INTRODUCCIÓN

1.1 Introducción

La Universidad Autónoma “Juan Misael Saracho”, en su visión de convertirse en una universidad para el desarrollo, tiene como necesidad marchar al ritmo de las nuevas tecnologías y ponerlas al servicio de la educación tanto a nivel académico como a nivel administrativo.

La universidad en su afán de brindar una educación superior de alta calidad, hace uso de tecnologías de información y comunicación en particular del servicio de Internet, medio que permite tanto a estudiantes, docentes y administrativos estar comunicados, entre sí, actualizados en la información que se genere dentro de la universidad y dotarles de una herramienta de investigación y colaboración.

Cuando hablamos de red de datos, también tenemos que referirnos al medio de acceso que estos usuarios puedan tener a disposición. El acceso inalámbrico, es una de las tecnologías de comunicación más utilizada hoy en día. Gracias a la capacidad de poder conectarse a los distintos servicios que puedan estar corriendo sobre la plataforma de red sin utilizar algún tipo de cable o medio físico, permitiéndole al usuario navegar en diferentes lugares, WI-FI es una abreviatura de Wireless Fidelity, también llamada WLAN (wireless lan, red inalámbrica) o estándar IEEE 802.11.

La versatilidad de las comunicaciones inalámbricas y la propagación de nuevas tecnologías portátiles como por ejemplo los teléfonos móviles, las tabletas electrónicas, computadoras personales entre otros, están tomando cada vez más auge en la vida de los diferentes usuarios, hoy en día las personas estamos utilizando múltiples dispositivos para comunicarnos, por ello crece la necesidad de desprenderse de todo tipo de conexión física que no le permita la libertad de movimiento en su entorno, este tipo de conexión nos brinda una posibilidad de desplazarnos en diferentes lugares dentro del rango de irradiación en el cual estamos conectados con las mismas características de una red cableada. Son innegables las oportunidades que las redes inalámbricas proporcionan a sus usuarios pero, a su vez, las limitaciones en

la seguridad han conducido a la investigación y desarrollo de nuevas soluciones de seguridad, alternativas a las inicialmente existentes, para proteger las redes Wi-Fi y proporcionar a las instituciones y organizaciones que las utilizan la garantía que necesitan para sus sistemas y datos.

El presente trabajo propone describir el diseño de la red y la tecnología utilizada en la implementación de la red inalámbrica en la universidad Autónoma "Juan Misael Saracho" descripción que contribuirá a comprender de mejor manera las nuevas tecnologías adoptadas en redes inalámbricas de vanguardia.

Teniendo en cuenta que esta tecnología está a disposición se describirá todos los factores que llevaron a implementar este tipo de tecnología de acuerdo a estudios y lineamientos que responden a la demanda las comunicaciones actuales.

1.2 Antecedentes

La Universidad Autónoma "Juan Misael Saracho" a través de su departamento de Tecnologías de la Información y Comunicación (DTIC), ha implementado en su primera fase un sistema WiFi, en esta primera etapa solo ha abarcado el 15% de todas las edificaciones de la UAJMS, las razones por las que solo se ha cubierto el 15% son las siguientes:

No se tenía experiencia en la implementación de este tipo de sistemas de comunicación, por lo que el presupuesto estimado en aquella oportunidad fue muy reducido.

Por la demora en la implementación de la primera etapa, los equipos considerados en aquella oportunidad han quedado obsoletos, por lo que era necesaria la actualización de los equipos.

Por la magnitud del este sistema, la primera etapa ha servido para una dimensionamiento cabal de los equipos requeridos, mediante el cual se ha realizado

un ajuste exacto de la cantidad de equipos necesarios para cubrir el resto de los edificios con señal WiFi.

Por la facilidad de acceso a las redes mediante este sistema, los sistemas WiFi son muy utilizados para el acceso a las redes, tales como el Internet y aplicaciones colaborativas.

En el caso de la UAJMS, con la implementación de la primera etapa ya se tienen registrado aproximadamente 700 usuarios entre estudiantes y profesores que hacen uso del sistema inalámbrico

1.3 Planteamiento del problema

La Universidad Autónoma Juan Misael Saracho, en la gestión 2009-2010 (primera etapa) y 2011 (segunda etapa), implementó un sistema de red de comunicación inalámbrica en el Campus Universitario para brindar servicio de Internet a Docentes, estudiantes, administrativos y usuarios invitados, pero actualmente si bien existe el proyecto con el cual se logró la implementación, no existe un documento que describa a detalle y en profundidad la tecnología utilizada, descripción detallada no solo de especificaciones técnicas sino de bondades y valor agregado de cada uno de los equipos implementados, ni tampoco se describe a fondo el comportamiento del diseño de red implementada.

1.4 Objetivos

1.4.1 Objetivo general

Describir el diseño, la tecnología, equipos y valor agregado implementados en el sistema de red inalámbrica en la Universidad Autónoma “Juan Misael Saracho”, a través de la formalización de un documento completo que provea de una descripción y especificación detallada de los componentes utilizados en su instalación.

1.4.2 Objetivos específicos

- Explicar el uso y las características más significativas de las redes wireless, describiendo las generalidades y funcionamiento de las redes inalámbricas.

- Presentar las normas que regularon la implementación de la red inalámbrica de la UAJMS, a través de la descripción del estándar IEEE 802.11 para redes de área local inalámbricas.

- Describir los desafíos que llevaron a la implementación de la red inalámbrica en la UAJMS, a partir de las experiencias y necesidades identificadas en la institución.

- Realizar cuadros y modelos explicativos que describan la infraestructura de la red de la UAJMS

- Exponer la solución tecnológica adoptada en la UAJMS, detallando el diseño de red inalámbrica implementado.

- Realizar un análisis comparativo de las características diferenciadoras de las redes inalámbricas respecto a otras redes existentes, con la finalidad de justificar la solución empleada.

- Describir el valor agregado del sistema implementado, a través de la exposición de las bondades y funcionalidades del diseño de red inalámbrica empleada.

1.5 Justificación

En la actualidad la universidad maneja la red inalámbrica en base al proyecto de la primera y segunda fase del Proyecto de implementación de su sistema WiFi, con la descripción en detalle y profundidad de este proyecto implementado se contará con un documento que sirva como modelo de información necesaria para estudiantes, profesionales, que deseen conocer a detalle de esta tecnología o implementar este tipo

de redes en otros ámbitos e instituciones que pretendan utilizar esta tecnología. Ya que día a día este tipo de redes están creciendo y con ella crece la necesidad del usuario de poder tener movilidad dentro de entornos interconectados.

1.5.1 Justificación Social

El avance tecnológico se sustenta fundamentalmente en el desarrollo recíproco de la sociedad que las adopta.

En este contexto, la descripción a detalle plasmado en un documento de la implementación de una red inalámbrica de vanguardia, nos permitirá conocer y comprender a detalle las tecnologías asociadas a esta, impulsando a la sociedad universitaria en la utilización de nuevas tecnologías y herramientas de colaboración aportando en gran medida al desarrollo tecnológico no solo de la universidad sino que sirva como modelo para la propagación de este tipo de redes en otras instituciones dentro de nuestra sociedad en general.

1.5.2 Justificación Técnica

El proyecto es justificable tecnológicamente por que se describirá a detalle una tecnología ya implementada como es el sistema de red inalámbrica en la UAJMS en su primera y segunda Fase.

1.5.3 Justificación Académica

La Constitución Política del Estado, en su cuerpo pertinente establece que la más alta función del Estado es la educación, y esta se encuentra bajo la responsabilidad de las instituciones universitarias públicas y privadas del país.

En este sentido, realizar la descripción de una tecnología de punta implementada se convierte en una documentación invaluable que alimente los conocimientos sólidos adquiridos en la formación de profesionales en la carrera de Ingeniería Informática.

1.6 Alcance

El presente trabajo, pretende describir la tecnología utilizada en la implementación de de la red inalámbrica en la UAJMS que permita comprender de mejor manera nuevas tecnologías que se dan en las redes, en el caso específico de la red inalámbrica de la Universidad Autónoma Juan Misael Saracho.

Los alcances específicos son:

- La descripción estará exclusivamente basada en la implementación de la red inalámbrica de la UAJMS y bajo los estándares adoptados de esta.
- El documento estará orientado comprender de mejor manera las nuevas tecnologías adoptadas en redes inalámbricas.
- El documento contemplará la descripción de los equipos utilizados en la implementación de la red inalámbrica implementa en la UAJMS
- El documento contemplará la descripción del software utilizado en la implementación de la red inalámbrica de la UAJMS.
- El documento contemplará las proyecciones de nuevos servicios que se puedan brindar sobre la actual plataforma inalámbrica de la UAJMS.

1.7 Limitaciones

Si bien el documento describirá el diseño y la tecnología adoptados en la implementación de la red inalámbrica, por políticas de seguridad en la información de la institución universitaria no se detallarán:

- Líneas de código en las configuraciones de los equipos.
- Tipo de seguridad perimetral adoptada en la red a nivel general.
- Tipo de seguridad implementado en sus Servidores o DMZ.

- Tipos de transacciones de información que corre por la red.

1.8 Cronograma de actividades.

Actividad	Gestión 2011										
	Octubre				Noviembre				Diciembre		
	5	10	20	30	5	10	20	30	10	20	27
Revisión de tecnologías adoptadas.											
Estudio del diseño adoptado											
Presentación del trabajo											

Figura 1: Cronograma de Actividades

MARCO TEÓRICO

2.1. Red Inalámbrica[10]

Una red inalámbrica es un sistema de comunicación de datos que proporciona conexión inalámbrica entre equipos situados dentro de la misma área (interior o exterior) de cobertura. En lugar de utilizar el par trenzado, el cable coaxial o la fibra óptica, utilizado en las redes LAN convencionales, las redes inalámbricas transmiten y reciben datos a través de ondas electromagnéticas usando el aire como medio de transmisión.

Actualmente nos encontramos con los siguientes tipos de redes inalámbricas:

WPAN (Wireless Personal Area Network - Red inalámbrica de ámbito personal). Estas redes están pensadas para cubrir un área del tamaño de una habitación. Tradicionalmente este tipo de redes fue basado en infrarrojos que permiten la comunicación entre dos elementos (ordenadores portátiles, PDAs, etc.) a baja velocidad y a una distancia cercana. Actualmente la tecnología de radio frecuencia denominada Bluetooth es el estándar en auge.

WLAN (Wireless Local Area Network - Red inalámbrica de ámbito local). Son las redes que cubren el ámbito de una casa, una oficina o el edificio de una empresa.

WWAN (Wireless Wide Area Network - Red inalámbrica de área extensa). Son las redes cuyo ámbito cubre áreas más amplias como por ejemplo: una ciudad. Por su gran tamaño, estas redes son explotadas por las empresas de telefonía móvil o ISPs (Internet Service Providers). Hasta la llegada de la telefonía móvil de tercera generación, el UMTS, la alternativa es el uso del GPRS, aunque su velocidad es bastante reducida.

2.1.1. Redes WLAN[10]

Una red de área local inalámbrica (WLAN) es una red que cubre un área equivalente a la red local de una empresa, con un alcance aproximado de cien metros. Permite que los nodos que se encuentran dentro del área de cobertura puedan conectarse entre sí. Existen varios tipos de tecnologías, entre ellas:

IEEE 802.11 en sus variantes 802.11 a, b, g ofrecía hasta el año 2009 una velocidad máxima de 54 Mbps. A partir de octubre del 2009 con el advenimiento del estándar 802.11 n supera los 100 Mbps. El organismo internacional generador de estos estándares es el conocido como Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)

hiperLAN2 (High Performance Radio LAN 2.0), estándar europeo desarrollado por ETSI (European Telecommunications Standards Institute). HiperLAN 2 permite a los usuarios alcanzar una velocidad máxima de 54 Mbps en un área aproximada de

2.2. Topologías básicas de red[9]

La topología de una red representa la disposición de los enlaces que conectan los nodos de una red.

Las redes pueden tomar muchas formas diferentes dependiendo de como están interconectados los nodos. Hay dos formas de describir la topología de una red: física o lógica. La topología física se refiere a la configuración de cables, antenas, computadores y otros dispositivos de red, mientras la topología lógica hace referencia a un nivel más abstracto, considerando por ejemplo el método y flujo de la información transmitida entre nodos.

A continuación se da una breve descripción de algunas topologías de red básicas:

Topología	Descripción
Bus o Barra	Todos los nodos están conectados a un cable común o compartido. Las redes Ethernet normalmente usan esta topología.
Estrella	Cada nodo se conecta directamente a un concentrador central. En una topología de estrella todos los datos pasan a través del concentrador antes de alcanzar su destino. Esta es una topología común tanto en redes Ethernet como inalámbricas.
Línea (o multi-concentrador)	Un conjunto de nodos conectados en una línea. Cada nodo se conecta a sus dos nodos vecinos excepto el nodo final que tiene sólo un nodo vecino.
Árbol	Una combinación de las topologías de bus y estrella. Un conjunto de nodos configurados como estrella se conectan a una dorsal (backbone).
Anillo	Todos los nodos se conectan entre sí formando un lazo cerrado, de manera que cada nodo se conecta directamente a otros dos dispositivos. Típicamente la infraestructura es una dorsal (backbone) con fibra óptica.
Malla completa	Existe enlace directo entre todos los pares de nodos de la red. Una malla completa con n nodos requiere de n(n-1)/2 enlaces directos. Debido a esta característica, es una tecnología costosa pero muy confiable. Se usa principalmente para aplicaciones militares
Malla parcial	Algunos nodos están organizados en una malla completa, mientras otros se conectan solamente a uno o dos nodos de la red. Esta topología es menos costosa que la malla completa pero por supuesto, no es tan confiable ya que el número de enlaces redundantes se reduce.

Figura 1: Descripción de las topologías básicas de red

2.3. Topologías de red relevantes en conexión de redes inalámbricas[9]

A continuación se hacen algunas observaciones generales que le ayudaran a entender cómo y porque algunas topologías de red, pueden o no, ser aplicadas a redes inalámbricas. Estas observaciones pueden sonar triviales, pero su comprensión es fundamental para lograr la implementación de una red inalámbrica exitosa.

La comunicación inalámbrica no requiere un medio, Obviamente la comunicación inalámbrica no requiere de cables pero tampoco necesita de algún otro medio, aire, eter u otra sustancia portadora. Una línea dibujada en el diagrama de una red inalámbrica, es equivalente a una (posible) conexión que se está realizando, no a un cable u otra representación física.

La comunicación inalámbrica siempre es en dos sentidos (bidireccional), No hay reglas sin excepción, en el caso de “sniffing” (monitoreo) completamente pasivo o eavesdropping (escucha subrepticia), la comunicación es no bidireccional. Esta bidireccionalidad existe bien sea que hablamos de transmisores o receptores, maestros o clientes.

Un radio es solo un radio y su rol posterior es determinado por el software Este software determina el comportamiento de las tarjetas de radio bajo las capas 1 y 2 del modelo OSI, por ejemplo en las capas física y de enlace.

Teniendo en mente estas observaciones generales, podemos evaluar la relevancia de las topologías de red para redes inalámbricas.

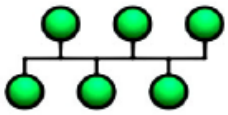
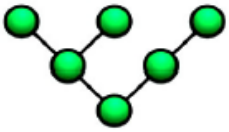
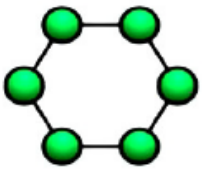
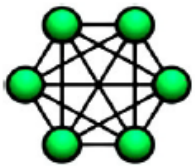
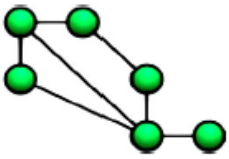
Topología	Representación visual	Relevancia en redes inalámbricas
Bus o Barra		No aplicable generalmente. Estudiando la topología de bus se puede notar que cada nodo se conecta a todos los demás nodos, en el punto donde un cable se conecta con otros cables. En el caso inalámbrico esta topología es equivalente a una red de malla completa operando en un canal único.
Estrella		Sí; esta es la topología estándar de una red inalámbrica.
Linea (multi-concentrador)		Sí; con dos o más elementos. Una línea de dos nodos es un enlace Punto a Punto.
Árbol		Sí; típicamente usado por ISP (Proveedores de servicio de Internet) inalámbricos.
Anillo		Sí; posible pero raro de encontrar.
Malla completa		Sí; pero la mayoría son mallas parciales.
Malla parcial		Sí.

Figura 2: Topologías en redes inalámbricas

2.4. Componentes de redes inalámbricas[9]

2.4.1. Punto de acceso

Un punto de acceso es un "concentrador" inalámbrico. El transmisor/receptor conecta entre si los nodos de la red inalámbrica y normalmente también sirve de puente entre ellos y la red cableada. Un conjunto de puntos de acceso (coordinados) se pueden conectar unos con otros para crear una gran red inalámbrica.

