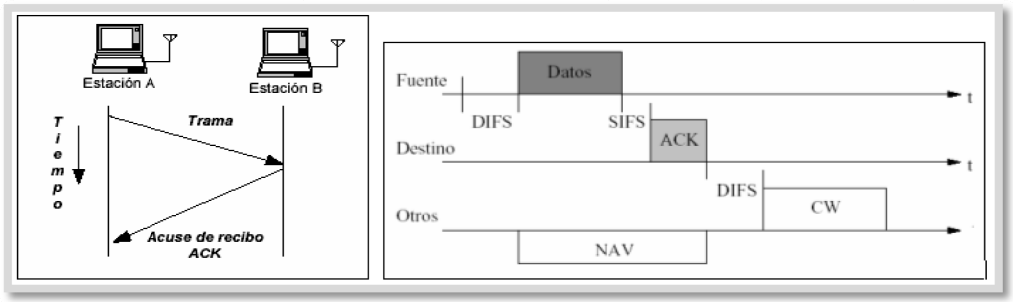


Figura 2.6: Función de coordinación distribuida.

2.9.2 Espaciado entre tramas

El intervalo de tiempo entre las tramas se denomina IFS. Durante este período mínimo, una estación estará escuchando el medio antes de transmitir. Cada intervalo IFS es definido como el tiempo entre el último bit de la trama anterior y el primer bit del preámbulo de la trama siguiente. Se definen diferentes IFS para proveer niveles de prioridad para el acceso al medio inalámbrico [19].

- **SIFS (*Short Interframe Space*):** SIFS es el intervalo más corto, se utiliza para permitir que las distintas partes de un diálogo transmitan primero. Esto incluye dejar que el receptor envíe un CTS para responder a un RTS, dejar que el receptor envíe un ACK para un fragmento o una trama con todos los datos y dejar que el emisor de una ráfaga de fragmentos transmita el siguiente fragmento sin tener que enviar un RTS nuevamente.

- **PIFS (*Point Coordination Function Interframe Space*):** el intervalo PIFS es utilizado únicamente para que estaciones que están operando como PCF (*Point Coordination Function*) obtengan prioridad en el acceso al medio al inicio de un período libre de colisiones y puedan transmitir inmediatamente después que han detectado que el medio está libre.

- **DIFS (*Distributed Coordination Function Interframe Space*):** es utilizado por estaciones que estén actuando como DCF para la transmisión de tramas de datos y de gestión, luego que hayan detectado mediante su mecanismo de portadora que el medio está libre.

- **EIFS (*Extended Interframe Space*):** es utilizado por una estación que ha detectado la recepción incorrecta o incompleta de una trama por medio del FCS (*Frame Check Sequence*), este intervalo de tiempo empieza luego que se detecta la trama incorrecta, el objetivo de este espaciado entre tramas es prevenir las colisiones de tramas pertenecientes a la misma comunicación.

2.9.3 PCF (*Point Coordination Function*)

En esta función las estaciones no compiten por el uso del medio inalámbrico, por lo tanto, las estaciones tienen prioridad para acceder al medio y están coordinadas por una función especial llamada PC (*Point Coordinator*). La PCF se limita a las redes que utilizan AP, los cuales aseguran que el medio sea asignado sin contienda y se utiliza en aplicaciones de tiempo real como voz y video, donde tiempos elevados de retardo no son tolerables [27].

Cuando se usa PCF, no funciona únicamente en el *contention-free period* (periodo libre de contención), el cual es controlado por DCF, sino que debe alternar entre *contention period* (periodo de contención), los cuales son controlados por PCF. El *contention period* debe ser lo suficientemente grande para permitir la transferencia de, al menos, una trama de tamaño máximo y su ACK correspondiente. La Figura 2.7, tomada de [21], muestra la transferencia de trama usando PCF.

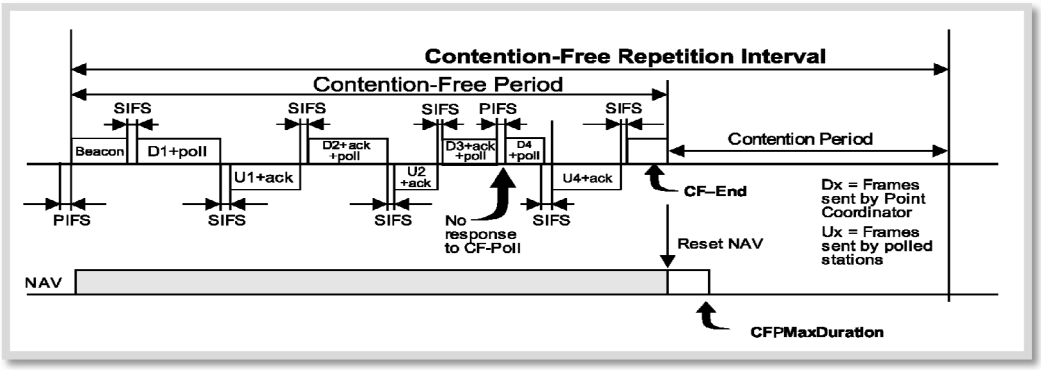


Figura 2.7: Transferencia de trama usando PCF.

Cada vez que el PC quiere comenzar un *contention-free period*, envía una trama *beacon*[7], estas tramas indican la máxima duración del periodo sin contenciones, además de toda la información que generalmente contienen. Todas las estaciones que la reciban, guardan en su vector NAV dicha duración y así se evita que accedan al medio las estaciones que trabajan con DCF. Esto es complementado con el espacio de tiempo entre tramas. Las tramas enviadas durante el *contention-free period* están separadas por SIFS y PIFS, ambos valores son menores que DIFS, que es el valor utilizado por las estaciones basadas en DCF, por lo que PCF tiene prioridad sobre DCF. El PC genera estos *beacons* en intervalos regulares de tiempo llamados TBTT (*Target Beacon Transmisión Time*), con lo cual cada estación sabe cuándo llegará el próximo beacon que iniciará el *contention-free period*. El valor del TBTT es anunciado en los *beacons* [28].

Durante el modo PCF, el PC va asignando el turno para transmitir a las estaciones que tienen datos para enviar. Una estación no puede transmitir hasta que es autorizado por el AP. Siguiendo una lista de estaciones, llamada *polling list*, el AP sabe que

7 Trama manejada por IEEE 802.11, contiene toda la información de la red. Es transmitida constantemente para anunciar la presencia de una WLAN.

estaciones debe consultar y habilitarlas para transmitir. La *polling list* se va llenando a medida que las estaciones se asocian al AP y solicitan que se las consulte [21] [28].

Utilizando un paquete CF-Poll, el AP le asigna el turno para transmitir a una estación de la lista. Para obtener el medio antes que cualquier otra, la estación consultada espera un tiempo SIFS para empezar a transmitir. Si durante un periodo SIFS, el AP no recibe nada de la estación que tiene el turno para transmitir, debe enviar el siguiente paquete después que pasó un tiempo PIFS desde el final de la última transmisión [28].

2.10 Trama MAC

El protocolo IEEE 802.11 establece que hay tres tipos de tramas MAC, las tramas son las siguientes [21]:

- **Trama de datos:** tienen un tamaño variable, en estas se depositan los datos que luego serán enviados por medio de los recursos de la capa física.

- **Trama de control:** esta trama se encarga de la entrega confiable de las tramas de datos. Los RTS, CTS, son ejemplos de tramas de control.

- **Trama de gestión:** las tramas de gestión, son usadas para manejar la comunicación entre las estaciones y los AP, también es usada para manejar los servicios, como por ejemplo las tramas *beacon*.

La Figura 2.8, tomada de [21], muestra el formato de la trama MAC.

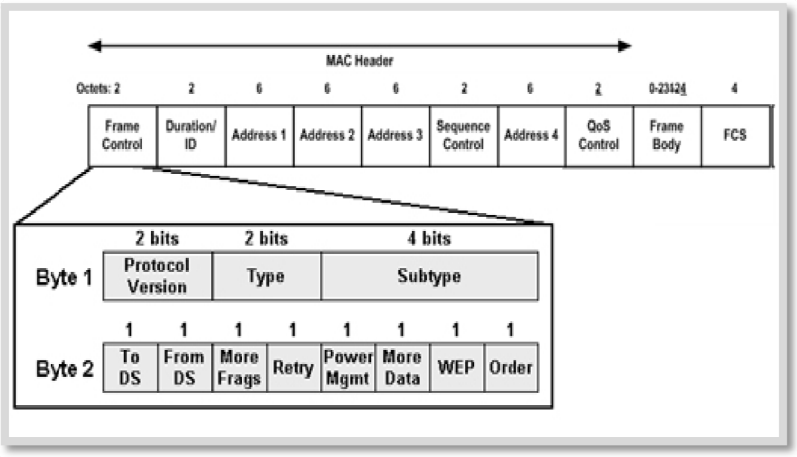


Figura 2.8: Formato de trama MAC IEEE 802.11.

El formato que se define a continuación es usado para todos los datos y control de tramas, pero no todos los campos son usados en todos los contextos, la Figura 2.8, tomada de [21], muestra el formato de la trama MAC. Los campos son los siguientes [21]:

- **Frame Control:** indica el tipo de trama y proporciona información de control. Las tramas pueden ser: tramas de datos, tramas de control y tramas de gestión.

- **Duration/Connection ID:** se utiliza como un campo de duración, indica el tiempo (en microsegundos) en que la trama estará haciendo uso del canal.

- **Addresses:** indica la dirección de origen, dirección de destino, dirección de la estación transmisora y dirección de la estación receptora. Trabaja con los campos To DS y From DS de la cabecera MAC.

- **Secuence Control:** indica el número de secuencia y el número de fragmento de la trama.

- **Frame Body:** contiene un MSDU (*MAC Service Data Unit*) o un fragmento de un MSDU. El MSDU es una unidad de dato del protocolo LLC o información de control MAC.

- **Frame Check Sequence**: se emplea para verificar la integridad del paquete mediante el algoritmo CRC-32, de esta forma se puede conocer si el paquete recibido ha sido alterado durante el proceso de transmisión.

El frame control de la trama contiene los siguientes campos [21]:

  - **Protocol Versión:** indica la versión del protocolo.
  - **Type:** indica si la trama es de control, de gestión o de datos.
  - **Subtype:** indica la función de la trama (RTS, ACK o CTS).
  - **To ds:** indica (valor = 1) si la trama está destinada al DS o no.
  - **From ds:** indica (valor = 1) si la trama fue enviada desde el DS.
  - **MF (More Fragments):** indica (valor = 1) si la información es fragmento de una MSDU.
  - **RT (Retry):** indica (valor = 1) si la trama es una retransmisión de la trama anterior.
  - **PM (Power Management):** indica el modo de administración de potencia del emisor. Tiene el valor de 0 si está en modo activo y el valor de 1 si está en modo de ahorro de energía.
  - **MD (More Data):** indica si el emisor tiene más datos para enviar.
  - **WEP:** indica (valor = 1) si la trama ha sido o no procesada con el algoritmo WEP.
  - **Order:** indica (valor = 1) si el servicio de entrega está en un orden estricto.

2.11 Calidad de servicio

Se define QoS o calidad de servicio, como la capacidad de una red para sostener un comportamiento adecuado del tráfico que transita por ella, cumpliendo a su vez con

los requerimientos de ciertos parámetros relevantes para el usuario final. Esto puede entenderse también, como el cumplimiento de un conjunto de requisitos estipulados en el contrato SLA[8] (*Service Level Agreement*) entre un proveedor de servicios de Internet y sus clientes [1].

La aplicación adecuada de calidad de servicio es para dar prioridad a los datos críticos, ya que se comparten simultáneamente los recursos de la red con otras aplicaciones. QoS hace un uso eficiente de los recursos de la red, ya que le da prioridad al tráfico utilizando diversos métodos de control y evasión de congestión. Uno de los grandes beneficios que ofrece la implementación de QoS, es una utilización del ancho de banda más eficiente.

El objetivo primordial de la QoS es brindar prioridad a los paquetes, incluyendo ancho de banda dedicado, variación de retardo (*jitter*) y latencia controladas, estos dos últimos parámetros son requeridos para tráfico en tiempo real o interactivo, es importante asegurar que al proveer prioridad para uno o más tipos de flujos, los otros flujos fallen.

QoS ofrece mejor servicio a ciertos flujos de paquetes, esto se logra incrementando la prioridad de un flujo o limitando la prioridad de otro flujo. Cuando se usan las herramientas de administración de congestionamiento, se trata de incrementar la prioridad, colocando en cola a todos los paquetes y asignando servicio en diferentes maneras. Esta herramienta de administración de filas de espera se usa para evitar congestión e incrementar la prioridad descartando los flujos de baja prioridad antes que los de alta prioridad. Las prioridades se definen por políticas.

2.11.1 Parámetros de calidad de servicio

Los parámetros de calidad de servicio son: retardo, ancho de banda, variación de retardo (*jitter*) y pérdida de paquetes, los cuales se explican a continuación [31]:

- **Retardo:** se refiere al retraso que sufren los flujos de datos hasta llegar a su destino. Un ejemplo de esto se puede observar en aplicaciones de video conferencia, donde se puede producir un retraso entre la señal de voz y la señal de video.

- **Ancho de banda:** es usado para determinar el límite en la cantidad de datos que pueden ser transferidos en un momento dado. Este parámetro se ve afectado por factores negativos, como lo es el retardo de la transmisión, que deteriora la calidad de la misma. El aumentar el ancho de banda implicaría poder transmitir más datos, pero también implicaría un incremento económico y en ocasiones, resulta imposible su aplicación sin cambiar de tecnología de red.

8 Contrato escrito entre un proveedor de servicio y su cliente, con objeto de fijar el nivel acordado para la calidad de dicho servicio.

- **Jitter:** también conocido como variación de retardo, indica una distorsión en el tiempo de llegada de los paquetes, en comparación con el tiempo de transmisión. Esta distorsión afecta de una manera considerable el tráfico multimedia. Por ejemplo, si un paquete tiene 100 milisegundos de latencia y el siguiente paquete tiene una latencia de 130 milisegundos, entonces el jitter es de 30 milisegundos.

- **Pérdida de paquetes:** se refiere a la cantidad de paquetes que se pierden durante la transmisión. Este parámetro se mide en porcentaje.

2.11.2 Clases de servicios

CoS (*Class of Service*) o clase de servicio, permite clasificar el tráfico que se considere crítico, para asegurar que fluya por la red, a pesar que haya en ese momento otras aplicaciones de menor importancia haciendo uso del ancho de banda disponible. Cada una de las aplicaciones, tendrá asociada una o más clases de servicio. Los tráficos de información generados que deben ser transmitidos por la aplicación, tendrán una prioridad asignada de acuerdo a la clase de servicio que vayan a utilizar.

A diferencia de la QoS este término no garantiza ancho de banda o latencia, pero permite a los administradores de red solicitar prioridad para el tráfico basándose en la importancia de éste [16].

2.11.3 Manejo de la congestión del tráfico

QoS es una forma de asignar recursos en los routers, para que los datos lleguen a su destino de forma rápida, consistente y segura, de acuerdo a las necesidades de cada aplicación. A medida que las aplicaciones demandan cada vez mayor ancho de banda y menor retardo y pérdida de paquetes, las capacidades QoS se están convirtiendo en una buena opción.

El manejo de la congestión, es usado para nombrar los distintos tipos de encolamiento que se usan para manejar situaciones donde la demanda solicitada excede el ancho de banda total de la red, controlando el tráfico a la red, para que ciertos paquetes tengan prioridad sobre otros, los diferentes tipos de manejo de la congestión del tráfico son [1]:

- **FIFO (*First* In *First Out*):** se basa en, el primer paquete en entrar a la interfaz, es el primero en salir.

- **WFQ (*Weighted Fair Queuing*):** se basa en proveer una justa asignación de ancho de banda para todo el tráfico de la red.

- **PQ (*Priority Queuing*):** se basa en un conjunto de colas clasificadas desde alta a baja prioridad. Cada paquete es asignado a una de estas colas, las cuales son servidas en estricto orden de prioridad.

- **CQ (*Custom Queuing*):** permite al administrador priorizar el tráfico sin los efectos laterales de inanición de las colas de baja prioridad, especificando el número de paquetes o bytes que deben ser atendidos para cada cola.

- **LLQ (*Low Latency Queueing*):** consta de colas de prioridad personalizadas, basadas en clases de tráfico, en conjunto con una cola de prioridad, la cual tiene preferencia absoluta sobre las otras colas.

2.11.4 Funcionamiento de QoS

Las redes están conformadas por dispositivos de red, estos dispositivos intercambian el tráfico entre ellos mediante interfaces. Si la velocidad en la que el tráfico llega a una interfaz es superior a la velocidad en la que otra interfaz puede enviar tráfico al siguiente dispositivo, se produce una congestión. Es aquí precisamente, donde los mecanismos de QoS funcionan al establecer preferencias en la asignación de este recurso a favor de cierto tráfico.

Para poder llevar a cabo la QoS, es necesario identificar los diferentes tráficos que pueden existir. Los tráficos que llegan a los dispositivos de red se separan en diferentes flujos mediante el proceso de clasificación de paquetes. El tráfico de cada flujo se envía a una cola en la interfaz de reenvío. Las colas de cada interfaz se gestionan de acuerdo con algunos algoritmos. El algoritmo de administración de cola determina la velocidad a la que se reenvía el tráfico de cada cola. De este modo, se determinan los recursos que se asignan a cada cola y a los flujos correspondientes [24]. La Tabla 2.2, tomada de [36], muestra la tabla de tareas usada por la política QoS. Para proporcionar QoS en redes, es necesario configurar y proporcionar a los dispositivos de red lo siguiente:

- Información de clasificación, por la que los dispositivos separan el tráfico en flujos.

- Colas y algoritmos de administración de cola, que controlan el tráfico de los diferentes flujos.

Tarea	Descripción
Diseñar la distribución de red.	Identificar los hosts y router de la red para proporcionar servicios diferenciados.
Definir las clases en las que los servicios de la red deben dividirse.	Examinar los tipos de servicios y acuerdos SLA que ofrece su organización.
Definir filtros para las clases.	Determinar el mejor modo de separar el tráfico de una clase específica del flujo de tráfico de la red.
Definir tasas de control de flujo para medir el tráfico cuando los paquetes salen del sistema IPQoS.	Determinar tasas de flujo aceptables para cada clase de tráfico.

Tarea	Descripción
Definir los puntos DSCP *(Differentiated Services Code Point)* o valores de prioridad de usuario que se deben utilizar en la política QoS.	Planificar un esquema para determinar el comportamiento de reenvío asignado a un flujo de tráfico cuando lo controla el router o nodo.
Si procede, definir un plan de supervisión de estadísticas para los flujos de tráfico de la red.	Evaluar las clases de tráfico para determinar qué flujos de tráfico deben supervisarse por cuestiones de recopilación de datos o estadísticas.

Tabla 2.2: Tabla de tareas de la política QoS (Mapa de Tareas).

2.12 IntServ (*Integrated Services*)

El modelo IntServ [3] propone una solución para el soporte de calidad de servicio extremo a extremo basado en la pre reserva de recursos en los diferentes equipos de conmutación que componen el trayecto que seguirá la información en la comunicación.

Con este modelo, se desea brindar soporte para un funcionamiento adecuado de aplicaciones con requisitos de tiempo real. Este modelo implica una mejora sobre el servicio tradicional de Internet, de forma que permite a las propias aplicaciones especificar los requisitos de calidad de servicio necesarios.

Esta lista de requisitos debe difundirse entre los diferentes elementos de conmutación (routers) por los que se encaminarán los paquetes de determinada aplicación. Estos equipos deben proporcionar mecanismos para el control de la calidad de servicio ofrecida a estos flujos de información, lo que se consigue mediante la reserva de recursos.

Este modelo se basa en la definición de dos elementos, una arquitectura donde los elementos de red permiten reservar recursos de conmutación, y un protocolo que permita a las aplicaciones transmitir sus requisitos a estos elementos de conmutación, se trata del protocolo RSVP (Resource Reservation Protocol) [4].

De esta manera cuando una aplicación desea comenzar una comunicación debe realizar una petición de recursos, esta petición atravesará todos los nodos que formen el trayecto para el flujo de información, y en función de los recursos disponibles será aceptada o rechazada.

2.13 DiffServ (*Differentiated Services*)

El RFC 2475 [2] define DiffServ como un protocolo de QoS, que ofrece la posibilidad de diferenciar clases de servicio marcando los paquetes IP, para que luego los routers los traten en base a esa marca, de tal forma que se da un tratamiento diferenciado a los paquetes. Cada tipo de clase corresponde a un tipo de QoS y el tráfico con el mismo tipo de clase se trata de la misma forma. Al definir los comportamientos específicos para cada clase de tráfico, se logra la diferenciación de servicios, lo que se

conoce como PHB (*Per Hop Behavior*). El PHB indica qué tratamiento han recibido los paquetes a lo largo de su transmisión, tales como: tipos de políticas, conformación de tráfico, posibles remarcados en el campo DS, encolamientos y gestión de tráfico. Dado que no se mantienen estados por flujo el PHB puede variar de salto en salto. Se han formulado dos estándares de PHB:

- **PHB de EF (*Expedited Forwarding*):** se refiere al nivel más alto de calidad. El PHB EF está orientado a dar servicio a flujos de tiempo real o rígido, que requieren ancho de banda asegurado, pocas pérdidas y bajos retardos por paquete, pues asegura que el tráfico no vea ninguna o poca cola en los buffer. PHB EF debe ser reservado para únicamente las aplicaciones más críticas, puesto que en situaciones de congestión de tráfico, no es factible tratar todo o gran parte del tráfico con alta prioridad. [23].

- **PHB de AF (*Assured* Forwarding):** se trata de un grupo de PHBs, entre los cuales es posible ofrecer niveles diferenciados de calidad relativa, por ejemplo, mediante prioridades de descarte. Los paquetes que lleven en el campo DS marcado con alguno de los niveles de *Assured Forwarding* tendrán prioridad de servicio más baja que los EF, pero su prioridad será más alta que la de los paquetes *Best-Effort*. [20].

  En PHB AF se definen cuatro clases de envío, permitiendo cuatro perfiles de tráfico diferentes. Dentro de cada clase, los paquetes son marcados por el cliente, o el proveedor de servicio, con uno de tres valores de prioridad de descarte. En caso de congestión, la prioridad de descarte de un paquete determina la importancia de ese paquete dentro de la clase de envío asegurado [34]. En la Figura 2.9, tomada de [34], se muestra el Codepoint para el PHB AF.

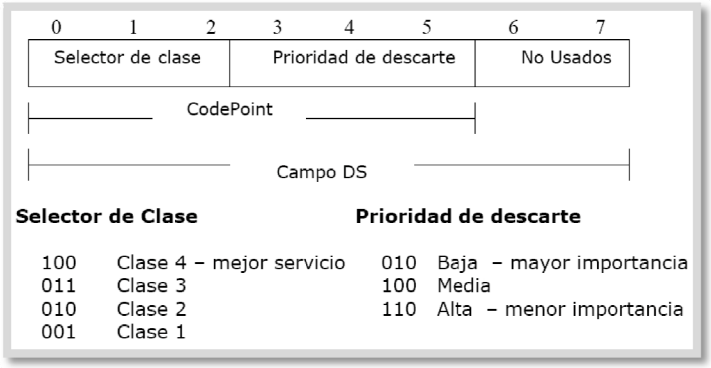


Figura 2.9: CodePoint para el PHB AF.

En la cabecera del paquete IP, se codifica un campo denominado DS (*Differentiated Services*) para especificar el grupo PHB al que pertenece dicho paquete y este valor determina el tratamiento que se le puede dar al paquete en cada router. Así mismo, el valor del campo DS permite tener paquetes con distinta prioridad dentro de un mismo PHB [2].

2.13.1 Clasificación del tráfico

Se utilizan procedimientos básicos de clasificación y asignación de prioridad para manejar los tráficos y otorgarles calidad de servicio, dichos procedimientos son denominados mapas de clase y mapas de política, los cuales se explican a continuación [1]:

- **Mapa de clase:** mecanismo para nombrar y aislar un flujo de tráfico específico. Éste define el criterio utilizado para comparar el tráfico para más tarde clasificarlo, el cual puede incluir selecciones mediante ACL[9] (*Acces Control List*) estándar o extendida, una lista especifica de DSCP[10], o valores de precedencia IP. Después que el paquete es confrontado al criterio del mapa de clase, es posible clasificarlo mediante el uso de mapas de política.

- **Mapa de política:** específica en qué clase de tráfico actuará. Las acciones pueden ser: confiar en los valores de CoS, DSCP o precedencia IP de la clase de tráfico, establecer un valor específico de éstos o especificar las limitaciones de ancho de banda y la acción a tomar, cuando el tráfico cae fuera del perfil definido en el mapa de política.

2.13.2 DS Field

Los paquetes son etiquetados para la especificación del servicio por medio del campo DS, el cual se sitúa en el campo de TOS (*Type of Service*) de una cabecera IPv4. La Figura 2.10, tomada de [25], muestra el campo DS en IPv4.

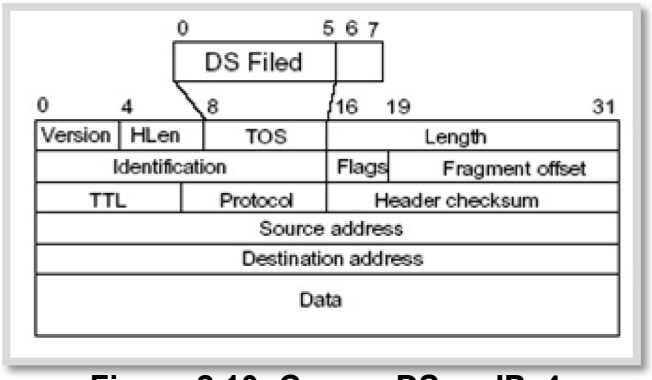


Figura 2.10: Campo DS en IPv4.

El RFC 2474 [25] define el campo DS con el siguiente formato: los 6 bits que están situados más a la izquierda forman un valor llamado DSCP (*CodePoint DS*) y los bits situados más a la derecha se quedan habitualmente sin usar. El DSCP es la etiqueta

9 Permiten controlar el flujo del tráfico en equipos de redes, tales como routers y switches. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.
10 Hace referencia al segundo byte en la cabecera de los paquetes IP, que se utiliza para diferenciar la calidad en la comunicación que quieren los datos que se transportan.

DS, que se emplea para clasificar paquetes para servicios diferenciados [2]. En la Figura 2.11, tomada de [34], se observa el campo DS.

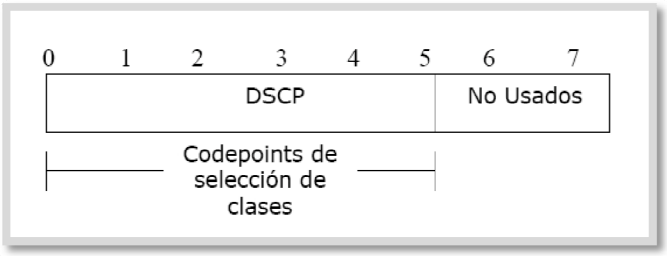


Figura 2.11: Campo DS.

Con un DSCP de 6 bits se pueden definir en principio 64 clases diferentes de tráfico, que se asignan considerando 3 conjuntos de DSCP, de la siguiente manera:

- DSCP de la forma xxxxx0, donde x puede ser 0 o 1, se reservan para su asignación como estándares.
- DSCP de la forma xxxx11, se reserva para uso local o experimental.
- DSCP de la forma xxxx01, se reservan para uso local o experimental, pero se pueden asignar para una acción de estándares futura.

El DSCP 000000 constituye la clase de paquete por defecto. La clase por defecto, es aquella que tiene el comportamiento de envío de mayor esfuerzo en los routers existentes. Tales paquetes, se transmiten en el orden en que se reciben, tan pronto como se dispone de la capacidad de enlace. Si otros paquetes de mayor prioridad están disponibles para su transmisión, se les da prioridad por delante de los paquetes de mayor esfuerzo.

Se reserva el DSCP de la forma xxx000 para proporcionar compatibilidad con versiones anteriores, utilizando así los bits del subcampo *IP Precedent*, del campo TOS de la cabecera IPv4. *IP Precedent* sirve como guía para la asignación de los recursos del router para sus datagramas.

En la Tabla 2.3, tomada de [16], muestra los valores estandarizados para DSCP.

DSCP	Descripción	DSCP	Descripción
111110	Reservado	011110	AF Clase 3 prioridad de descarte alta
111100	Reservado	011100	AF Clase 3 prioridad de descarte media

DSCP	Descripción	DSCP	Descripción
111010	Reservado	011010	AF Clase 3 prioridad de descarte baja
111000	Reservado	011000	Configurable por el usuario
110110	Reservado	010110	AF Clase 2 prioridad de descarte alta
110100	Reservado	010100	AF Clase 2 prioridad de descarte media
110010	Reservado	010010	AF Clase 2 prioridad de descarte baja
110000	Reservado	010000	Configurable por el usuario
101110	Expedited Forwarding	001110	AF Clase 1 prioridad de descarte alta
101100	Configurable por el usuario	001100	AF Clase 1 prioridad de descarte media
101010	Configurable por el usuario	001010	AF Clase 1 prioridad de descarte baja
101000	Configurable por el usuario	001000	Configurable por el usuario
100110	AF Clase 4 prioridad de descarte alta	000110	Configurable por el usuario
100100	AF Clase 4 prioridad de descarte media	000100	Configurable por el usuario
100010	AF Clase 4 prioridad de descarte baja	000010	Configurable por el usuario
100000	Configurable por el usuario	000000	Best Effort (default)

Tabla 2.3: Valores de DSCP.

2.13.3 Modelo de arquitectura de servicios diferenciados

En esta arquitectura se pueden diferenciar 2 tipos de routers, los cuales son: routers frontera DS de entrada y salida y routers internos, como se puede observar en la Figura 2.12, tomada de [18]. Este conjunto de routers, define el dominio DiffServ y presenta un

tipo de políticas y grupos de comportamiento por salto PHB, que determinarán el tratamiento de los paquetes en la red.

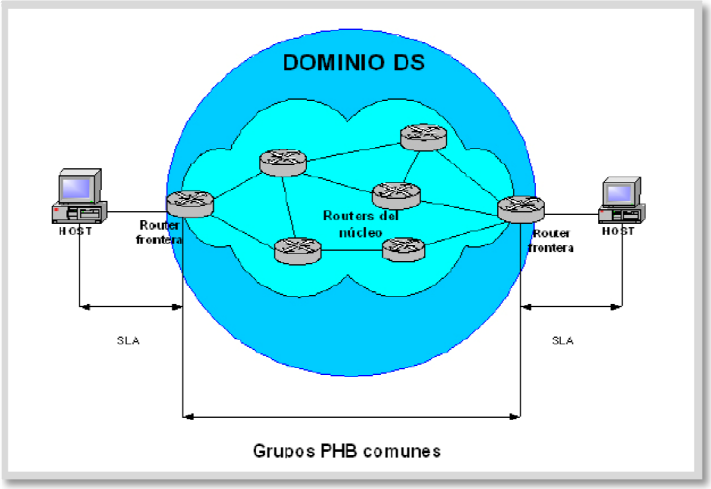


Figura 2.12: Arquitectura DiffServ.

A continuación se mencionan las funciones de los distintos tipos de routers [2]:

- **Routers frontera DS:** los nodos frontera realizan funciones complejas tales como, el acondicionamiento de tráfico entre los dominios DiffServ, que consisten en un conjunto de routers contiguos, donde es posible llegar desde cualquier router del dominio a cualquier otro router por una ruta que no tenga routers fuera del dominio, como se puede observar en la Figura 2.13, tomada de [18].

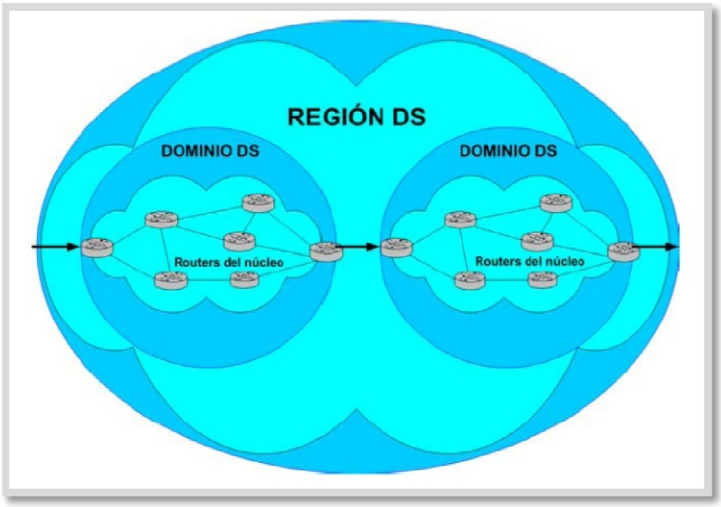


Figura 2.13: Dominios DS.

- **Routers internos DS:** los routers internos realizan funciones más simples que los nodos externos, tales como remarcado de DSCP. Estos nodos sólo se conectan a routers internos o routers frontera de su propio dominio. La selección

de PHB es realizada sólo analizando el contenido DSCP conocido como BA[11] (*Behavior Aggregate*).

En los routers frontera se incluyen mecanismos PHB, así como otros mecanismos de acondicionamiento de tráfico más sofisticados necesarios para proporcionar el servicio deseado. Así los routers internos tienen una funcionalidad mínima en la provisión de servicio DS, mientras que la mayor parte de la complejidad, se queda en los routers frontera. La función de los routers frontera también puede ser proporcionada por un sistema central adjunto al dominio, en representación de las aplicaciones que tenga ese sistema central. La función de acondicionamiento del tráfico consta de cinco elementos, los cuales se mencionan a continuación [34]:

- **Clasificador:** separa los paquetes enviados en clases diferentes.
- **Medidor:** realiza una medición del tráfico transmitido para ver si se ajusta a un perfil.
- **Marcador:** controla el tráfico volviendo a marcar los paquetes con un codepoint diferente según se vaya necesitando.
- **Conformador**: controla el tráfico retardando uno o todos los paquetes según sea necesario, de forma que el flujo de paquetes de una determinada clase no exceda la velocidad de transmisión especificada en el perfil de dicha clase.
- **Bloque de descarte de paquetes:** rechaza los paquetes cuando la tasa de transferencia de paquetes de una determinada clase exceda lo especificado en el perfil de dicha clase.

En la Figura 2.14, tomada de [33], se puede observar la relación que existe entre los elementos del acondicionamiento de tráfico.

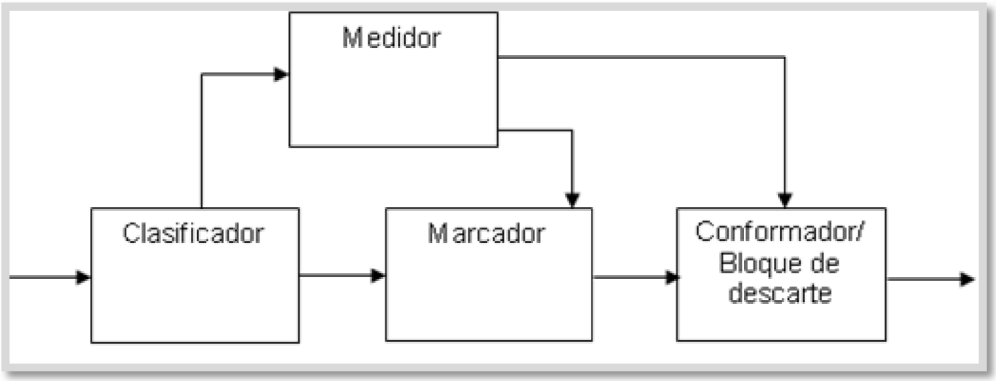


Figura 2.14: Acondicionador de tráfico DS.

11 Selecciona paquetes basándose exclusivamente en el campo DS.

2.14 IEEE 802.11e MAC - nivel de enlace

El estandar IEEE 802.11e define una nueva función de coordinación llamada HCF (*Hybrid Coordination Function*), la cual es usada por un conjunto de servicios básicos para dar soporte de calidad de servicio, QBSS (*Quality Basic Service Set*). La función HCF define dos modos de operación [22]:

- **EDCA (*Enhanced Distributed Channel Access*):** también conocida como acceso al canal distribuido mejorado, consiste en una función de acceso al canal basado en contienda, fue diseñada para soportar la priorización de tráficos, tal como hace Diffserv.

- **HCCA (*HCF Controlled Channel Access*):** conocida como acceso al canal controlado, es un mecanismo de sondeo controlado por el HC (*Hybrid Coordinator*) y a su vez soporta tráfico parametrizado, de la misma forma que Intserv. Este punto coordinador, se encuentra situado junto al QAP (*QoS Access Point*).

El concepto básico de estas funciones de acceso a canal es TXOP (*Transmision Opportunity*). Un TXOP es un intervalo de tiempo limitado, durante el cual una QSTA (*Quality of Service Station*) puede transmitir una serie de tramas. El periodo TXOP se define a través de un tiempo de inicio y una duración máxima. Si el periodo TXOP se obtiene usando el acceso a canal basado en contienda, entonces recibirá el nombre de EDCA-TXOP. Si por el contrario, se obtiene a través de HCCA se conocerá como HCCA-TXOP [22].

La duración del periodo EDCA-TXOP se controla a través del QAP y se transmite al resto de estaciones QSTA en las tramas *beacon* junto con otros parámetros relacionados con EDCA. La duración del periodo HCCA-TXOP se transmite a las estaciones QSTA directamente por el HC como parte de la trama QoS CF-Poll, la cual garantiza el periodo HCCA-TXOP [22]. La Figura 2.15, tomada de [16], muestra el esquema de funcionamiento HCF.

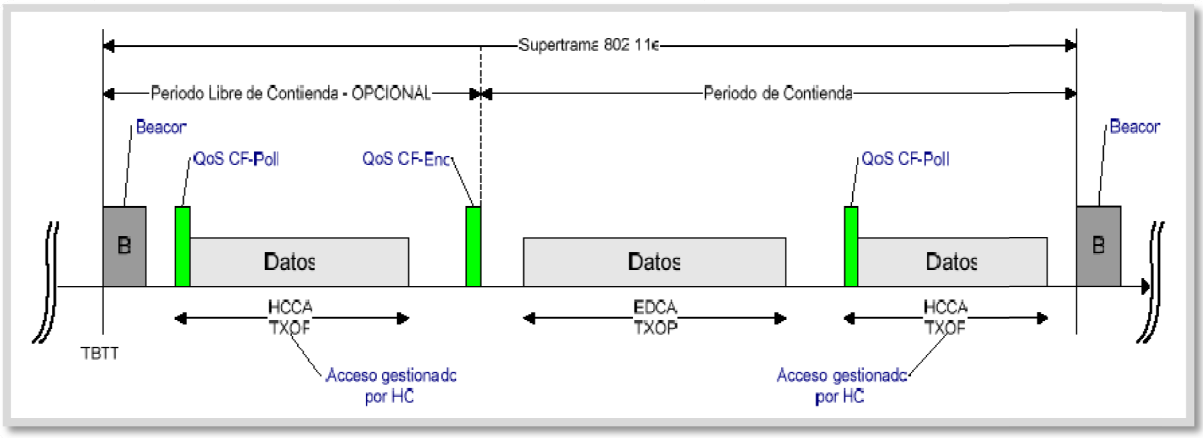


Figura 2.15: Esquema de funcionamiento HCCA.

El IEEE 802.11, obligaba el envío de tramas de confirmación para cada trama recibida correctamente. En IEEE 802.11e, estas tramas de confirmación han pasado a ser opcionales. De esta forma, cuando se utiliza una política basada en no utilizar confirmación, la capa MAC no deberá enviar mensajes ACK por cada trama recibida correctamente. Esto implica que la fiabilidad de este tráfico se vería reducida, pero mejora el rendimiento general de la capa MAC para tráfico sensible a retardo.

El trabajar sin tramas de confirmación trae consigo serios requisitos de tiempo real, ya que la siguiente trama a transmitir debe estar preparada en un tiempo SIFS desde el final de la anterior transmisión.

2.14.1 EDCA (*Enhanced Distributed Channel Access*)

El acceso distribuido en IEEE 802.11e se denomina EDCA. Es una extensión para mejorar el mecanismo de acceso DCF, el cual provee acceso con prioridad al medio inalámbrico. Forma parte del modo HCF, no es una función de coordinación separada. EDCA define un mecanismo de AC (*Access Category*), que provee soporte para las prioridades en las estaciones. Cada estación puede tener hasta cuatro AC para ocho UP (*User Priorities*). Una o más prioridades de usuario son asignadas a una categoría de acceso. Las estaciones acceden al medio basado en la categoría de acceso de la trama a ser transmitida [28].

Para que una AC, que tenga una mayor prioridad, es decir, que pueda conseguir acceso al medio con anterioridad a las demás ACs que tengan una menor prioridad, se le asigna un tiempo de *backoff* menor, lo que implica que la AC con mayor prioridad tenga que esperar menos tiempo.

Cada categoría de acceso dispone de su propia cola de transmisión, caracterizada por unos determinados parámetros. La priorización entre las diferentes categorías se consigue configurando adecuadamente los parámetros de cada cola de acceso. Los parámetros de mayor interés son los siguientes [16]:

- **AIFSN (*Arbitrary Inter-Frame Space Number*):** se corresponde con el intervalo mínimo desde que el medio físico se detecta como vacío hasta que se comienza la transmisión.

- **CW (*Contention Window*):** un número aleatorio se escoge en este rango para lanzar el mecanismo de espera *backoff*.

- **TXOP (*Transmission Oportunity*):** es la duración máxima durante la cual una QSTA puede transmitir tras haber obtenido el TXOP.

Con respecto al funcionamiento de EDCA, al llegar los datos al AP, es la capa MAC del 802.11e la que tiene la responsabilidad de clasificar correctamente los datos y envía la MSDU a la cola correspondiente. Luego, los bloques de información MSDU de las diferentes colas compiten internamente por el EDCA-TXOP.

El algoritmo de contienda interno calcula el tiempo de espera *backoff* para cada cola independientemente, según los parámetros: AIFSN, CW, y un número aleatorio. El mecanismo de espera es similar al de DCF, y la cola con el menor *backoff* ganará la competición interna [16].La cola vencedora competiría externamente por el acceso al medio inalámbrico. El algoritmo de contienda externo no se ha modificado significativamente comparado con DCF, excepto que en DCF el *backoff* y tiempos de espera eran fijos para un medio físico concreto, mientras que en IEEE 802.11e estos son variables, y se configuran adecuadamente según la cola correspondiente.

Mediante un ajuste adecuado de los parámetros de las colas, el rendimiento del tráfico de diferentes colas puede ser ajustado, y se puede lograr la priorización de tráfico. Esto requiere un punto de coordinación central, como un QAP para mantener un conjunto común de parámetros en las colas y garantizar así un acceso justo entre las diferentes estaciones que componen la red QBSS [16]. En la Figura 2.16, tomada de [16], se muestra el funcionamiento de EDCA.

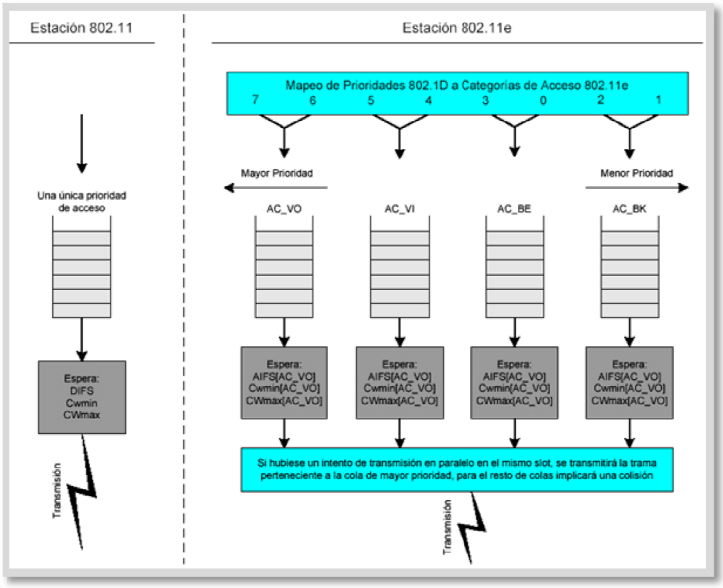


Figura 2.16: Funcionamiento de EDCA.

2.14.2 HCCA (*HCF Controlled Channel Access*)

HCCA suministra QoS basado en parametrización y el acceso al medio está basado en la escucha del medio inalámbrico. HCCA hace uso de algunas de las reglas empleadas por PCF e introduce algunas extensiones.

HCCA hace uso de la función HCF, este método hace uso de una funcionalidad provista por el HC que se encuentra ubicado en el AP. El concepto más destacado en HCCA es el CAP (*Controlled Access Phase*), que consiste en un intervalo de tiempo limitado formado por la concatenación de TXOPs-HCCA. En este caso, la clasificación y determinación de los CAP es responsabilidad del HC. El PC funciona en ambos periodos, tanto en el periodo de contienda como en el libre de contienda, esto no quiere

decir que para transferir datos con QoS utilice el periodo libre de contienda. Otra diferencia es que el HCF puede consultar a las estaciones que soportan QoS y otorgarles TXOPs.

El HC tiene el control del medio inalámbrico cuando necesita enviar una trama de datos o alguna trama en particular que soporte QoS. Para que esto pueda ser posible, el HC espera una cantidad de tiempo menor a la espera que tienen que realizar las otras estaciones usando EDCA entre cada transmisión.

Para evitar que una estación sin soporte QoS intente transmitir en un periodo libre de contenciones, el HC puede incluir el tiempo de duración del periodo de contención en las tramas *beacon*, para que la estación pueda establecer el valor del NAV y no intente transmitir mientras ese valor sea mayor a cero. Esto causa que la estación suponga que existe un PC en el BSS.

El HC debe escuchar el medio para comenzar un periodo libre de contienda, o un TXOP en el periodo de contienda, si el medio esta libre por un periodo de tiempo igual al PIFS, el HC transmitirá la primera trama de un conjunto de tramas que se intercambiarán, para así indicar la duración de TXOP o del periodo libre de contienda.

Este intervalo de tiempo recibe el nombre de CAP, y el medio esta bajo el control de HC, si pasa un tiempo PIFS desde el final del TXOP y el HC no reclama el medio, el CAP finaliza.

El HCF también puede operar como un punto de coordinación consultando a las estaciones que no tienen la capacidad de soportar QoS, para esto usa los formatos de tramas, secuencia de intercambio de tramas y todas las demás reglas especificadas para PCF [22].

El estándar IEEE 802.11e, introduce una serie de nuevos subtipos de tramas de control para el soporte de QoS. Para HCCA-TXOP la trama QoS CF-Poll se usa para garantizar el intervalo TXOP, y comienza la transferencia de datos usando tramas de datos QoS. Las tramas QoS-Null pueden ser utilizadas para terminar el periodo HCCA-TXOP si la estación no tiene datos que enviar. La gran variedad de tipos de tramas de control de QoS y las reglas de uso asociadas logran aumentar la eficiencia de la capa MAC 802.11e, aunque también aumenta la complejidad del clasificador HCCA [22] [28].

2.15 Estándares de compresión de video

Gracias a la evolución de los métodos matemáticos, los circuitos integrados digitales y las computadoras, se produjo la digitalización del video. Esto permitió una gran revolución en los métodos de compresión, convirtiéndose así, en un campo de investigación importante al final de los años 80s y principios de los 90s. Estos estudios permitieron la creación de una gran variedad de aplicaciones tales como: el almacenamiento de video en DVDs y CDs, la difusión del video sobre cable, satélite y televisión digital terrestre.

El surgimiento de diferentes tipos de tecnologías provenientes de distintos grupos de investigación, tiene como resultado que se generen una gran cantidad de productos que intentan resolver el mismo problema, pero que son totalmente incompatibles entre sí. Por ello surge la necesidad de la estandarización de tecnologías, para lo cual se han creado a través de los años diferentes organizaciones que se encargan de la investigación y estandarización de las mismas.

Lo que se busca con la compresión de video es minimizar y descartar los datos redundantes, para que de esta manera se pueda enviar y almacenar el archivo digital de una forma más eficiente. Así mismo, hace falta aplicar un algoritmo al video original para poder comprimirlo, transmitirlo o almacenarlo, mientras que para reproducir el video comprimido se aplica el algoritmo inverso.

Es importante para codificar y decodificar el video hacer uso de el mismo estándar de compresión, al comprimir un video con un estándar, no se puede realizar la descompresión del mismo con otro estándar diferente, ya que los estándares no son compatibles entre sí [17].

2.15.1 Serie H de compresión de video

La ITU (*International Telecom Union*) ha combinado una serie de estándares de codificación de audio, codificación de video, para crear un conjunto de estándares [26]. La Tabla 2.3, tomada de [29], muestra una lista de algunos de los estándares de la serie H, así como la aplicación para la cual fueron diseñados.

Serie	Aplicación
H.261	Estándar de la ITU para codificación de videoconferencia. 1990.
H.263	Codificación de video para comunicaciones con bajas de transferencia.
H.310	Sistemas y terminales de comunicación audiovisual de banda ancha.
H.320	Sistemas y equipo terminales de telefonía visual de escaso ancho de banda.
H.322	Sistemas y equipos de terminales de telefonía visual para redes de área local que provee una calidad de servicio garantizada.
H.323	Sistemas y equipos de terminales de telefonía visual para redes de área local que provee una calidad de servicio no garantizada.
H.324	Terminal para comunicaciones multimedia con tasas de transmisión bajas.
H.331	Tipos de transmisión de sistemas audiovisuales multipunto.

Tabla 2.4: Estándares de la serie H.

2.16 Estándar H.323

El estándar H.323 surgió con la finalidad de poder establecer comunicaciones de audio, video y datos, en tiempo real.

H.323 utiliza protocolos de transporte confiables, donde la transmisión es orientada

a la conexión, garantizando que los mensajes le llegan al receptor en secuencia y libre de errores, también utiliza protocolos de transporte no confiables donde la transmisión no es orientada a conexión y donde los paquetes pueden llegar fuera de secuencia, duplicados, o algunos de ellos se pueden perder. Las señales de control y los datos requieren de protocolos de transporte confiables como TCP, debido a que deben ser recibidos en el orden en que fueron enviados y no pueden sufrir pérdidas. Por otro lado, el video y la voz son muy sensibles a los retardos y no permiten el manejo de las retransmisiones para recuperar errores, por lo que para este tipo de información se utiliza protocolos de transporte no confiables como UDP.

Este estándar incluye RTP (*Real Time Protocol*). A través de dicho protocolo se le agrega a cada trama de información la identificación del tipo de información que contiene, el número de secuencia y la información de la hora en que fue generada. Esto permite que el receptor transmita la información al usuario al mismo ritmo en que esta fue generada y a su vez permite conocer si hubo descartes de información.

Otro protocolo que trabaja en conjunto con RTP, es el denominado RTCP (*RTP Control Protocol*). Dicho protocolo, se basa en la transmisión periódica a todos los participantes de una sesión, de paquetes de control, los cuales contienen información acerca de la calidad de la comunicación. Dado que mediante el uso de RTP, el receptor puede conocer los retardos, las variaciones de retardo y las pérdidas de información, que se están experimentando en la comunicación. Dicha información puede ser utilizada para que el receptor informe sobre la calidad del servicio que se está obteniendo.

H.323 es una especificación significativa, porque permite el desarrollo de una nueva generación de aplicaciones multimedia. Con la versión 2 de H.323, aprobada en febrero de 1998, se incluyen procedimientos para establecer la seguridad de las comunicaciones, tales como: identificación, integridad, confidencialidad y no negación de la participación de la conferencia [26].

2.16.1 Componentes H.323

El estándar H.323 especifica cuatro tipos de componentes, los cuales se explican a continuación [27]:

- **Terminales:** los terminales son utilizados para las comunicaciones multimedia bidireccionales en tiempo real. Un terminal H.323 puede ser un computador personal o un dispositivo stand-alone.

- **Gateways:** permite conectar una red H.323 con otra red no H.323. Sus dos funciones básicas son:

    - Traducir los distintos protocolos de establecimiento y fin de llamada empleados por las distintas redes.

- Realizar la conversión de formatos de audio/video.

- **Gatekeepers:** es un elemento opcional en la red, pero cuando está presente, es el punto central en la topología de una red H.323. Este dispositivo tiene las siguientes funciones:

  - Autenticación y control de admisión, para permitir o denegar el acceso de usuarios.

  - Proporciona servicios de control de llamada.

  - Servicio de traducción de direcciones, para usar nombres en lugar de direcciones IP.

  - Gestionar y controlar los recursos de la red: administración del ancho de banda.

  - Localizar los distintos Gateways y MCU's cuando se necesita.

- **MCUs (*Multipoint Control Units*):** permiten la conferencia entre tres terminales o más. Todos los participantes de una conferencia establecen una conexión con el MCU. El MCU maneja los recursos de la conferencia encargándose del procesamiento, mezcla, conmutación y distribución del audio y el video a los diferentes participantes de la conferencia. El MCU también realiza las negociaciones entre los terminales para determinar la codificación de audio y video a utilizar.

2.17 SIP (*Session Initiation Protocol*)

Es un protocolo de señalización para el establecimiento, mantenimiento y terminación de sesiones interactivas entre usuarios, estas sesiones pueden tratarse de conferencias multimedia, chat, sesiones de voz o distribución de contenidos multimedia. SIP no define por sí mismo un sistema de comunicaciones ni ofrece servicio alguno, es un protocolo flexible que se limita a ofrecer una serie de primitivas que las aplicaciones pueden utilizar para implementar servicios [30].

2.17.1 Componentes SIP

SIP define cinco componentes lógicos [30]:

- **Agente de usuario:** es una aplicación con arquitectura cliente/servidor, que se utiliza para iniciar y terminar las sesiones. UAC (*User Agent Client*) se encarga de realizar peticiones SIP, mientras que el UAS (*User Agent Server*) notifica al usuario cuando se recibe una petición y responde a dicha petición.

- **Servidor de redirecciones:** acepta una petición SIP y envía una respuesta al cliente que contiene las direcciones de los servidores con los que debe contactar el cliente.

- **Servidor proxy**: contiene funciones de servidor y cliente, actúa como un intermediario que realiza peticiones en nombre de otros clientes: para ello interpreta la cabecera del mensaje y la reescribe identificando al proxy como el que inicia la solicitud, recibe la respuesta del destinatario y se la reenvía al cliente.

- **Servidor de registro:** almacena o actualiza en una base de datos la información de contacto del usuario que realiza la petición.

- **Servidor de localización:** permite consultar la ubicación actual del usuario.

2.18 Diferencias entre H.323 y SIP

La principal diferencia es la velocidad, SIP hace en una sola transacción lo que H.323 hace en varios intercambios de mensajes. Adicionalmente, SIP usa UDP, mientras que H.323 debe usar necesariamente TCP para la señalización, lo que origina que una llamada SIP sea atendida más rápido [30]. La Tabla 2.4, tomada de [32], muestra las diferencias entre H.323 y SIP.

Descripción	SIP	H.323
Codificación	Textual	Binaria
Formatos	Tipos MIME-IANA	Series G.XXX y H.XXX, MPEG, GSM
Servidores	Proxy, redirect y registro	Gatekeeper
Autenticación	Análogo a http	H.235
Localización	DNS	Gatekeeper (puede usar DNS)
Transporte	TCP, UDP, SCTP, CDP, etc.	TCP, UDP
Cliente	User Agent	Terminal H.323
QoS	Delegada a otros protocolos	Soportada por el Gatekeeper
Complejidad	Tipo http	Uso de un conjunto de protocolos distintos

Tabla 2.5: Diferencias entre H.323 y SIP.

2.19 MJPEG (*Motion JPEG*)

MJPEG es un estándar de codificación de video proporcionado por JPEG (*Joint Photographic Experts Group*), el cual utiliza el estándar JPEG de compresión de imágenes fijas para codificar los cuadros individuales de una secuencia de video. La ausencia de compensación de movimiento en este estándar, permite que sea utilizado en la captura de video de alta calidad en tiempo real o en aplicaciones de edición, sin

embargo, la ausencia de compensación de movimiento, también provoca que el nivel de compresión no sea elevado, por lo que una vez que se ha capturado o editado el video en este formato generalmente se codifica en otros formatos tales como MPEG-1, MPEG-2 o MPEG-4 para su transmisión o almacenamiento [29].

2.20 MPEG-1 (*Moving Picture Experts Group 1*)

MPEG creó en 1992 el estándar MPEG-1, desarrollado con la finalidad de manejar video almacenado digitalmente a velocidades de hasta 1,5 Mbps. Este estándar se crea con funcionalidades adicionales requeridas para el acceso aleatorio de medios de almacenamiento digital [26].

El estándar define cuatro tipos de imágenes de acuerdo al tipo de compresión de las mismas [29]:

- **Imágenes codificadas intra (Imágenes I o *intraframe*):** son aquellas que para su codificación no requieren más información que la existente en ellas mismas.

- **Imágenes codificadas por predicción (Imágenes P o *predicted*):** son aquellas que se codifican mediante la predicción con una imagen anterior en el tiempo.

- **Imágenes codificadas bidireccionalmente (Imágenes B o *bidirectional-predicted*):** son aquellas que se codifican mediante la predicción con imágenes anteriores y/o posteriores en el tiempo.

- **Imágenes de DC (Imágenes D):** son un caso especial de las imágenes I, ya que se codifican con información sólo de ellas mismas, pero utilizan los coeficientes de DC de la DCT, por lo que su calidad es sumamente baja y son poco utilizadas.

2.21 MPEG-2 (*Moving Picture Experts Group 2*)

En 1994, se genera el estándar MPEG-2, creado para el manejo de servicios Broadcast, distribución de televisión por cable, servicios de televisión interactiva y para el manejo de HDTV (*High Definition Television,*). Este estándar es muy similar al MPEG-1, sin embargo utiliza refinamientos y funcionalidades adicionales.

La velocidad máxima de MPEG-2 es de 15 Mbps, pudiéndose transmitir un canal de televisión con una muy buena calidad a una velocidad entre 2 y 4 Mbps [26].

El estándar MPEG-1 fue diseñado para codificar y almacenar audio y video en medios con tasas de error muy bajas, por lo que el manejo de errores no es muy robusto. Por otro lado, el estándar MPEG-2 es más general e incluye una gran cantidad de aplicaciones, por lo que debe incluir una mayor flexibilidad a la existencia de errores.

El grupo MPEG inicio el desarrollo de un nuevo estándar bajo el nombre de MPEG-3, cuya aplicación principal sería la HDTV, sin embargo, se descubrió que el estándar MPEG-2 era lo suficientemente completo para abarcar esta aplicación, por lo cual se abandonó el desarrollo de MPEG-3, de tal manera que hoy en día las principales aplicaciones del estándar MPEG-2 se encuentran en la HDTV [29].

2.22 MPEG-4 (*Moving Picture Experts Group 4*)

El estándar MPEG-4 trata de hacer frente a los retos de las aplicaciones multimedia, tomando como base la rápida convergencia que se empieza a observar en la industria de las telecomunicaciones, la computación, industria del cine y la televisión. La idea del MPEG-4, es la de manejar la información multimedia, de manera tal que pueda ser transmitida y accesada de forma eficiente en ambientes de red heterogéneos y posiblemente bajo condiciones severas de error. También trata de manejar funcionalidades altamente interactivas que permitan presentar, manipular y almacenar la información de una manera altamente flexible.

Las velocidades que maneja el MPEG-4 son entre 5 y 64 Kbps para aplicaciones de video móviles o que utilizan la red telefónica, y de hasta 2 Mbps para aplicaciones de televisión y películas [26].

A diferencia de los estándares convencionales, el estándar MPEG-4 introduce una nueva forma de representar una escena basándose ahora en su contenido. La idea principal, es que una escena es vista como un conjunto de objetos de video, con propiedades intrínsecas, tales como forma, movimiento y textura. Esta representación basada en contenido permite el acceso arbitrario a objetos específicos de la escena así como su manipulación.

El estándar MPEG-4 permite comprimir video con tasas de transmisión por debajo de los 64 kbits/s, lo cual lo hace apropiado para su uso en videoconferencia o internet. La idea principal de dividir una imagen en objetos permite que sea una herramienta muy importante en la edición y producción de video [29].

Capítulo 3

Propuesta de la solución de videovigilancia

En este capítulo se presenta una breve introducción sobre la descripción de la red de datos y la red inalámbrica que se encuentra implementada en el Edificio el Rectorado, así como también contempla el diseño de la solución de videovigilancia con cámaras IP soportada en el diseño de una WLAN basándose en una serie de requerimientos propuestos por la organización y de igual forma detallando los componentes necesarios para la implementación de la red.

3.1 Descripción de la red de datos e inalámbrica

La Red Corporativa de Datos de la UCV está conformada principalmente por un backbone constituido de enlaces de fibra óptica monomodo que unen cuatro nodos principales utilizando switchs capa 3.

Los cuatro nodos principales que conforman el backbone son: el nodo Principal que se encuentra en el Edificio de Telecomunicaciones, el nodo de Ingeniería que se encuentra ubicado en el CPD (Centro de Procesamiento de Datos), el nodo de Ciencias el cual se ubica en el Centro de Computación y el nodo de Medicina que se encuentra en la escuela de Medicina Luis Razetti, los cuales se interconectan formando una estrella, siendo el nodo Principal el centro de la estrella. A su vez existen enlaces redundantes entre los nodos Ingeniería-Ciencias y entre Ciencias-Medicina.

La velocidad de transmisión en el backbone corporativo es de 10 Gbps, mientras que la velocidad de transmisión de los enlaces redundantes es de 1 Gbps.

En la Figura 3.1, tomada de [15], se puede observar un diagrama con los 4 nodos que conforman el backbone de la Red de Datos de la UCV.

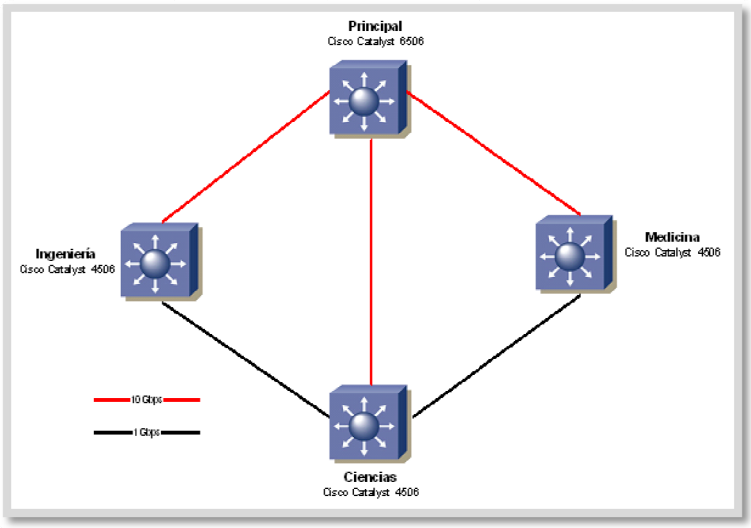


Figura 3.1: Red de datos de la UCV.

Los equipos que conforman el backbone corporativo son switchs, cada uno de estos equipos es a su vez el centro de una estrella, que permite interconectar a otros nodos correspondientes a otras dependencias, escuelas, facultades y edificios de la UCV. Uno de estos equipos es el nodo Rectorado, el cual se encuentra conectado directamente al nodo Principal de la UCV, mediante un enlace que ofrece una velocidad de transmisión de 1 Gbps, utilizando como medio físico fibra óptica monomodo.

En la Figura 3.2, tomada de [15], se muestra el nodo Rectorado conectado al nodo Principal de la UCV.

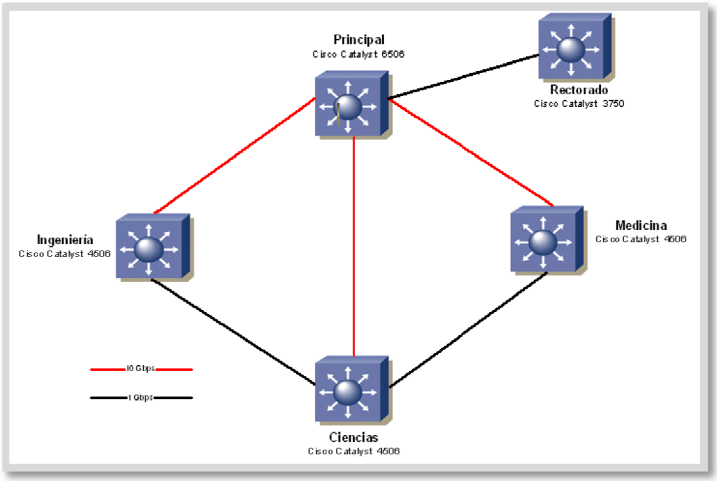


Figura 3.2: Nodo rectorado de la UCV.

Debido a que la propuesta de diseño abarca el Edificio el Rectorado, la Plaza Cubierta y el Complejo Cultural Aula Magna, se explicará por zonas específicas las redes que se relacionan o de las cuales depende el diseño.

3.2 Nodo rectorado

El nodo Rectorado es el punto central, del cual se deriva toda la red de datos y la red inalámbrica del Edificio el Rectorado. El detalle de cómo esta implementada esta red se explica a continuación:

3.2.1 Planta baja

En el Edificio el Rectorado los switchs se encuentran en un cuarto de cableado ubicado en la DTIC, en un área que cumple, según la DTIC, con los requerimientos necesarios para el correcto desempeño de todos estos equipos.