Desde el punto de vista de los clientes inalámbricos (como las computadoras portátiles o las estaciones móviles), un punto de acceso provee un cable virtual entre los clientes asociados. Este "cable inalámbrico" conecta tanto a los clientes entre si, como los clientes con la red cableada.

Un punto de acceso debe distinguirse de un enrutador inalámbrico, que es muy común en el mercado actual. Un enrutador inalámbrico es una combinación entre un punto de acceso y un enrutador, y puede ejecutar tareas más complejas que las de un punto de acceso. Considere un enrutador inalámbrico como un puente (entre la red inalámbrica y la red Ethernet) y un enrutador (con características de enrutamiento IP).

En una red inalámbrica se pueden encontrar trabajando juntos dispositivos inalámbricos como puntos de acceso, enrutadores, puentes. Los enrutadores y los puentes se pueden encargar de interconectar dos redes (p.e. Internet y su red local, o dos redes locales). Los enrutadores a diferencia de los puentes pueden hacer mas eficiente el transporte de paquetes entre las redes debido al uso de tablas de enrutamiento que permiten determinar la mejor ruta que puede seguir un paquete de datos para llegar a su destino, además un enrutador inalámbrico se encargara de realizar la traducción de direcciones de red (NAT) o enmascaramiento.

Los puntos de acceso podrán captar las señales de los enrutadores y clientes, amplificándolas para dar una mayor cobertura a la red. A pesar de que los puntos de acceso son "transparentes" para los otros dispositivos de la red, siempre se les debe asignar una dirección IP que permita su configuración.

Esto aplica a todos los dispositivos de la red, los cuales para ser gestionados requieren tener asignada una dirección IP.

Los clientes se conectan a un punto de acceso mediante su nombre. Este mecanismo de identificación se conoce como SSID-Service Set Identifier- (Identificador del Conjunto de Servicio) y debe ser el mismo para todos los miembros de una red inalámbrica específica. Todos los punto de acceso y clientes que pertenecen a un mismo ESS -Extended Service Set- (Conjunto de Servicio extendido) se deben configurar con el mismo ID (ESSID).

Cuando hablamos de SSID pensamos en la etiqueta de un punto (socket) de Ethernet. Conectarse a una red inalámbrica con SSID "x" es equivalente a conectar su computador a un punto de red sobre una pared identificado con la etiqueta "x". Para mas detalles mire la unidad "Configuración de puntos de acceso".

2.4.2. Clientes inalámbricos

Un cliente inalámbrico es cualquier estación inalámbrica que se conecta a una red de área local (LAN -Local Area Network) inalámbrica para compartir sus recursos. Una estación inalámbrica se define como cualquier computador con una tarjeta adaptadora de red inalámbrica instalada que transmite y recibe señales de Radio Frecuencia (RF).

Algunos de los clientes inalámbricos más comunes son las computadoras portátiles, PDAs, equipos de vigilancia y teléfonos inalámbricos de VoIP.

2.5. Redes Wi-Fi

2.5.1. Definición Wi-Fi [1], [2], [3], [4]

Wi-Fi es una de las tecnologías de comunicación inalámbrica (sin cables) más extendidas. También se conoce como WLAN o como IEEE 802.11. Las redes Wi-Fi son sistemas que utilizan un medio de comunicación de radiofrecuencia a través del aire, para transmitir o recibir información de cualquier tipo, (se envían en forma de paquetes sobre las redes computacionales).

Wi-Fi es un estándar de protocolo de comunicaciones del IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) que define el uso de los dos niveles más bajos de la arquitectura OSI (La capa Física y la capa Enlace).

2.5.2. Clasificación de los Paquetes Wi-Fi [1], [3]

El estándar IEEE 802.11 Wi-Fi define distintos tipos de paquetes con diversas funciones.

Los paquetes de Management: Son transmitidos de la misma manera que las tramas de datos para intercambiar información de administración, pero no son transportadas a las capas superiores. Un ejemplo de ellos son el *Association request, Association response, Beacon, Auntenticación*, etc.

Los paquetes de Control: Ayudan en la entrega de datos. Tienen funciones de coordinación.

Los paquetes de Datos: Contienen la dirección MAC del remitente y destinatario, un ejemplo de ello es el SSID (*Service Set Identifier*), etc.

2.5.2.1. Paquetes de Management [1]

Requerimiento de Asociación (*Association Request*), Incluye la información necesaria para que el Access Point considere la posibilidad de conexión. Uno de los

datos es el SSID de la red inalámbrica Wi-Fi o del Punto de Acceso al que se intenta conectar.

Respuesta de Asociación (*Association Response*), Es el tipo de paquete que envía el access point avisando de la aceptación o denegación del pedido de conexión.

Beacon, Los puntos de acceso inalámbricos Wi-Fi, periódicamente envían "señales", para anunciar su presencia y que todas las estaciones que estén en el rango (100 metros, aproximadamente) sepan cuales access point están disponibles. Estos paquetes se denominan "Beacons" y contienen varios parámetros, entre ellos el *Service Set Identifier* del Punto de Acceso.

Authentication, Es el paquete mediante el cual el punto de acceso inalámbrico acepta o rechaza a la estación que pide conectarse. Existen redes inalámbricas Wi-Fi abiertas donde no se requiere autenticación y en las redes inalámbricas protegidas se intercambian varios paquetes de autenticación con "desafíos" y "respuestas" para verificar la identidad del cliente.

Disassociation, Es un tipo de paquete que envía la estación cuando desea terminar la conexión, de esta manera el Punto de Acceso Inalámbrico sabe que puede disponer de los recursos que había asignado a esa estación.

2.5.2.2. Paquetes de Control [3]

Requerimiento para Transmitir (*RTS, Request to Send*), en este caso la estación envía al destinatario un pedido de transmisión y espera que la estación le responda que el medio se encuentra libre para hacerlo.

Libre para Transmitir (*CTS, Clear to Send*), tiene la función de responder a los RTS. Todas las estaciones que captan un CTS, saben que deben esperar un tiempo para transmitir pues alguien está ya usando el canal. Existe un tiempo de espera "slot time", que es distinto para cada estándar.

Acknowledgement (ACK), la estación receptora del paquete enviado, chequea el paquete recibido por si tiene errores. Si lo encuentra correcto, envía un "ACK" con lo cual el remitente sabe que el paquete llegó correcto, pues si no, lo debe enviar otra vez. Una vez que las demás estaciones captan el ACK, saben que el canal está libre y pueden intentar ellas enviar sus paquetes.

2.5.2.3. Paquetes de Datos [1], [3]

Estos paquetes llevan mucha información "administrativa" y, además los datos que se quiere transmitir a través de la red Wi-Fi. Generalmente la red inalámbrica Wi-Fi debe utilizar muchísimos paquetes de datos, para transmitir un archivo de datos. Mucho más aún cuando lo que se desea transmitir es video. Los paquetes de datos Wi-Fi, tienen muchos campos con información necesaria para la transmisión. Uno de ellos es la "Mac Address" de la estación receptora y del remitente, el BSSID (*Basic Service Set Identifier*), el número de secuencia de ese paquete, etc.

2.5.3. Tipos de Redes Inalámbricas Wi-Fi [2], [3], [5], [4]

Las redes inalámbricas Wi-Fi se pueden conectar, básicamente, de dos maneras muy diferentes:

2.5.3.1. Red Wi-Fi de Infraestructura

Esta arquitectura se basa en dos elementos: uno, o más puntos de acceso y estaciones cliente (fijas o móviles) que se conectan al servidor a través del punto de acceso.

2.5.3.2. Red Wi-Fi Ad-Hoc

Esta arquitectura se basa en un sólo elemento: Estaciones cliente (fijas o móviles). Las redes Ad-Hoc se conectan entre sí para intercambiar información de manera inalámbrica.

2.5.4. Identificación de Puntos de Acceso Wi-Fi en Redes Inalámbricas [1], [4]

Direcciones MAC (*Media Access Control*), Es un número de 48 bits asignado por el fabricante a los dispositivos inalámbricos: puntos de acceso, tarjetas Wi-Fi, USBs Wi-Fi, etc. Aunque está grabado en el hardware, se puede modificar por software.

Identificador de Conjunto de Servicios (SSID*, Service Set Identifier*), cada AP tiene hasta 32 bytes. Sirve para identificar a la red inalámbrica.

Conjunto de Servicios Básicos Independientes (IBSS*, Independent Basic Service Set*), identifica a las redes Ad-Hoc pues hay que recordar que en éstas no hay Punto de Acceso.

2.6. El estándar 802.11[7]

El estándar 802.11 o WiFi es una familia de especificaciones desarrolladas por la IEEE (Institute of Electrical and Electronic Engineers) para la tecnología de redes de área local inalámbricas, y que define el uso de los dos niveles más bajos de la arquitectura OSI (capa física y de enlace de datos).

En éste estándar se especifica una interfaz sobre el aire entre el cliente y la estación base o entre dos clientes inalámbricos. Actualmente incluye seis técnicas de transmisión por modulación que utilizan todos los mismos protocolos.

Esta familia ha desarrollado una serie de estándares, además del original (802.11), como lo son: el 802.11h, 802.11i, 802.11e y otros en evolución como 802.11r, 802.11s de los que incluso existen productos comerciales pre-estándar actualmente en el mercado.

Aún así, los que más se conocen y que han sido aprobados hasta ahora son el 802.11a, 802.11b y 802.11g, los cuales están en el mercado con un gran éxito comercial.

Otro estándar del que se ha escuchado y leído bastante últimamente es el 802.11n. Éste es uno de los estándares en evolución que surge debido a la gran demanda de las WLAN (Wireless Local Area Network).

Durante la segunda mitad del año 2003 la IEEE aprueba la creación del IEEE 802.11 Task Group N. Éste grupo desarrollaría una nueva revisión del estándar 802.11, en el cual la velocidad real de transmisión podría llegar a los 600 Mbps (esto significa que las velocidades teóricas de transmisión podrían ser mayores), debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. Además, con el desarrollo de éste nuevo estándar, se espera que el alcance de operación de las redes sea mayor con la incorporación de la tecnología MIMO (Multiple Input-Multiple Output), la cual permite la utilización de varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas.

A finales de enero del 2006 se aprobó el primer borrador del estándar y en marzo del 2007, después de un intenso debate y controversia entre todos los miembros que forman parte del IEEE, se aprobó la versión borrador 2.0, la cual también se conoce como “pre-11n”.

802.11	Estándar original
802.11a	54 Mbps en la banda 5Ghz
802.11b	Mejora en el 802.11, para la banda de 2.4 Ghz soporta 5.5 Mbps y 11 Mbps
802.11d	Extensiones internacionales para roaming, configura dispositivos automáticamente para cumplir las regulaciones RT locales
802.11e	Introduce mejoras de calidad de servicio
802.11f	Protocolo Inter-access Point Protocol(IAPP), define comunicaciones del punto de acceso interno para facilitar WLAN múltiples
802.11g	54 Mbps en la banda de 2.4 Ghz
802.11h	Define la gestión del espectro de la banda 5Ghz
802.11i	Mejora en la seguridad
802.11j	Adaptación para Japón
802.11k	Medidas de recursos radio
802.11n	Mejoras de rendimiento "throughput".
802.11p	WAVE: wireless access for vehicular enviroment
802.11r	Roaming rápido
802.11s	Redes ad-hoc wireless
802.11t	Predicción de rendimiento wireless(WPP)
802.11u	Interworking con otras redes
802.11v	Gestión de redes Wireless

Figura 3: Resumen de los estándares 802.11

2.6.1. Arquitectura del estándar 802.11[10]

Las especificaciones del estándar definido por el IEEE denominado 802.11x (x comprende letras que definen las variantes de la norma 802.11 a, 802.11 b, 802.11 g, 802.11 n), abarcan las capas física (Capa 1) y la subcapa de acceso al medio (MAC) de la capa de enlace del modelo OSI.

Veamos algunos detalles que nos ayudarán a entender el funcionamiento y acotar los problemas con los que nos vamos a encontrar.

2.6.2. Topología de Red en 802.11[10]

El estándar IEEE 802.11 define el concepto de Conjunto Básico de Servicio (BSS, Basic Service Set) que consiste en dos o más nodos inalámbricos o estaciones que se reconocen una a la otra y pueden transmitir información entre ellos.

Un BSS puede intercambiar información de dos modos diferentes:

1 – Cada nodo se comunica con el otro en forma directa y sin ninguna coordinación. Este modo es comúnmente llamado Ad-Hoc o IBSS (Independent Basic Service Set). Este modo solo permite la transmisión entre los nodos inalámbricos y no resuelve el problema de extender una LAN cableada.

Figura 4: Ad-Hoc o IBSS

2 – Existe un elemento llamado comúnmente AP (Access Point) que coordina la transmisión entre los nodos inalámbricos. Este modo es llamado modo Infraestructura y permite vincular la red inalámbrica con la red cableada ya que el AP actúa como bridge entre las dos redes. La existencia de varios AP conectados a un sistema de distribución (DS: Distribution System), que puede ser una LAN cableada es lo que denominamos EBSS (Extended Basic Service Set). La tecnología 802.11 permite el roaming entre los distintos AP.

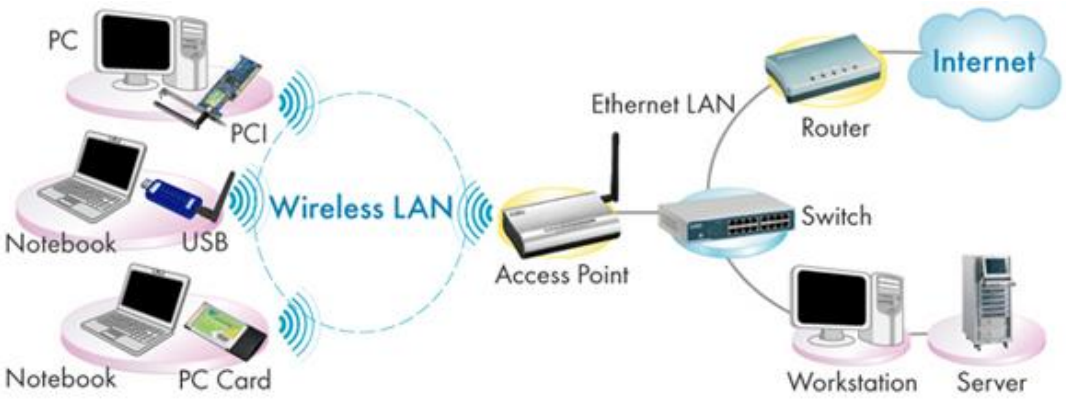


Figura 5: AP (Access Point)

2.6.3. Itinerancia (roaming) [10]

La itinerancia es el proceso o capacidad de un cliente inalámbrico de moverse de una célula o BSS a otra sin perder la conectividad de la red. Los AP pasan el cliente de una a otro, siendo esto invisible para el usuario. El estándar no define como debe llevarse a cabo la itinerancia, pero si define los bloques constructivos básicos, que incluyen el escaneado activo y pasivo y el proceso de reasociación.

Servicios soportados por el sistema de distribución (DS) Si bien el DS no es parte de la norma 802.11, la misma especifica los servicios que este sistema debe soportar, los cuales son:

1 – Servicios de Estación (SS: Station Services)

a) Autenticación: antes de que un nodo pueda unirse a la red, debe establecer su identidad, para ello debe superar una serie de tests que permitan saber que quien se quiere conectar es quien dice ser. 802.11 ofrece 2 tipos de servicios de autenticación:

Autenticación Abierta (Open System Authentication), significa que cualquiera que solicite autenticarse será aceptado.

Autenticación de llave compartida (Shared Key Authentication), significa que para poder autenticarse en la red, el nodo debe conocer la frase de paso.

b) Deautenticación: ocurre cuando el AP o el nodo inalámbrico desea terminar la autenticación. Implica una desasociación.

c) Privacidad: está satisfecha en 802.11 con un sistema de encriptación llamado WEP (Wired Equivalent Privacy). Es opcional.

d) Transporte de unidad de Servicios de capa MAC (MSDU: MAC Service Data Unit Delivery): se ocupa de que la información necesaria para operación de la subcapa MAC sea transportada entre los distintos AP.

2 – Servicios provistos por el Sistema de Distribución DS

a) Asociación: un nodo inalámbrico debe estar asociado a un AP para poder hacer uso de la red. Solo puede estar asociado a un AP por vez, así el DS sabe perfectamente en que AP se encuentra el nodo. Es iniciado por el nodo.

b) Reasociación: este servicio permite que un nodo deje la asociación de un AP para pasar a asociarse a otro AP. Es también iniciado por el nodo.

c) Desasociación: el servicio que permite a cualquiera de las partes (AP o nodo) terminar la asociación.

d) Distribución: es el servicio por el cual se llevan los datos desde el origen al destino. Los datos son enviados al AP local, de ahí a través del DS al AP remoto (donde está asociado el nodo destino) y este lo pasa al nodo destino directamente. El servicio de distribución se invoca inclusive si ambos nodos están asociados al mismo AP.

e) Integración: es el servicio que permite integrar el sistema inalámbrico a otra red, por ejemplo una LAN cableada, realizando las conversiones de protocolo necesarias.