Así mismo, en la planta baja del Edificio el Rectorado se ubica el MDF (*Main Distribution Frame*), donde se encuentra el nodo Rectorado, el cual es un switch Cisco Catalyst WS-3750, con capacidad de enrutamiento y una velocidad de transmisión de 1 Gbps, este switch es el Principal del Edificio y brinda conexión a todos los pisos con una topología en estrella, que está conectada a la DTIC que a su vez tiene cuatro switchs Cisco Catalyst WS-2960G, conectados por cable UTP categoría 5e, a una velocidad de transmisión de 1 Gbps. Igualmente al switch Principal del Edificio, se conecta a través de cable UTP categoría 5e, la oficina de Grado, que tiene 2 switchs Cisco Catalyst WS-2950 conectados en cascada entre si y cada uno posee 2 puertos GigabitEthernet de fibra óptica y 24 puertos UTP FastEthernet. Estos switchs tienen una velocidad de transmisión de 100 Mbps.

En planta baja se encuentran 4 APs modelo Cisco Aironet 1131, de los cuales 3 se encuentran conectados a los switchs de la DTIC y uno de estos se conecta directamente al Principal del Edificio, uno de estos AP se ubica en el Edificio de Telecomunicaciones. Con estos 4 APs, se logra dar una buena y amplia cobertura de señal inalámbrica a toda el área que corresponde a la planta baja del Edificio el Rectorado, así como también a sus áreas adyacentes como lo son: oficina de Grado y las cercanías al Edificio de Telecomunicaciones. En la Figura 3.3, tomada de [15], se muestra un diagrama de los elementos que conforman la red de planta baja del Edificio el Rectorado.

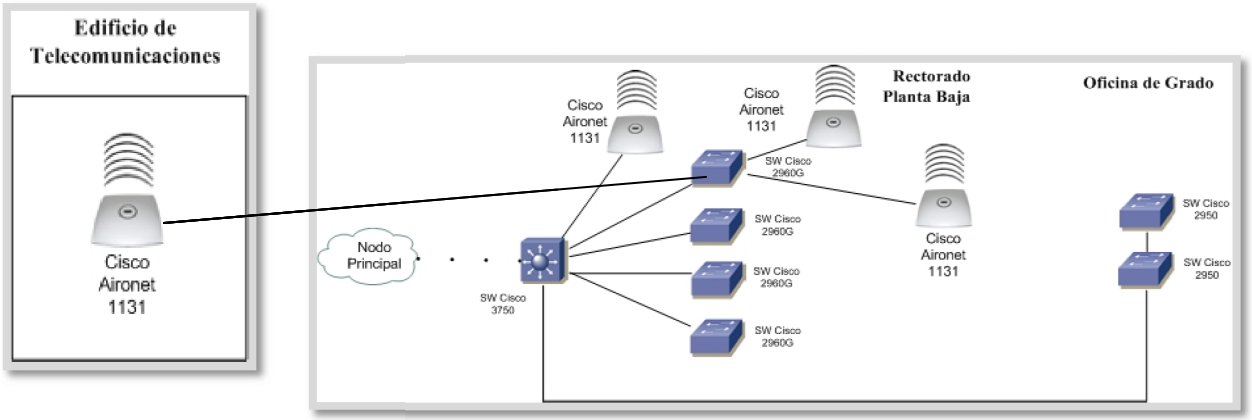


Figura 3.3: Planta baja.

3.2.2 Primer piso

El cuarto de cableado del piso está conformado por 3 switchs Cisco Catalyst WS-3750G apilados, cada uno con 4 puertos GigabitEthernet de fibra óptica y 24 puertos UTP GigabitEthernet. A su vez, los switchs se encuentran conectados por fibra óptica multimodo al switch Principal del Edificio, a una velocidad de 1Gbps. Estos switchs se encuentran en un cuarto de cableado ubicado justo detrás de los ascensores, específicamente al lado de la oficina de secretaria del Rectorado.

En este piso, se cuenta con 2 APs modelo Cisco Aironet 1131, ubicados en los extremos del pasillo, específicamente uno en el Consejo Universitario y el otro en el Despacho del Rectorado, los cuales dan cobertura de señal inalámbrica a todo el piso, menos al área de los ascensores que se encuentra en la zona central del edificio.

En la Figura 3.4, tomada de [15], se muestra un diagrama de los elementos que conforman la red del primer piso del Edificio el Rectorado.

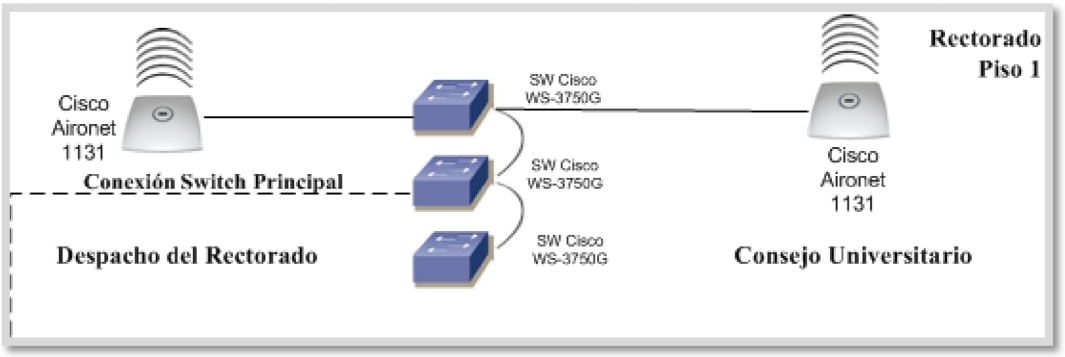


Figura 3.4: Primer piso.

3.2.3 Segundo piso

Este piso tiene un cuarto de cableado ubicado en el Vicerrectorado Administrativo que cuenta con 4 switchs Cisco Catalyst WS-2950, conectados entre sí con una topología estrella, mediante cable UTP categoría 5e, donde el switch central de esta topología, es el que se conecta con el switch Principal del Edificio de planta baja, mediante fibra óptica multimodo a una velocidad de 1Gbps. Cada uno de los switchs están conformados por 2 puertos GigabitEthernet de fibra óptica y 24 puertos UTP FastEthernet.

Este piso dispone de 2 APs modelo Cisco Aironet 1131, donde uno de ellos se ubica en el Vicerrectorado Académico y el otro en el Vicerrectorado Administrativo, los cuales dan cobertura de señal inalámbrica en todo el piso, pero al igual que en el piso 1, el área de los ascensores no posee señal inalámbrica.

En la Figura 3.5, tomada de [15], se muestra un diagrama de los elementos que conforman la red del segundo piso del Edificio el Rectorado.

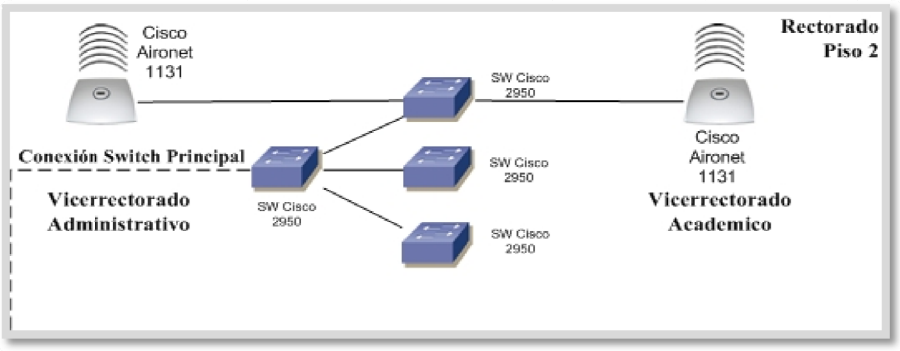


Figura 3.5: Segundo piso.

3.2.4 Tercer piso

Este piso tiene 2 cuartos de cableado, el cuarto de cableado principal tiene 3 switchs Cisco Catalyst WS-3750G con 4 puertos GigabitEthernet de fibra óptica y 24 puertos UTP GigabitEthernet, los cuales se encuentran apilados y se conectan al switch Principal del Edificio mediante un enlace de fibra óptica multimodo a una velocidad de 1Gbps. Este cuarto de cableado se encuentra en las oficinas de Compensación y Desarrollo. A este grupo de switchs se conecta un AP modelo Cisco Aironet 1131.

El otro cuarto de cableado consta de 2 switchs Cisco Catalyst WS-3750G apilados y un tercer switch Catalyst 2950 con 2 puertos GigabitEthernet de fibra óptica y 24 puertos UTP FastEthernet, el cual está conectado en cascada a los switchs WS-3750G. Este cuarto de cableado, se conecta al cuarto de cableado principal de este piso mediante un enlace de fibra óptica multimodo, a una velocidad de 1Gbps. Este conjunto de switchs se encuentran ubicados en la Dirección de Recursos Humanos y al igual que los demás grupos de switchs, están en un cuarto que cumple, según la DTIC, con las especificaciones necesarias para un buen desempeño de los equipos.

El área de cobertura en este piso por parte del AP es un poco más limitada, ya que, solo cuenta con un solo AP y por lo tanto, solo se da cobertura de señal inalámbrica a la mitad del pasillo del piso 3.

En la Figura 3.6, tomada de [15], se muestra un diagrama de los elementos que conforman la red del tercer piso del Edificio el Rectorado.

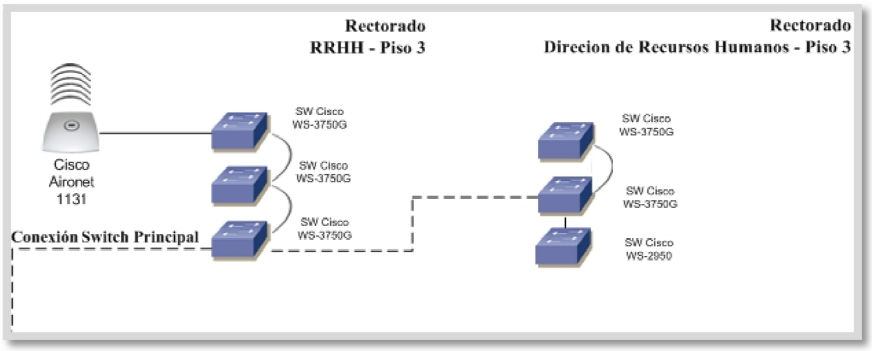


Figura 3.6: Tercer piso.

A continuación se muestra la Figura 3.7, tomada de [15], donde se puede observar como es la estructura completa de la red que se encuentra implementada en el Edificio el Rectorado y el Edificio de Telecomunicaciones.

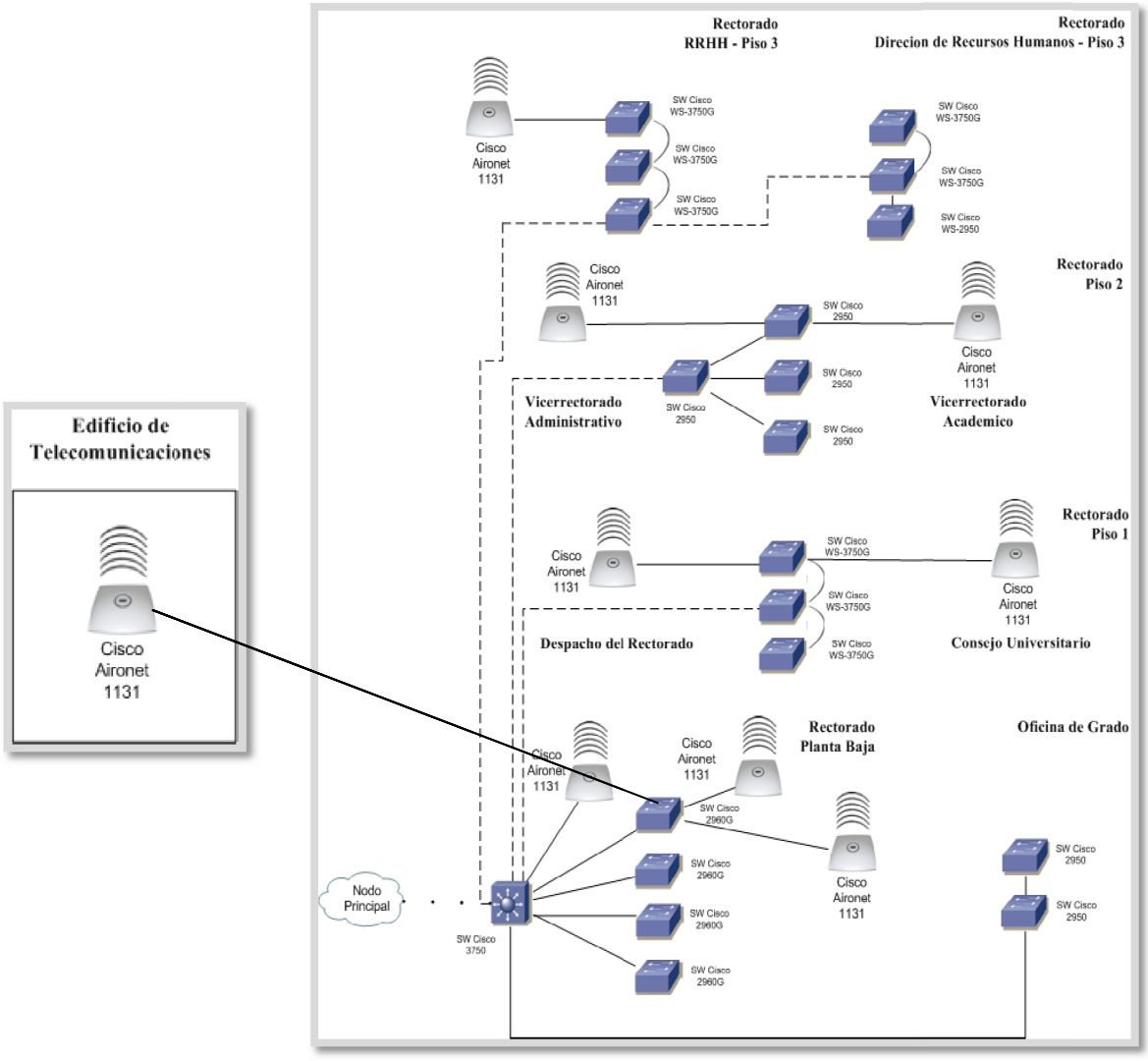


Figura 3.7: Diagrama de datos de la DTIC.

3.3 Complejo Cultural Aula Magna

Con relación al Complejo Cultural Aula Magna, es necesario mencionar que dispone de 4 cuartos de cableado, que permiten que las oficinas que conforman el Complejo Cultural Aula Magna se conecten a la red corporativa de la UCV, dichas entidades son las siguientes: El Edificio de la Biblioteca, Sala Multimedia, Sala C, Teatro el Chichón y la DIC (Dirección de Información y Comunicaciones).

A continuación se describen los elementos de red que podrían dar soporte a la conexión de diversos dispositivos inalámbricos en el Complejo Cultural Aula Magna:

3.3.1 Edificio de la biblioteca

Cuenta con un switch Cisco Catalyst WS-3750, conectado al nodo Principal mediante fibra óptica monomodo, a una velocidad de 1Gbps. Este switch está conformado por 12 puertos GigabitEthernet de fibra óptica.

3.3.2 Oficina de multimedia

Ubicada en el mezanina del Edificio de la Biblioteca, cuenta con un switch Cisco Catalyst WS-2960, conectado al switch del Edificio de la Biblioteca, mediante fibra óptica multimodo, a una velocidad de 1Gbps. Este switch cuenta con 24 puertos UTP FastEthernet y 2 puertos GigabitEthernet de fibra óptica. A esta sala Multimedia se encuentra conectada la sala C, la cual se describe a continuación:

- **Sala C:** cuenta con un switch Cisco Catalyst WS-2960, conectado al switch de oficina de Multimedia mediante cable UTP categoría 5e, a una velocidad de transmisión de 100 Mbps. Este switch cuenta con 24 puertos UTP FastEthernet y 2 puertos GigabitEthernet de fibra óptica.

  Así mismo, se encuentran 2 APs modelo Cisco Aironet 1131, los cuales dan cobertura de señal inalámbrica a toda la Sala C, oficina de Multimedia y parte de la planta baja del Edificio de la Biblioteca.

3.3.3 Teatro el chichón

Aquí se encuentra un switch Cisco Catalyst WS-2950, conectado al nodo principal mediante cable UTP categoría 5, con una velocidad de transmisión de 100 Mbps, con 24 puertos UTP FastEthernet y 2 puertos GigabitEthernet de fibra óptica. A la red del teatro el Chichón se conecta la DIC la cual se describe a continuación:

- **Dirección de Información y Comunicaciones (DIC):** dispone de 2 switchs Cisco Catalyst WS-2960, conectado al switch del Teatro el Chichón, mediante cable UTP categoría 5e, a una velocidad de un 1 Gbps. Este switch cuenta con 24 puertos UTP FastEthernet y 2 puertos UTP GigabitEthernet.

Seguidamente se observa la Figura 3.8, tomada de [15], donde se puede apreciar esquemáticamente como es la estructura de la red que se encuentra implementada en el Complejo Cultural Aula Magna.

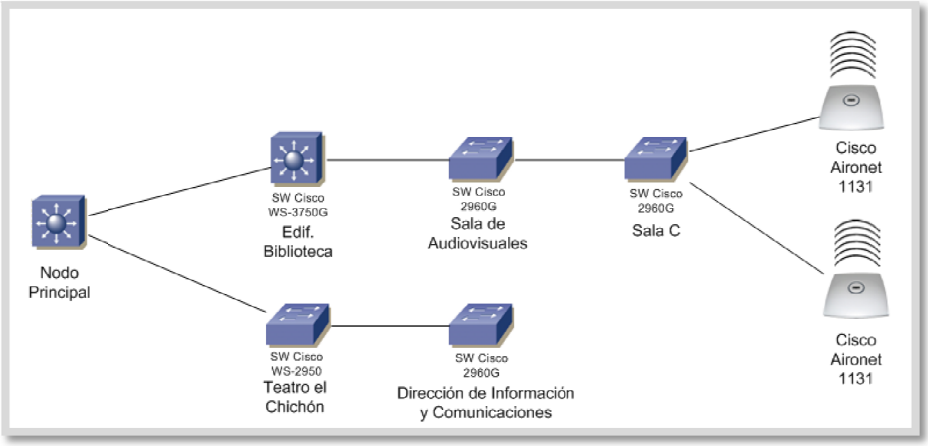


Figura 3.8: Red del Complejo Cultural Aula Magna.

3.4 Lineamientos, políticas y normativas propuestas por la Dirección de Tecnología de Información y Comunicaciones (DTIC) en relación a la administración de la infraestructura inalámbrica

Con respecto a la Administración de la Infraestructura Inalámbrica de la UCV existe una normativa, la cual determina los lineamientos a seguir con relación a los diferentes eventos que se puedan presentar. La normativa es la siguiente [15]:

1. Cuando se requiera instalar un equipo que brinde acceso inalámbrico a RedSI-UCV (Red de Servicios Integrados-UCV), se deberá presentar una solicitud por escrito a la DTIC, suscrita por el titular de las Dependencias, en donde explique y justifique la necesidad de dicha instalación, identifique la(s) persona(s) que tendrá a su cargo la instalación y administración de éstos equipos y la descripción de los equipos a ser instalados. El caso será analizado conjuntamente con la persona asignada por la Dependencia Central que solicita. La autorización para la instalación de la solución estará sujeta al cumplimiento de las normativas y políticas generales que en materia de Tecnología de Información y Comunicaciones esta Dependencia Central ha promulgado para garantizar el buen funcionamiento de la plataforma tecnológica de la institución.

2. La instalación de redes inalámbricas de la UCV, estará destinada a brindar a la comunidad universitaria, acceso a RedSI-UCV con fines académicos, de investigación, de extensión o administrativos, de acuerdo con el propósito fundamental de la Universidad. Por tanto, se prohíbe su uso para otros fines.

3. Para aprobar una solicitud de instalación de equipos que brinden acceso inalámbrico a la red corporativa, se deberán garantizar condiciones mínimas de

seguridad física a fin de evitar el hurto de los mismos o el acceso a puertos de datos.

4. El administrador del servicio de redes inalámbricas de la UCV deberá entender que por la naturaleza propia de las bandas de uso libre ISM, las redes inalámbricas son altamente vulnerables entre sí, esto quiere decir que de no encontrarse correctamente configuradas pueden causarse problemas serios de interferencia e interoperabilidad entre ellas impidiendo su correcto funcionamiento de manera global. Por ello, la DTIC deberá conocer la ubicación, configuración y especificaciones técnicas de cualquier equipo o servicio de redes inalámbricas a fin de optimizar su uso, especialmente aquellos equipos que se conectan a los servicios de la red corporativa.

5. Se entiende por administrador de un servicio de redes inalámbricas de la UCV, al personal técnico designado por una Dependencia Central o Facultad solicitante, autorizado por las autoridades de la Facultad o Dependencia Central para tales fines y debidamente informado a la DTIC.

6. Queda terminantemente prohibida la instalación de dispositivos que brinden acceso inalámbrico a la red sin la debida autorización de la DTIC.

7. Los equipos que brinden acceso inalámbrico debidamente autorizados, son propiedad de la Dependencia Central que los haya adquirido, sin embargo, de ser necesario y bajo mutuo acuerdo con esta Dependencia Central, la DTIC se reserva el derecho de administrarlos.

8. Los equipos que brindan servicio de redes inalámbricas conectadas a la red corporativa, se encuentran sujetos a las mismas reglas y políticas de administración y seguridad que se aplican a todos los dispositivos electrónicos de comunicación de la red cableada.

9. El administrador deberá colocar un código de acceso y una clave para el acceso de los usuarios a la red inalámbrica. El acceso no puede estar abierto sin restricciones.

10. Será responsabilidad de la Dependencia Central que ofrece el servicio de red inalámbrica establecer a través de su Unidad de Tecnología mayores mecanismos de seguridad para el acceso de sus usuarios.

11. Como unidad designada por el Consejo Universitario para el desarrollo, actualización, integración, gestión, normalización y regulación de soluciones de tecnologías de información y comunicaciones en la UCV, la DTIC reservará su potestad reglamentaria de bloquear el acceso a la Red Corporativa a las bases inalámbricas cuando determine que están causando problemas al resto de la red.

12. La DTIC creará un registro en el que quedarán censadas tanto las redes inalámbricas autorizadas como las solicitudes de nuevas redes. En este registro

deberán quedar recogidas todas las características técnicas de las mismas, así como el personal técnico y administrativo responsable.

13. La DTIC será la encargada de la vigilancia, supervisión y cumplimiento de esta normativa.

14. La DTIC informará a los usuarios de los servicios de acceso inalámbrico a la red y a las unidades de tecnología que administren estos servicios, las políticas de uso, privacidad y seguridad, que se han establecido en la Institución.

15. La DTIC se reservará el derecho de controlar o negar el acceso al servicio de redes inalámbricas a aquellas personas que no cumplan con los requisitos de uso establecidos en esta normativa.

16. La DTIC se reservará el derecho de deshabilitar o desconectar cualquier equipo que brinde acceso inalámbrico sin contar con la debida autorización, independientemente de la existencia de otros equipos de red conectados a ese equipo.

17. La DTIC se reservará el derecho de aprobar o rechazar una solicitud de instalación de equipos que brinden acceso inalámbrico a la red de acuerdo a criterios de necesidad (justificación), seguridad física y lógica de la instalación, capacidad de administración de los equipos y el servicio y criterios técnicos relacionados con los equipos y componentes propuestos para ser instalados.

18. La DTIC deberá crear, mantener y actualizar las políticas y los estándares de seguridad en los servicios de red inalámbrica.

19. La DTIC deberá instalar, configurar y administrar los servicios de redes inalámbricas en áreas públicas de la Institución, siempre que cuente con el presupuesto para ello.

20. La DTIC se reservará el derecho de aprobar o rechazar posibles cambios o modificaciones físicas o lógicas sobre equipos y componentes que brinden acceso inalámbrico a la red de acuerdo a criterios eminentemente técnicos y de seguridad.

21. La DTIC asesorará permanentemente a las autoridades universitarias y a las Dependencias Centrales que lo requieran, en lo referente al diseño, elaboración y ejecución de políticas de implementación, uso, mantenimiento y crecimiento de los servicios de acceso inalámbrico a la red.

22. La DTIC podrá suspender los privilegios de uso de los servicios de redes inalámbricas a un determinado usuario por razones relacionadas con la seguridad y bienestar de otros miembros de la Institución o de la propiedad institucional.

23. Las redes inalámbricas ya existentes dentro de los campus Caracas y Maracay, así

como en los extramuros, deberán adaptarse a lo establecido en la presente normativa antes de un período de 6 meses a partir de la fecha de aprobación de las siguientes normativas.

24. Si la naturaleza de las tareas y actividades a realizar a través de la red inalámbrica solicitada, tienen una justificación válida y atiende a una necesidad comprobada de la comunidad universitaria pero puede implicar una afectación negativa a la red corporativa, y por ende, pueda potencialmente interferir en las actividades que normalmente realizan los usuarios de ella, entonces la red inalámbrica deberá instalarse totalmente desconectada de la plataforma tecnológica operativa de la Universidad. Igualmente si por la naturaleza de las actividades a realizar, se comprueba la necesidad de conexión temporal a la plataforma tecnológica de la UCV, deberá coordinarse y planificarse con la DTIC; y dicha conexión deberá realizarse en los horarios de menor afectación.

25. Las redes inalámbricas de la UCV hacen uso del espectro de radio frecuencias en las bandas libres ISM (Industrial, Scientific and Medical) de 2.4 GHz. y 5 GHz. para interconectar equipos y componentes a la red cableada que permiten el acceso a red corporativa y en consecuencia a las redes externas como Internet e Internet2, entre otras. Este servicio no está diseñado para sustituir a la red cableada tradicional sino que debe considerarse como una solución complementaria o una extensión de la red cableada para áreas públicas, por ende serán instaladas siempre y cuando no exista posibilidad alguna de implementar soluciones de redes cableadas o instaladas en sitios estratégicos de alto tránsito de usuarios de la red como pudieran ser bibliotecas, salas de lectura, auditorios, laboratorios de docencia/investigación, salas de reuniones, etc.

26. Las redes inalámbricas que hacen uso de las bandas libres ISM serán utilizadas principalmente para acceso y navegación web. Aquellos servicios críticos, como sistemas administrativos o sistemas que contengan información institucionalmente sensible, crítica y/o confidencial, deberán utilizar protocolos de seguridad correctamente configurados.

3.5 Requerimientos establecidos por la DTIC

Antes de realizar un diseño de una WLAN, es de suma importancia conocer todos los requerimientos con lo que esta red debe cumplir. A continuación se describen los requerimientos especificados por la DTIC:

- El personal de la DTIC de la UCV, contempla el uso del nuevo estándar IEEE 802.11n para el diseño de la WLAN, donde la ventaja más notable de este estándar es la mejora sustancial en confiabilidad y alto rendimiento de las aplicaciones.

- Los elementos de infraestructura tanto de la red WLAN, como los de la solución de videovigilancia deben ser del fabricante Cisco Systems. La decisión de utilizar

dispositivos específicamente de Cisco Systems, viene dada por la idea de estandarizar toda la plataforma tecnológica de comunicaciones, además dicho fabricante ofrece un excelente rendimiento, personalización y una robusta configuración de Calidad de Servicio.

- Se requiere de una herramienta de gestión y monitoreo que sea robusta, flexible, fácil de usar, que permita obtener reportes y estadísticas fácilmente, que permita a los administradores de la red planificar, implementar, monitorear, resolver fallas de manera exitosa.

- Todas las instalaciones que se deriven de la WLAN deberán cumplir con la normativa del Consejo de Preservación y Desarrollo (COPRED), ya que la UCV fue declarada Patrimonio Mundial, Cultural y Natural de la Humanidad por la UNESCO en el año 2000 [37].

- Se debe tomar en cuenta la seguridad física de los dispositivos, APs, cámaras de videovigilancia y a su vez la seguridad lógica de la solución para garantizar el acceso seguro por parte de personal administrativo, autoridades, personal obrero y estudiantes a la Red.

- La WLAN implementada deberá permitir a futuro la incorporación e integración de tecnologías importantes, como lo es Outdoor Wireless Mesh y videovigilancia de Cisco, para extender la red inalámbrica al Campus Universitario, poder ofrecer Voz sobre la WLAN, rastreo de dispositivos con RFID y transmisión de videos usando cámaras inalámbricas.

- El diseño de la WLAN con cámaras inalámbricas de videovigilancia deberá ser apto para monitorear las 24 horas los accesos a las oficinas del Edificio el Rectorado, los accesos a la Plaza Cubierta y al Complejo Cultural Aula Magna, esto viene dado por exigencia de la Dirección de Seguridad de la UCV.

Además de estos requisitos que se mencionaron anteriormente, es necesario contemplar los cuatro principales requisitos de una solución WLAN, los cuales se explican a continuación [10]:

- **Alta disponibilidad:** se consigue con la redundancia del sistema y el diseño adecuado de área de cobertura.

- **Escalabilidad:** se consigue soportando varios APs por área de cobertura que utilizan varias frecuencias y canales no superpuestos.

- **Manejabilidad:** se logra utilizando dispositivos WLAN que soporten protocolos de administración remota.

- **Interoperabilidad:** es necesario que los dispositivos implementados cumplan con los estándares, como por ejemplo, IEEE 802.11 a,b,g,n.

3.6 Lineamientos de diseño para la WLAN

- La actual red inalámbrica implementada en el Edifico el Rectorado despliega un único SSID (*Service Set IDentifier*) denominado UCVDATOS, este parámetro se tomara en cuenta y se mantendrá igual para la nueva WLAN a implementar en la Plaza Cubierta y el Complejo Cultural Aula Magna.

- Los APs implementados en la Plaza Cubierta, el Complejo Cultural Aula Magna y el Edificio el Rectorado, serán utilizados en principio para el buen desempeño de la solución de videovigilancia, así mismo, la WLAN podrá brindar una conexión inalámbrica a todos los usuarios que así lo requieran.

- El controlador Cisco Wireless 4404 será el responsable de las funciones inalámbricas en todo el sistema, tales como políticas de seguridad, prevención de intrusos, gestión de RF, QoS, y movilidad, así como también, será el encargado de gestionar todos los puntos de acceso (100 APs como máximo). Este controlador será instalado en el Data Center de la UCV.

- El Cisco WCS permitirá a los administradores de la WLAN planificar, implementar, monitorear, resolver fallas y generar reportes de manera exitosa, para que el administrador pueda controlar todos los dispositivos y lo que sucede en la red en un software centralizado, obteniendo una mayor productividad de la WLAN.

- El tráfico de paquetes generado por las cámaras de videovigilancia será destinado a una VLAN exclusiva, esto evitara la congestión total de la WLAN. Es importante mencionar que cada paquete será tratado con servicios diferenciados para asegurar que sean atendidos según la prioridad asignada.

- Los APs serán instalados físicamente en posiciones tan cercanas como sea posible a las sugeridas por la herramienta de Cisco WCS.

- Los dispositivos (APs, cámaras de videovigilancia) estarán ubicados en zonas estratégicas y cada uno de ellos dispondrá de seguridad física para evitar daños.

- Los APs que actualmente forman parte de la red inalámbrica del Edificio el Rectorado, corresponden al modelo Cisco Aironet 1130AG. El modelo que se propone para ampliar la WLAN es el Cisco Aironet 1140, el cual brinda mejores prestaciones, como por ejemplo, soporta el estándar 802.11n.

- Las cámaras que se utilizaron para realizar las pruebas de videovigilancia son del fabricante Cisco Systems, modelo WVC2300, así mismo, debido a los requerimientos exigidos por la Dirección de Seguridad de la UCV y la DTIC se propone la utilización de las cámaras Serie 4000 de Cisco Systems.

3.7 Arquitectura de conectividad de la WLAN

La infraestructura de conectividad de la WLAN estará basada en un modelo centralizado, conformado por un controlador, los APS y un WCS (*Wireless Control System*).

3.7.1 Wireless Lan Controllers

Los Controladores inalámbricos de Cisco son unos de los componentes fundamentales de la solución de Cisco UWN (*Unified Wireless Network*) y son responsables de las funciones inalámbricas en todo el sistema, tales como políticas de seguridad, prevención de intrusos, gestión de RF, QoS, y movilidad. Estos trabajan en conjunto con los APs de Cisco y el WCS, para soportar aplicaciones inalámbricas críticas del negocio. Los controladores inalámbricos de Cisco proveen el control, escalabilidad, seguridad y confiabilidad que se necesita para implementar redes inalámbricas seguras.

Los controladores inalámbricos de Cisco se integran con facilidad a redes empresariales existentes. Estos dispositivos soportan un gran número de configuraciones y gestiones inalámbricas de manera automatizada, a lo largo de todas las ubicaciones dentro de la empresa o campus universitario.

Debido a que los controladores soportan 802.11 a/b/g y el estándar IEEE 802.11n, las organizaciones pueden implementar la solución que mejor se adapte a sus necesidades, pueden ofrecer una cobertura robusta con 802.11 a/b/g y brindar gran desempeño usando 802.11n y soluciones inalámbricas de Cisco.

Los Cisco 4400 Wireless LAN Controllers son diseñados para medianas o grandes localidades. La Serie Cisco 4400 está disponible en dos modelos, el 4402 con dos puertos Gigabit y viene en configuraciones de 12, 25 Y 50 APs, y el 4404 con cuatro puertos Gigabit Ethernet que soporta hasta 100 puntos de acceso.

El Cisco WLC 4400 es ideal para implementaciones de soluciones inalámbricas para empresas, proveedores de servicios y campus universitarios. Simplifica la implementación y operación de las redes inalámbricas, ayudando a obtener un mejor desempeño, mejorar la seguridad y maximizar la disponibilidad. El Cisco WLC 4400 gestiona todos los APs dentro del ambiente del campus y ubicaciones remotas, eliminando la complejidad y suministrando a los administradores de redes visibilidad y control de sus redes inalámbricas [6].

En la Figura 3.9, tomada de [6], se muestra la serie 4400 del Cisco Wireless Controller.

Figura 3.9: Cisco Wireless Controller Serie 4400.

3.7.2 Access Points

El fabricante Cisco Systems posee gran cantidad de puntos de accesos, los diferentes modelos de APs pueden estar orientados para ambientes de interiores o de exteriores, con una o dos interfaces de radio y con soporte para las especificaciones de capa física 802.11 a/b/g/n. A continuación se da una breve descripción de los diferentes modelos tomados en cuenta para la presente propuesta:

- **Cisco Aironet 1130AG**

Los Cisco Aironet 1130AG Series Access Point se apoya en un sistema de gestión basado en el software Cisco IOS y utiliza dos radios integrados (IEEE 802.11g y IEEE 802.11a), mientras que el AP 1131G utiliza solo un radio integrado (IEEE 802.11g).

Se puede configurar y controlar el AP utilizando la interfaz de línea de comandos (CLI), el navegador basado en el sistema de gestión, o Simple Network Management Protocol (SNMP).

El Cisco Aironet 1130AG Series está disponible en dos versiones: unificada o autónomos. Los unificados operan con LWAPP (*Lightweight Access Point Protocol*) y trabajan en conjunto con los controladores de LAN inalámbricas de Cisco y el Cisco WCS (*Wireless Control System*). Cuando se configura con LWAPP, la serie Cisco Aironet 1130AG puede detectar automáticamente la mejor ubicación del controlador de LAN inalámbrica y descargar las políticas adecuadas y la información de configuración. Los APs autónomos se basan en Cisco IOS software y, opcionalmente, pueden operar con el CiscoWorks WLSE (*Wireless LAN Solution Engine*) [7].

En la Figura 3.10, tomada de [7], se muestra un Cisco Aironet 1130.

Figura 3.10: Cisco Aironet 1131.

- **Cisco Aironet 1140**

Algunas de las características más resaltantes de los Access Points Cisco Aironet 1140 son [8]:

- Combina todas las prestaciones del protocolo 802.11n.
- Se completa con estándar 802.3af (PoE), que proporciona un ahorro considerable en gastos y mantenimiento, ya que evita la necesidad de alimentar independientemente el AP.
- Ofrece hasta 6 veces el rendimiento de redes 802.11 a/g.
- Aumento en la capacidad general de los canales inalámbricos.
- Reducción de los huecos de cobertura inalámbrica de dispositivos anteriores.

En la Figura 3.11, tomada de [8], se muestra un Cisco Aironet 1140.

Figura 3.11: Cisco Aironet 1140.

La Tabla 3.1 muestra las características más resaltantes de estos dispositivos.

Características	AP 1130AG	AP 1140
Foto Referencial		
Estándar Compatible	802.11a y 802.11g	802.11a, 802.11g y 802.11n
Antena	Omnidireccional integrada con ganancia de 3.0 dbi en la banda de 2.4 GHz y 4.5 dBi en la banda de 5 GHz	Omnidireccional integrada con ganancia de 4.0 dbi en la banda de 2.4 GHz y 3.0 dBi en la banda de 5 GHz
Interfaces de red cableada	1 interfaz FastEthernet (10/100BASE-T Mbps) para la conexión a la red cableada. Un puerto de consola.	1 interfaz FastEthernet (10/100/1000BASE-T Mbps) para la conexión a la red cableada. Un puerto de consola.
PoE (Power-Over_Ethernet)	Si	Si
Seguridad	WPA, WPA2 (802.11i), TKIP, WEP keys of 40 y 128 bits.	WPA2, WPA ,AES,TKIP

Tabla 3.1: Características de los APs.

3.7.3 WCS (*Wireless Control System*)

Cisco WCS soporta la entrega de aplicaciones de alto desempeño y soluciones indispensables. Esta plataforma integral cumple con las necesidades de redes inalámbricas pequeñas, medianas y de gran tamaño en ubicaciones locales, remotas, nacionales e internacionales. Esta solución les proporciona a los administradores de red acceso inmediato a herramientas que necesitan para implementar nuevas redes inalámbricas y mantener de una forma eficiente las redes existentes.

Esta plataforma de gestión permite a los administradores planificar, implementar, monitorear, resolver fallas y generar reportes sobre redes *indoor* y *outdoor* de manera exitosa.

A diferencia de otras herramientas de gestión, Cisco WCS disminuye los costos operacionales incorporando los amplios requerimientos de gestión, desde RF hasta controlador de servicios en una plataforma unificada [9].

3.8 Ubicación física de los APs

A continuación se mostrara la ubicación física de los dispositivos que conformaran la WLAN, tomando en cuenta que se eliminaron las zonas sin cobertura que anteriormente existían, dándole una continua comunicación a los dispositivos inalámbricos en las áreas del Edificio el Rectorado, Plaza Cubierta y el Complejo Cultural Aula Magna.

En la Figura 3.12, tomada de [14], se muestra el plano específicamente del piso 1 del Edificio el Rectorado, donde se agregaron 2 APs nuevos, ubicados físicamente en la entrada de la oficina del Rectorado y el otro ubicado en la oficina de la Secretaria, dándole una total cobertura al área de los ascensores, como lo muestra la onda expansiva de la señal en la Figura 3.13, tomada de [14].

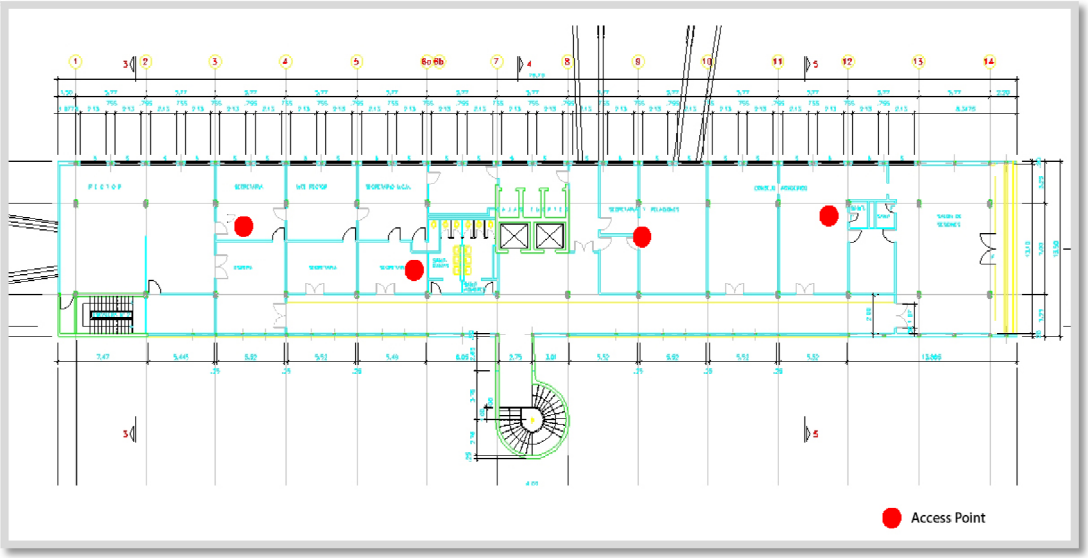


Figura 3.12: Ubicación física de los APs en piso 1.

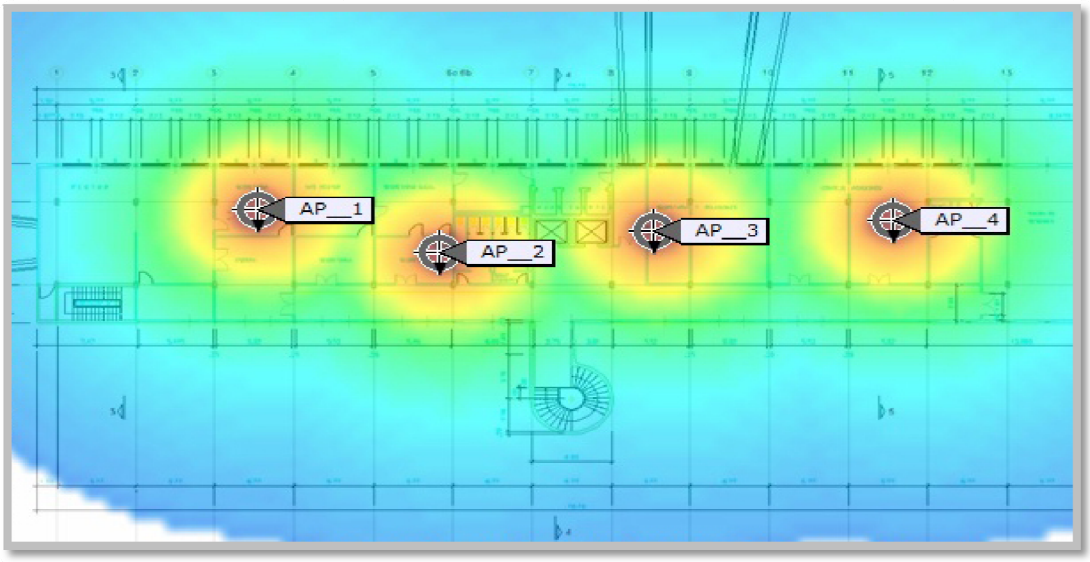


Figura 3.13: Onda expansiva de los APs en piso 1.

En la Figura 3.14, tomada de [14], se muestra el plano del piso 2, donde se agregaron 2 APs a la red, ubicados en la entrada de la Dirección de Administración del Rectorado y el otro ubicado en el Vicerrectorado Administrativo, al igual que en piso 1 se colocaron específicamente en estas zonas para dar una cobertura al área de los ascensores. La Figura 3.15, tomada de [14], muestra la onda expansiva de la señal en el piso 2.

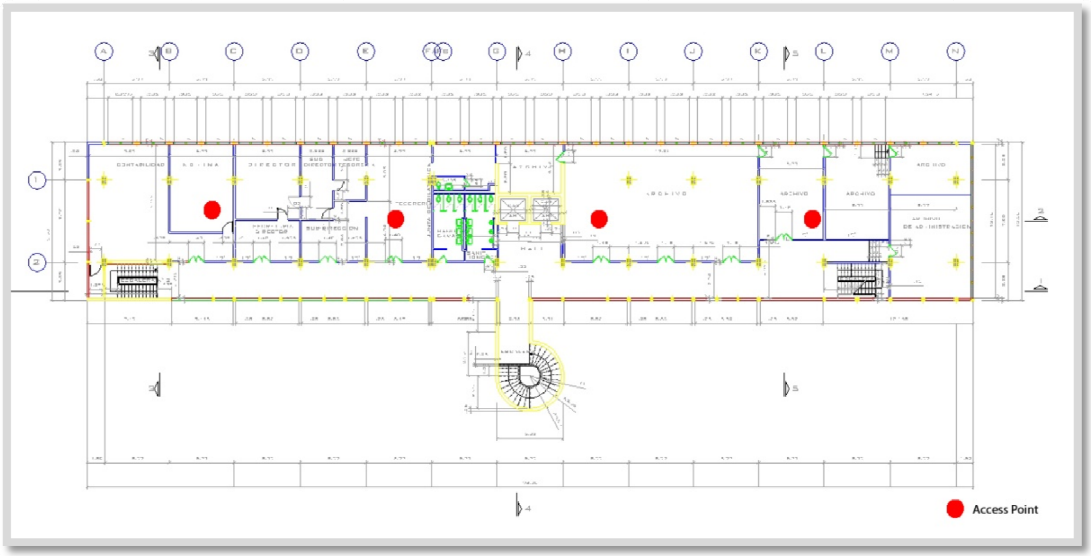


Figura 3.14: Ubicación física de los APs en piso 2.

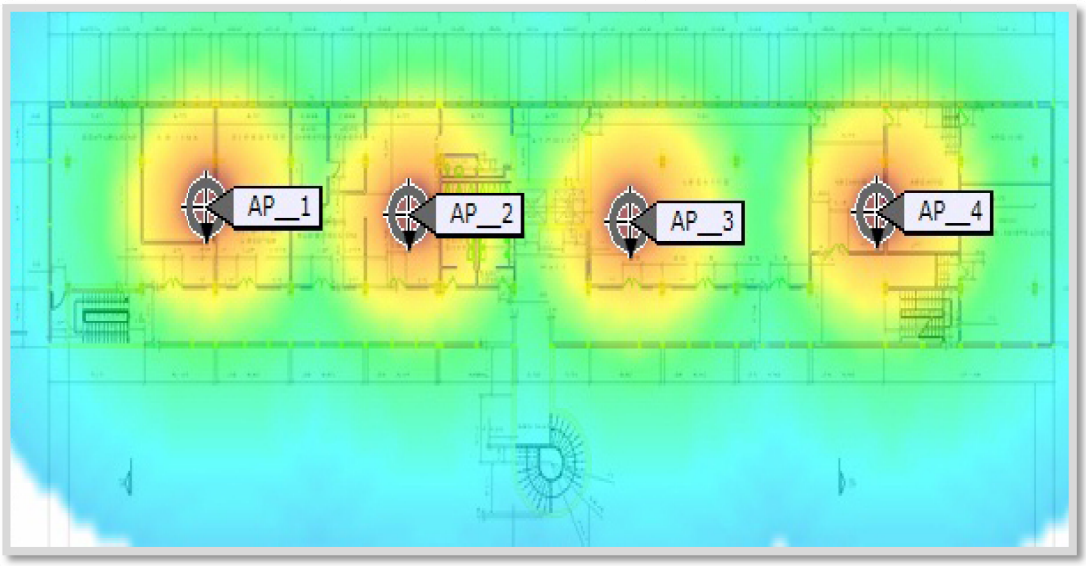


Figura 3.15: Onda expansiva de los APs en piso 2.

En el piso 3 se agregaron 3 APs como se muestra en la Figura 3.16, tomada de [14], dotando de señal inalámbrica a todo el piso.

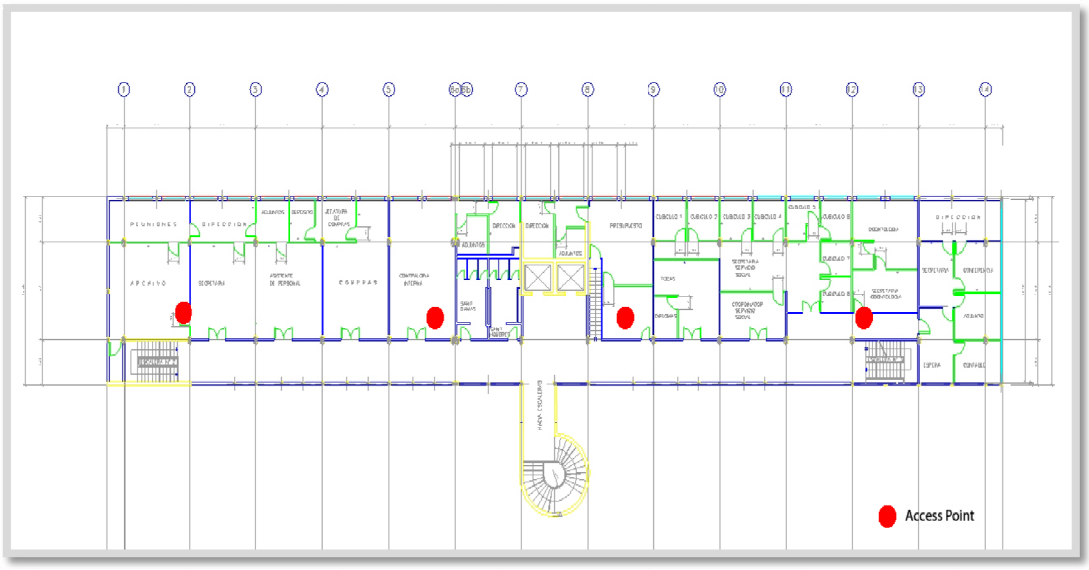


Figura 3.16: Ubicación física de los APs en piso 3.

La Figura 3.17, tomada de [14], muestra la onda expansiva de la señal de los APs en el piso 3.

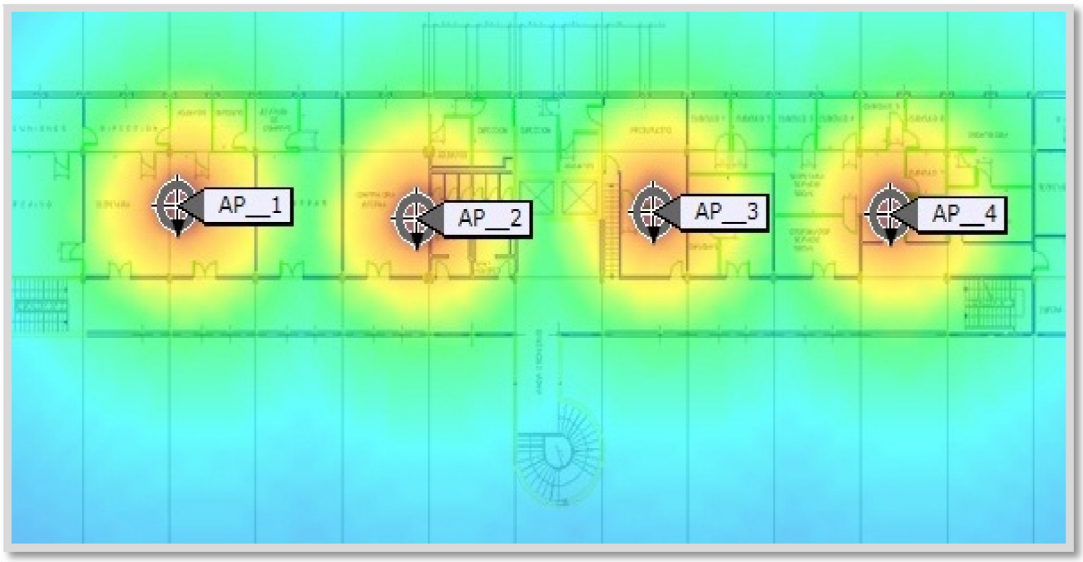


Figura 3.17: Onda expansiva de los APs en piso 3.

La Plaza Cubierta y el Complejo Cultural Aula Magna no disponen de ninguna red inalámbrica, por lo cual se realizó un estudio para determinar la mejor ubicación de los APs, dando como resultado una cobertura de señal inalámbrica a toda la Plaza Cubierta y al Complejo Cultural Aula Magna.

En la Figura 3.18, tomada de [14], se pueden observar las ubicaciones de los APs en la Plaza Cubierta, seguidamente en la Figura 3.19, tomada de [14], se mostrará la expansión de la onda generada por los APs.

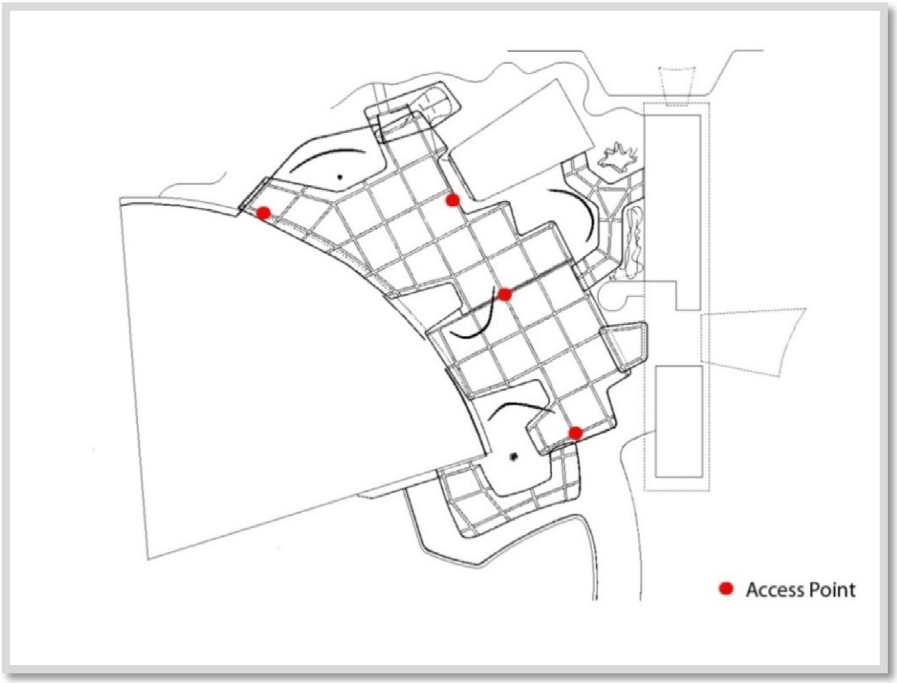


Figura 3.18: Ubicación física de los APs en la Plaza Cubierta.

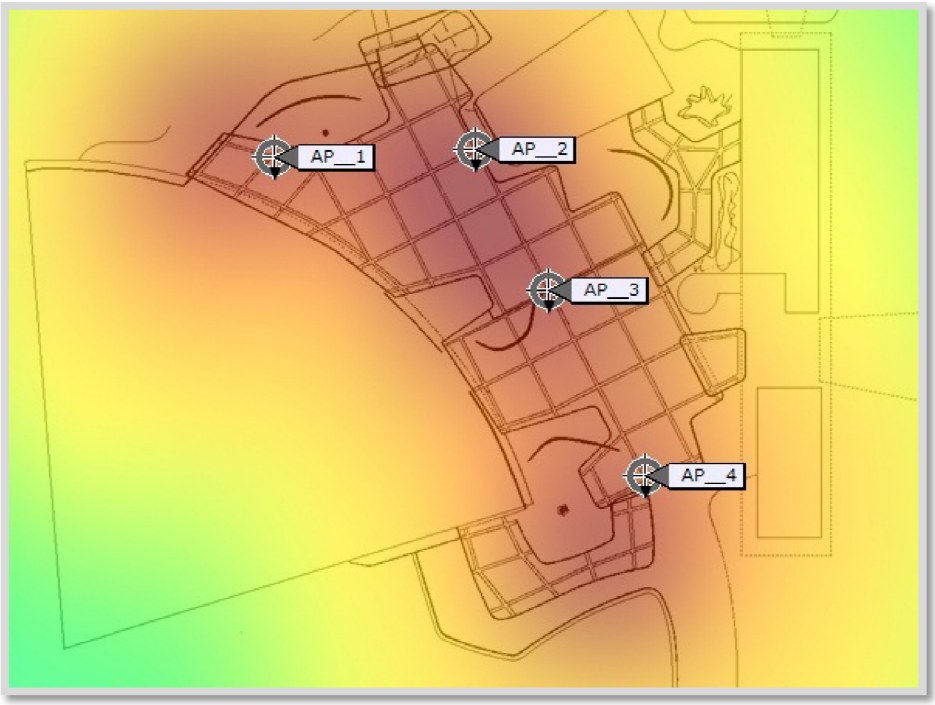


Figura 3.19: Onda expansiva de los APs en la Plaza Cubierta.

En el Complejo Cultural Aula Magna se agregaron 4 APs, como lo muestra la Figura 3.20, tomada de [14].

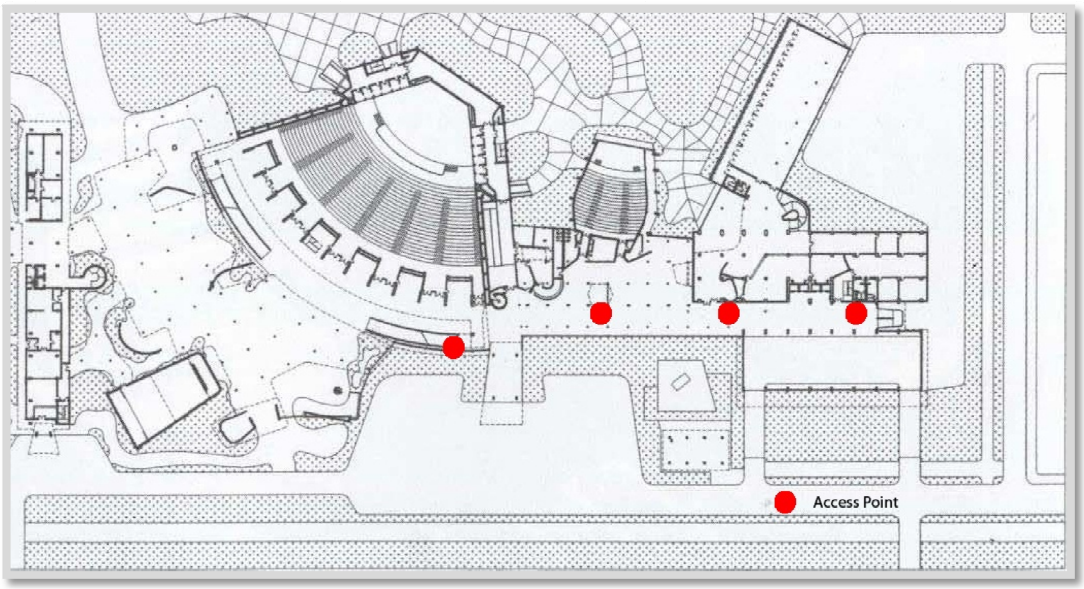


Figura 3.20: Ubicación física de los APs en el Complejo Cultural Aula Magna.

La expansión de la onda de los APs ubicados en el Complejo Cultural Aula Magna se muestra en la Figura 3.21, tomada de [14].

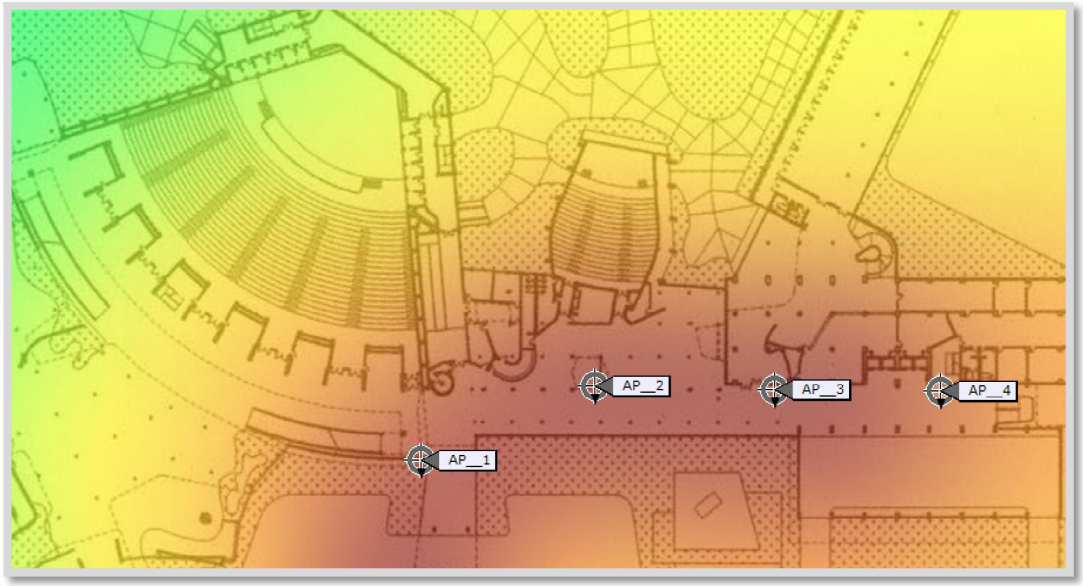


Figura 3.21: Onda expansiva de los APs en el Complejo Cultural Aula Magna.

3.9 Cámaras inalámbricas

El fabricante Cisco Systems posee diferentes modelos que pueden ser implementados tanto en ambientes interiores como exteriores, esto depende de las necesidades requeridas. A continuación se da una breve descripción de los diferentes modelos tomados en cuenta para la presente propuesta:

3.9.1 Cisco WVC210

Los productos de videovigilancia de Cisco ofrecen diferentes opciones a las pequeñas empresas para vigilarlas y protegerlas. Estas soluciones de alta calidad pueden ser optimizadas para aplicaciones y sitios web.

El pan/tilt y zoom digital son funciones que permiten controlar remotamente el movimiento de la cámara y el enfoque, dándole flexibilidad a una distancia máxima. Hasta 10 usuarios simultáneos de unidifusión pueden acceder a la cámara en cualquier momento. La reproducción está disponible en Windows Media Player, sin necesidad de un reproductor propietario. También puede activar el modo de seguridad, con que cuenta la cámara, para que envíe un correo con un video adjunto, a un máximo de tres direcciones de correo electrónico, cada vez que detecta movimiento en su campo de visión [11].

En la Figura 3.22, tomada de [11], se muestra una Cámara Cisco WVC210.

Figura 3.22: Cámara Cisco WVC210.

3.9.2 Cisco WVC2300

El WVC2300 Cisco utiliza una alta calidad de escaneado progresivo de CCD (*charge-coupled device*). El sensor CCD también tiene baja sensibilidad a la luz, de modo que el vídeo puede ser capturado incluso en ambientes con muy poca luz. Además, la cámara incorpora un puerto de infrarrojos (IR) que permite la captura de vídeo en total oscuridad.

La cámara Cisco WVC2300 admite códecs duales (MPEG-4 y MJPEG). Ambos codecs pueden utilizarse simultáneamente. MPEG-4 permite el consumo eficaz de ancho de banda con buena calidad de la compresión y es óptimo para la visualización del video en tiempo real. MJPEG ofrece una calidad de vídeo óptima con pérdida de compresión, lo que es ideal para el almacenamiento en dispositivos de gran volumen como NAS (*Network Attached Storage*). Las capacidades de audio WVC2300 de Cisco incluyen audio bidireccional, micrófono integrado, altavoz externo y puertos para micrófono [12].

En la Figura 3.23, tomada de [12], se muestra una Cámara WVC2300.

Figura 3.23: Cámara Cisco WVC2300.

3.9.3 Cisco Serie 2500

La Serie 2500 de Cisco, es una serie de cámaras IP de videovigilancia diseñadas para un rendimiento superior en una amplia variedad de aplicaciones de videovigilancia.

Las cámaras IP de videovigilancia Cisco serie 2500, son cámaras de alta definición y rendimiento superior, que combina la mejor resolución y compresión de video. Utilizan MPEG-4, y transmiten hasta 30 cuadros por segundo (fps) a una resolución NTSC (720 x 480) y 25 fps en resolución D1 PAL (720 x 576), lo cual permite un uso eficaz de la red y proporciona video de la más alta calidad.

La Serie 2500 de Cisco ofrece una variedad de beneficios, incluyendo:

- **Amplio rango dinámico:** la cámara utiliza una potente tecnología de imagen digital, permitiendo capturar imágenes de alta calidad en una amplia variedad de condiciones de iluminación.

- **Notificación de eventos:** la cámara también dispone de dos entradas digitales y dos salidas digitales, que pueden ser utilizados para iniciar acciones específicas cuando se detecta una alarma.

- **Capacidades inalámbricas:** este modelo de cámara IP inalámbrica soporta la tecnología MIMO, la cual proporciona un mejor rendimiento de datos y enlaces más amplios que los diseños de una única antena. La cámara IP inalámbrica 2500 ofrece seguridad inalámbrica utilizando WPA / WPA2 [13].

En la Figura 3.24, tomada de [13], se muestra una Cámara Cisco Serie 2500.

Figura 3.24: Cámara Cisco Serie 2500.

Debido a los diferentes modelos de cámaras de videovigilancia inalámbricas que presenta el fabricante Cisco Systems, se muestra la Tabla 3.2, donde se pueden observar las características más resaltantes de estos dispositivos.