2.6.4. La capa Física en 802.11[10]

La capa física de la especificación IEEE 802.11 ofrece dos tipos de técnicas para las transmisiones en frecuencias de radio y una especificación para transmisiones infrarrojas.

Las técnicas de radio frecuencia trabajan basadas en el concepto de "Espectro Ensanchado" o Spread Spectrum (SS). Este concepto se basa en un ensanchamiento forzado del espectro de ancho de banda usando una función XOR con una secuencia Numérica Pseudorandómica larga, esto disminuye la densidad de potencia espectral y reduce la potencia de pico. La potencia total transmitida no varía pero la señal se hace mucho mas inmune a las interferencias y al ruido ambiente.

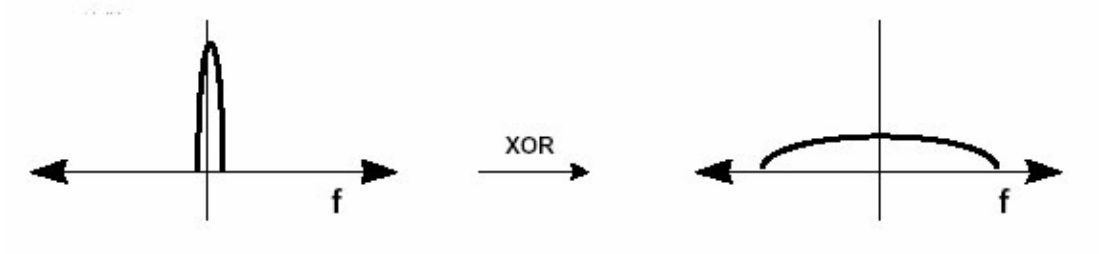


Figura 6: Spread Spectrum (SS)

Las dos técnicas previstas en la norma 802.11 son:

Salto de Frecuencia (Frecuency Hoping Spread Spectrum, FHSS) Es la forma más simple de modulación de espectro ensanchado, normalmente la mayoría de los sistemas de salto de frecuencia definen un conjunto de saltos uniformes dentro de una banda de frecuencia aunque esto no es absolutamente necesario ya que ambos extremos de la transmisión conocen de antemano el patrón de salto de frecuencias utilizado. Esta técnica consigue una alta inmunidad a las interferencias y al ruido ambiente, sobre todo cuando usa patrones aleatorios de salto de frecuencia. La desventaja de esta técnica es que solo se ha desarrollado en el mercado para velocidades que no superan los 2 Mbps. Existen 75 subcanales de 1 MHz que permiten definir secuencias de saltos que no se solapan entre si.

Secuencia Directa (Direct Secuence Spread Spectrum, DSSS). En la técnica de secuencia directa se usa un código de pseudo-ruido generado localmente para codificar la señal digital a transmitir. Este código se ejecuta a frecuencias varias veces más altas que la frecuencia de la señal.

Si ejecutamos una función EXOR con la señal, obtenemos una señal codificada que luego será modulada usando BPSK (Binary Phase Shift Key) antes de ser transmitida.

Esta señal, al ser recibida en el otro extremo, es decodificada usando una réplica local del código de pseudo-ruido usado en el emisor. De este modo, el receptor solo decodificará la señal que esté codificada con un código determinado, resultando en un filtro natural para las interferencias y señales espurias.

Las técnicas no son interoperables entre si. En cualquiera de los dos casos, las señales de Espectro Ensanchado (SS) se convierten en señales que tienen una baja probabilidad de interferencia con señales de espectro estrecho debido a que la energía es desparramada en un ancho de banda que puede ser 100 veces el ancho de banda de la señal a transmitir.

Este tipo de modulación es exigida por la FCC de los EEUU y por la mayoría de los entes regulatorios de los países para utilizar las bandas de frecuencias libres llamadas ISM (Industrial, Scientific and Medical) que operan entre los 2.400 GHz y los 2.483 GHz y también entre los 5.725 y los 5.875 GHz. Para lograr velocidades de 1, 2, 5.5 y 11 Mbps, es necesario un AB de alrededor de 20 MHz por canal por lo que se debe entender que la norma 802.11 tiene solamente 3 canales no solapados en la banda ISM de 2.4 GHz.

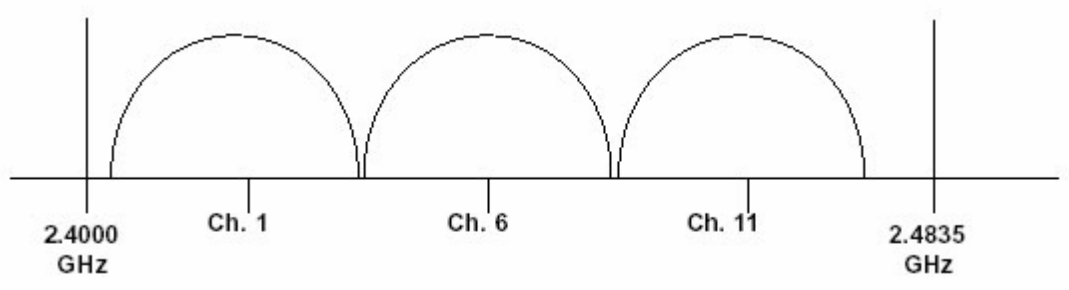


Figura 7: Canales no solapados por la banda ISM de 2.4 GHz

En los sistemas de secuencia directa (DS), es necesario compensar el ruido que se introduce en cada canal debido a su ancho de banda, para ello cada bit de datos se convierte en una serie de patrones de bits redundantes llamados "chips". La redundancia que presenta cada chip combinada con el ensanchamiento de la señal a través de los 20 MHz provee un mecanismo solido de detección y corrección de errores, minimizando las retransmisiones.

2.6.5. La capa de Enlace en 802.11[10]

La capa de enlace de datos en 802.11 consiste en dos subcapas:

1. Capa de Control lógico de Enlace, o Logical Link Control (LLC)

2. Capa de Control de Acceso al Medio o Media Access Control (MAC) o capa de Acceso Múltiple.

2.6.5.1. La subcapa de Control Lógico de Enlace (capa LLC)

Esta capa es exactamente igual a la capa LLC utilizada por las redes cableadas del tipo 802.3 con un sistema de direccionamiento de 48 bits idéntico (MAC Address). Esto permite simplificar al extremo los puentes (bridges) entre los dos tipos de red.

2.6.5.2. La subcapa de Acceso Múltiple en 802.11 (capa MAC)

El método de acceso múltiple en IEEE 802.11 es la llamada Función de Distribución Coordinada (Distributed Cordination Function, DCF) que utiliza el conocido método

de Acceso Múltiple por Censado de Portadora con Prevención de Colisiones, (Carrier Sense Multiple Access / Collision Avoidance, CSMA/CA).

Este método requiere que cada nodo inalámbrico escuche el medio compartido para saber si otros nodos se encuentran transmitiendo. Si el canal está desocupado, el nodo puede transmitir, caso contrario, el nodo escucha hasta que la transmisión finalice, y entra en un período de espera aleatorio para luego volver a ejecutar el procedimiento. Esto previene que algunas estaciones monopolicen el canal al comenzar a transmitir inmediatamente después que termine la otra.

La recepción de los paquetes en el DCF requiere de confirmaciones por parte del destino. Hay un corto período de tiempo entre el envío del ACK por parte del destinatario llamado Short Inter Frame Space, SIFS. En 802.11, los paquetes de confirmación ACK tiene prioridad frente a cualquier otro tráfico, logrando una de las características sobresalientes que es la gran velocidad de las confirmaciones.

Cualquier transmisión distinta a un ACK deberá esperar por lo menos un DIFS (DCF Inter Frame Space) antes de transmitir algún dato. Si el transmisor detecta un medio ocupado nuevamente, vuelve al tiempo de BackOff pero reduciendo el tiempo de espera. Así se repetirá hasta que el tiempo de espera llegue a CERO donde se habilita al nodo a transmitir, luego de que termine la próxima transmisión.

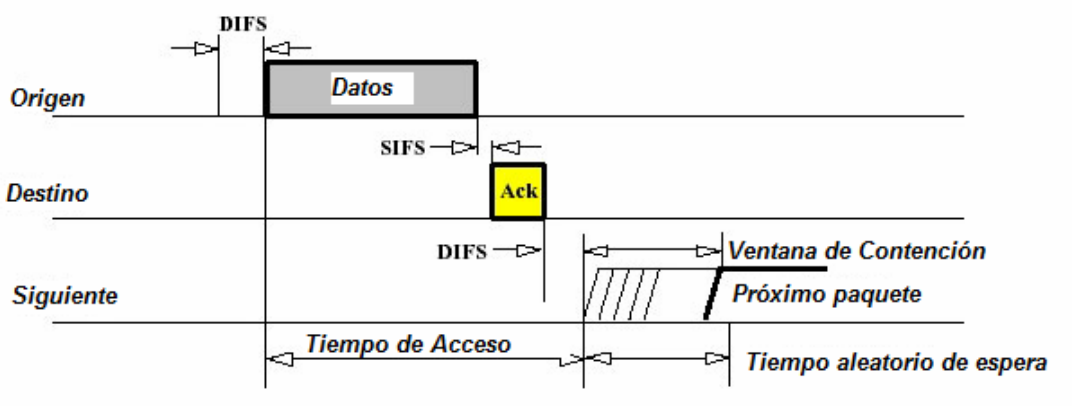


Figura 8: Función de Distribución Coordinada (Distributed Cordination Function, DCF)

Este método es similar al utilizado en el protocolo Ethernet 802.3 y supone que todos los nodos escuchan simultáneamente el canal.

Esto no es siempre cierto en un canal inalámbrico, donde se puede dar el caso del Nodo oculto. Veamos el siguiente caso, los nodos A y B están dentro del rango del Access Point pero el Nodo B no sabe que existe el Nodo A porque está fuera de su rango y por lo tanto no puede saber si está transmitiendo o no.

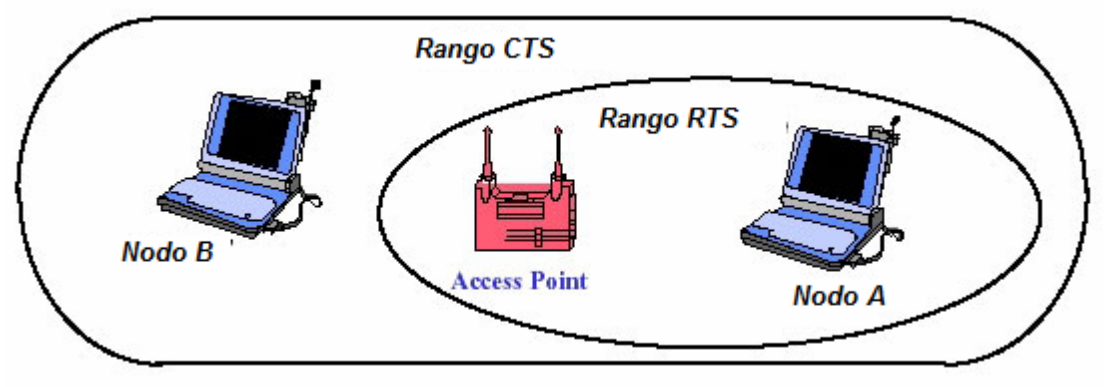


Figura 9: Caso del Nodo oculto

Esto se resuelve usando un segundo método de censado de portadora llamado Censado Virtual de Portadora (Virtual Carrier Sense) que habilita a un nodo a reservar el canal por un determinado período de tiempo usando tramas RTS/CTS.

En el ejemplo de arriba, El Nodo A envía un RTS (Request To Send) al Access Point. Este RTS, tiene un campo que especifica el tiempo que solicita la reserva y no es escuchado por el Nodo B porque esta fuera del alcance. La información de la reserva es almacenada por los restantes nodos dentro del alcance de A en una base llamada Network Allocation Vector (NAV). El AP responde con un CTS que contiene el tiempo asignado para la reserva. El nodo B que recibe el CTS del AP actualiza su tabla NAV de acuerdo a la información suministrada, resolviendo así el problema del nodo oculto.

2.6.6. Estándar 802.11b [7]

El estándar 802.11b fue aprobado en 1999, permitiendo una tasa de transmisión máxima de 11 Mbps, utilizando el mismo método de acceso al medio que el 802.11. En la práctica no era posible superar los 6 Mbps con TCP (Transmission Control Protocol) y los 7 Mbps con UDP (User Datagrama Protocol). Los primeros equipos aparecieron muy rápidamente,

ya que era una extensión a una modulación DSSS (Direct-Sequence Spread Spectrum) del estándar original. El aumento de velocidad y el reducido costo consiguieron un rápido crecimiento de la demanda y oferta.

El protocolo se puede utilizar en topologías punto a-multipunto (las más habituales) o punto-a-punto, con enlaces con distancias proporcionales a las características de las antenas y potencia utilizada. Además, si existen problemas de calidad de señal, es posible transmitir a 5.5, 2 y 1 Mbps, que utilizan métodos más redundantes de codificación de datos.

El estándar divide el espectro en 14 canales que se traslapan, a una distancia de 5 Mhz cada uno de ellos. Esto provoca que cada canal interfiera con los dos adyacentes a cada lado, ya que el ancho de banda es 22 Mhz, a partir de donde la señal cae 30 dB como mínimo. Es por ello que se recomienda optar por los canales disjuntos (ej. canales 1,6 ó 11), que no representan traslapes especiales, produciéndose interferencias mínimas Los canales disponibles en cada país difieren de acuerdo a la reglamentación del mismo. Así, mientras en los Estados Unidos hay 11 canales disponibles, en Europa se disponen de 13 y en Japón 14.

2.6.7. Estándar 802.11a [7]

El estándar fue aprobado en 1999. Se basa en el estándar original, operando en la banda de 5 Ghz, pero utilizando la técnica OFDM (Orthogonal Frequency Division Multiplexing) de modulación con 52 canales, alcanzando tasas de transmisión de hasta 54 Mbps, que se pueden corresponder con un rendimiento real de 20 Mbps. De

forma similar al estándar 802.11b, la tasa se puede reducir a 48, 36, 24, 18, 12, 9 y 6 Mbps. El estándar dispone de 12 canales no traslapados.

Utilizar la banda de 5 GHz permite disponer de menos interferencias, pero condiciona las instalaciones a disponer de línea de vista, además de tener una mayor absorción.

En un primer momento fue utilizado en Estados Unidos y Japón, sin obtener licencia para operar en Europa, que en ese momento optaba por apostar por el estándar Hiperlan, hasta que en 2003 fue admitido.

De las 52 subportadoras, 48 se utilizan para datos y cuatro actúan como pilotos, con una separación de 312.5 Khz. Cada subportadora puede ser BPSK (Binary Phase Shift Keying), QPSK (Quaternary Phase Shift Keying), 16 QAM (Quadrature Amplitud Modulation) o 64 QAM. La duración del símbolo es de 4 microsegundos, con un periodo de guardia de .8 microsegundos.

Esta tecnología no fue tan adoptada como la basada en el 802.11b, ya que tenía un rango menor y estaba limitada en Europa. Hoy en día está ganando aceptación al existir intervalos duales.

2.6.8. Estándar 802.11g [7]

En Junio de 2003 se aprobó el tercer estándar, el 802.11g. Este estándar funciona en la banda de los 2.4 Ghz, como el 802.11b, pero con una tasa máxima de 54 Mbps (y efectiva de 24.7 Mbps). Es compatible con el 802.11b y utiliza las mismas frecuencias.

Desafortunadamente, los conflictos con los equipos 802.11b, las interferencias y el hecho de que las frecuencias más altas estén más expuestas a sufrir perdidas han reducido la efectividad de la tecnología.

El hecho de que hayan aparecidos chips y equipos tri banda han favorecido el despliegue de la tecnología. Una característica adicional, llamada SuperG, hace

posible duplicar la señal, pero ocasiona conflictos con otros equipos provocando que no sea compatible en muchos casos.

2.6.9. Estándar 802.11n [7],[8]

El Borrador de este estándar fue publicado el año 2007 y aprobado en 2009, entre las características más importantes de este estándar destacan:

OFDM, mejora al 802.11a/g, usando una más alta tasa de código y escasamente más ancho de banda. Éste cambio mejora la máxima velocidad alcanzable de datos a 65 Mbps de 54 Mbps en los estándares existentes.

Múltiple Entrada Múltiple Salida MIMO (Multiple-input multiple-output), Esta es una tecnología que, mediante el empleo de varias antenas, ofrece la posibilidad de resolver información coherentemente desde varias rutas de señales mediante antenas receptoras separadas espacialmente.

Las señales multi-ruta son las señales reflejadas que llegan al receptor en cualquier momento después de la señal original o de la línea de vista que ha sido recibida. Generalmente la multi-ruta es considerada como interferencia que reduce la habilidad del receptor para recuperar información inteligente. MIMO proporciona la oportunidad de resolver espacialmente las señales multi-rutas, al proporcionar ganancias de diversidad que contribuyen a la habilidad de un receptor para recuperar la información inteligente.

Multiplexado por División Espacial (Spatial Division Multiplexing, SDM), el cual crea una división espacial multiplexada en varios flujos de datos independientes, transferidos simultáneamente dentro de un canal espectral del ancho de banda.

El MIMO SDM puede incrementar notablemente el rendimiento de datos, así como la cantidad de flujos espaciales permitidos.

Conjunto de antenas con diferente orientación. Algoritmos que tienen en cuenta donde está el emisor y la dirección por la que entra la señal. Mejor rendimiento en 5 GHz, se puede usar en 2.4 GHz si las frecuencias están libres.

SITUACIÓN DE LA RED INALAMBRICA DE LA UAJMS

3.1. Universidad Autónoma Juan Misael Saracho

3.1.1. Ubicación

La Universidad Autónoma Juan Misael Saracho se encuentra localizada en la Ciudad de Tarija, cuenta con diversas unidades distribuidas en la ciudad, así como en las provincias. Entre las unidades que se encuentran en la ciudad, destacan el Rectorado, Campus Universitario, Post-Grado, Instituto de Idiomas, entre otras. En las provincias se cuentan con facultades y carreras en: Bermejo, Yacuiba, Palmar, Villa Montes, Caraparí y Entre Ríos.

3.1.2. Plantel Estudiantil, Docente y Administrativo

La Universidad Autónoma Juan Misael Saracho alberga en su seno a 17.717 estudiantes, 1.096 docentes y al personal administrativo, los cuales se constituyen en la comunidad universitaria que forman parte de esta importante institución.

FACULTAD O UNIDAD	ESTUDIANTES
Fac. de Ciencias Jurídicas y Políticas.	1507
Fac. Ciencias Económicas y Financieras.	3646
Fac. Ciencias y Tecnología.	4686
Fac. de Humanidades.	1232
Fac. Ciencias de la Salud.	2180
Fac. de Odontología	749
Fac. de Ciencias Agrícolas y Forestales	879
Fac. Integrada de Villa Montes	573
Fac. Integrada de Bermejo	780
Fac. de Gran Chaco	1485
Docentes (Titulares e interinos)	1.096
Total de Nº Estudiantes y Docentes	18.813

Figura 1: Nº de estudiantes y docentes de la UAJMS

3.1.3. Distribución de la infraestructura

Tal como se indicaba anteriormente, la universidad cuenta con diversos edificios distribuidos en la ciudad de Tarija y en las provincias del Departamento, las mismas que detallamos a continuación.

UBICACIÓN O LUGAR.	DESCRIPCIÓN DEPARTAMENTO O UNIDAD.
Campus Universitario.	Bloque Ing. Forestal.
	Bloque Ing. De Alimentos.
	Bloque nuevo Ing. Agronómica.
	Bloque antiguo Fec. De Agronomía.
	Bloque Biblioteca de Agronomía.
	Bloques. Ceanid y laboratorios de Química.
	Bloque Ing. Química.
	Bloque Ing. Civil.
	Bloque Antiguo Ing. Civil.
	Bloque antiguo Arquitectura.
	Bloque Hidráulica.
	Bloque DTIC.
	Bloque Medicina.
	Bloque A Fac. de Ciencias Económicas.
	Bloque B Fac. de Ciencias Económicas.
	Bloque C Fac. de Ciencias Económicas.
	Bloque nuevo Fac. de Humanidades.
	Bloque nuevo Arquitectura.
	Bloque Edificio de Informática.
Ciudad Tarija.	Edificio del Rectorado.
	Bloque Ex – YPFB.
	Bloque Secretaría de desarrollo universitario.
	Edificio de la carrera de informática.
	Edificio de ciencias de la salud.
	Bloque Antiguo Ciencias Juirídicas.
	Bloque Antiguo Humanidades.
	Bloque PostGrado.
	Bloque Odontología.

	Bloque Enfermería.
Bermejo	Bloque Fac. Integral.
	Sistema Bermejo.
	Agropecuaria Bermejo.
Yacuiba.	Gran Chaco Yacuiba.
El Palmar	Ingeniería Agronómica
Villa Montes.	Veterinaria Villa Montes.
	Gas y Petróleo Villa Montes.
Caraparí	Bloque Carrera de Construcción.
Entre Ríos	Bloque Carreras de medio ambiente y topografía.

Figura 2: Unidades de la UAJMS

3.2. Tecnología

Las redes inalámbricas de área local (WIFI) se caracterizan en que las terminales o equipos de los usuarios no están interconectados físicamente mediante un cable, sino que se utilizan ondas de radio para este fin.

Esta tecnología hace uso de las frecuencias libres de licencia: las redes de área local inalámbricas o redes Wireless. Las LAN inalámbricas utilizan básicamente longitudes de onda correspondientes a las microondas (2,4 GHz y 5 GHz) y permiten tener anchos de banda apreciables (desde 1 MB/s en las primeras versiones hasta llegar a los 54 MB/s de los últimos estándares).

En muchos sitios, las redes Ethernet de cable tradicional, han sido ampliadas con la implantación de este tipo de redes inalámbricas. La interconexión de varias redes locales (como por ejemplo en el caso de redes inalámbricas que se extienden en todo el campus universitario) ha propiciado que algunos visionarios hayan visto la posibilidad de crear una red metropolitana con gran ancho de banda y con la posibilidad de acceso a Internet, de forma que se pudiera acceder a cualquier servicio de los que comúnmente se utilizan en Internet (correo, web, ftp, etc.) desde cualquier lugar dentro del ámbito metropolitano donde llega la señal de radio frecuencia.

ESTÁNDAR	VELOCIDAD MÁXIMA	INTERFASE DE AIRE	ANCHO DE BANDA DE CANAL	FRECUENCIA
802.11b	11 Mbps	DSSS	25 MHz	2,4 GHz
802.11a	54 Mbps	OFDM	25 MHz	5,0 GHz
802.11g	54 Mbps	OFDM/DSSS	25 MHz	2,4 GHz
802.11n	300 Mbps	OFDM/DSSS	40 MHz	2,4 – 5 GHz
HomeRF2	10 Mbps	FHSS	5 MHz	2,4 GHz
HiperLAN2	54 Mbps	OFDM	25 MHz	5,0 GHz
5-UP	108 Mbps	OFDM	50 MHz	5,0 GHz

Figura 3: Características de tecnologías inalámbricas

3.3. Beneficios

Mejor gestión académica y administrativo en el proceso enseñanza aprendizaje, mediante el ágil uso de las TICs.

Estudiante, profesores, directores y administrativos contarán con herramientas de fácil acceso a las TICs.

La facilidad que representará el poder acceder a la red de computadoras de la UAJMS, los sistemas universitarios y el Internet por parte de los usuarios de la UAJMS, ya que estos de aquí en adelante no tendrán que depender de un punto de acceso fijo a la Red.

Con este sistema se disminuyen los costos que representa la instalación de los nuevos puntos de red para equipos con interfaces inalámbricas, en especial en equipamiento, cables de red, accesorios de red y mano de obra.

Creación de grupos de usuarios dentro la UAJMS para una mejor administración de los anchos de banda, en especial para el control de acceso a Internet.

Mayor capacitación a los recursos humanos de la UAJMS en el campo de las tecnologías de comunicaciones.

3.4. Justificación de la Instalación de una Red Inalámbrica

Se decidió implementar una red inalámbrica por las siguientes razones:

Los sistemas WiFi son cada vez mas implementados en las universidades por que este facilita el acceso a las redes sin tener que depender de un punto de red Fijo.

Es eminente que el uso de los equipos portátiles se irá masificando en reemplazo por los equipos de escritorio. Muchos estudiantes ya en la actualidad cuentan con estos equipos, los mismos que son usados en los previos universitarios.

En lo que respecta a los sistemas de seguridad, paralelamente a los avances tecnológicos, los sistemas también cada día se van volviendo más vulnerables. Esto hace que se tenga que pensar en la implementación de sistemas que permita reducir los ataques de intrusos que intentan vulnerar los sistemas informáticos.

3.5. Estudio Legal

La implementación del presente proyecto desde el punto de vista legal conlleva las siguientes consideraciones:

La tecnología WiFi data en el mundo entero desde los principios de los años 1990, por la gran facilidad de acceso a las redes, este sistema ha venido creciendo últimamente con gran fuerza. Entre los aspectos legales a considerar es que al tratarse de un sistema de comunicación inalámbrica, los estándares bajo los cuales trabajan este sistema son 802.11b, 802.11g y 802.11n, las dos primeras trabajan en la frecuencia de 2.4Ghz y la última trabaja en 2.4Ghz y 5Ghz.

En nuestro país el uso de estas frecuencias no deben superar los 50 mW de potencia, es decir no se cancela a ninguna entidad si la potencia de los equipos no superan los 50 microwatts, y en particular cuando se trata de usar esta tecnología en ambientes cerrados como es el caso del presente proyecto, el uso es libre, por lo que no se tendrá ningún problema legal.

Todos los equipos a usarse para la implementación de este sistema están internacionalmente estandarizados, por lo que no se tendrá ningún problema de compatibilidad al momento de su funcionamiento.

En lo que respecto a la seguridad informática de los datos, en varios países del mundo ya existen leyes que sancionan las intromisiones a los sistemas informáticos, en el caso de Bolivia, desafortunadamente a la fecha no existen leyes que regulen o que sancionen el mal uso de la información.

Sin embargo este tipo de acciones en contra de los datos de la UAJMS pueden ser regulados mediante la implementación de normas o reglamentos internos al interior de la universidad.

3.6. Estudio de Sostenibilidad

Considerando que se trata de un proyecto de equipamiento, el tiempo de vida útil de los equipos son limitados, esto a que rápidamente estos pueden quedar obsoletos, en tal sentido el tiempo vida del proyecto será de 5 años.

Luego de 5 años para continuar ofreciendo los servicios de WiFi a los estudiantes se deberá pensar en otra etapa que permita por lo menos la actualización de los mismos.

En lo que respecta a Seguridad, igualmente dentro de unos 3 años se deberá evaluar la confiablidad del sistema de seguridad instalado para en caso necesario actualizar los equipos.

3.7. Consideraciones para la Implementación

Este proyecto durante su implementación estará a cargo directamente por la DTIC, dado que en la DTIC se cuenta con los recursos humanos con la suficiente experiencia en la implementación de este tipo de proyectos.

La infraestructura necesaria para la instalación de los equipos son descritos a continuación:

3.8. Implementación de la Red Wi-Fi

En la actualidad el sistema de comunicación inalámbrica en la universidad Juan Misael Saracho ya se encuentra implementado, para tal efecto se consideraron dos etapas, la primera implementada en la gestión 2009-2010 y la segunda en la gestión 2011.

Implementación de la Red Wi-Fi (Primera Etapa), abarca el 15% de las edificaciones de la UAJMS y ha llegado al máximo de su capacidad.

Implementación de la Red Wi-Fi (Segunda Etapa), abarca alrededor del 80% de las instalaciones de la UAJMS se implementa un sistema de seguridad para el resguardo de los datos.

3.9. Implementación de la Red Wi-Fi (Primera Etapa)

En la primera etapa se ha implementado un sistema WiFi, que sólo ha abarcado el 15% de todas las edificaciones de la UAJMS, debido a la falta de experiencia sobre la implementación de esta tecnología se considero solo una parte de los edificios de la Universidad:

LUGAR	Nº	UNIDAD
Ciudad Tarija.	1	Edificio del Rectorado.
	2	Bloque Ex – YPFB.
	3	Bloque Secretaría de desarrollo universitario.
	4	Edificio de ciencias de la salud.

Figura 4: Edificios con conexión WiFi (Primera Etapa)

Esta instalación del sistema de seguridad informática y sistema inalámbrico (WIFI) trabajaba a su máxima capacidad, por lo que no cabía la posibilidad de incrementar su cobertura.

3.9.1. Descripción General de la Implementación de la red Inalámbrica

Durante la primera etapa la oferta de los servicios de WiFi y seguridad que ofrecía la UAJMS eran limitados, logrando cubrir sólo el 15% en 4 edificios de la ciudad de Tarija.

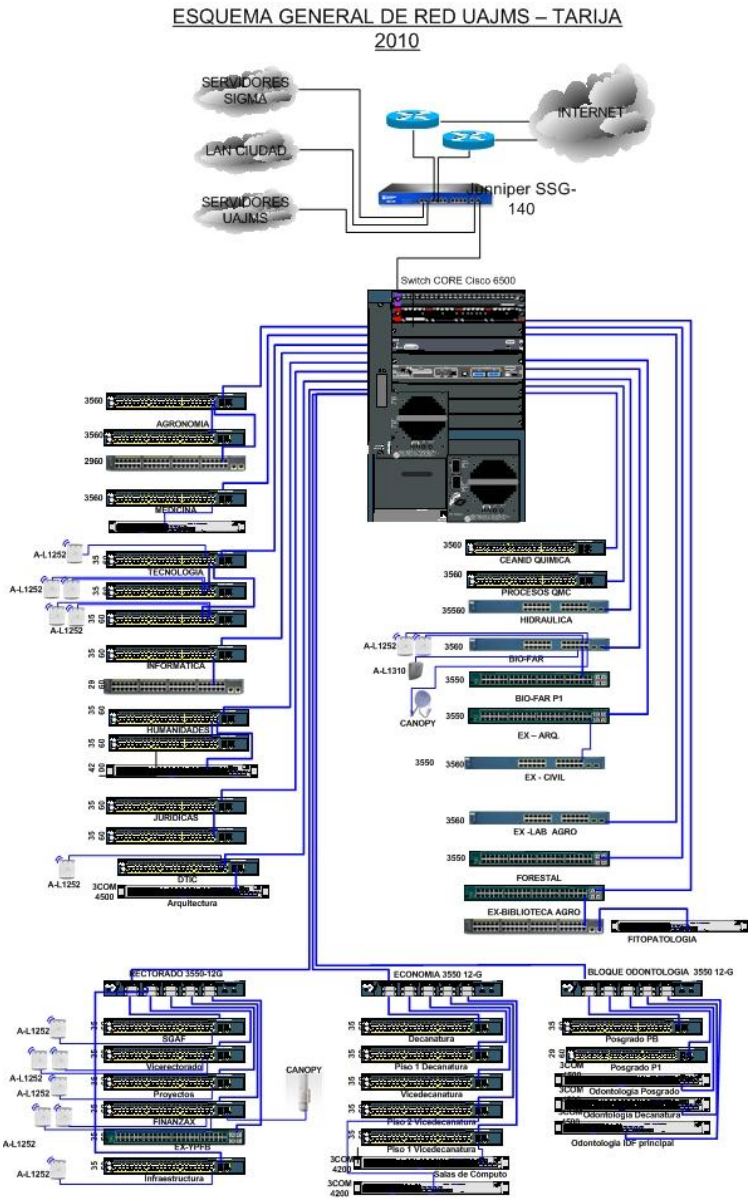


Figura 5: Esquema de la red

Es necesario hacer notar que en la primera etapa se pretendía cubrir toda la infraestructura de la UAJMS, sin embargo este fue reducido solamente a los edificios anteriormente nombrados, las razones son las siguientes:

Por falta de experiencia, y al no existir en el medio cercano redes inalámbricas de similar envergadura no se hizo un real dimensionamiento del equipamiento requerido.

Los equipos dimensionados en aquella oportunidad a la fecha de la implementación del proyecto fueron discontinuados.

Los equipos no estaban en función a los actuales equipos que fueron implementados en base a otros proyectos.

3.9.1.1. Equipos de comunicación inalámbrica

A continuación presentamos el detalle de los equipos de comunicación inalámbrica con los que se cuenta en la actualidad:

NRO	DESCRIPCIÓN	CANT.
1	APs Indoor Marca Cisco Modelo: AIR-LAP1252G-A-K9.	24
2	APs Outdoor Marca Cisco Modelo: AIR-LAP1310G-A-K9	2
3	Wireless Lan Controller Marca Cisco Modelos: AIR-WLC2112-K9.	4
4	Wireless Controller System: WCS-PLUS-UPG-K9 para 50 APs.	1
5	Módulo Wireless Lan Controller Cisco Modelo: WS-SVC-WiSM-1-K9.	1

Figura 6: Equipo WiFi

La capacidad de estos equipos no daba para expandir al resto de los edificios, mucho menos para llegar a las unidades de las provincias.