Características	Cisco WVC210	Cisco WVC2300	Cisco Serie 2500
Foto Referencial			
Estándar Compatible	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, IEEE 802.1p (QoS), IEEE 802.1Q (VLAN), 802.11e	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, IEEE 802.1p (QoS), IEEE 802.1Q (VLAN), 802.11e	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, IEEE 802.1p (QoS), IEEE 802.1Q (VLAN), 802.11e
Protocolos Soportados	TCP/IP, HTTP, DHCP, SMTP, FTP, DNS.	TCP/IP, HTTP, DHCP, SMTP, FTP, DNS.	DHCP, FTP, HTTP, SMTP y TCP/IP.
Puertos	Ethernet, antena, entrada de micrófono, altavoz de salida, fuente de poder (5V 2A)	Ethernet, entrada de micrófono, altavoz de salida, fuente de poder (12V, 1A)	Ethernet, entrada de micrófono, altavoz de salida, fuente de poder (12V, 1A)

Características	Cisco WVC210	Cisco WVC2300	Cisco Serie 2500
Resolución de Video	640 x 480, 320 x 240, 160 x 120	640 x 480 (VGA), 320 x 240 (QVGA), 160 x 120 (QQVGA)	720 x 480
Comprensión de Video	MPEG-4 y MJPEG	MPEG-4 y MJPEG	MPEG-4
PoE (Power-Over_ Ethernet)	Si	Si	Si

Tabla 3.2: Comparación entre cámaras Cisco.

3.10 Ubicación física de las cámaras

Una vez diseñada la WLAN, se procederá a mostrar la ubicación física de las cámaras de videovigilancia basadas en la tecnología IEEE 802.11, tomando en cuenta que se realizaron pruebas para medir la expansión de las ondas de RF de los APs y de esta manera asegurar un correcto desempeño de las cámaras en las áreas del Edificio el Rectorado, Plaza Cubierta y el Complejo Cultural Aula Magna.

En el plano correspondiente a la Planta Baja del Edificio el Rectorado, como se muestra en la Figura 3.25, tomada de [14], se propone 1 cámara de videovigilancia, la cual estará encargada de monitorear la entrada principal del Edificio el Rectorado. Así mismo, esta cámara recibirá señal inalámbrica de los APs que ya se encuentran implementados en la DTIC.

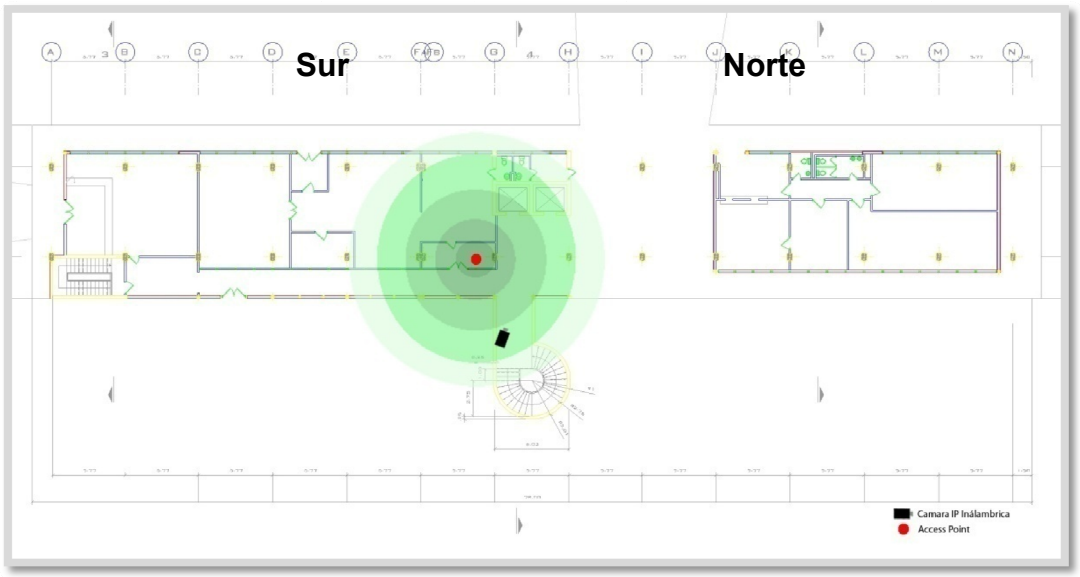


Figura 3.25: Ubicación de las cámaras en Planta baja.

En la Figura 3.26, tomada de [14], se muestra el plano del piso 1 del Edificio el Rectorado, donde es importante mencionar que en el ala sur se propone colocar una cámara en la entrada de la oficina del Rectorado, otras 2 cámaras en el área central del edificio monitoreando tanto los ascensores como las escaleras y 2 cámaras más en el

ala norte del edificio.

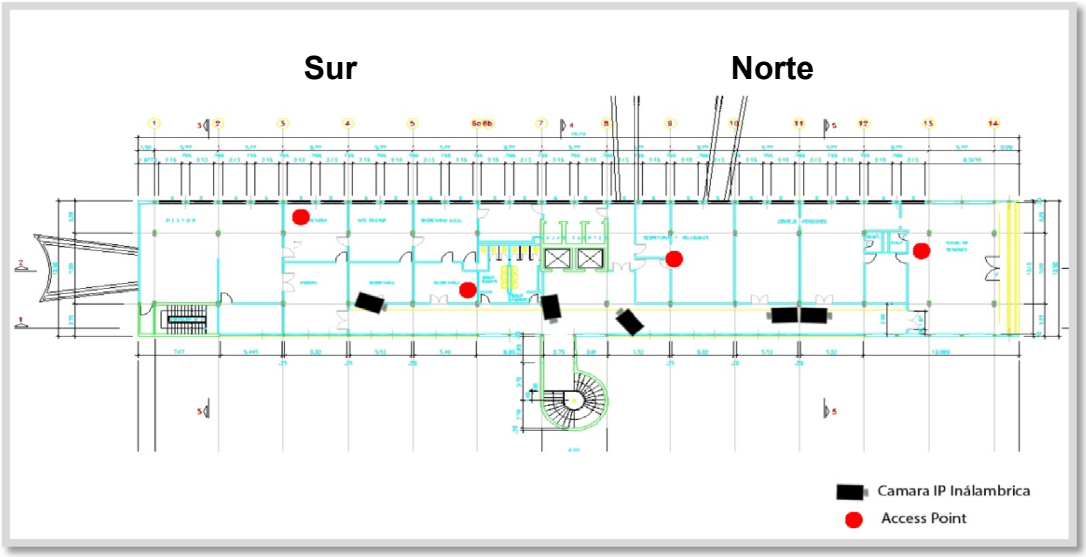


Figura 3.26: Ubicación de las cámaras en piso 1.

Seguidamente en la Figura 3.27, tomada de [14], se observa que las cámaras reciben una buena señal por parte de los APs.

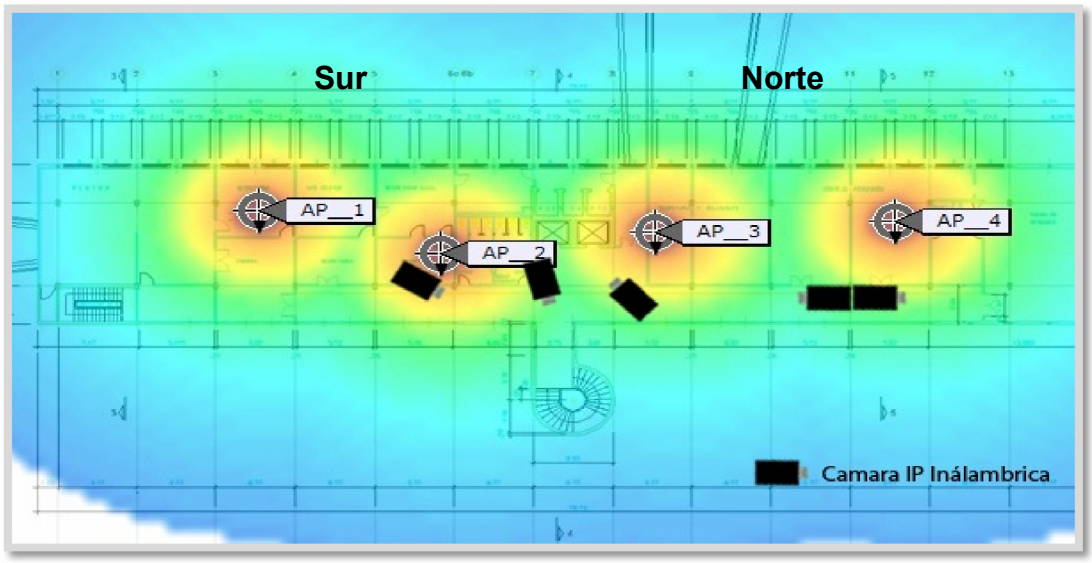


Figura 3.27: Señal captada por las cámaras en piso 1.

En el piso 2 del Edificio el Rectorado, se colocaron cámaras en puntos estratégicos para monitorear los accesos a los pasillos, ascensores y escaleras, como se puede observar en la Figura 3.28, tomada de [14]. De igual forma en la Figura 3.29, tomada de [14], se muestra que la onda de RF generada por los APs les brinda cobertura a las cámaras.

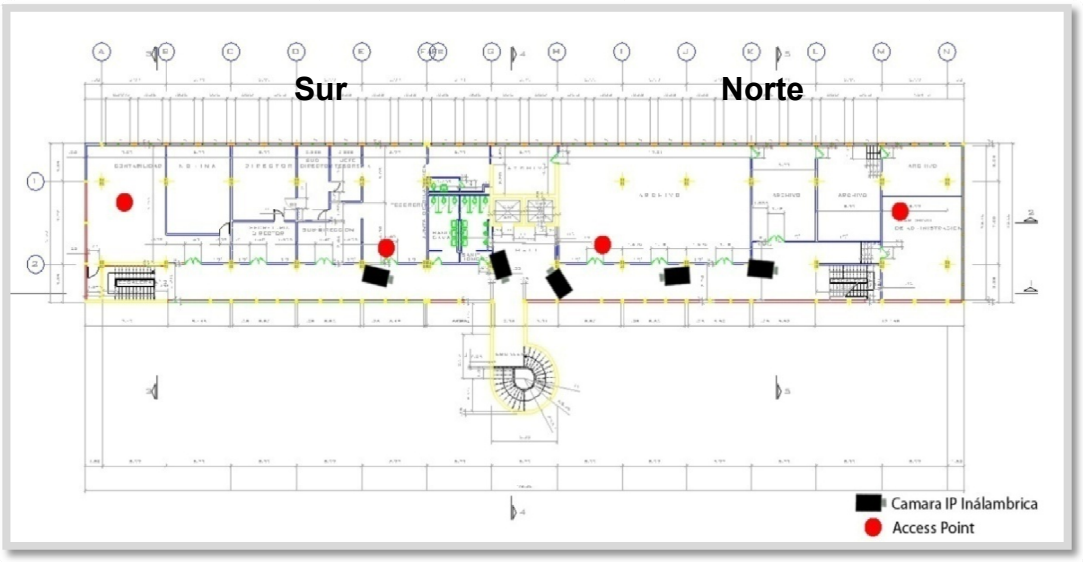


Figura 3.28: Ubicación de las cámaras en piso 2.

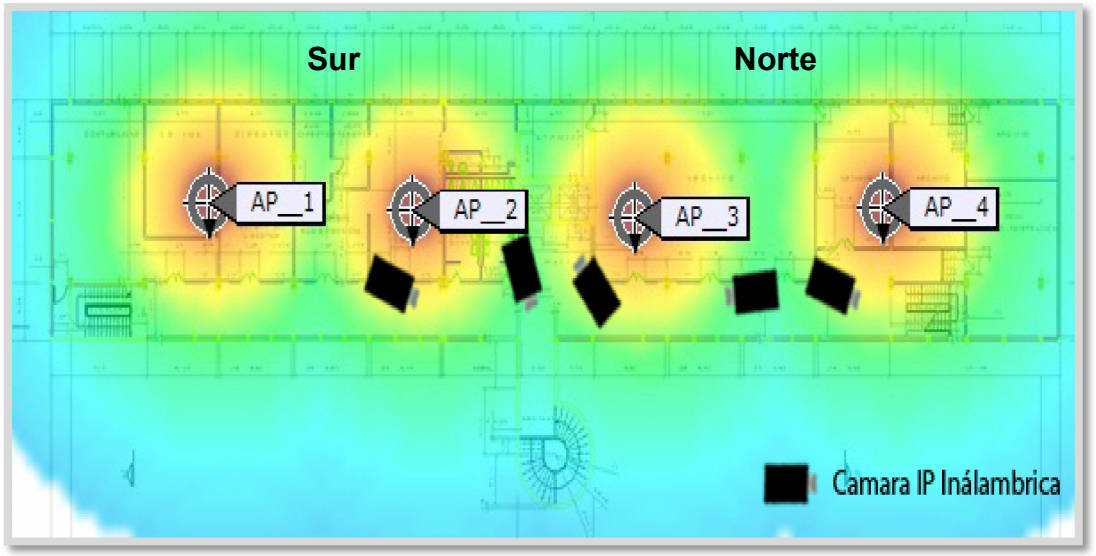


Figura 3.29: Señal captada por las cámaras en piso 2.

Al igual que en los pisos anteriores, el piso 3 se proponen cámaras para monitorear el acceso al mismo, como se puede observar en la Figura 3.30, tomada de [14].

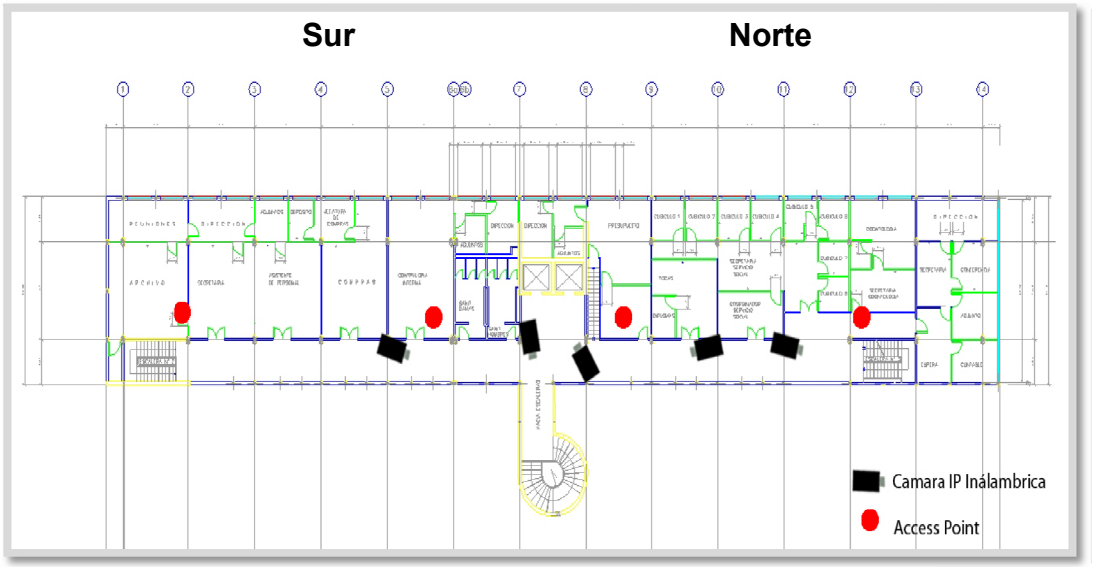


Figura 3.30: Ubicación de las cámaras en piso 3.

En la Figura 3.31, tomada de [14], se muestra que las cámaras disponen al igual que en los pisos anteriores una buena señal inalámbrica.

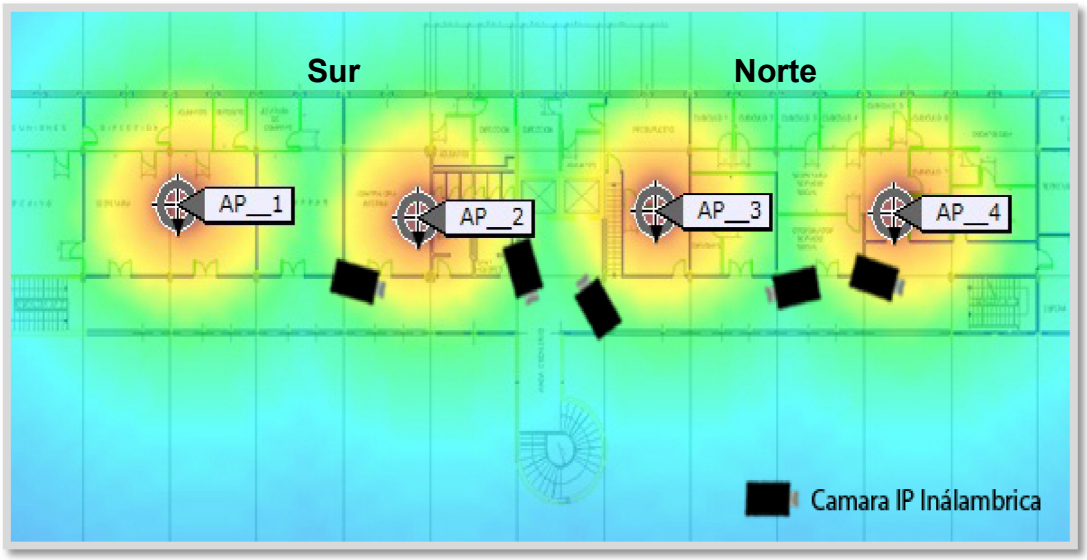


Figura 3.31: Señal captada por las cámaras en piso 3.

Así mismo, se llevaron a cabo reuniones con la Dirección de Seguridad de la UCV, con la finalidad de establecer cuáles son los puntos críticos que deben ser monitoreados, siendo estos principalmente todos los accesos a la Plaza Cubierta y en el Complejo Cultural Aula Magna. En la Figura 3.32, tomada de [14], se muestra la ubicación de las cámaras en la Plaza Cubierta.

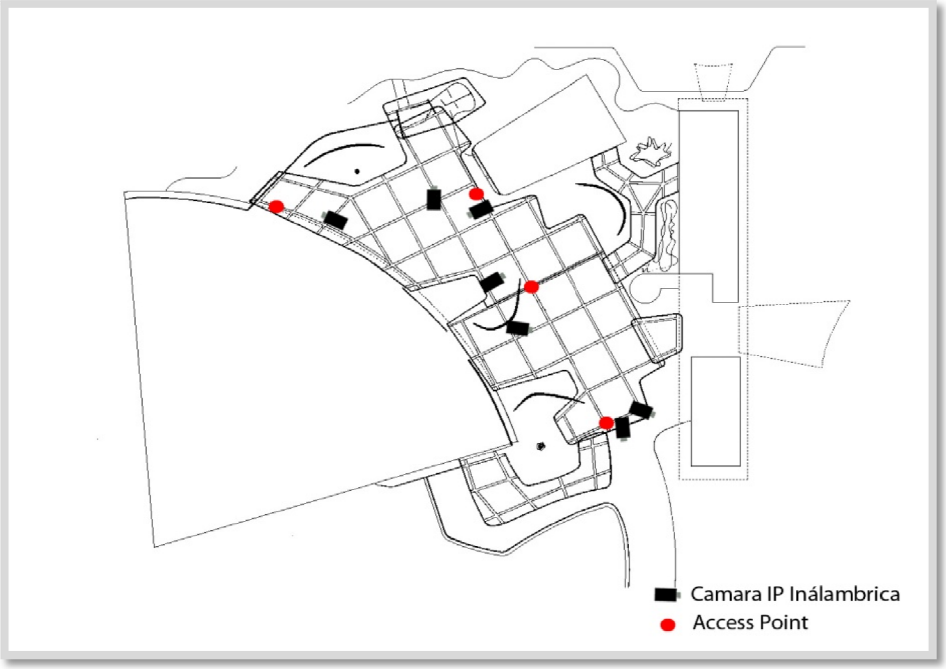


Figura 3.32: Ubicación de las cámaras en la Plaza Cubierta.

En la Figura 3.33, tomada de [14], se observa que los APs ubicados en la Plaza Cubierta le brindan una buena señal inalámbrica a todas las cámaras propuestas.

Figura 3.33: Señal captada por las cámaras en la Plaza Cubierta.

En el Complejo Cultural Aula Magna se proponen 6 cámaras de videovigilancia, las cuales estarán monitoreando los siguientes puntos: el estacionamiento de la Biblioteca Central, las taquillas del Aula Magna y los camerinos de la misma, la Biblioteca Central,

pasillo de acceso a la Biblioteca Central, Edificio de la Biblioteca Central y las escaleras de la imprenta universitaria. La Figura 3.34, tomada de [14], muestra la ubicación de las cámaras en el Complejo Cultural Aula Magna.

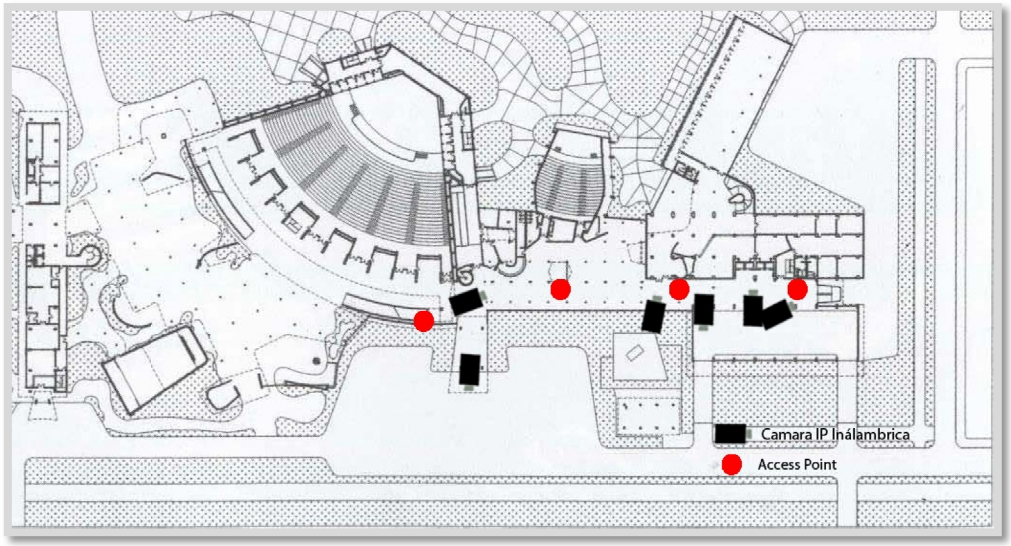


Figura 3.34: Ubicación de las cámaras en el Complejo Cultural Aula Magna.

En la Figura 3.35, tomada de [14], se muestra que las cámaras ubicadas en el Complejo Cultural Aula Magna reciben una buena señal inalámbrica.

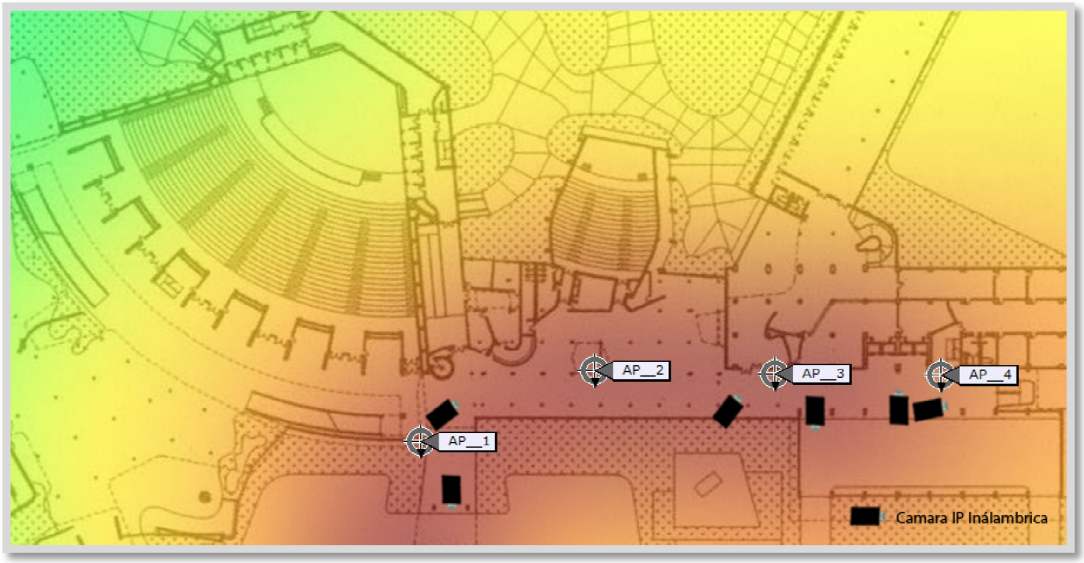


Figura 3.35: Señal captada por las cámaras en el Complejo Cultural Aula Magna.

Capítulo 4

Implementación de los escenarios de pruebas

En el presente capitulo, se procederá a detallar la configuración de los distintos software asociados al diseño de la solución de videovigilancia y al diseño de la WLAN, igualmente, este capítulo platea diversos escenarios de pruebas que validan el diseño de la solución. Cada escenario verifica el correcto funcionamiento de los componentes involucrados.

4.1 Instalación y configuración de los diferentes componentes tecnológicos

El objetivo principal de la instalación y configuración de los componentes tecnológicos, es garantizar que tenga un correcto funcionamiento toda la infraestructura tecnológica necesaria para poder llevar a cabo las pruebas, asegurando que todos los dispositivos utilizados, tanto de software como de hardware, tengan un buen desempeño de todas sus funciones.

4.1.1 Software Utilizados

- **Linksys One:** es una herramienta para el monitoreo de cámaras, específicamente las correspondientes a la Serie Business del fabricante Cisco Systems. Dispone de tres módulos integrados que permiten monitorear, grabar y visualizar las grabaciones. Adicionalmente posee una interfaz muy intuitiva que permite agregar una cámara fácilmente, para posteriormente ser visualizada en el modulo de monitoreo. Este software solo dispone de una versión comercial, la cual se utilizó para el ambiente de pruebas.

- **Wireless Control Systems (WCS):** es una herramienta que provee Cisco Systems, que está disponible para Windows y Linux. Su función principal es gestionar redes inalámbricas y brindarle a los administradores de red facilidades como planificar, monitorear, generar reportes, entre otras, de la plataforma inalámbrica. La versión que se utilizó para realizar las pruebas fue la 6.0.132.0 y se instaló bajo el sistema operativo Windows Server 2003.

4.1.2 Instalación del componente Linksys One

La instalación del componente Linksys One consistió en los siguientes pasos:

1. Al insertar el CD donde se encuentra el software, la primera pantalla que se presenta es la que se muestra en la Figura 4.1, posterior a esto hacer click en Install Viewer & Recorder Utility.

2. En la Figura 4.2 se muestra la pantalla de bienvenida del InstallShield Wizard, para dar inicio a la instalación hacer click en *Next*.

Figura 4.1: Pantalla de inicio Linksys One.

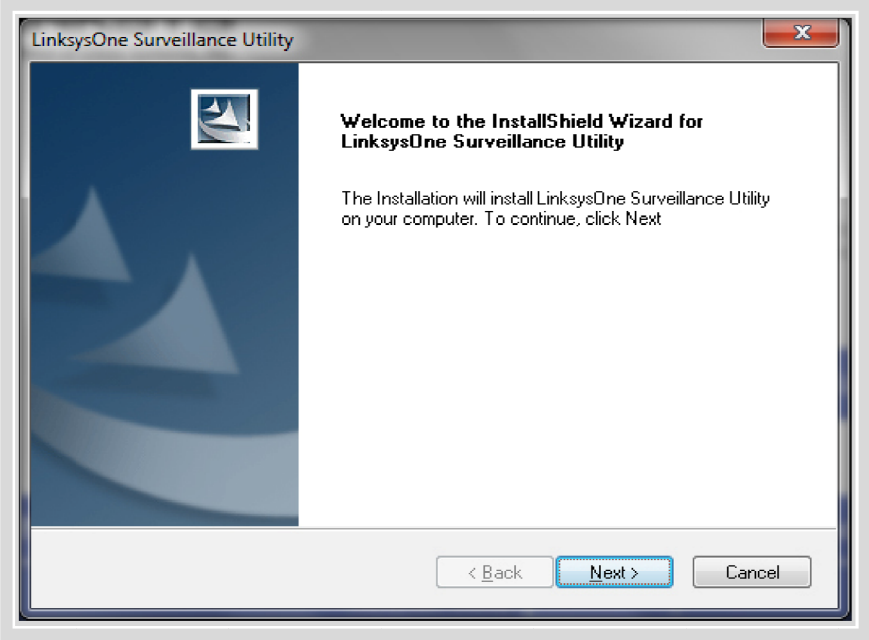


Figura 4.2: Pantalla de bienvenida para la instalación de Linksys One.

3. Una vez presentada la pantalla de bienvenida, se procede a seleccionar la ruta donde se almacenara el Linksys One, como se muestra en la Figura 4.3.

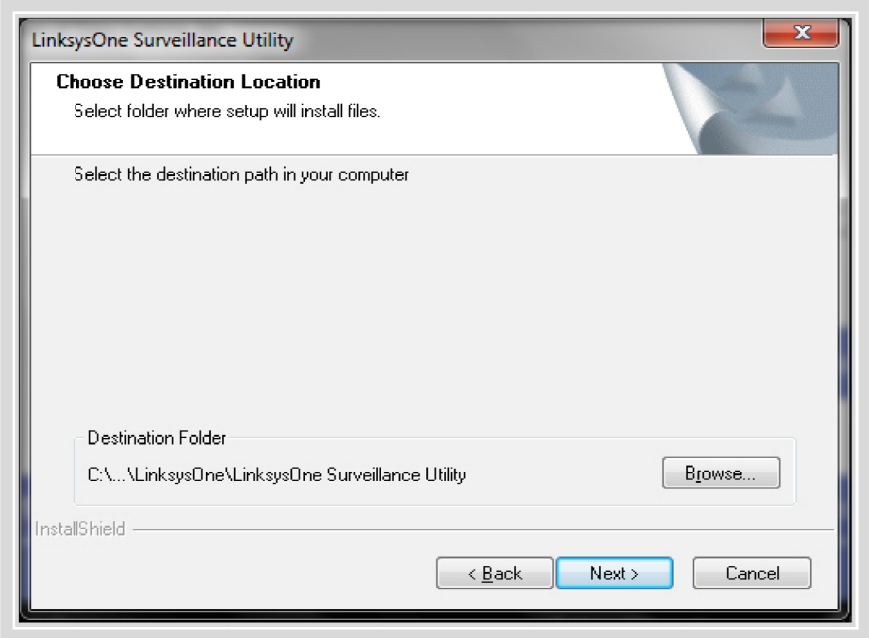


Figura 4.3: Pantalla de selección de ruta.

4. En la Figura 4.4, se muestra el estatus de la instalación del software Linksys One.

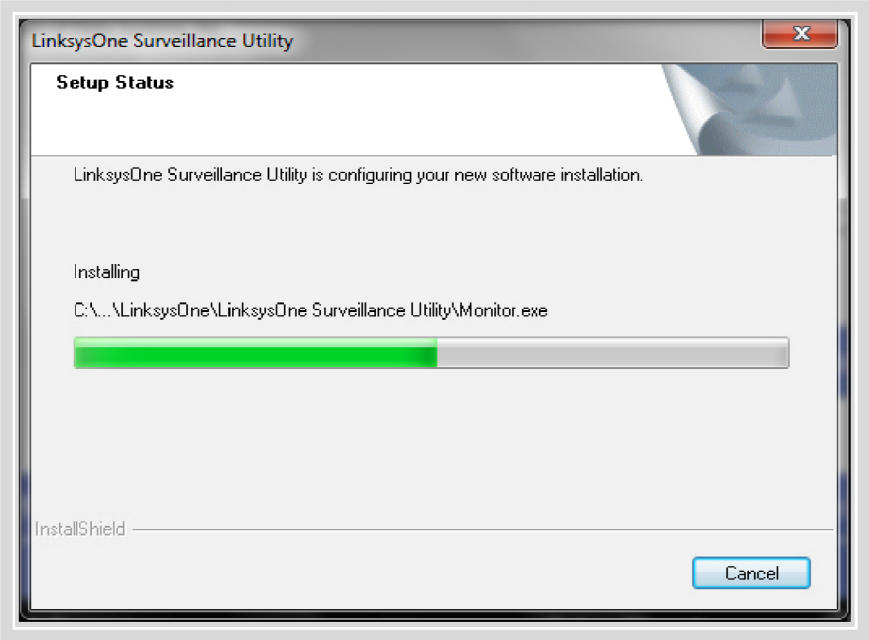


Figura 4.4: Pantalla de selección de ruta.

5. Una vez terminada la instalación del software, se muestra la pantalla de finalización del InstallShield Wizard, como se observa en la Figura 4.5.