3.9.1.2. Equipo de Seguridad

En lo que respecta a la seguridad, no se contaba con un sistema de seguridad que permita una correcta monitorización de los sistemas de la UAJMS, excepto un firewall que solamente se encarga de habilitar y deshabilitar los acceso a cada segmente de red. Se utilizaba dos firewall: uno en funcionamiento y otro de backup. Las características de estos equipos son los siguientes:

Marca y modelo	Juniper SSG-140
Number of Ports:	11
Interfaces/Ports:	8 x RJ-45 10/100Base-TX LAN, 2 x RJ-45 10/100/1000Base-T LAN, 1 x RJ-45 Console Management, 1 x RJ-45 Auxiliary Management, 1 x USB
Technical Information	
Virtualization:	32000 Concurrent Session, 8000 Concurrent Session, 500 Security Policies Tenant, 125 Concurrent VPN Tunnel, 50 Tunnel Interface
Firewall Protection:	Worm Scanning, Trojan Horse, Network Attack Detection, Denial of Service (DoS), Brute Force Attack Mitigation, SYNflood Protection, Malformed Packet Protection, Distributed Denial of Service (DDoS), Backdoor Detection
Encryption Standard:	AES (256-bit), DES, 3DES (168-bit)
Authentication:	MD5, SHA-1, LDAP, RSA SecurID, RADIUS, XAUTH
VPN Support:	□ All management via VPN tunnel on any interface □ Redundant VPN gateways □ Remote access VPN □ VPN tunnel monitor □ Auto-Connect VPN
Features:	PAT, Virtual IP (VIP)
Media & Performance	
Firewall Throughput:	350 Mbps
I/O Expansions	
Number of Expansion Slots:	4
Expansion Slots:	(4 Total) Expansion Slot
Management & Protocols	

Management:	□ CLI □ Telnet □ SNMP v2 □ Web-based Management □ Networks NetScreen-Security Manager
Memory	
Standard Memory:	512 MB
Memory Technology:	DRAM

Figura 7: Características del equipo Firewall

Figura 8: Firewall Perimetral Instalado

Las características del equipo firewall con que se cuenta en la DTIC son las que se describen a continuación:

Éste está instalado a nivel perimetral, es decir es el que controla el acceso y la salida al Internet.

Se han creado varias zonas para la segmentación de la red, el equipo firewall es la que controla quienes tienen los permiso para al acceso a cada una de estas zonas.

El equipo tiene la capacidad simplemente de habilitar permisos por puertos y protocolos.

3.9.2. Problemas presentados en la Primera Etapa

Los problemas presentados después de la implementación del proyecto en su primera etapa fueron:

- Falta de acceso a redes mediante el sistema WiFi en al menos 85% de los edificios de la universidad.

- Sistemas implementados en la DTIC vulnerables ante cualquier tipo de intrusos.

3.10. Implementación de la Red WiFi (Segunda Etapa)

La segunda etapa del proyecto consiste en la implementación de un sistema de comunicación Inalámbrica y de Seguridad de datos en los predios universitarios, que permita contar con un acceso a redes inalámbricas en un 80% más de lo que se cuenta en la actualidad y garantizar la seguridad de datos en un 100%.

3.10.1. Metas planteadas para la Segunda Etapa

Que el 90% de los estudiantes y docentes de la universidad cuenten con facilidades de acceso a redes inalámbricas que les permita acceder a las redes sin depender de un punto de red físico.

Cubrir al menos el 80% de los edificios de la universidad mediante señal de redes inalámbricas, mas el 15% de la primera etapa, se tendrá una cobertura WiFi en el 95% de los edificios de la uajms (Ciudad y provincias)

Instalar un sistema de seguridad de aplicaciones para la base de datos, de tal manera que todos los datos e información de los servidores de la universidad se encuentren debidamente protegidos contra posibles intromisiones externas.

3.10.2. Cobertura a cubrir

A continuación se detallan los edificios considerados para la implementación del servicio en la segunda etapa:

UBICACIÓN O LUGAR.	NRO.	DESCRIPCIÓN DEPARTAMENTO DONDE SE INSTALARÁN LOS PUNTOS DE ACCESO.
Campus Universitario.	1	Bloque Ing. Forestal.
	2	Bloque Ing. De Alimentos.
	3	Bloque nuevo Ing. Agronómica.
	4	Bloque antiguo Fec. De Agronomía.
	5	Bloque Biblioteca de Agronomía.

	6	Bloques. Ceanid y laboratorios de Química.
	7	Bloque Ing. Química.
	8	Bloque Ing. Civil.
	9	Bloque Antiguo Ing. Civil.
	10	Bloque antiguo Arquitectura.
	11	Bloque Hidráulica.
	12	Bloque DTIC.
	13	Bloque Medicina.
	14	Bloque A Fac. de Ciencias Económicas.
	15	Bloque B Fac. de Ciencias Económicas.
	16	Bloque C Fac. de Ciencias Económicas.
	17	Bloque nuevo Fac. de Humanidades.
	18	Bloque nuevo Arquitectura.
	19	Bloque Edificio de Informática.
Ciudad Tarija.	20	Bloque Antiguo Ciencias Juirídicas.
	21	Bloque Antiguo Humanidades.
	22	Bloque PostGrado.
	23	Bloque Odontología.
	24	Bloque Enfermería.
Bermejo	25	Bloque Fac. Integral.
	26	Sistema Bermejo.
	27	Agropecuaria Bermejo.
Yacuiba.	28	Gran Chaco Yacuiba.
Villa Montes.	29	Veterinaria Villa Montes.
	30	Gas y Petróleo Villa Montes.
Caraparí	31	Bloque Carrera de Construcción.
Entre Ríos	32	Bloque Carreras de medio ambiente y topografía.

Figura 9: Edificios para conexión WiFi.

Todos los edificios o bloques arriba nombrados, no fueron considerados en la primera etapa del proyecto.

En los que respecta al sistema de seguridad, la demanda en este servicio se resume en lo siguiente:

- Necesidad de la implementación de un firewall a nivel de la bases de datos de la UAJMS.

- Necesidad de controlar los tráficos mediante los puertos habilitados en el firewall entre las diferentes zonas creadas.

- Detección y bloqueo de posibles intrusos que intenten penetrar la red de la UAJMS.

- Necesidad de filtrado de contenido a los sitios web desde la LAN a la WAN.

- Necesidad de implementar un sistema de copias de seguridad automatizado para los sistemas de la UAJMS.

3.10.3. Implementación del Componente WiFi

El componente Wifi segunda etapa consiste en la adquisición de equipamiento informático e instalación de equipos WiFi en los predios universitarios no considerados en la primera etapa.

La implementación de este sistema no solamente contempló a las unidades de la Ciudad de Tarija, si no que éste también contempla las unidades de las provincias (Bermejo, Yacuiba, Palmar, Villa Montes, Caraparí y Entre Ríos).

Este componente permitirá que estudiantes, docentes y administrativos que cuenten con equipos portables o PCs de con acceso inalámbricos puedan acceder a la red local sin necesidad de depender de un punto de red físico.

La posibilidad de acceso a la red inalámbrica de cada unos de los miembros, en especial estudiantes y docentes, coadyuvará a la mejora del proceso de enseñanza aprendizaje, dado que estos tendrán fácil acceso a la red e Internet.

Entre las principales características de este componente son descritos a continuación:

- Potenciamiento del centro de datos instalados en la DTIC, en el Campus Universitario mediante la dotación de mejor equipamiento de red.

- Instalación de Puntos de Acceso, APs en los interiores de los ambientes universitarios para la dotación de acceso a redes dentro de cada edificio.

- Instalación de puntos de acceso, APs en los exteriores de cada edificio para la dotación de acceso a redes a las personas que se encuentren en los jardines, kioscos o cafeterías.

- Capacitación de recursos humanos de la DTIC en el uso de las tecnologías WiFi mediante cursos oficiales de certificación en la marca del producto ofertado.

3.10.4. Implementación de un sistema de seguridad en redes

El componente de seguridad de datos está abocado a precautelar los datos, la información, el correo electrónico, los sitios web y velar por el buen uso del servicio de Internet dentro la Universidad Juan Misael Saracho.

Los actuales sistemas implementados en la universidad requieren ser protegidos por modernos sistemas de controles de acceso e intrusos.

Las principales características de este sistema de seguridad son descritas a continuación:

- Control de acceso a los sistemas de la universidad implementados en la DTIC.

- Monitorio en línea de todo el tráfico que generan los usuarios hacia los sistemas de la universidad.

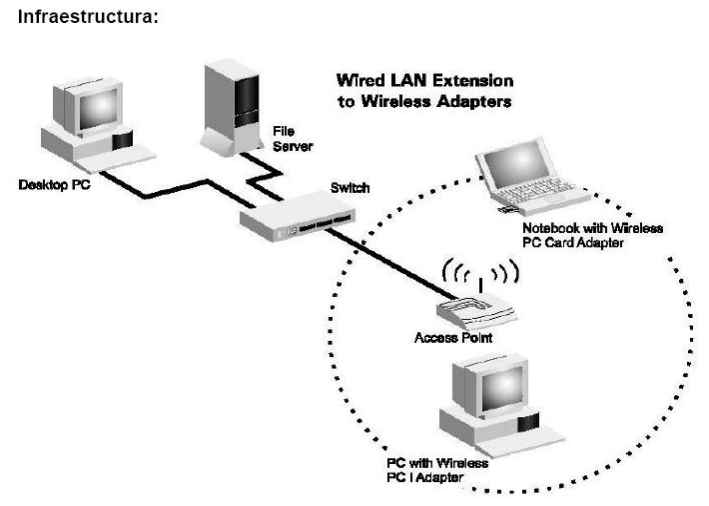
- Detección de posibles ataques de intrusos a los sistemas de la universidad.

3.10.5. Descripción General de la Implementación de la red Inalámbrica

Las redes Wi-Fi utilizan los estándares denominados IEEE 802.11a, 802.11b y 802.11g para proporcionar conectividad wireless fiable, rápida y segura. Una red Wi-Fi puede ser utilizada para conectar ordenadores entre sí o conectarse a Internet o a una red cableada tradicional (las cuales usan el IEEE 802.3 o Ethernet). Wi-Fi opera en las bandas de radio 2.4 y 5 GHz, con ratios de transferencia de 11Mbps (802.11b) y 54 Mbps (802.11a y 802.11g). Por tanto, las redes Wi-Fi pueden proporcionar un rendimiento similar a las redes Ethernet cableadas básicas 10BaseT utilizadas en muchas oficinas.

Para la Arquitectura de la red WI-FI de la Universidad Autónoma Juan Misael de Saracho, se ha optado por una red inalámbrica con el estándar desarrollado por IEEE 802.11, que describe las normas a seguir por cualquier fabricante de dispositivos Wireless para que puedan ser compatibles entre sí.Las redes inalámbricas se construyeron utilizando los Puntos de Acceso (AP), y es tipo Infraestructura como en las redes ethernet, en las cuales se dispone de un Switch o concentrador para unir todos los Host. Los Punto de Acceso (AP) son los encargados de "crear esa conversación" para que se puedan conectar el resto de Host inalámbricos que están dentro de su área de cobertura.

Figura 10: Topología WiFi



El cableado se realiza entre el AP y el Switch de cada Facultad cumpliendo todas las normas y Estandares de Cat. 5e.

La Alimentación de los puntos de acceso recibe la alimentación eléctrica mediante el cable de red Ethernet.

Se ha optado por este método, ya que de está forma se evita tener que llevar electricidad (220V CA) hasta los puntos de Acceso, los cuales están ubicados en lugares poco accesible o lejos de los tendidos eléctricos.

Utilizar el estándar Power over Ethernet (PoE) permite que un inyector de alimentación, inserte tensión en corriente continua (48V CC) en los pares no utilizados del cable trenzado (pares 7-8 y 4-5).

3.10.5.1. Componente WiFi

En lo que respecta a este componente, mediante la segunda etapa se habrá cubierto el 95% de los edificios mediante señal WiFi al servicio de los estudiantes de la UAJMS. En el siguiente cuadro se puede reflejar un detalle de los equipos necesarios.

NRO	DESCRIPCIÓN	CANTIDAD
1	Wireless Lan Controller	3
2	Access Point Indoor	110
3	Access Point Outdoor	30
4	Power inyector para Access point indoor	110

Figura 11: Requerimiento de Equipo Wifi

Dado que se trata de la instalación mayormente de APs indoor y outdoor, estos serán instalados en cada uno de los edificios de la UAJMS, tanto en las unidades de la Ciudad de Tarija y las unidades de las provincias.

Afortunadamente a la fecha en todos los edificios de la UAJMS ya se cuenta con la infraestructura de red que soporte la instalación de estos esquipo y el funcionamiento de este sistema de comunicación.

El resto de los equipos de este componente se encontrarán instalados en el Data Center de la DTIC y los IDFs instalados en cada edificio donde se cuentan con las condiciones necesarias para soportar estos equipos.

3.10.5.2. Componente Seguridad

En lo que respecta al sistema de seguridad, como se ha mencionado en los puntos anteriores, solo se contaba con un solo equipo Firewall, el cual solamente habilitaba e inhabilitaba los puertos para el acceso a los sistemas de la UAJMS, este equipo no hacía ningún tipo de análisis de tráfico de datos.

En el siguiente cuadro se detalla de los equipos restantes que se pretende instalar para la implementación de este sistema:

CANT	UNID	DETALLE
1	Global	Curso Oficial de certificación en seguridad de redes.
		Sub Total
1	Unidad	Sistema de Análisis y monitoreo para Redes. NAM-3
1	Unidad	Sistema de Autenticación para redes Wireless.
1	Unidad	Administrador de seguridad con Base de datos para filtrado web
1	Unidad	Administrador de servicios para redes.
1	Unidad	Módulo Switch de 24 puertos SFP capa 3. para Cisco Catalyst 6500
1	Unidad	Sistema de administración para equipos de red.

Figura 12: Requerimiento Equipo de Seguridad

En lo que se refiera a los equipos de seguridad, todos estos equipos se encontrarán instalados en el Data Center de la DTIC, dado que es en este lugar donde tienen instalados todo el sistema de gestión académica y administrativa de la UAJMS.

3.10.5.3. Identificación de Puntos de Acceso (APs)

En el siguiente cuadro se muestra la cantidad de puntos máximos estimados que se pretende atender por cada bloque.

UNIDADES CAMPUS UNIVERSITARIO					
BLOQUE	LUGAR	ANT. INDOOR	ANT. OUTDOOR	CONTRO LLER	ID-BLOQ
Agronomía bloque antiguo y Lab. De Fitopatología	Campus Tarija	3	2	0	CA01-0A
Laboratorios Agrícolas	Campus Tarija	2	1		CA01-0B
Bloque Antiguo Ing. Civil y Arquitectura	Campus Tarija	2	0		CA01-0C
Laboratorios de CEANID, Química y Física	Campus Tarija	4	2		CA01-0D
Bloque Ing. Química y Aulas Civil	Campus Tarija	4	1		CA01-0E
Bloque Laboratorios de Hidráulica, suelos y DTIC	Campus Tarija	4	2		CA01-0F
Bloque nuevo de Agrícolas e Ing. Forestal.	Campus Tarija	7	2		CA01-0E
Bloque de Medicina	Campus Tarija	2	1		CA02-0A
Bloques A, B y C de Ciencias Económicas y Financieras	Campus Tarija	6	1		CA02-0B
Bloque Nuevo de Biblioteca Central.	Campus Tarija	4	1		CA02-0C
Bloque Nuevo Comedor Universitario	Campus Tarija	3	1		CA02-0D

Bloque Nuevo Fac. Derecho	Campus Tarija	3	1		CA02-0E
Bloque Nuevo Fac. Humanidades	Campus Tarija	3	1		CA02-0F
Bloque Ing. Informática	Campus Tarija	3	1		CA02-0G
Bloque Nuevo de Arquitectura.	Campus Tarija	4	1		CA03-0A
Sub Total Campus Universitario		54	18	0	
UNIDADES DENTRO LA CIUDAD					
Odontología	Bolivar L.P. Ingavi	5	2	0	ODT-01
Enfermería	Calle Sta. Cruz	3	1	1	ENF-01
ExDerecho	Calle Campero	3	1	1	
Sub Total Fuera del Campus	11		4	2	
UNIDADES PROVINCIAS					
Fac. de Bermejo	Bermejo	6	1	1	BJO-F1
Inst. Agropecuario	Bermejo	4	0	0	BJO-F2
Fac. del Gran Chaco	Yacuiba	7	2	1	YCB-A1
Veterinaria ZooTecnia	Villaontes	4	1	1	VMT-V1
Gas y Petroleo y				1	
Agropecuaria	El Palmar	4	1	1	VMT-V1
Construcción	Caraparí	2	1	1	
Medio ambiente y Topografía	Entre Rios	2	1	1	
Sub Total Provincias	29		7	7	
CONTINGENCIA PARA NUEVOS EDIFICIOS					
Nuevos edificios en la UAJMS	11		6	1	

4.1.

Figura 13: Puntos de Acceso a Instalar

3.10.5.4. Identificación de equipamiento y requerimiento componente Wi-Fi.

En el siguiente cuadro se detallan el equipamiento necesario para la implementación del componente de Wi-Fi.