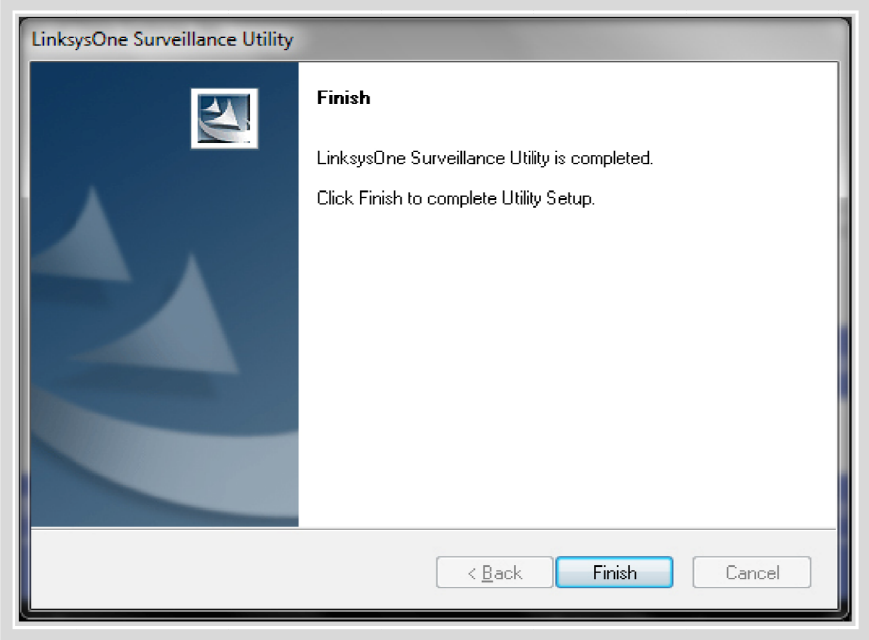


Figura 4.5: Pantalla de selección de ruta.

6. Una vez instalado el software aparece la siguiente pantalla, como se muestra en la Figura 4.6, la cual se utilizará para observar lo que las cámaras están monitoreando.

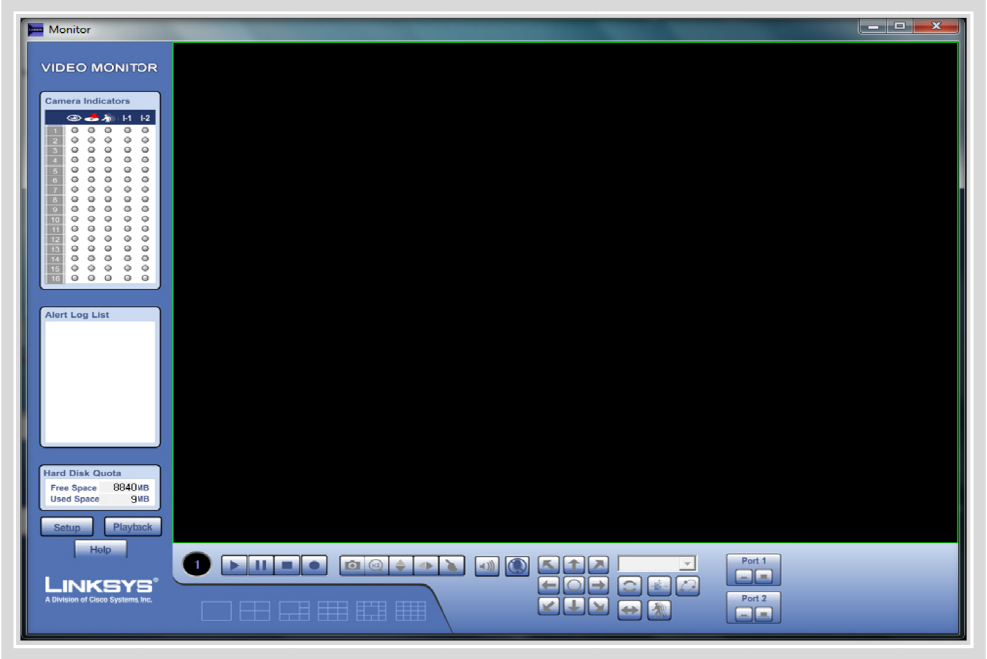


Figura 4.6: Pantalla de monitoreo.

7. En la Figura 4.7, se observa la configuración de la cámara donde específicamente se muestra, la dirección IP, el Local ID, nombre de la cámara, entre otras.

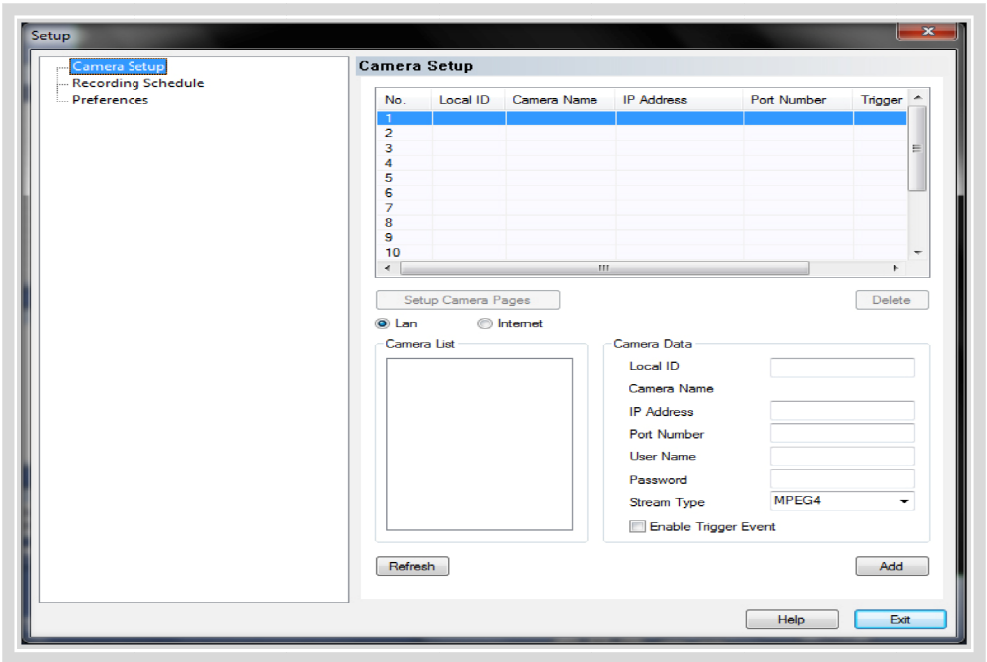


Figura 4.7: Pantalla de configuración.

8. Posteriormente configurada la cámara, debemos volver a la pantalla principal, la que se observa en la Figura 4.8 y hacer click en *Click Here to Start* para iniciar el programa.

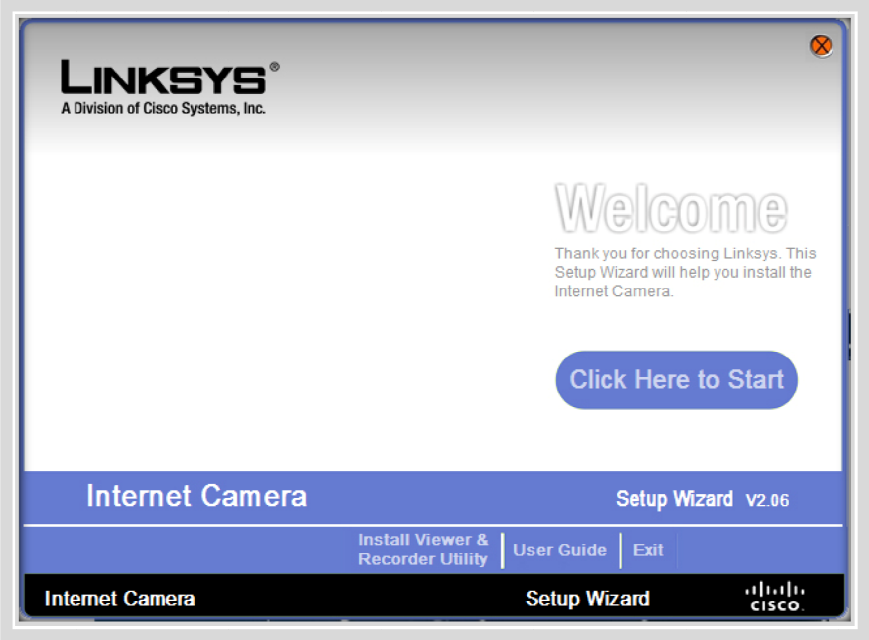


Figura 4.8: Pantalla de inicio Linksys One.

9. En la Figura 4.9, se observa el proceso en el que el software detecta la cámara configurada previamente.

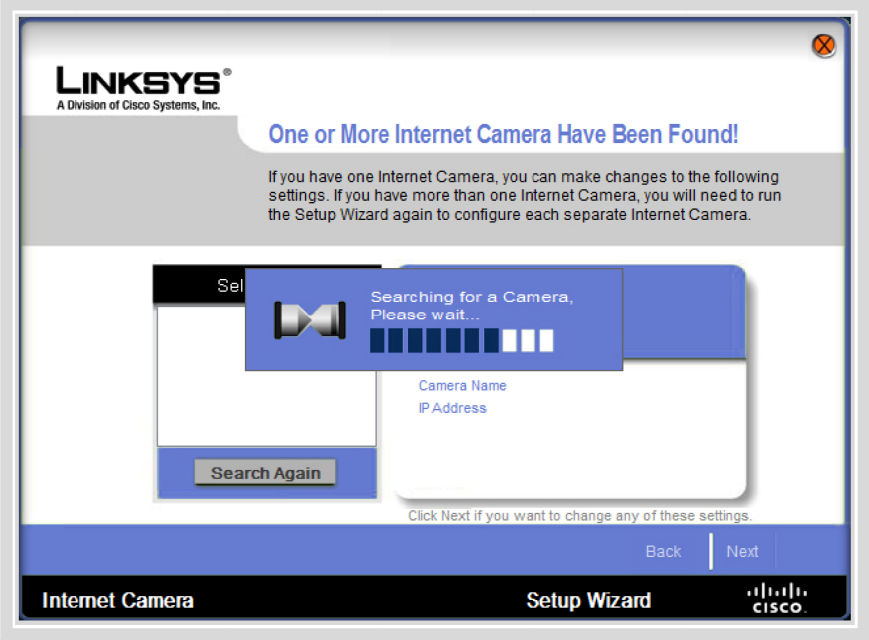


Figura 4.9: Pantalla de búsqueda.

10. Una vez detectada la cámara, como se muestra en la Figura 4.9 podemos observar las características propias de la misma.

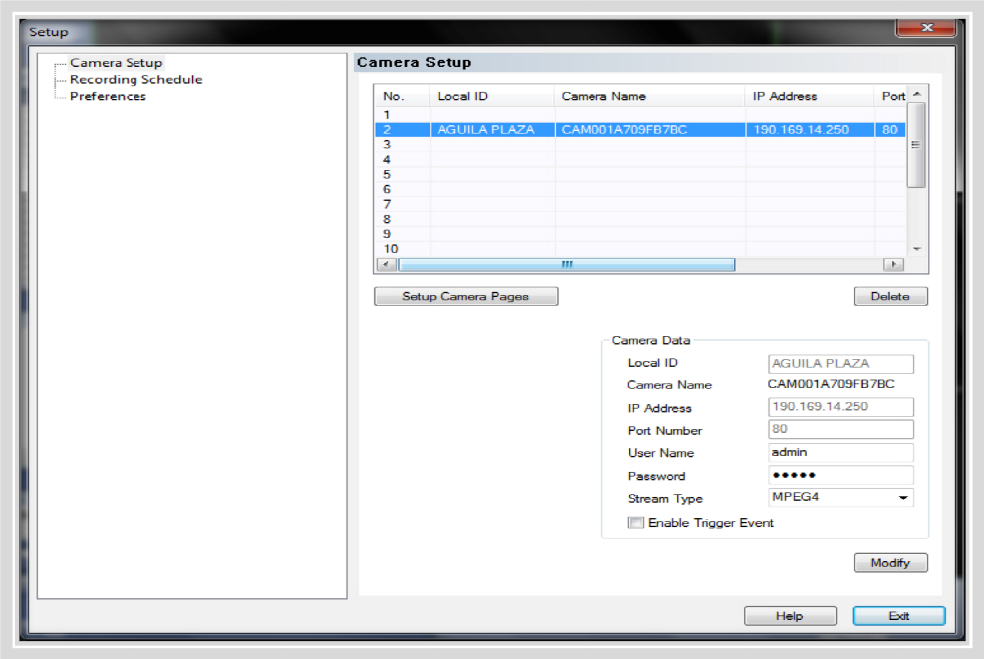


Figura 4.10: Pantalla de configuración.

4.1.3 Instalación del WCS

El WCS fue el software utilizado para verificar que el Edificio el Rectorado, la Plaza Cubierta y el Complejo Cultural Aula Magna, estén dotados de una excelente calidad de señal inalámbrica, para que de esta manera se asegure el correcto desempeño de la solución de videovigilancia. Para su instalación se realizaron los siguientes pasos:

1. La instalación de WCS se llevo a cabo en un servidor, que cuenta con el Sistema Operativo Windows 2003 Server. La versión sobre la cual se realizaron las pruebas corresponde a la 6.0.132.0. La Figura 4.11 muestra la pantalla de introducción a la instalación del WCS. Para continuar con el proceso de instalación hacer click en el botón Next.

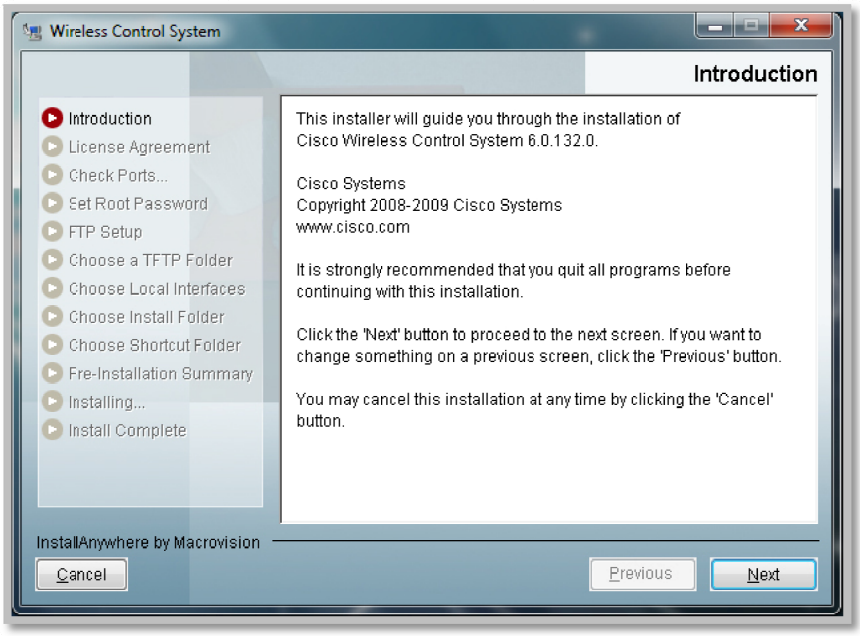


Figura 4.11: Pantalla de introducción.

2. Del mismo modo en la Figura 4.12, aparece el acuerdo de licencia, para continuar con el proceso de instalación hacemos click en Next, sino se está de acuerdo con el contrato se cancela la instalación haciendo click en el botón de Cancel.

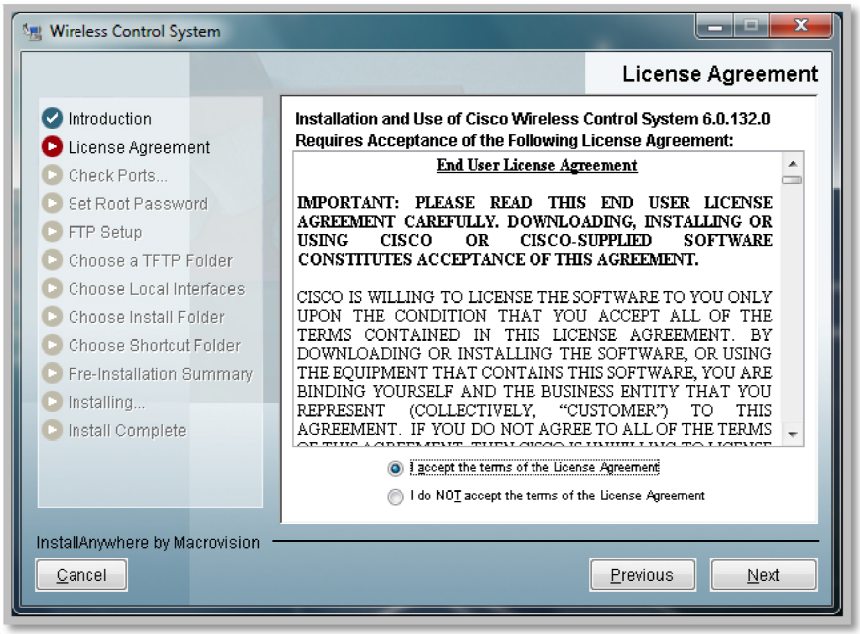


Figura 4.12: Pantalla de acuerdo de licencia.

3. Una vez aceptado el acuerdo de licencia, se selecciona el modo de instalación del WCS, ya sea secundario o primario. La instalación realizada fue modo primary WCS server, como se muestra en la Figura 4.13.

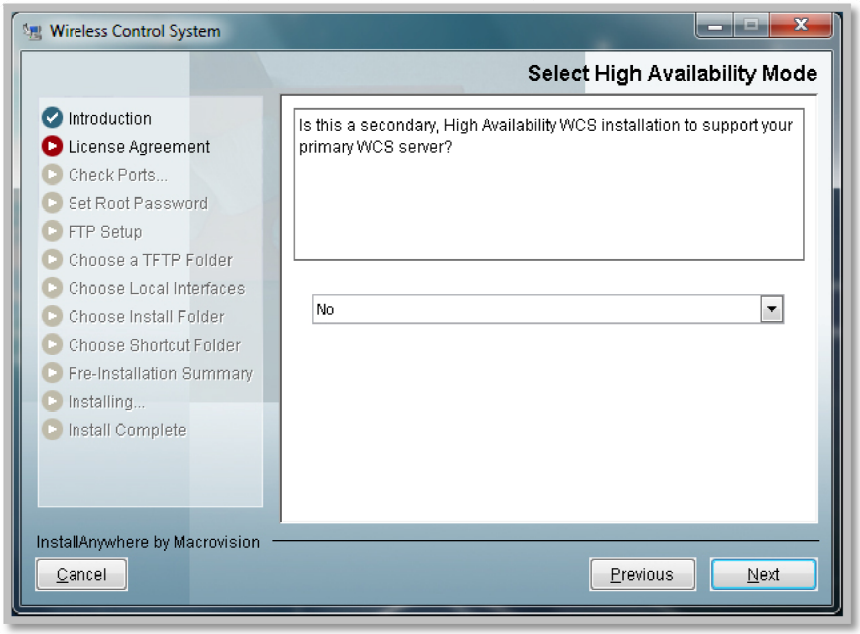


Figura 4.13: Pantalla de modo de instalación.

4. La Figura 4.14 muestra el chequeo de puertos, y por defecto esta seleccionado el puerto 80 para http, el 443 para https y el 8082 para el Health Monitor.

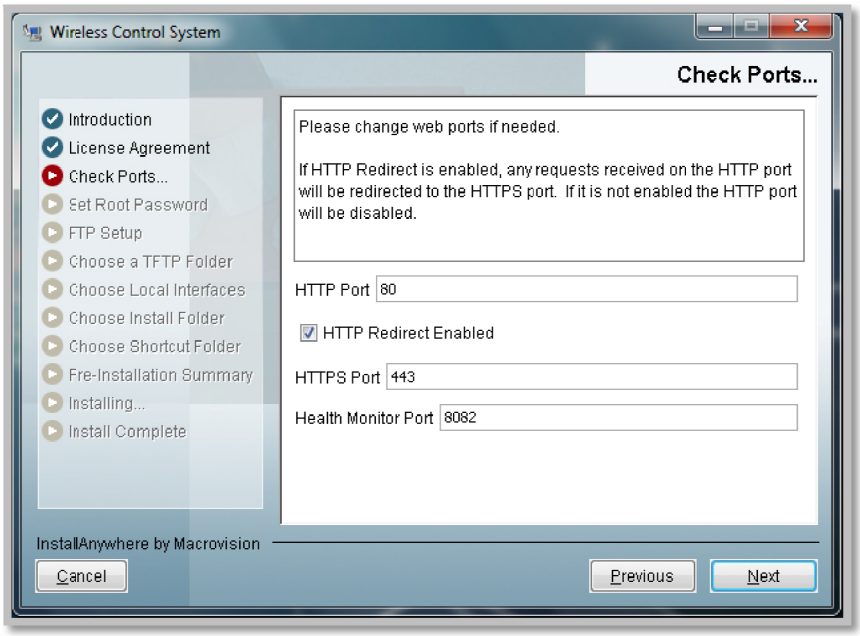


Figura 4.14: Pantalla de chequeo de puertos.

5. Seguidamente, se procede a introducir el password del root y la confirmación de dicho password, como se muestra en la Figura 4.15 y en la Figura 4.16.

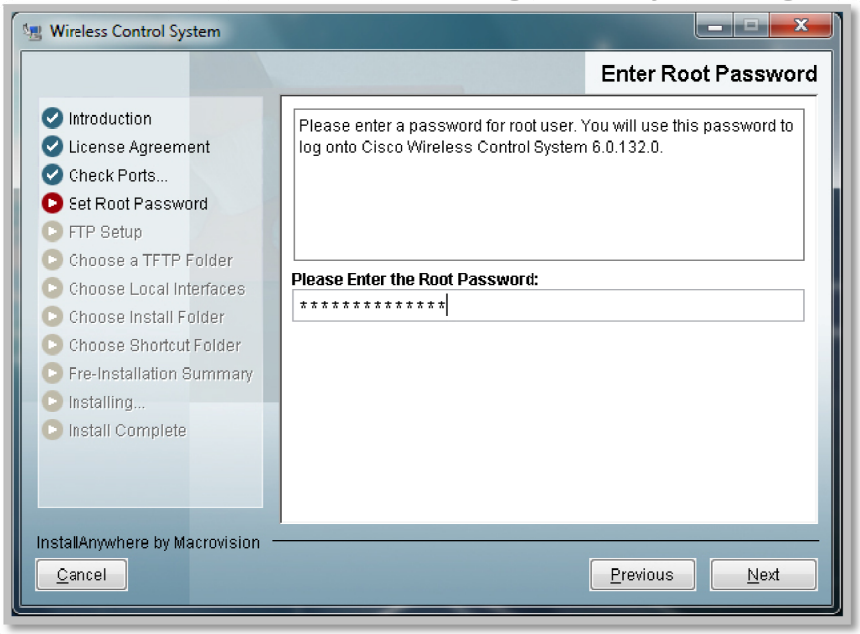


Figura 4.15: Pantalla de entrada para el password del root.

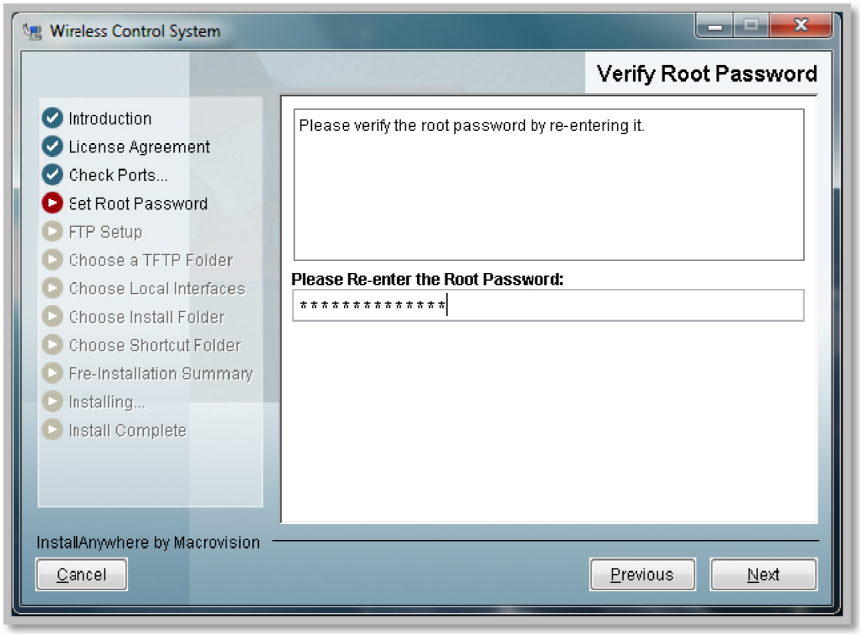


Figura 4.16: Pantalla de verificación del password del root.

6. Una vez colocado el password del root, se procede a colocar el password del root FTP Server, como se muestra en las Figuras 4.17 y 4.18.

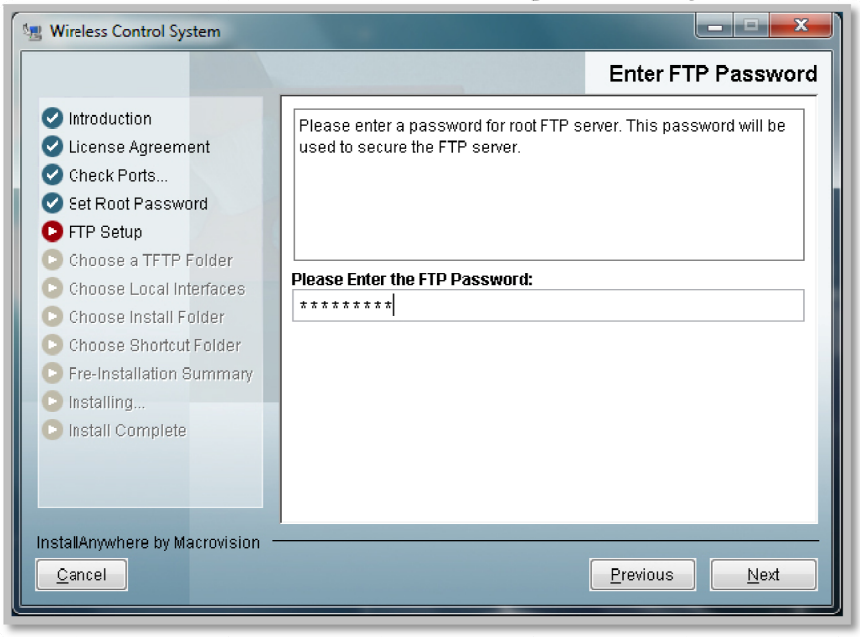


Figura 4.17: Pantalla de entrada para el password del root FTP.

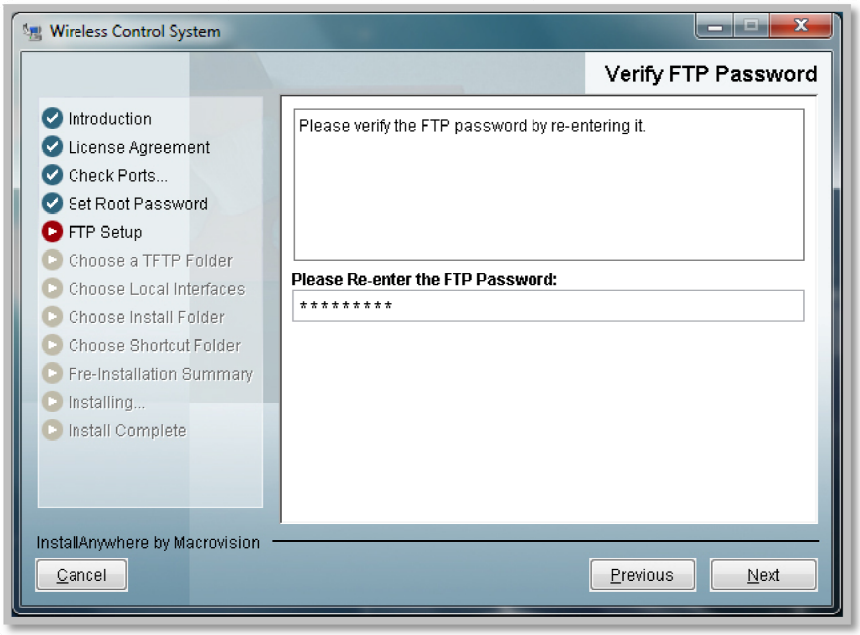


Figura 4.18: Pantalla de verificación del password del root FTP.

7. La Figura 4.19 y 4.20 muestra, las carpetas donde se van a almacenar todos los archivos del FTP y del TFTP.

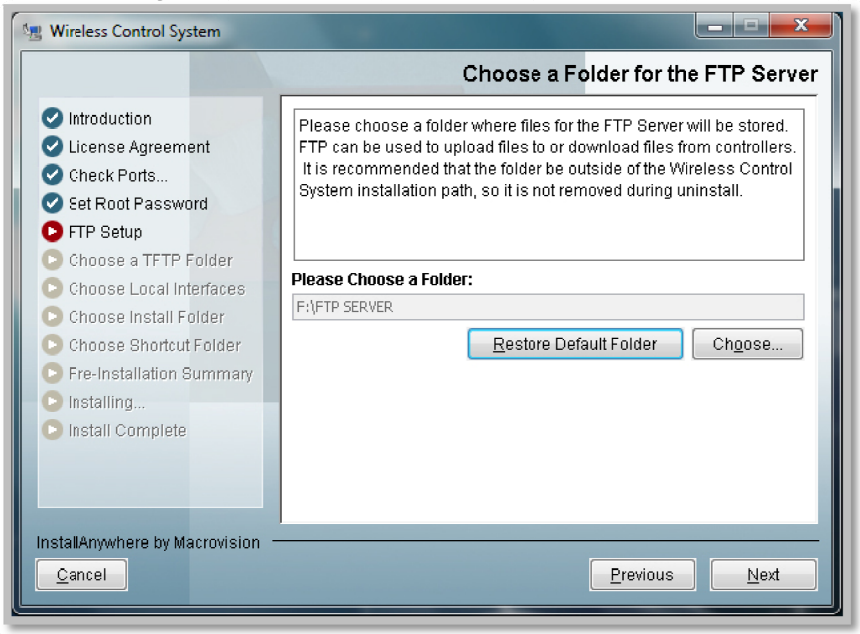


Figura 4.19: Pantalla de selección de carpeta para el FTP.

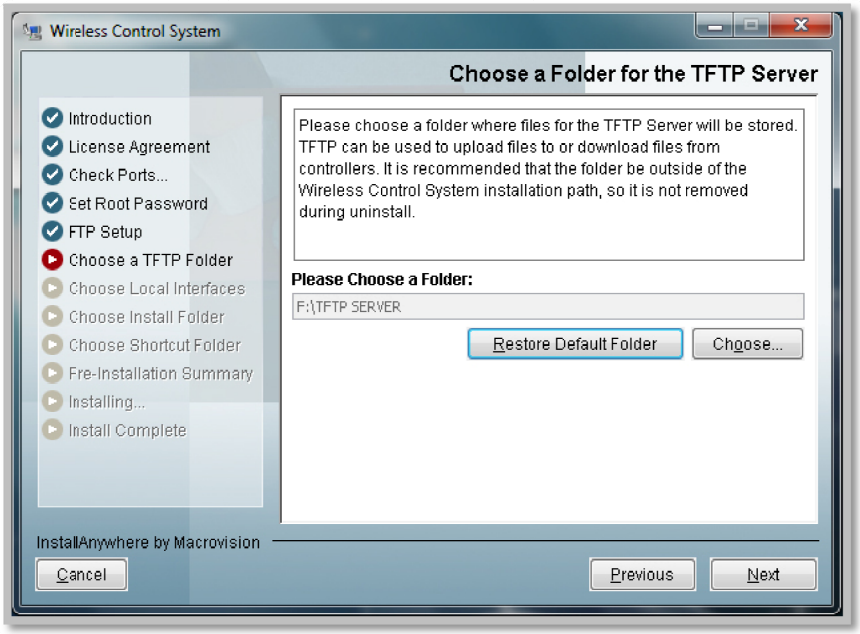


Figura 4.20: Pantalla de selección de carpeta para el TFTP.

8. Posteriormente, en la Figura 4.21, se muestra la selección de las interfaces para la comunicación con el controlador y el FTP.

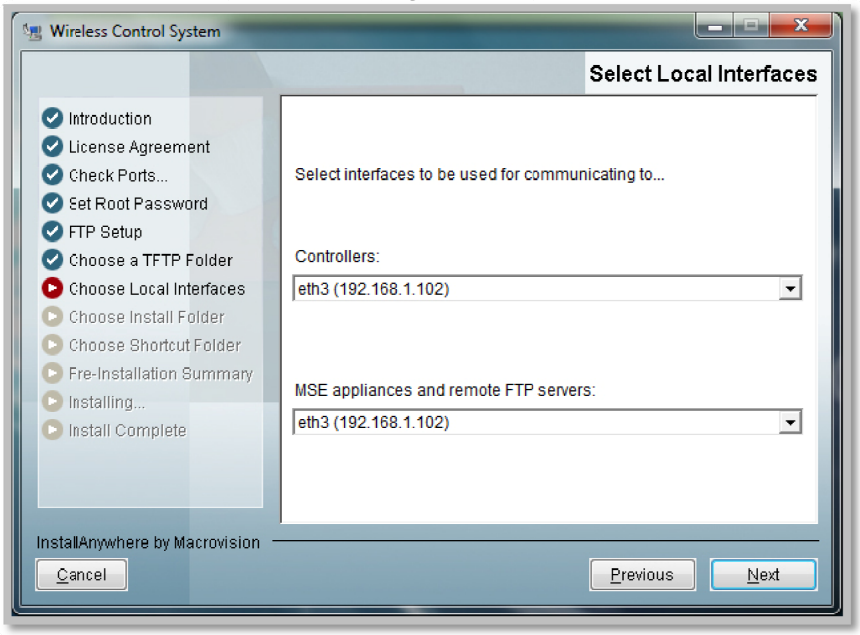


Figura 4.21: Pantalla de selección de interfaces.

9. La Figura 4.22, muestra la carpeta donde se va a realizar la instalación del Software WCS.

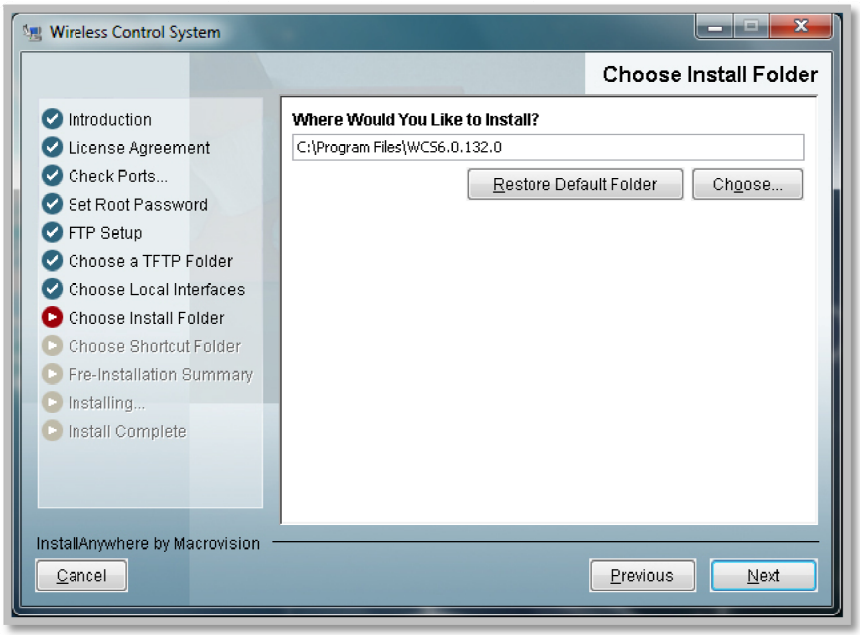


Figura 4.22: Pantalla de selección de carpeta.

10. Seguidamente, se selecciona si se quiere que los iconos del programa instalado se muestren en un solo grupo o en un grupo ya existente, se recomienda seleccionar que se muestren en un solo grupo, como se muestra en la Figura 4.23.

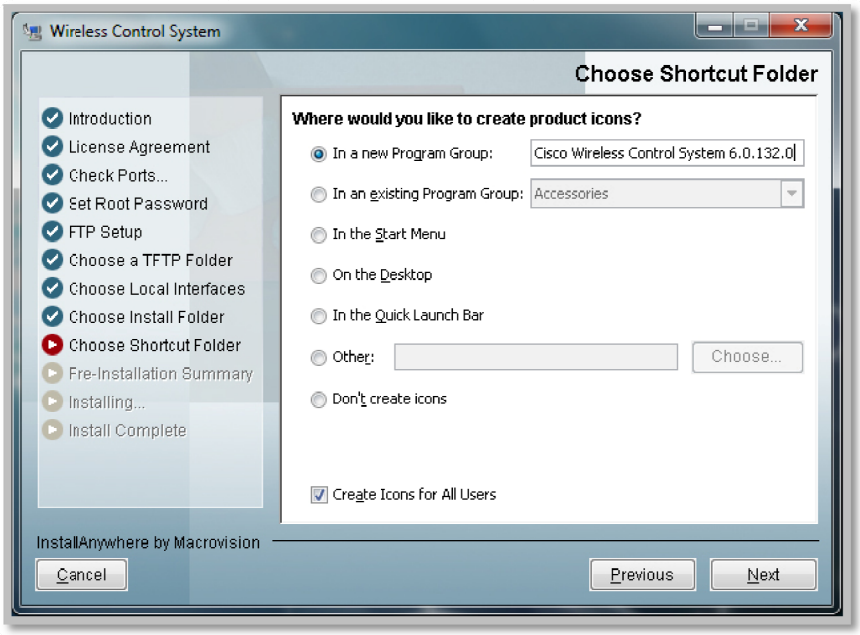


Figura 4.23: Pantalla de shortcut folder.

11. La Figura 4.24, muestra un resumen de la instalación del WCS, para iniciar la instalación hacer click en Install.

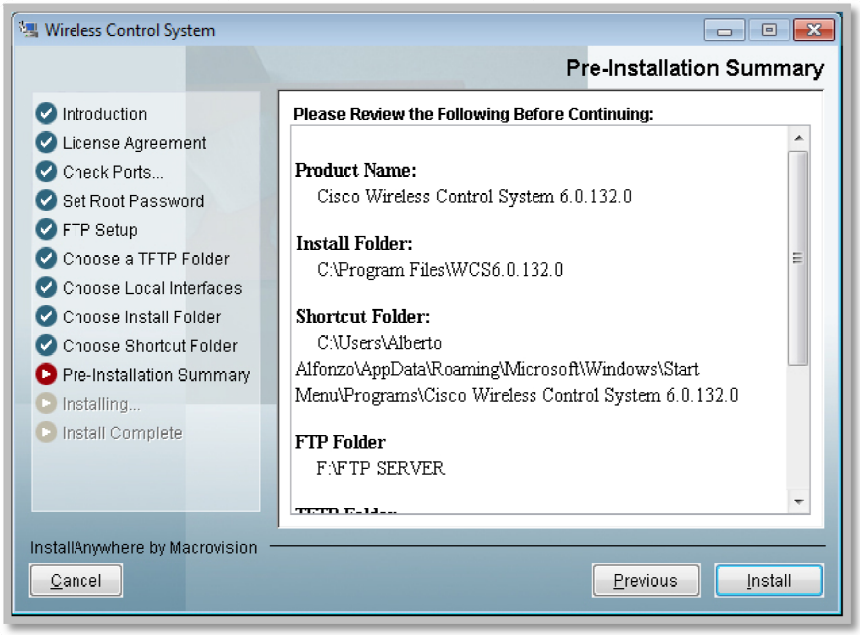


Figura 4.24: Pantalla de resumen de la instalación.

12. Se muestra el proceso de instalación del programa WCS, como se observa en la Figura 4.25.

Figura 4.25: Pantalla de instalación.

13. Una vez terminado el proceso de instalación, se procede a iniciar el servicio WCS, como se muestra en la Figura 4.26, y seguidamente se debe de ir a inicio y buscar el grupo llamado WCS y hacer click en Start WCS para iniciar el servicio, se levanta el Health Monitor y comienzan a ejecutarse una serie de servicios como se muestra en la Figuras 4.27 y 4.28.

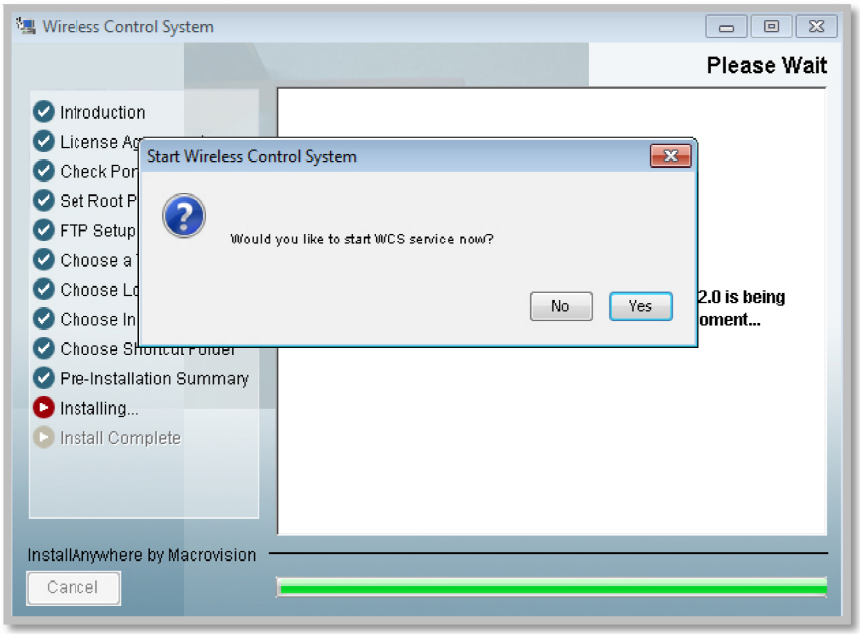


Figura 4.26: Pantalla de inicio del servicio WCS.

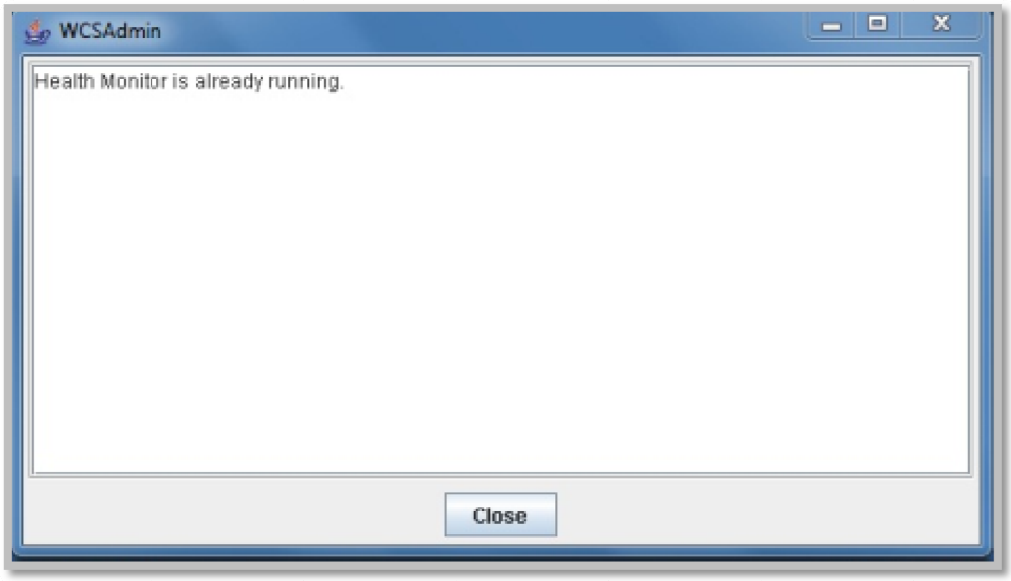


Figura 4.27: Pantalla de inicio del Health Monitor.

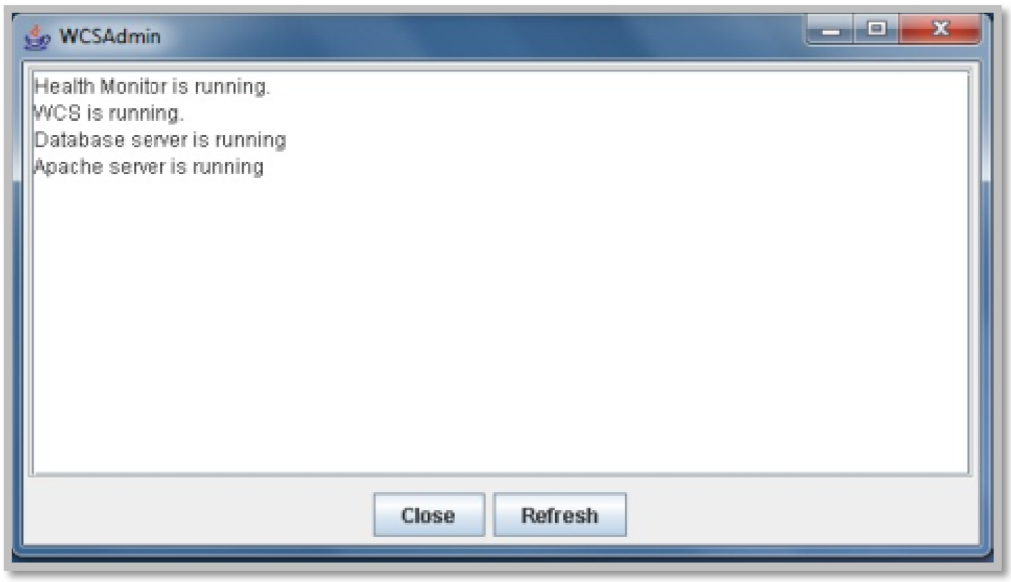


Figura 4.28: Pantalla de inicio de servicios.

4.1.4 Configuración de las cámaras de videovigilancia WVC2300

En todas las pruebas que se llevaron a cabo para monitorear los puntos críticos de cada una de la áreas de estudio, se utilizó la cámara Linksys (Cisco), modelo WVC 2300, Wireless-G Business Internet Video Camera with Audio.

Lo primero que se realizó fue la configuración básica de las cámaras, la cual se divide en 3 grupos:

- **Configuración del dispositivo:** aquí se encuentran los parámetros que conciernen al nombre que va a tener la cámara en la red, alguna descripción

que el usuario quiera colocar para tener una referencia más específica de la cámara. Del mismo modo, en este apartado se realiza la configuración de la zona horaria, para que luego se puedan aplicar reglas de activación y desactivación de alarmas, grabaciones previamente programadas, entre otras.

- **Configuración de red:** el primer parámetro configurable, es para elegir si la cámara va a tener una dirección IP fija o la va a obtener por DHCP (*Dynamic Host Configuration Protocol*). En caso de colocarle una dirección IP fija, los siguientes parámetros que se tienen que configurar son: la máscara de sub red, la puerta de enlace y los DNS (*Domain Name Server*) tanto primario como secundario. En caso contrario, si la opción es obtener la dirección IP por DHCP, el dispositivo va a obtener los parámetros de configuración anteriormente mencionados automáticamente.

- **Configuración inalámbrica:** aquí principalmente se configura el SSID de la red inalámbrica a la que se va a conectar la cámara, se selecciona el tipo de red (infraestructura o Ad-hoc), y por último se selecciona el tipo de seguridad que posee la red inalámbrica (WEP, WPA, WPA2).

En la Figura 4.29 se muestra la configuración básica de las cámaras WVC2300.

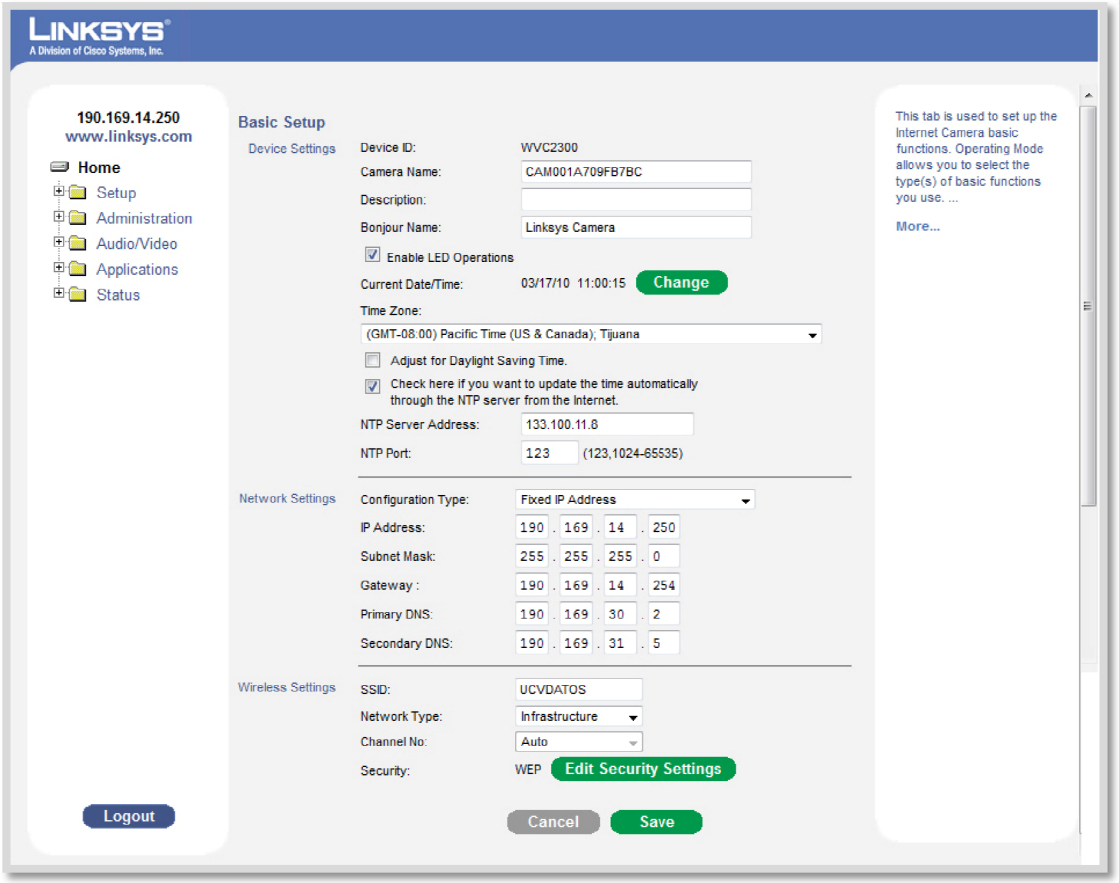


Figura 4.29: Configuración básica de la cámara WVC2300.

Una configuración que es de suma importancia, es la de QoS utilizando DiffServ, para que todos los paquetes se marquen con una etiqueta específica, sean atendidos con la mayor prioridad, para asegurar que no existan perdidas de paquetes en la red.

Para optimizar la diversidad de paquetes que transitan por la red, se emplean los siguientes mecanismos [16]:

- **Identificación del tráfico:** para poder priorizar cierto tipo de tráfico sobre otro se requiere un proceso previo de identificación. Los mecanismos habituales para realizar esta identificación son: por dirección MAC, tipo de protocolo de transporte (TCP o UDP), por campo DSCP o por número de puerto TCP/UDP.

- **Marcado de paquetes**: para permitir que los switchs puedan manejar de forma diferenciada los distintos tipos de tráfico, es necesario que los paquetes sean marcados con una determinada etiqueta, esto se logra marcando el campo DSCP del paquete, de esta forma los switchs podrán tratar de manera diferente a los paquetes en relación a las prioridades.

- **Asignación de recursos**: esta asignación se limita a la reserva de espacio dentro de los buffers internos de los switchs y al uso de algoritmos para optimizar la transmisión de los paquetes.

La configuración avanzada de la cámara WVC2300, ofrece la posibilidad de habilitar la opción de QoS, seleccionando si es para tráfico de voz o video. Este mecanismo de QoS se basa en DiffServ. En la Figura 4.30, se puede observar la configuración avanzada de la cámara.

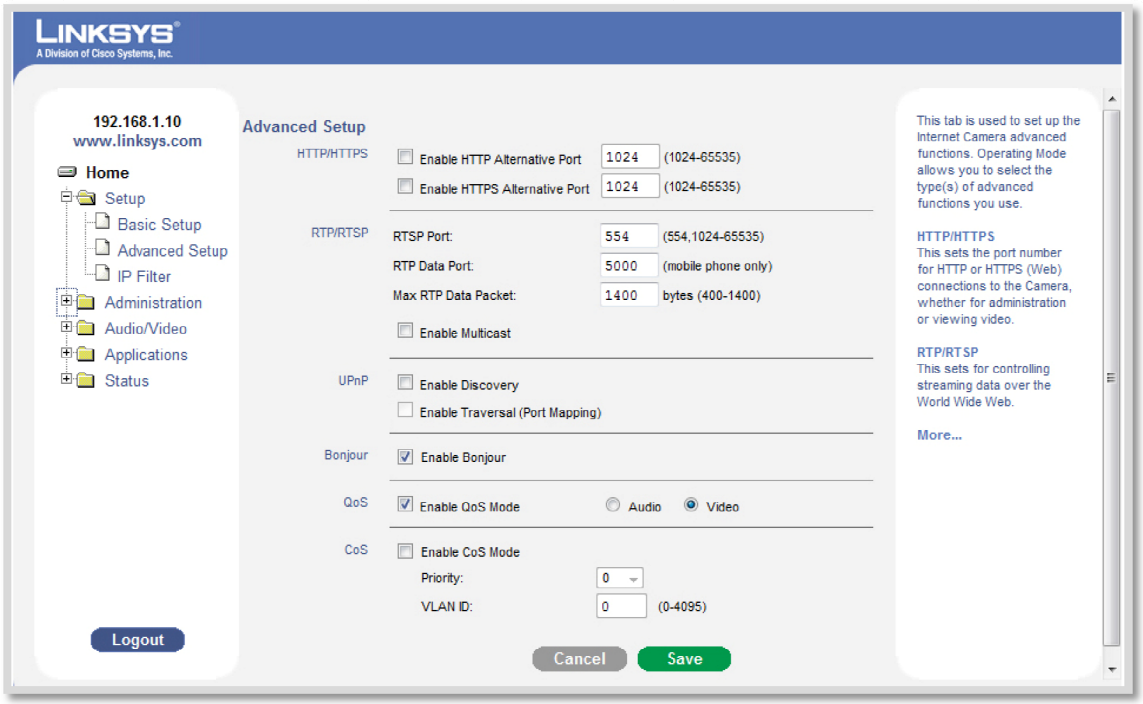


Figura 4.30: Configuración avanzada de la cámara WVC2300.

Gran parte de la configuración del dispositivo, específicamente aquella no relacionada directamente con este diseño, permaneció por defecto como viene de fábrica. Solo se agregaron o modificaron fragmentos de la configuración relevantes para la red WLAN de la UCV.

Para verificar que la opción de QoS seleccionada en la configuración de la cámara se hizo correctamente, se realizaron unas capturas del tráfico que circulaba por la red con el software *Wireshark*[12], donde se pudo evidenciar que se estaban marcando correctamente los paquetes que correspondían a transmisiones de video. En la Figura 4.31, se muestra la captura del tráfico de la red sin el marcado de paquetes, es decir, con la configuración predeterminada que trae la cámara. Seguidamente en la Figura 4.32, se muestra una captura del tráfico de la red, luego de haber seleccionado la opción de QoS.

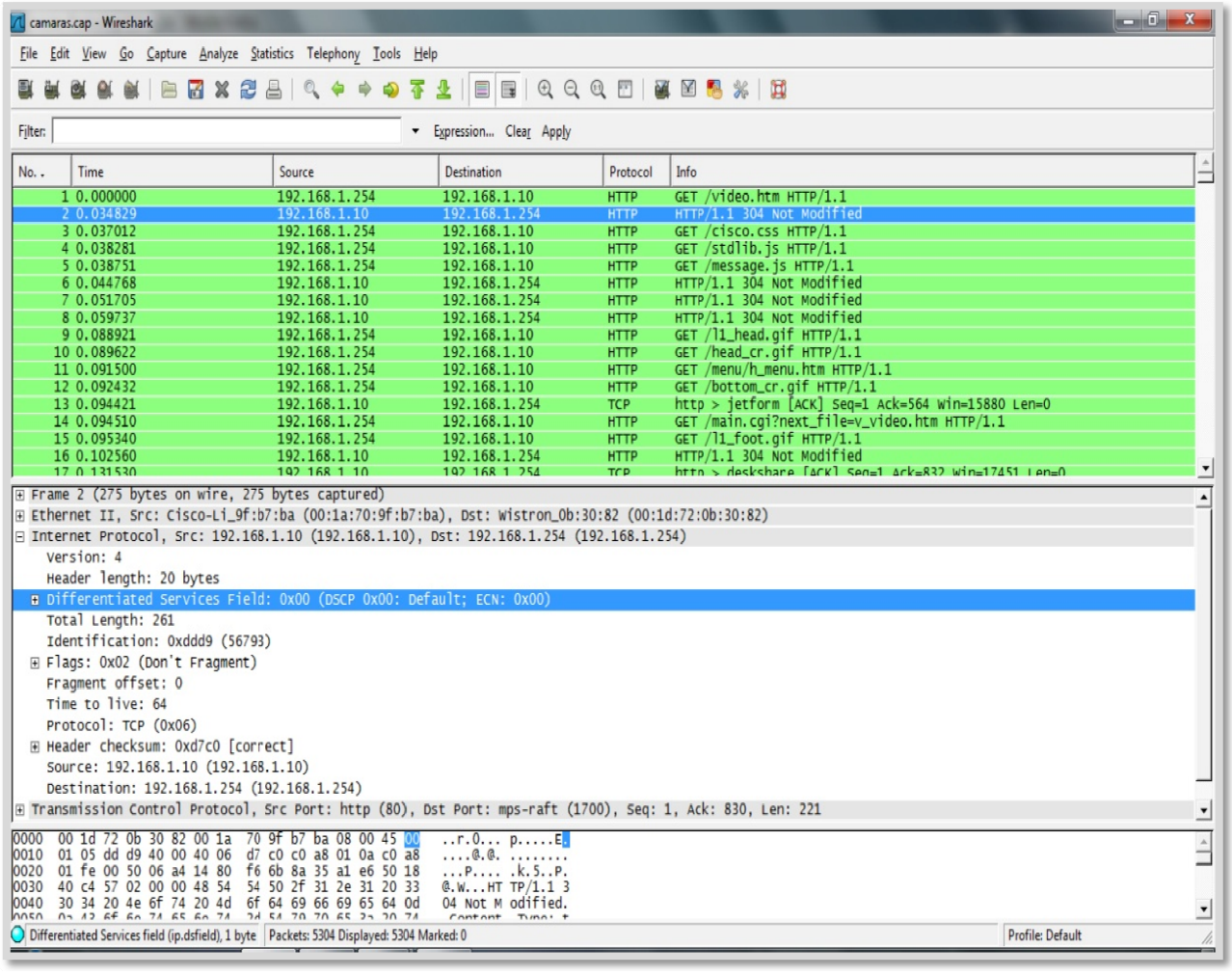


Figura 4.31: Captura del tráfico sin QoS.

[12] Analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones.

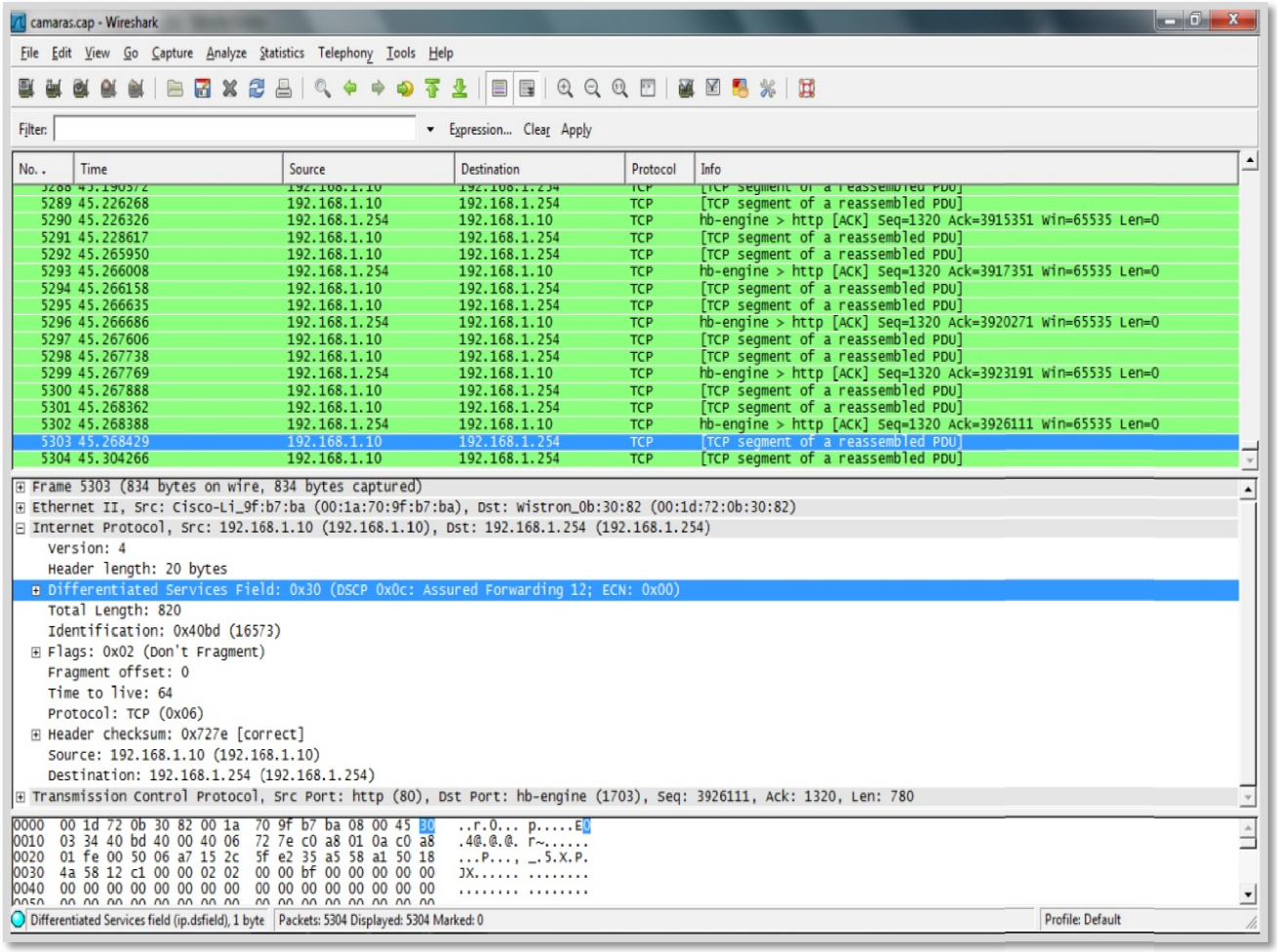


Figura 4.32: Captura del tráfico con QoS.

4.1.5 Configuración de QoS del AP Cisco Aironet 1130AG

A continuación se muestra la Figura 4.33, donde se aplican las políticas de QoS que corresponden a la configuración del AP utilizado para realizar las pruebas de conectividad de los dispositivos inalámbricos a la WLAN de la UCV.

Al configurar QoS en el AP Cisco Aironet 1130AG, lo que se busca es crear una política de QoS para que de acuerdo a unas listas de control acceso previamente definidas en el switch principal, se re-marquen los paquetes de acuerdo a cierta prioridad establecida en dichas listas. Este tipo de configuración viene dado por normativas y reglas de la DTIC, en cuanto a los tráficos de paquetes que transitan por la red.

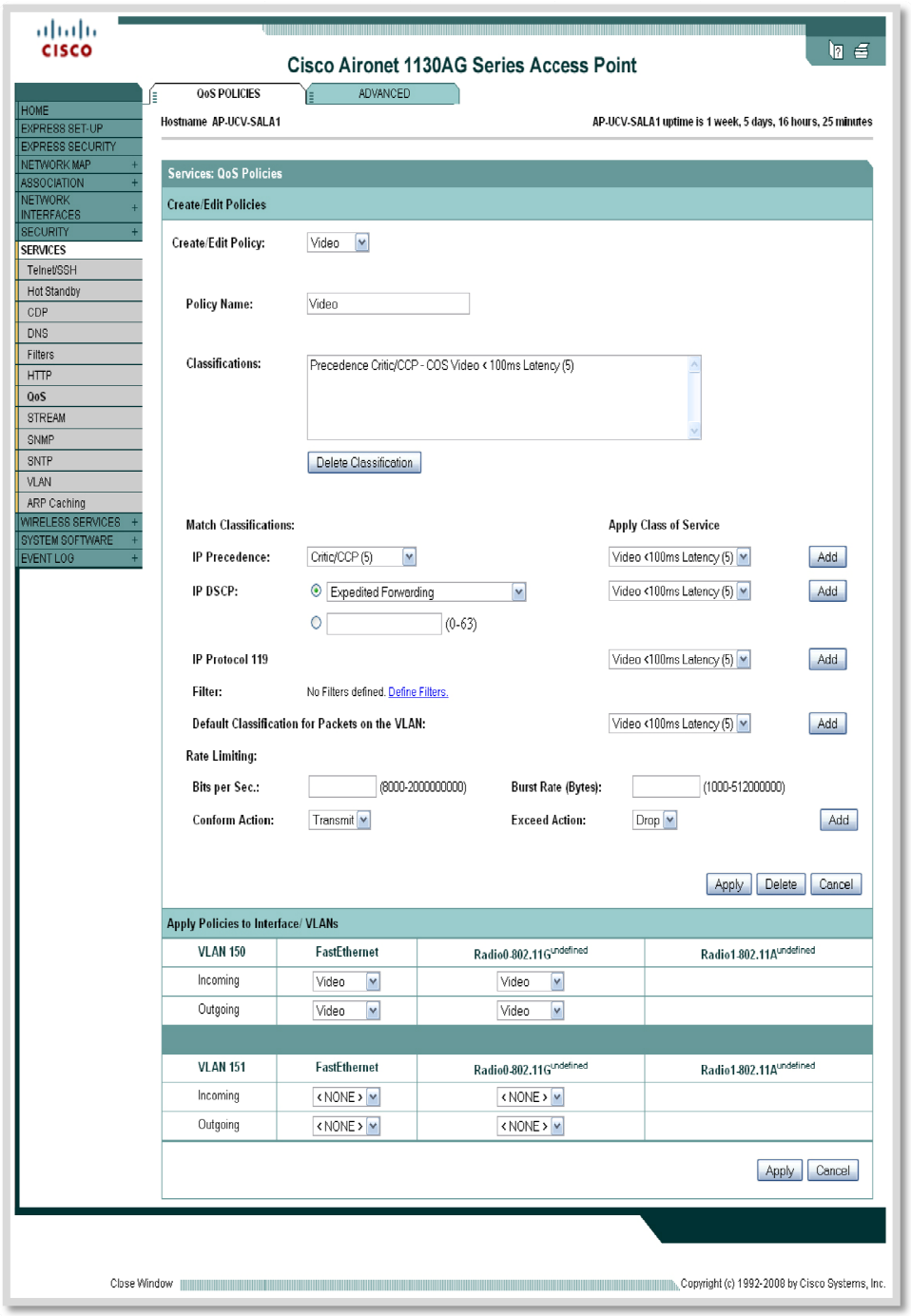


Figura 4.33: Configuración de QoS en el AP Cisco Aironet 1130AG.