Nro	DESCRIPCIÓN	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
1	Wireless Lan Controller	3	57.139	171.418
2	Access Point Indoor	110	17.703	1.947.343
3	Access Point Outdoor	30	22.221	666.621
4	Power inyector para Access point indoor	110	1.951	214.618
COSTO TOTAL.				3.000.000

Figura 14: Cantidad y precio de Equipamiento WiFi requerido

En el cuadro anterior se puede apreciar la cantidad de Acceses Point Internos y Externos, Wireless Lan Controllers y otro equipamiento requeridos para el componente de WiFi.

DESCRIPCIÓN DEL DISEÑO DE RED INALÁMBRICA IMPLEMENTADA EN LA UAJMS

4.1. Descripción General del Diseño de Red Inalámbrica Implementada en la UAJMS

El diseño de la red inalámbrica para la Universidad Autónoma Juan Misael Saracho está relacionado con la consolidación de los recursos de control, administración, seguridad y monitoreo de los dispositivos que interactúan en la red Inalámbrica de una forma centralizada. Se implementó sobre una solución unificada que brindan los productos de la línea Cisco, y que permite un mejor desarrollo y alcanzar un alto desempeño.

4.1.1. Plataforma Unificada

Una solución unificada de redes inalámbricas contempla la integración de seguridad, administración y operación centralizada así como el acceso a usuarios invitados dentro de la red Inalámbrica. Dicha solución permite correr servicios de video, voz y datos dentro de una misma plataforma de red. La solución unificada de redes inalámbricas de área local (WLAN) permite el acceso seguro a recursos disponibles, así como acceso a invitados, permitiendo una fácil administración de su infraestructura mediante la centralización de la operación.

La administración centralizada de redes inalámbricas reduce sus costos de operación al tener que asignar menos recursos para su buen funcionamiento. La solución unificada de redes inalámbricas integra el acceso seguro a la red mediante el método más conveniente, dependiendo de las políticas de seguridad implementadas así como la proyección de crecimiento. La administración se ve significativamente mejorada debido a la autoconfiguración de su infraestructura inalámbrica y a la fácil visualización de la red, donde cada operación es realizada desde un solo punto permitiendo de esta forma reducir costos en recursos asignados con dicho propósito.

4.1.2. Beneficios

Dentro de esta alternativa existen algunos beneficios que sustentan la implementación de una solución unificada para redes inalámbricas.

- Administración y Operación Centralizada
- Seguridad mediante el acceso Inalámbrico.
- Localización de dispositivos Wi-Fi en tiempo real.
- Cobertura en áreas internas, exteriores o extensas.
- Una sola plataforma para correr servicios de Datos, Voz y Video.

4.1.3. Cobertura de la Red Inalámbrica en la Ciudad de Tarija (Campus Universitario)

La figura 25 muestra una imagen satelital del campus universitario donde se delimita claramente el área total del campus.

La siguiente imagen muestra la cobertura inalámbrica garantizada en el campus Universitario, donde los círculos amarillos hacen referencia a la cobertura alcanzada con los puntos de acceso externos al edificio, y los círculos celestes hacen referencia a los puntos de acceso para interiores (indoor).

Figura 1: Cobertura inalámbrica en el campus Universitario

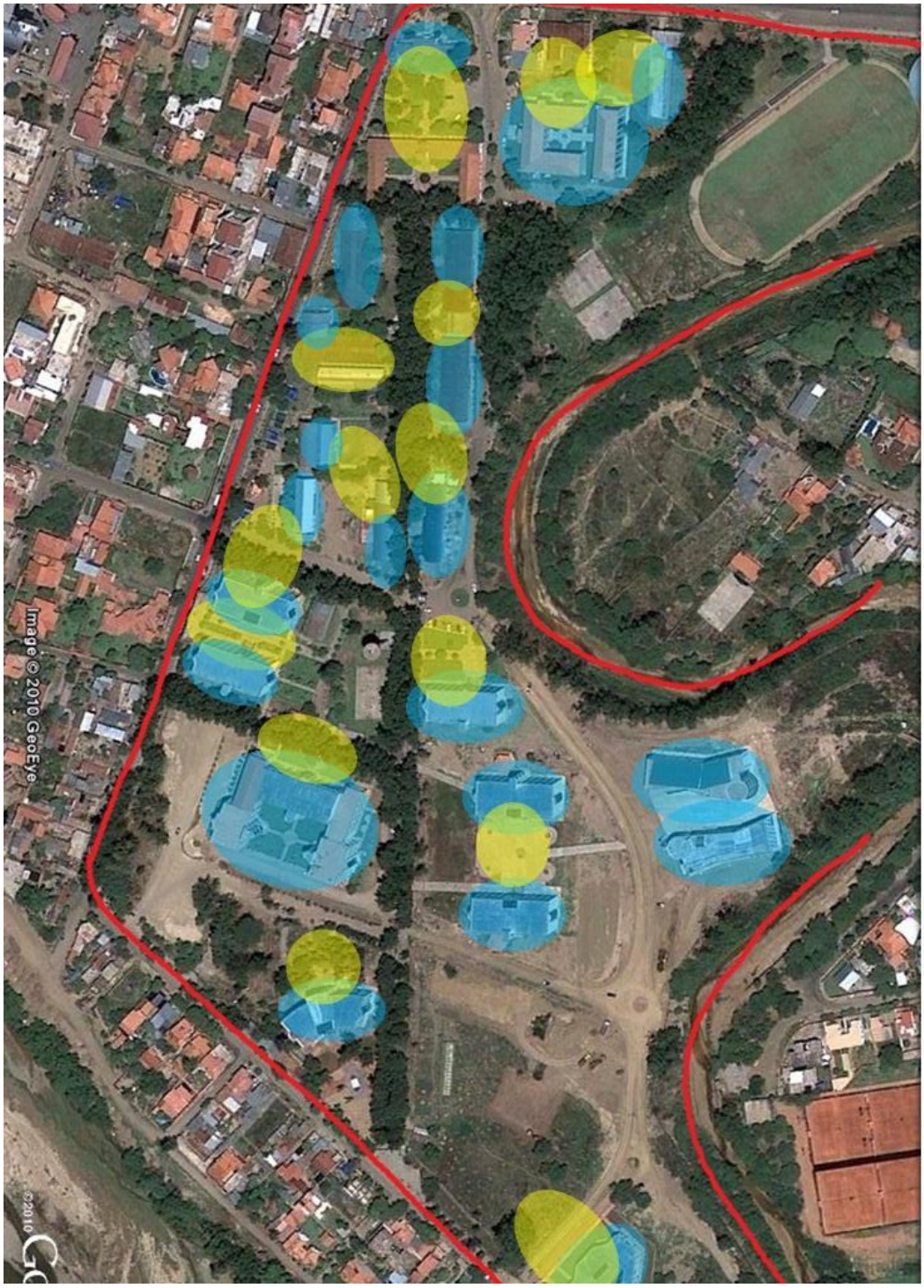


Figura 2: Figura 25: Cobertura inalámbrica en el campus Universitario mostrando los puntos de accesos internos y externos

4.1.4. Diagrama General de la Red Inalámbrica de la UAJMS

El siguiente diagrama muestra la plataforma de red unificada de la UAJMS donde cada uno de los edificios o bloques se interconectan con un enlace redundante de fibra óptica de tipo monomodo. Si bien en la UAJMS se tiene algunos edificios físicamente fuera del campus universitario, estos lógicamente pertenecen al backbone del campus universitario como el edificio central del Rectorado, Departamento de Finanzas, Facultad de Odontología y el Departamento de Posgrado representados por una interconexión simple o no redundante de fibra óptica también de tipo monomodo.

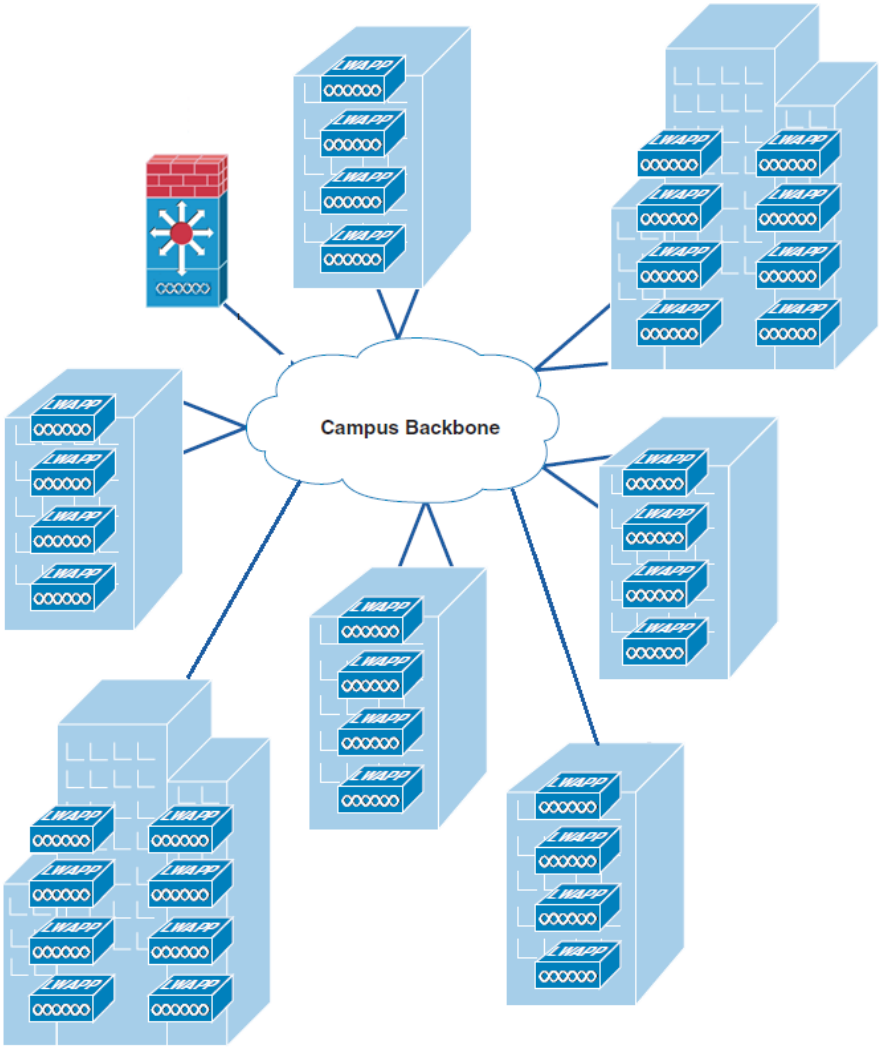


Figura 3: Diagrama de la Red Inalámbrica en la Ciudad de Tarija

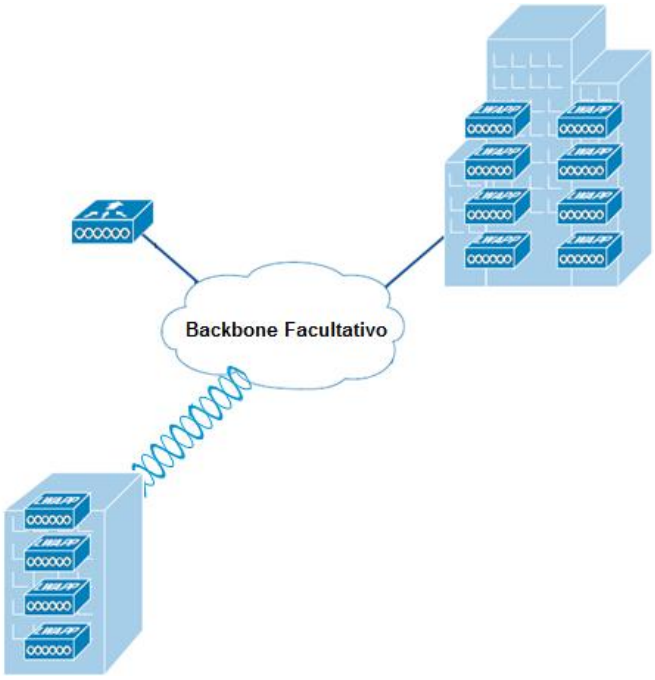


Figura 4: Diagrama General de la Facultad de Ciencias Integradas De Bermejo

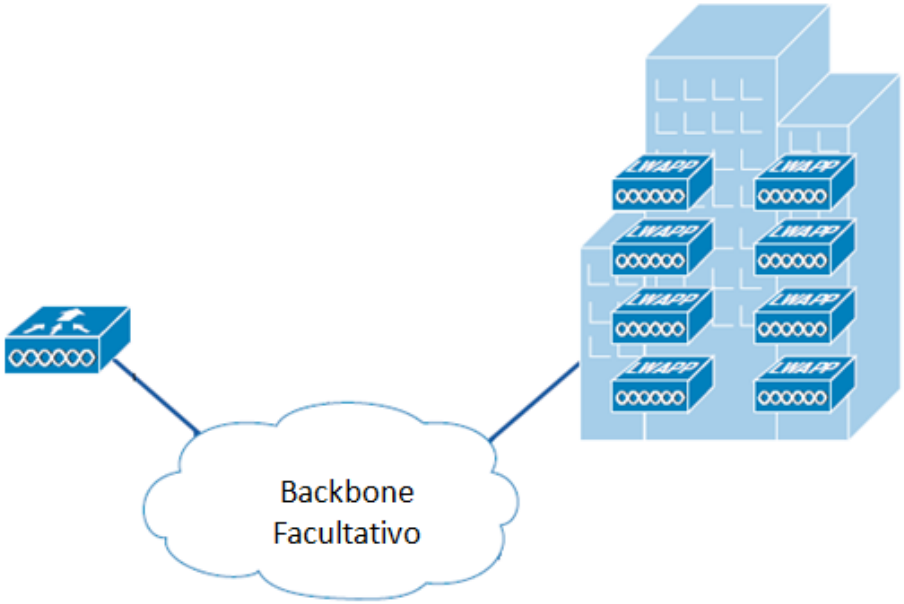


Figura 5: Diagrama General de la Facultad de Gran Chaco y Villamontes

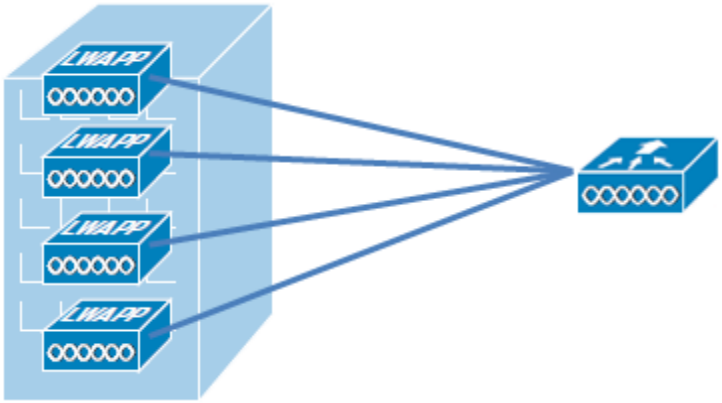


Figura 6: Diagrama General de los Programas de Ingeniería Agropecuaria de El Palmar, Entre Rios y Caraparí

4.1.5. Características Generales de la red inalámbrica de la UAJMS

4.1.5.1. Roaming

El roaming se define como la libertad para movilizarse libremente dentro de un espacio determinado, sin que exista lapsos de interrupción entre la comunicación de los usuarios cuando pasan de la cobertura de un punto de acceso a la cobertura de otro (Figura 31). Para permitir la itinerancia (roaming) y movilidad de los usuarios, es necesario colocar los Access Point de tal manera que haya "overlapping" o superposición entre los radios de cobertura.

Existen dos clases de roaming, cuando un usuario cambia de un punto de acceso a otro, reasociándose con este nuevo punto de acceso pero que pertenece a la misma subred. El cambio entre diferentes puntos de acceso que se encuentran en otros niveles de red (subredes), se denomina roaming de capa 3.El Roaming dentro de la red de la UAJMS permitirá velocidades máximas de hasta 100 km/h a 12 Mbps.

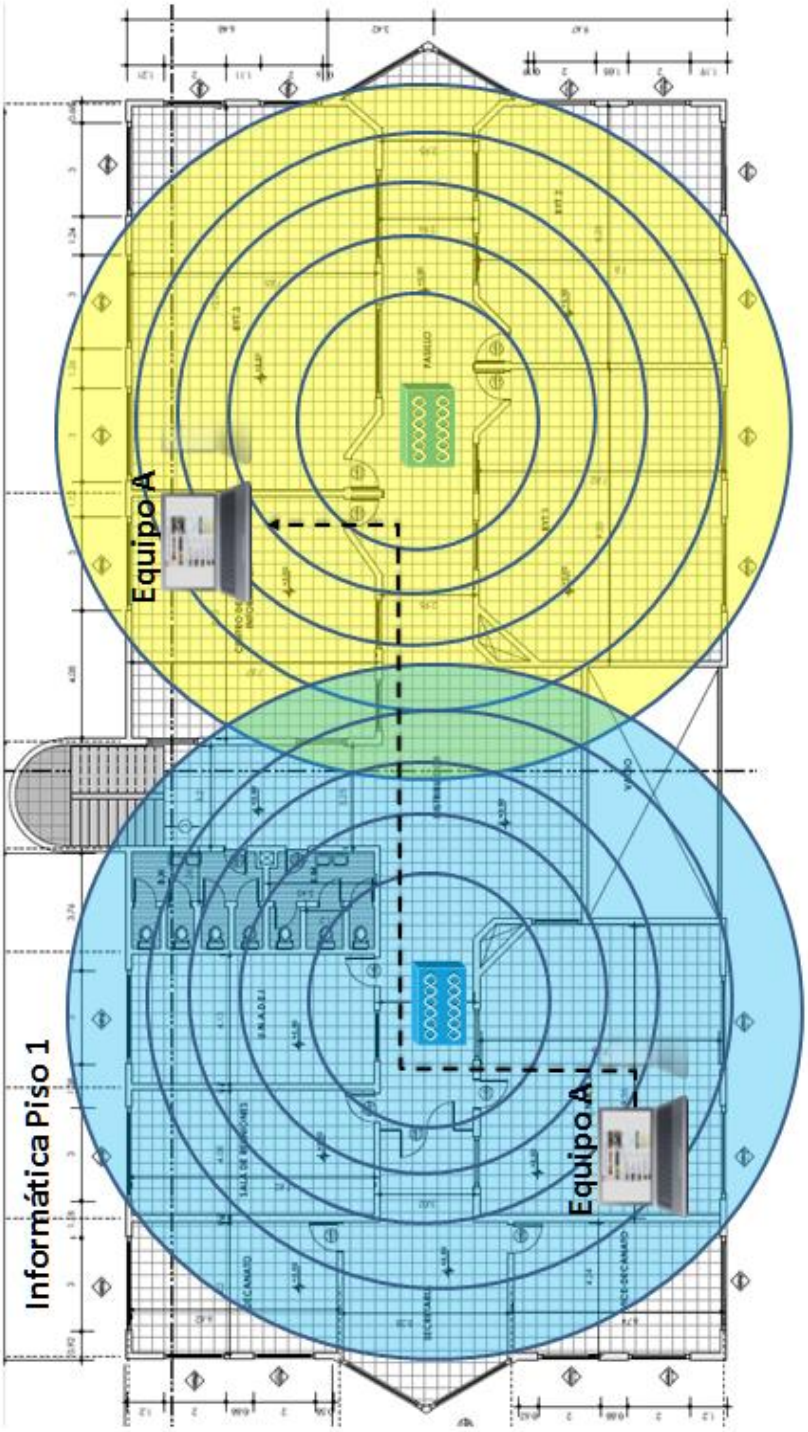


Figura 7: Roadming

4.1.5.2. Balanceo de Carga

El protocolo LWAPP permite el balanceo de carga dinámico entre los puntos de acceso asociados a un controlador para aumentar el rendimiento. Los controladores tienen acceso a la potencia de señal que hay en los puntos de acceso. Cuando un cliente quiere asociarse a un punto de acceso, el controlador tiene acceso a la cantidad de señal que recibe el cliente de los diferentes APs.

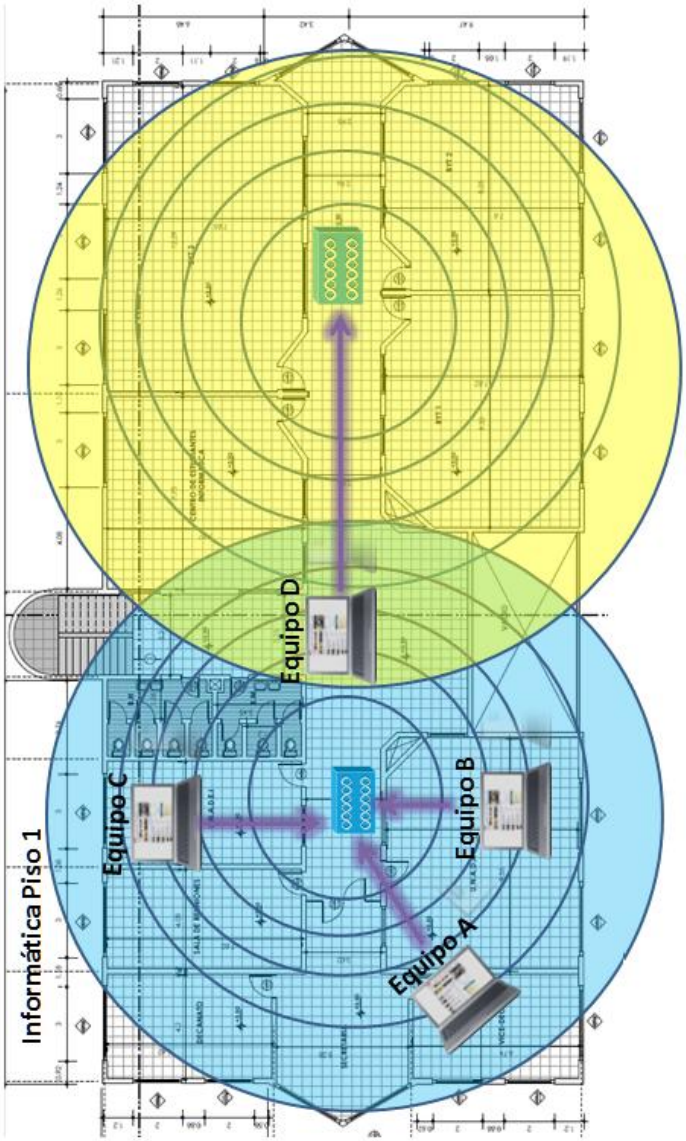


Figura 8: Balanceo de Carga

Entonces, el controlador escoge qué punto de acceso es el más adecuado para el cliente, en función de la potencia y la relación señal-ruido (SNR).

4.1.6. Mejoramiento de la Radiofrecuencia Mediante la Tecnología CleanAir

La resolución de problemas de rendimiento y de seguridad en redes inalámbricas se convierte en una prioridad cada vez más alta. EL sistema CleanAir puede detectar las interferencias de RF que otros sistemas no pueden ver, la identificación de la fuente de interferencia y localización sobre un plano. Proporcionar ajustes automáticos para optimizar la cobertura inalámbrica en torno a la interferencia. La tecnología CleanAir vine embebida dentro de los Access Points mediante un chip cargado con parte de un software que analiza el espectro (Spectrum Expert) que puede realizar el monitoreo en tiempo real y sin desasociar a sus usuarios que puede contener en ese momento para medir la calidad de RF en el aire conjuntamente con otros Access Points, estos interactúan con el WCS/WLC, el WLC es el cerebro y el que decide la configuración más adecuada para propagar radiofrecuencia de manera que esta RF sea la más óptima para brindar conectividad a los usuarios.

La naturaleza dinámica del espectro viene dada en la capa física, se refleja en las cosas, la radiofrecuencia es absorbida por las cosas, es un medio compartido en lo que no toda RF es netamente dedicada solo para nuestros usuarios y no toda radiofrecuencia es netamente de uso para nuestra red. Pueden existir y convivir dentro de nuestra red inalámbrica otros dispositivos que generen degradación de radiofrecuencia en el aire.

La figura 33 ilustra cómo es el comportamiento del espectro en nuestro tráfico 802.11n cuando hay una cámara de video inalámbrica que transmite con una AP que no es parte de nuestra red.

4.1.7. Mejoramiento de la Radiofrecuencia Mediante la Tecnología Cleanair

La resolución de problemas de rendimiento y de seguridad en redes inalámbricas se convierte en una prioridad cada vez más alta. EL sistema CleanAir puede detectar las interferencias de RF que otros sistemas no pueden ver, la identificación de la fuente de interferencia y localización sobre un plano. Proporcionar ajustes automáticos para optimizar la cobertura inalámbrica en torno a la interferencia. La tecnología CleanAir vine embebida dentro de los Access Points mediante un chip cargado con parte de un software que analiza el espectro (Spectrum Expert) que puede realizar el monitoreo en tiempo real y sin desasociar a sus usuarios que puede contener en ese momento para medir la calidad de RF en el aire conjuntamente con otros Access Points, estos interactúan con el WCS/WLC, el WLC es el cerebro y el que decide la configuración más adecuada para propagar radiofrecuencia de manera que esta RF sea la más óptima para brindar conectividad a los usuarios.

La naturaleza dinámica del espectro viene dada en la capa física, se refleja en las cosas, la radiofrecuencia es absorbida por las cosas, es un medio compartido en lo que no toda RF es netamente dedicada solo para nuestros usuarios y no toda radiofrecuencia es netamente de uso para nuestra red. Pueden existir y convivir dentro de nuestra red inalámbrica otros dispositivos que generen degradación de radiofrecuencia en el aire.

La figura 33 ilustra cómo es el comportamiento del espectro en nuestro tráfico 802.11n cuando hay una cámara de video inalámbrica que transmite con una AP que no es parte de nuestra red.

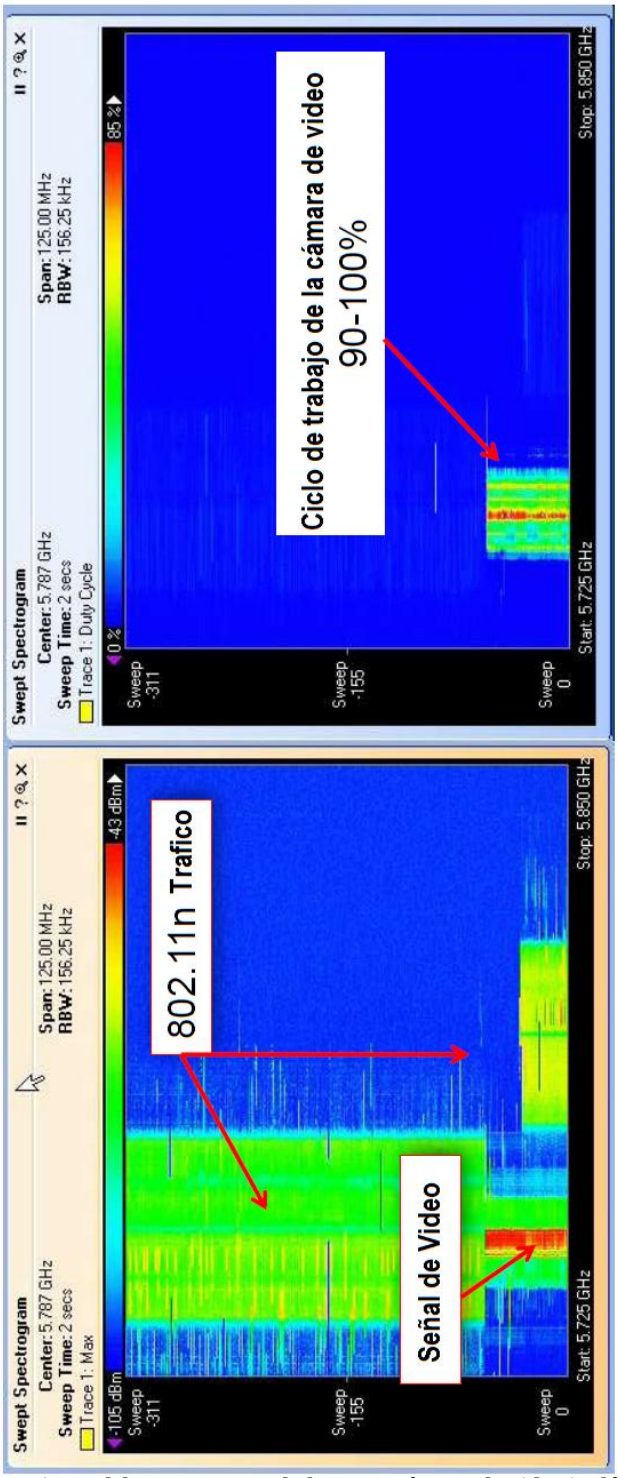


Figura 9: Comportamiento del espectro cuando hay una cámara de video inalámbrica que transmite con una AP que no es parte de la red

El Software Spectrum Expert muestra que la señal de Radiofrecuencia de nuestro tráfico en 802.11n se degrada entre un 90 y 100%. Es de esta manera que los Access Points instalados en la UAJMS con tecnología CleanAir procesan ese tipo de información envían al WLC para que lo interprete identifique el problema y lo mitigue ya sea cambiando a un canal distinto en el cual está trabajando esa cámara inalámbrica o si no existiera canales más limpios puede llegar a cambiar de frecuencia de trabajo.

La Figura 34 muestra el ejemplo de la cámara de video que transmite en el canal 6 en 802.11n el cual degrada la señal de toda la readiofrecuencia de nuestro usuario que está en la misma frecuencia y en el mismo canal pero en distinto Access Point.

Nuestro Access Point identifica mediante la tecnología CleanAir la degradación de nuestro espectro de radiofrecuencia, envía los reportes al WCS/WLC y es el WLC quien envía nuevas configuraciones de manera automática al Access Point para que éste cambie a un canal que no tenga esta interferencia en el espectro. (Figura 35)