La Figura 4.34, muestra las líneas de código que se generan al realizar la configuración vía interfaz grafica.

```
class-map match-all _class_Data0
   match ip precedence 0
class-map match-all _class_Video0
   match ip precedence 5
!
!
policy-map Video
   class_class_Video0
   set cos 6
policy-map Data
   class_class_Data0
   set cos 0
!
interface Dot11Radio0.150
  service-policy input Video
  service-policy output Video
!
interface FastEthernet0.150
  service-policy input Video
  service-policy output Video
```

Figura 4.34: Configuración de QoS en el AP vía líneas de comando.

Una vez creadas las políticas de QoS, para evitar que la interferencia producida cuando múltiples dispositivos inalámbricos se conecten al mismo AP, afecte directamente al tráfico generado por la solución de videovigilancia, existe la posibilidad de reservar un ancho de banda específico tanto en la interfaz inalámbrica como en la Fastethernet para el tráfico generado por las cámaras, asegurando de esta forma que las transmisiones de los paquetes de video no se vean afectadas por otro tipo de tráfico.

La Figura 4.35, muestra los comandos utilizados para reservar el ancho de banda específico para las transmisiones de los paquetes generados por la solución de videovigilancia.

```
AP-UCV#config t
AP-UCV(config)#policy-map Video
AP-UCV(config-pmap)#class _class_Video0
AP-UCV(config-pmap-c)#bandwidth percent 20
```

Figura 4.35: Configuración de reservación de ancho de banda.

4. 2 Escenarios de pruebas

En este apartado se plantean diversos escenarios de pruebas que validan la propuesta de diseño de una solución de videovigilancia soportado en cámaras IP con tecnología IEEE 802.11. Cada uno de los escenarios plateados busca verificar el correcto funcionamiento de los dispositivos inalámbricos, del mismo modo se presentará un breve análisis de los resultados obtenidos.

La topología física del ambiente de pruebas, consistió de dos switchs Catalyst 2960 con IOS 12.2, tres computadoras con sistema operativo Windows XP (Alpha, Beta y Gamma), y una cámara modelo WVC 2300 (Delta), las conexiones de los equipos fue a 100 Mbps, como se muestra en la Figura 4.36.

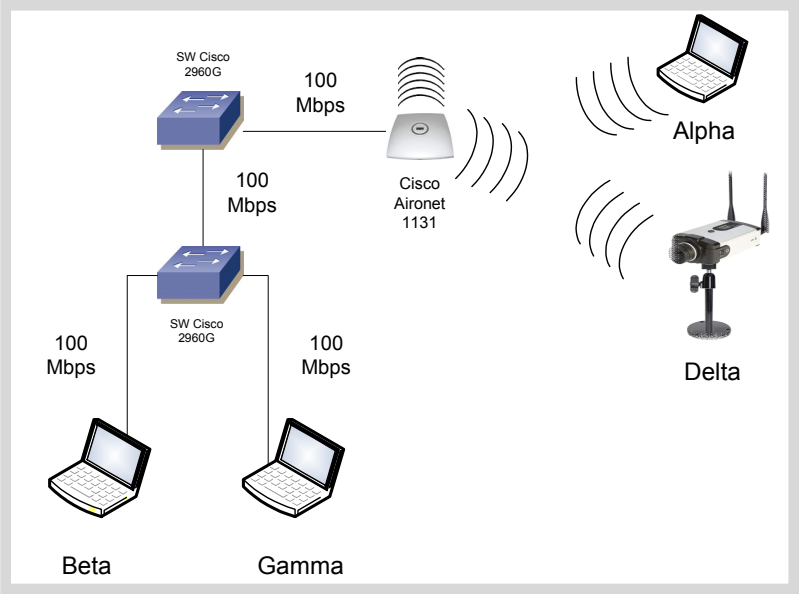


Figura 4.36: Topología del ambiente de pruebas.

En la topología de la Figura 4.36, la computadora Alpha, donde se encuentra instalado el *Wan Killer*[13], genera 97,8 Mbps aproximadamente de tráfico, el cual va dirigido a la computadora Beta por la VLAN (*Virtual Local Area Network*) de datos. Del mismo modo, la cámara Delta genera 2,2 Mbps de tráfico de video aproximadamente, dirigido hacia Gamma por la VLAN de video. Como los enlaces son de 100 Mbps, con la cantidad de tráfico que genera Alpha y Delta se garantiza que el enlace estará totalmente congestionado, para posteriormente realizar pruebas sin aplicar QoS y aplicando QoS.

[13] Generador de tráfico para la WAN.

4.2.1 Escenario de prueba 1: Evaluación del tráfico de videovigilancia sin aplicar QoS.

- **Descripción del escenario:** en este escenario se comprueba que si no se realiza la configuración de QoS para darle cierta prioridad al tráfico, va a existir una gran probabilidad que se presenten características que influyan directamente en la entrega no segura o en la pérdida total de los paquetes transmitidos.

- **Ejecución de la prueba:** esta prueba está basada en la ejecución de los siguientes pasos:

1. Al momento de realizar la configuración avanzada de la cámara usada para las pruebas, modelo WVC 2300 Wireless-G Business Internet Video Camera with Audio, no se realizó el marcado de QoS, por lo tanto los paquetes de video que genere la cámara viajaran sin ningún tipo de prioridad.

2. La resolución de las cámaras con las cuales se realizaron las pruebas quedo establecida en 640 x 480.

3. Al realizar la configuración del AP usado, modelo Cisco Aironet 1130AG, no se estableció ninguna política de QoS para el marcado y envío de paquetes a la red.

4. Se realizó la conexión de la cámara a la computadora, y se levanto el software de monitoreo para comenzar la grabación de un video con movimiento constante. Los paquetes comienzan a transitar por la red, sin ningún tipo de marcado que indique que viajan con QoS, al llegar al switch, dichos paquetes son atendidos sin ningún tipo de prioridad y son tratados como paquetes de datos, lo cual no da ninguna garantía que no ocurran pérdidas de paquetes durante la transmisión.

5. Se utilizó el software *Wan Killer* propiedad de *SolarWinds*, para congestionar el enlace.

6. Se ingreso a la configuración de los dispositivos y mediante la interfaz de línea de comandos, se solicito ver el estatus del puerto, para verificar la cantidad de paquetes perdidos en la transmisión.

- **Resultados obtenidos:** en la Tabla 4.1, se muestran los resultados obtenidos al transmitir paquetes de video sin ninguna política de QoS en los dispositivos involucrados en las pruebas. Se puede observar que ocurre perdida de paquetes, aunque en muy baja escala, pero al tratarse de paquetes de video de la solución de videovigilancia, los paquetes perdidos pueden resultar ser claves. Es importante acotar que al perderse paquetes durante la trasmisión, los mismos no pueden ser reenviados, ya que el video se transmite en tiempo real.

- **Análisis de los resultados:** como se observa en la Tabla 4.1, en este escenario ni la red ni los dispositivos inalámbricos, tiene algún mecanismo de QoS aplicado, es decir, la red solo utiliza el mecanismo de *Best Effort.* Basándose en los resultados obtenidos se observo que el tráfico que se considere crítico en una red, debe recibir algún tipo de atención en particular, para asegurar la entrega de ese tráfico sin que se presente la pérdida que paquetes.

	Paquetes enviados	Paquetes recibidos	Paquetes perdidos	% Paquetes perdidos	Ancho de Banda Promedio
Videovigilancia/Datos	**2270329**	**2270275**	**54**	**0,002 %**	**100 Mbps**

Tabla 4.1: Tráfico de videovigilancia sin QoS.

4.2.2 Escenario de prueba 2: Evaluación del tráfico de videovigilancia aplicando QoS.

- **Descripción del escenario:** en este escenario se comprueba que al aplicar la configuración de QoS en todos los dispositivos involucrados en la pruebas, va a existir una probabilidad mucho menor que hayan perdida de paquetes al realizar la transmisión de los mismos. Según políticas establecidas por la DTIC, se creará una VLAN específica para la transmisión única de paquetes de video, el ancho de banda que maneja esta VLAN en particular queda a potestad única del ente que gestiona las redes dentro de las UCV.

- **Ejecución de la prueba:** esta prueba está basada en la ejecución de los siguientes pasos:

1. Al momento de realizar la configuración avanzada de la cámara usada para las pruebas, modelo WVC 2300 Wireless-G Business Internet Video Camera with Audio, se realizó el marcado de QoS, por lo tanto los paquetes de video que genere la cámara viajaran marcados.

2. La resolución de las cámaras con las cuales se realizaron las pruebas quedo establecida en 640 x 480.

3. Al realizar la configuración del AP usado, modelo Cisco Aironet 1130AG, se establecieron políticas de QoS para el marcado y envío de paquetes a las red.

4. Se realizó la conexión de la cámara a la computadora, y se levanto el software de monitoreo para comenzar la grabación de un video con movimiento constante. Los paquetes que comienzan a transitar por la red viajan marcados, al llegar al AP, el mismo los remarca y los envía al switch, para que sean atendidos y encolados según la marca que posean. La marca que se le coloca al paquete indica si el mismo se considera como tráfico crítico o no, en el caso de las pruebas realizadas, la marca asignada al paquete de video es de gran

prioridad, para dar alguna garantía que no ocurran pérdidas de paquetes durante la transmisión.

5. Se utilizó el software *Wan Killer* propiedad de *SolarWinds*, para congestionar el enlace.

6. Se ingreso a la configuración de los dispositivos y mediante la interfaz de línea de comandos, se solicito ver el estatus del puerto, para verificar la cantidad de paquetes perdidos en la transmisión.

- **Resultados obtenidos:** en la Tabla 4.2, se muestran los resultados obtenidos al transmitir paquetes de video aplicando políticas de QoS en los dispositivos involucrados en las pruebas, lo que da como garantía que no haya pérdida de paquetes durante la transmisión de video.

- **Análisis de los resultados:** en este escenario, tanto la red como los dispositivos inalámbricos, tienen aplicado algún mecanismo de QoS, es decir, al llegar los paquetes a la red, los mismo son encolados y atendidos dependiendo de la prioridad con la que fueron marcados. Apoyándose en los resultados obtenidos, se observo que el tráfico que viaja con alguna marca, recibe una atención en particular, lo que asegura la entrega confiable de los paquetes que se consideren críticos, como es el caso de los paquetes de voz y de video. Es importante acotar, que aunque hay pérdida de paquetes en este escenario, los mismos pertenecen al tráfico de datos.

	Paquetes enviados	Paquetes recibidos	Paquetes perdidos	% Paquetes perdidos	Ancho de Banda Promedio
Datos	**2056321**	**2056248**	**73**	**0,003 %**	**100 Mbps**
Videovigilancia	**105437**	**105437**	**0**	**0%**	**2,2 Mbps**

Tabla 4.2: Tráfico de videovigilancia con QoS.

4.2.3 Escenario de prueba 3: Evaluación del tamaño de los archivos de grabación generados por la cámara WVC2300.

- **Descripción del escenario:** en este escenario lo que se busca es verificar cuanto es el tamaño de los archivos de grabación de una de las cámaras.

- **Ejecución de la prueba:** esta prueba está basada en la ejecución de los siguientes pasos:

1. Se utilizó una laptop, en simulación de un servidor, para fines de almacenar el video grabado.

2. Se colocó en funcionamiento la cámara WVC2300, en modo grabación, durante 1 minuto, con movimientos constantes durante todo el minuto.

3. Se colocó en funcionamiento la cámara WVC2300, en modo grabación, durante 1 minuto, con movimientos cada 20 segundos.

4. Se colocó en funcionamiento la cámara WVC2300, en modo grabación, durante 1 minuto, con movimientos cada 10 segundos.

5. Se colocó en funcionamiento la cámara WVC2300, en modo grabación, durante 1 minuto, sin movimientos.

- **Resultados obtenidos:** en la tabla 4.3 se muestran los resultados obtenidos al verificar el tamaño de los archivos de grabación de la cámara WVC2300.

- **Análisis de los resultados:** en este escenario se realizaron 4 grabaciones de un área específica, donde cada grabación tiene una duración de 1 minuto, con variaciones en la cantidad de movimiento. De esta forma, se pudo comprobar que el tamaño de los archivos de grabación, dependen directamente de la cantidad de movimiento que la cámara haya percibido.

	Movimiento	**Tamaño en Kb de 1 minuto de grabación**	**Tamaño en Mb de 24 horas de grabación**	**Tamaño en Mb de 30 días de grabación**
Grabación # 1	Constante	2408	3386.2	101587.5
Grabación # 2	Cada 10 seg.	1138	1600.3	48009.3
Grabación # 3	Cada 20 seg.	945	1328.9	39867.1
Grabación # 4	No hubo	926	1302.1	39065.6

Tabla 4.3: Tamaño de los archivos de grabación.

Capítulo 5

Conclusiones y recomendaciones

Para el desarrollo de este Trabajo Especial de Grado se realizó un estudio teórico del funcionamiento de las WLANs, para que de esta manera se pueda realizar un diseño eficiente y estable sobre el cual se pueda soportar la solución de videovigilancia que se propone. Adicionalmente, se realizó un estudio del protocolo DiffServ para el manejo de la calidad de servicio, con el fin de proponer su implementación en la WLAN.

Cumplidas las actividades propuestas en la metodología, en relación directa con los requerimientos tanto de la DTIC como de la Dirección de Seguridad de la UCV, se puede afirmar que:

- Una vez realizada la evaluación de la WLAN que posee el Edificio el Rectorado, se pudo constatar, que como consecuencia a que no se realizó un estudio previo para determinar cuál era la ubicación más idónea de los APs, existen puntos ciegos, lo que imposibilita obtener una continua señal inalámbrica. Sin embargo, los equipos que conforman la WLAN actual, podrán ser utilizados en el diseño propuesto. Igualmente, en la evaluación se comprobó, que la Plaza Cubierta y el Complejo Cultural Aula Magna no disponían de ningún tipo de señal inalámbrica.

- Luego de realizar la evaluación del circuito cerrado que se encuentra implementado en el Edificio el Rectorado, se determinó que el área de los ascensores y escaleras, no disponen de cámaras que permitan monitorear la entrada y salida de personas a los pasillos del mismo, por lo que fue necesario contemplar esta situación en el diseño que se propuso.

- Se determinó que la cámara que corresponde al modelo Serie 2500 de Cisco Systems, es la que mejor se adapta a las necesidades requeridas por la organización, debido a que posee una alta definición.

- La WLAN que se encuentra implementada en el Edificio, cuenta con APs modelo Cisco Aironet 1130AG, y los APs que se proponen para el complemento de la WLAN son modelo Cisco Aironet 1140, debido a que soportan el estándar 802.11n. Para tener un total control de la administración de todos los APs, se sugiere la implementación de un controlador inalámbrico modelo Cisco Wireless Lan Controller Serie 4400.

- Se diseño una red inalámbrica de área local (WLAN), con la finalidad de reforzar la WLAN que ya se encontraba implementada en el Edificio el Rectorado. Este diseño no solo se llevo a cabo en el Edificio, sino que se extendió hasta la Plaza Cubierta y el Complejo Cultural Aula Magna.

- En la propuesta de diseño de la WLAN, se evaluó que no existieran puntos ciegos, logrando una constante cobertura en todas las áreas de estudio. Así mismo, es importante acotar que El Edificio el Rectorado cuenta con 6 APs que conforman la actual WLAN y que para poder cubrir todos los puntos ciegos que presenta el Edificio, se sugiere la implementación de 6 nuevos APs. Para la Plaza Cubierta y el Complejo Cultural Aula Magna se sugirió la implementación de 8 APs, para garantizar una cobertura total de señal inalámbrica en estas áreas.

- Una vez diseñada la WLAN, se procedió al diseño de la solución de videovigilancia con cámaras IP, verificando que cada una de las cámaras recibiera una buena calidad de señal inalámbrica, cumpliendo a su vez con los requerimientos de monitorear las zonas criticas planteadas por la Dirección de Seguridad de la UCV. En el Edificio el Rectorado se propone la implementación de 16 cámaras, igualmente para lograr una cobertura total de todos los puntos críticos en la Plaza Cubierta se sugiere la implementación de 7 cámaras y en el Complejo Cultural Aula Magna se propone que se implementen 6 cámaras. Al sugerir la implementación de estas cámaras IP de videovigilancia en cada una de las áreas de estudio, se garantiza que la solución de videovigilancia propuesta es robusta y de gran beneficio a toda la comunidad universitaria.

- La solución de videovigilancia propuesta, así como la WLAN, son totalmente escalables en cuanto al número de dispositivos inalámbricos soportados, ya que, debido a la gran cobertura que ofrecen los APs se puede incrementar el número de cámaras fácilmente. Debido a que la serie 4400 de los controladores Cisco Wireless Lan Controller soportan entre 12, 25, 50 y 100 APs, no sería un problema agregar nuevos APs para expandir la cobertura de la WLAN.

- En los escenarios de pruebas, el mecanismo que se utilizó para darle prioridad a los paquetes de video que transitan por la red fue DiffServ, garantizando de esta forma que los paquetes lleguen a su destino sin sufrir ninguna pérdida, debido a que las transmisiones son en tiempo real. Estas pruebas no se realizaron en la red de datos de la DTIC, sino que se planteó un ambiente de pruebas independiente por requerimiento de la organización.

- La UCV, específicamente el Edificio el Rectorado, Plaza Cubierta y el Complejo Cultural Aula Magna, ahora pueden contar con una buena propuesta de solución de videovigilancia que plantea brindar numerosas ventajas, ya que, se incrementaran los niveles de vigilancia y esto ayudara a tomar decisiones que faciliten velar por la seguridad de la comunidad universitaria, así mismo, la

solución de videovigilancia ayudará a preservar las instalaciones y bienes de la UCV.

Finalizadas las pruebas sobre la solución de videovigilancia, puede concluirse que se han cumplido exitosamente los objetivos y la metodología planteada para este Trabajo Especial de Grado.

Limitaciones

Entre las limitaciones que se presentaron durante el desarrollo de este Trabajo Especial de Grado se tienen:

- Debido a que por requerimientos de la DTIC solo se utilizaron las tecnologías del fabricante Cisco Systems, no se tuvo la oportunidad de evaluar las bondades de otro tipo de dispositivos existentes en el mercado, desarrolladas por diferentes fabricantes.

- Los APs que ya se encontraban implementados en el Edificio el Rectorado, fueron colocados para cubrir una necesidad específica, es decir, no se realizaron evaluaciones para su ubicación. Dichos APs no se permitieron mover para cubrir los puntos ciegos existentes, trayendo como consecuencia que se agregaran nuevos dispositivos al diseño propuesto para dar cobertura a todas las áreas.

- Al momento de iniciar el desarrollo de este Trabajo Especial de Grado, la DTIC ya disponía de unas cámaras de videovigilancia. Luego de la evaluación de los distintos modelos de cámaras inalámbricas, se pudo descubrir que la cámara con la cual se realizaron las pruebas no era la más avanzada en el mercado.

Trabajos futuros

Algunos de los trabajos futuros que se pueden sugerir son:

- Utilizar la misma metodología de este Trabajo Especial de Grado para extrapolar esta solución de videovigilancia a los demás edificios y entradas de la UCV. Lo que garantizaría que todas las áreas de la UCV estén monitoreadas y traería como beneficio un incremento en la vigilancia para poder brindar más seguridad a la comunidad universitaria.

- Extender el diseño de la WLAN a todo el resto del Campus Universitario. No solamente para dar soporte a la solución de videovigilancia, sino, a otras aplicaciones que lo requieran y a su vez prestar el servicio de una conexión a Internet inalámbrica a toda la comunidad universitaria, ya que hoy en día muchas áreas comunes brindan este servicio de forma gratuita.

Recomendaciones finales

- La solución de videovigilancia planteada en estos momentos se encuentra actualizada tecnológicamente, es decir, que los dispositivos inalámbricos que se sugieren para esta implementación manejan tecnología de vanguardia. Es por ello que se recomienda realizar evaluaciones de tecnologías emergentes cada cierto tiempo para mantener la plataforma actualizada.

- Dada la limitación de evaluar sólo la tecnología del fabricante Cisco Systems, es recomendable realizar un estudio sobre las distintas tecnologías en cuanto a cámaras de videovigilancia que existen en el mercado actualmente.

- Una recomendación importante para un mejor desempeño de la solución de videovigilancia, es utilizar el software Cisco Video Surveillance Stream Manager, el cual ofrece varios módulos de administración, que permiten realizar un monitoreo de la red, generar reportes, verificación de alarmas, monitoreo, control y administración de todas las cámaras de la solución de videovigilancia. Así mismo, si la necesidad que se presenta es monitorear más de 16 cámaras simultáneamente, este software ofrece esa posibilidad. Igualmente go1984, es un software que permite monitorear más de 16 cámaras de videovigilancia. Ambos software son de tipo propietario.

- Para dar garantía que los paquetes de video en la WLAN no se vean afectados por los distintos tipos de tráfico generados por otros dispositivos inalámbricos, se recomienda reservar un 20% del ancho de banda de las interfaces inalámbricas de los APs.

- Se recomienda realizar pruebas de interferencia en las zonas de estudio, con el fin de evitar que dispositivos interfieran en la degradación del servicio lo que causaría que la señal inalámbrica captada por las cámaras se vea afectada.

- Se propone realizar pruebas con antenas omnidireccionales para extender la cobertura de la señal inalámbrica generada por los APs, en caso que se quiera minimizar el número de los mismos en las zonas de estudio.

- Para almacenar los videos de la solución de videovigilancia, por un máximo de 30 días, se recomienda que se disponga de 1800Gb en el ambiente de almacenamiento para garantizar que todos los videos generados por las 29 cámaras puedan ser almacenados de forma satisfactoria.

Referencias bibliográficas

[1] Álvarez S., González A. Estudio y configuración de calidad de servicio para protocolos IPv4 e IPv6 en una red de fibra óptica WDM. Volumen 13 Nº 3. Universidad Técnica Federico Santa María. Valparaíso, Chile. Julio 2005.

[2] Blake S., Black D., Carlson M., Davies E., Wang Z., Weiss W. An Architecture for Differentiated Service. RFC 2475. Diciembre 1998.

[3] Braden R., Clark D., Shenker S. Integrated Services in the Internet Architecture. RFC 1633. Junio 1994.

[4] Braden R., Zhang L., Berson S., Herzog S., Jamin S. Resource ReSerVation Protocol (RSVP). RFC 2205. Septiembre 1997.

[5] Cisco Systems. CCNA Exploration 4.0.

[6] Cisco Systems. Datasheet. Cisco Wireless LAN Controllers. Enero 2010.

[7] Cisco Systems. Datasheet. Cisco Cisco Aironet 1130AG and Aironet 1130G Series. Enero 2010.

[8] Cisco Systems. Datasheet. Cisco Aironet 1140 Series Access Point. Enero 2010.

[9] Cisco Systems. Datasheet. Cisco Wireless Control System (WCS). Febrero 2010.

[10] Cisco Systems. Fundamentos de Redes Inalámbricas, Séptima Edición. Pearson Educación. 2006.

[11] Cisco Systems. Datasheet. Cisco WVC210 Wireless-G Pan Tilt Zoom (PTZ) Internet Video Camera: 2-Way Audio Cisco Small Business Video Surveillance Cameras. Diciembre 2009.

[12] Cisco Systems. Datasheet. Cisco WVC2300 Wireless-G Business Internet Video Camera with Two-Way Audio Cisco Small Business Video Surveillance Cameras. Octubre 2009.

[13] Cisco Systems. Datasheet. Cisco 2500 Series Video Surveillance IP Camera. Diciembre 2009.

[14] Consejo de Preservación y Desarrollo (COPRED). Noviembre 2009.

[15] Dirección de Tecnología de Información y Comunicaciones (DTIC). Febrero 2010.

[16] García C. Propuesta de arquitectura de QoS en entorno inalámbrico 802.11e basado en Diffserv con ajuste dinámico de parámetros. Tesis Doctoral, Universidad Carlos III, Madrid, España. 2006.

[17] García M., Ramírez A. Video sobre IP: introducción. Segundo Encuentro Regional Académico. Tijuana, Baja California, México. Noviembre 2006.

[18] García T. Análisis de los modelos de servicios diferenciales y servicios integrales para brindar QoS en internet. Trabajo de Grado, Universidad Tecnológica de la Mixteca. Oaxaca, México. 2007.

[19] Guzmán J. L. Análisis y diseño de una red inalámbrica para la empresa Bio–Electrónica Blanco S.A. Trabajo de grado, Escuela Politécnica Nacional. Quito, Perú. 2009.

[20] Heinanen. J., Baker. F., Weiss. W., Wroclawski. J. Assured Forwarding PHB Group. RFC 2598. Marzo 2010.

[21] IEEE. 802.11 Supplement to IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements— Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band. IEEE 1999.

[22] IEEE. 802.11e Wireless LAN Medium Access Control and Physical Layer specifications. IEEE. 2005.

[23] Jacobson. V., Nichols. K., Poduri. K. An Expedited Forwarding PHB. RFC 2598. Marzo 2010.

[24] Murrazo M.A. Interoperabilidad de los Mecanismos de QoS en Internet. Octava Jornada Universitaria de Informática. Universidad Nacional de San Juan. Facultad de Ciencias Exactas Físicas y Naturales. Departamento de Informática. San Juan, Argentina. 2001.

[25] Nichols K., Blake S., Baker F., Black D. Definition of the Differentiated Services Field. RFC 2474. Diciembre 1998.

[26] Pérez G. Análisis sobre el transporte de voz y video en redes frame-relay. Trabajo de grado, Universidad Central de Venezuela. Caracas, Venezuela. 2000.

[27] Pozo N.A. Estudio y diseño de una red LAN inalámbrica con calidad de servicio para voz y datos en el colegio de ingenieros geólogos, minas y petróleos (CIGMYP),

empleando los estándares IEEE 802.11g, IEEE 802.11e. Trabajo de grado, Escuela Politécnica Nacional. Quito, Perú. 2009.

[28] Robles M. QoS en redes wireless con IPv6. Trabajo de grado. Universidad Nacional de La Plata. Buenos Aires, Argentina. 2008.

[29] Sánchez A. Software para la compresión y descompresión de video utilizando la norma MPEG. Trabajo de grado, Instituto Politécnico Nacional. México D.F, México. 2005.

[30] Schulzrinne H., Agboh C. Session Initiation Protocol (SIP)-H.323 Interworking. RFC 4123. Julio 2005.

[31] Shenker S., Partridge C., Guerin R. Specification of Guaranteed Quality of Service. RFC 2212. Mayo 1994.

[32] Soriano J. Consideraciones para la mejora del rendimiento en redes de video IP. Valencia. España. Ralco Networks, S.L. Mayo 2005.

[33] Stallings, W. Ph.D. Comunicación y Redes de Computadoras. Séptima Edición. Prentice Hall. 2004.

[34] Stallings, W. Ph.D. Redes e Internet de Alta Velocidad Rendimiento y Calidad de Servicio. Segunda Edición. Prentice Hall. 2004.

[35] Stallings, W. Ph.D. Wireless Communications and Networks. Segunda Edición. Prentice Hall. 2004.

[36] Sun Microsystems. “Servicios IP”. Abril 2009.

[37] Unesco, http://whc.unesco.org/en/list/986. Septiembre 2009.

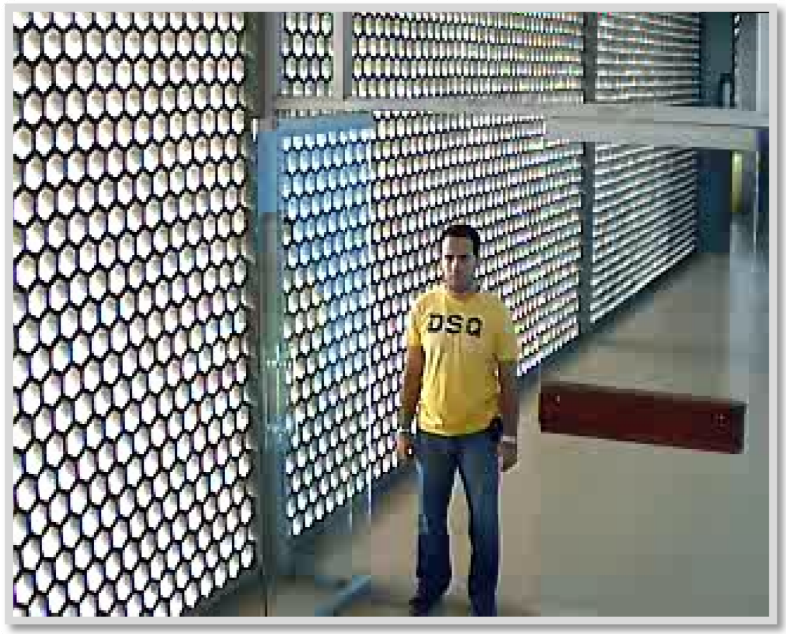
[38] Villapol, M.E. Introducción a las redes móviles e inalámbricas. Universidad Central de Venezuela, Facultad de Ciencias, Escuela de Computación. Caracas, Venezuela. 2007.

[39] Villapol, M.E. Redes de área local y personal inalámbricas: 802.11. Primera Parte. Universidad Central de Venezuela, Facultad de Ciencias, Escuela de Computación. Caracas, Venezuela. 2007.

Anexos

Pruebas de las Cámaras WVC2300 en el Edificio el Rectorado

Piso 1.



Piso 1.

Piso 1.

Piso 1.

Piso 2.

Piso 2.

Piso 2.

Piso 2.

Piso 3.

Piso 3.

Piso 3.

Piso 3.

Pruebas de las Cámaras WVC2300 en la Plaza Cubierta

Plaza Cubierta.

Plaza Cubierta.

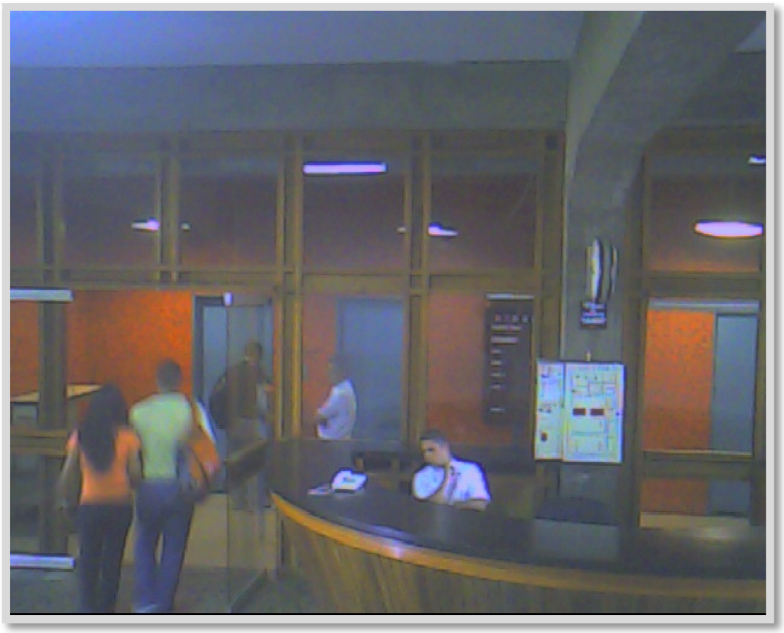
Plaza Cubierta.

Plaza Cubierta.

Complejo Cultural Aula Magna.

Complejo Cultural Aula Magna.

Complejo Cultural Aula Magna.



Complejo Cultural Aula Magna.