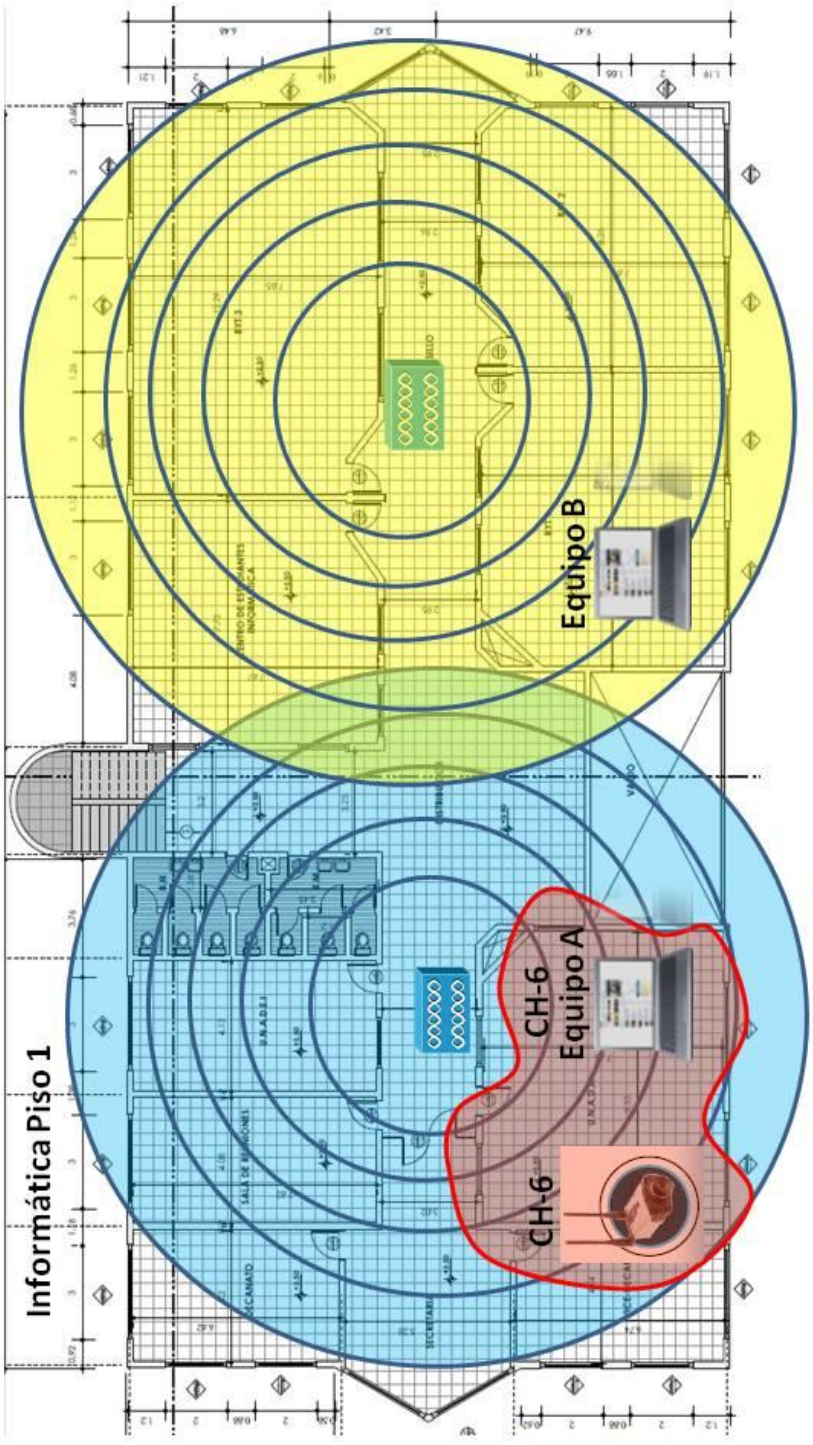


Figura 10: Cámara de video que transmite en el canal 6 en 802.11n

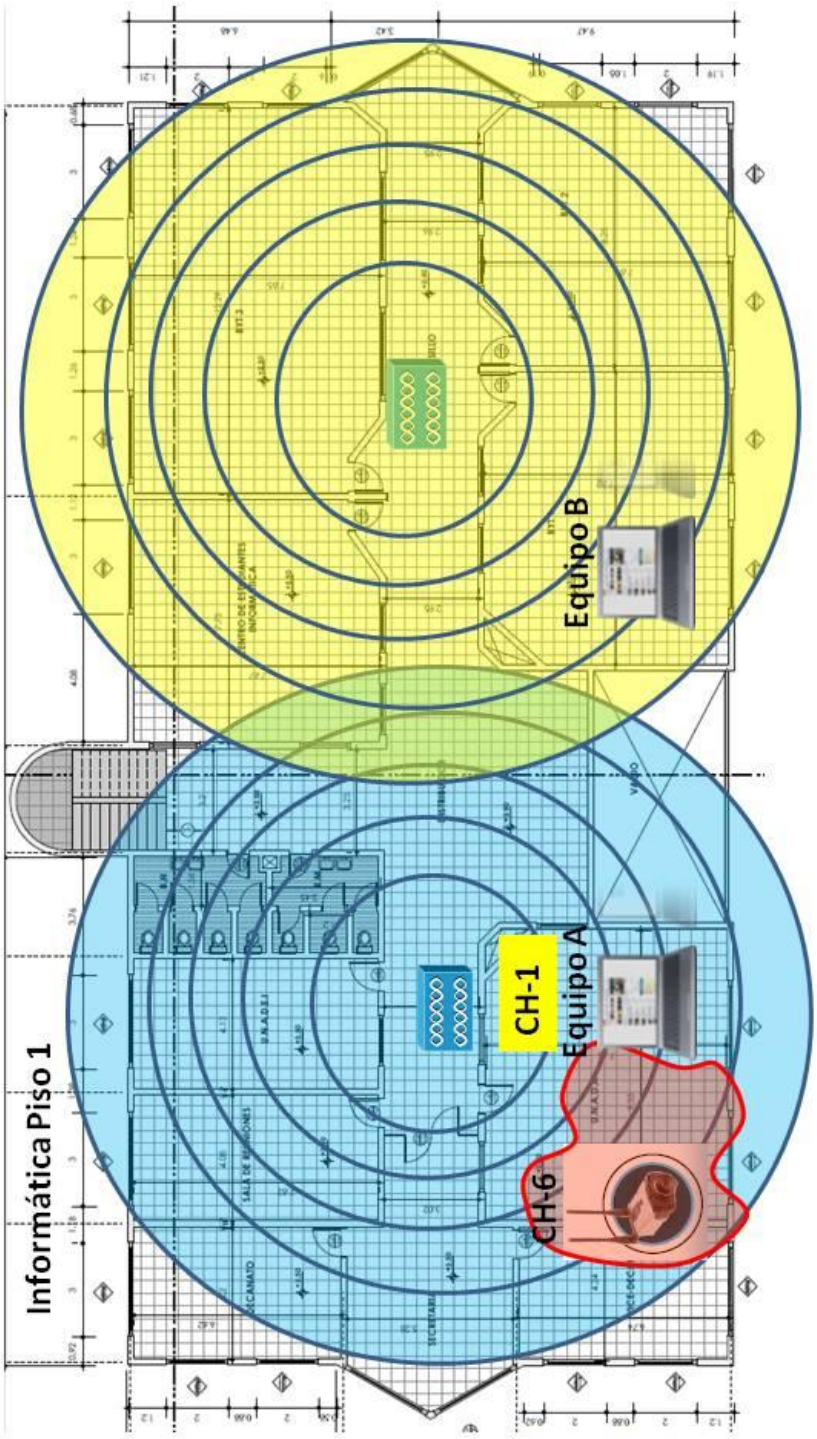


Figura 11: Access Point que identifica mediante la tecnología CleanAir la degradación del espectro de radiofrecuencia

De esta manera nuestro tráfico que corría por en 802.11n dentro del canal 6 cambia a otro canal con espectro de radiofrecuencia más limpio mejorando notablemente el rendimiento de conexión entre el usuario y el Access Point.

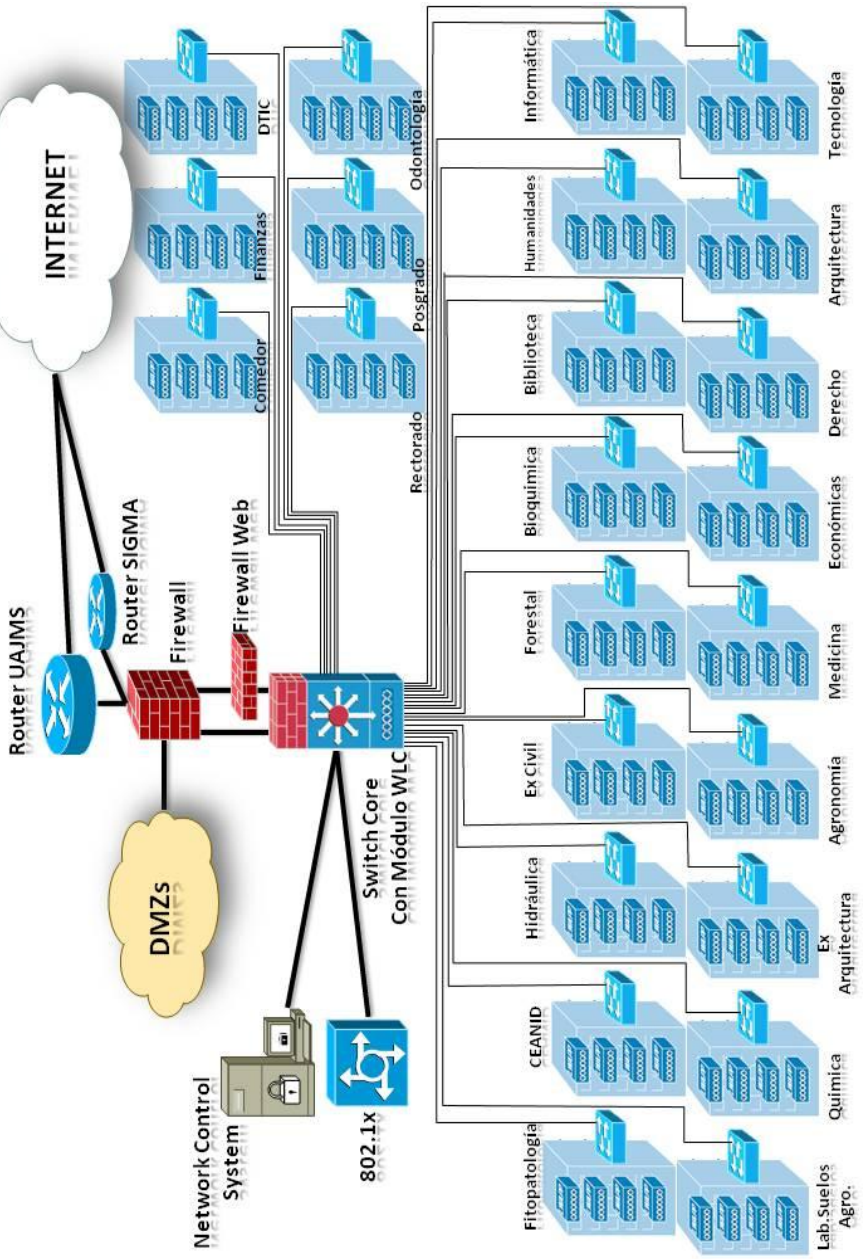


Figura 12 Diagrama General de la Red Wifi de la Ciudad de Tarija

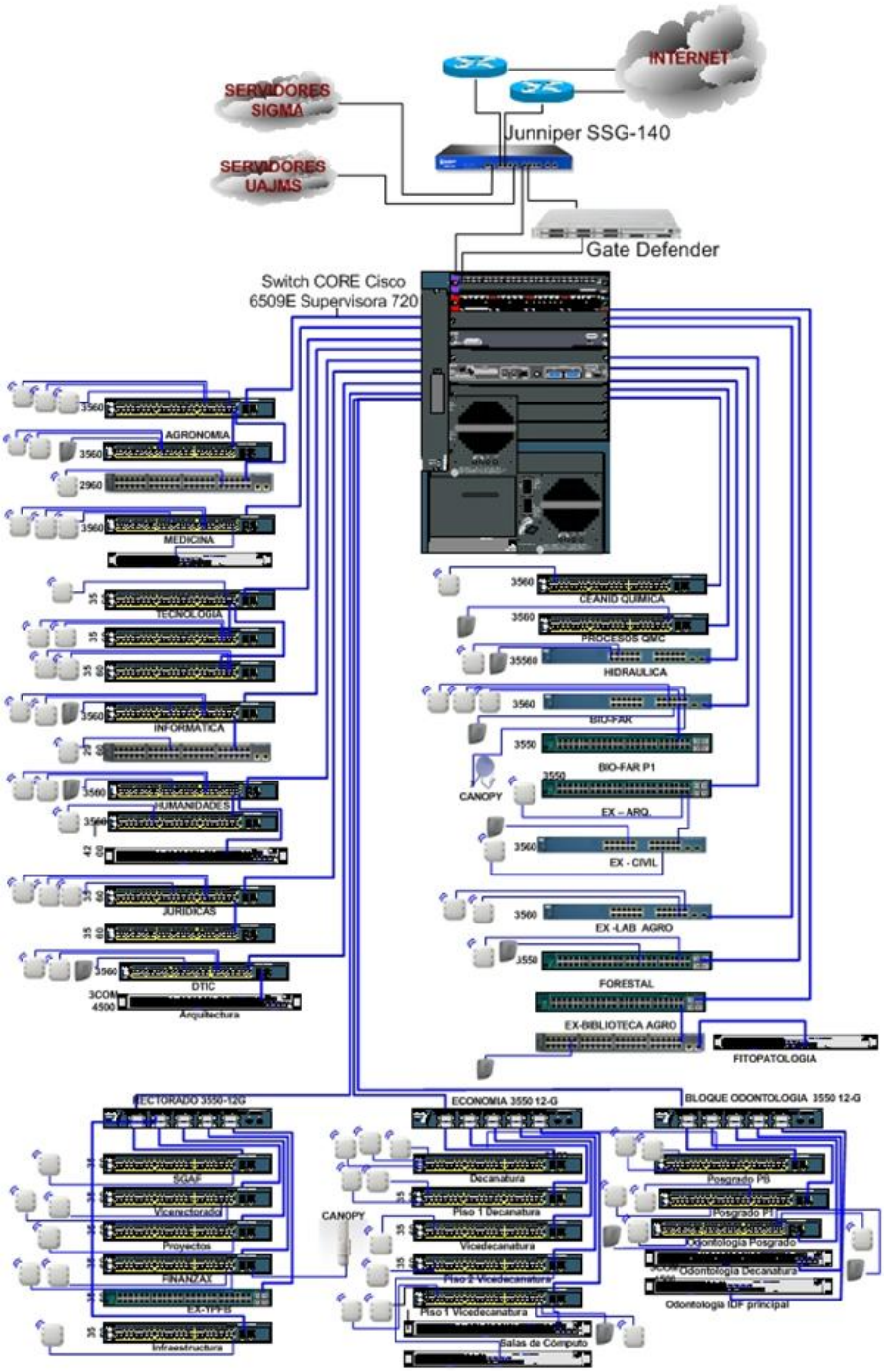


Figura 13: Esquema General de la red UAJMS Tarija-2011

4.2. Descripción General de la Implementación de la red Inalámbrica (Primera Etapa)

Dentro de la red cableada de la UAJMS por la cantidad de usuarios conectados y las demandas existentes de brindar conexión a nuevos usuarios tanto en el área estudiantil mediante sus salas de cómputo, centro de estudiantes. En el área de Docentes mediantes sus direcciones de departamentos, salas docentes, salas de investigación. O en el área administrativa dispersas por todas las facultades académicas, departamentos, direcciones, secretarías tanto dentro como fuera del campus, estas demandas de conexión que en un gran porcentaje son para poder explotar recursos de red interna como sistemas académicos, sistemas administrativos y sobre todo porque cada día aparecen más aplicaciones colaborativas que se requieren para desarrollar los trabajos en las distintas áreas dentro de la UAJMS pero estas aplicaciones son cada vez más exigentes, como las aplicaciones de video, voz, aplicaciones en Web 2.0 entre otras. Por ende estas aplicaciones requieren mayores anchos de banda con menor latencia en la comunicación entonces debemos poder soportar distintos tipos de comunicaciones o servicios con mayores anchos de banda.

Es por estos motivos que al querer brindar un servicio inalámbrico dentro de ambientes exigentes donde se requiere llegar con radiofrecuencia de forma confiable no solamente con conexiones referidas a 8002.11n sino también donde se puedan emplear distintos tipos de comunicación como bluethoo, telefonía celular y otros, hace de que se tenga que brindar una solución que sea confiable en nuestros sistemas de radiofrecuencia en estos ambientes que pueden llegar a ser propensos.

También se consideró comunicaciones confiables y predecibles en todos los ambientes que necesitamos iluminar con radiofrecuencia. Predecibles porque necesitamos la misma confiabilidad de conexión aún cuando nos estemos desplazando por estos ambientes iluminados con RF, entonces la cobertura tiene que ser consistente con una conectividad sin inconvenientes.

En base a los desafíos que se tenía y los requerimientos de los mismos, Se busca tener una comunicación con las mismas características de calidad, disponibilidad y confiabilidad con las que cuenta las redes cableadas. La pregunta que nos hicimos es ¿Cual es el protocolo o tecnología inalámbrica que nos puede dar una solución en esta nueva generación de comunicación? Pues la respuesta más efectiva que se encontró es el protocolo 8002.11n. Con este protocolo es donde encontramos varias soluciones a las necesidades o desafíos que se estaba requiriendo para la implementación de un sistema inalámbrico dentro de la UAJMS.

4.2.1. Descripción del modelo jerárquico implementado

El diseño de WLAN dentro del campus universitario, se describe de acuerdo a un modelo de niveles de jerarquía definidos mediante la figura 38, cada nivel describe las características de comportamiento presentes en el diseño y divide a la red WLAN, donde serán los encargados de transformar o poder configurarla para permitir la escalabilidad, redundancia, incremento de usuarios en la red, fácil detección de errores y la adaptación a cambios tecnológicos.

Nivel 1

Este nivel ofrecerá una conexión lo más rápida posible entre los puntos de distribución, y consta de un ruteador principal el mismo que provee la conectividad entre el exterior y la red interna

Nivel 2

El tráfico en la red es dirigido a través de cada uno de los servicios mediante un Switch de Core capa 3, él mismo que permite alternativas de poder segmentar los dominios de colisión y broadcast, para procurar evitar las congestiones en la red principal. Posee un switch de core que forma el backbone principal de la red, el mismo que permite la comunicación de los edificios que existen en el campus universitario, mediante la utilización de fibra óptica monomodo. Además maneja un

control al borde de la red con servicios de red inteligentes, incluye calidad de servicio (QoS), clasificación y priorización de tráfico.

Nivel 3

Este nivel permite la administración y sirve como punto de concentración para acceder a cada unos de los servicios de la red inalámbrica. Los switches manejan una conmutación de paquetes a nivel de capa 3 y 2 del modelo OSI. Además con la funcionalidad de administración de los diferentes sectores que conformará la red, a través de dispositivos específicos para el monitoreo y gestión de redes inalámbricas, se configuró de una manera que permita obtener una seguridad efectiva a través de un servidor de RADIUS (802.1X). La administración de los recursos de radio frecuencia de todos los Puntos de Acceso conectados se la realiza a través del Wireless LAN Controller (WLC).El Wireless Control System (WCS) es una plataforma que permite direccionar la planificación LAN Wireless, configuración, administración y movilidad de servicios. Provee un recurso poderoso que permite que el administrador diseñe, controle y monitoree las redes Wireless desde una ubicación centralizada simplificando las operaciones.

Nivel 4

Es la capa de acceso de los usuarios a los distintos servicios ofrecidos por la red, la cual se encarga de distribuir los diferentes enlaces inalámbricos hasta el nivel del usuario. Se encuentran ubicados los puntos de acceso con sus respectivas configuraciones dependiendo de la capacidad del número de usuarios finales y la cobertura de cada celda emitida por el Access Point. Los dispositivos finales de comunicación se encuentran accediendo a cada aplicación de red, a través de los puntos de acceso ya que corresponden a la arquitectura de la red Inalámbrica de la UAJMS. Estos pueden ser equipos portátiles o de escritorio, así como cualquier otro dispositivo que embeba la tecnología Wi-Fi.

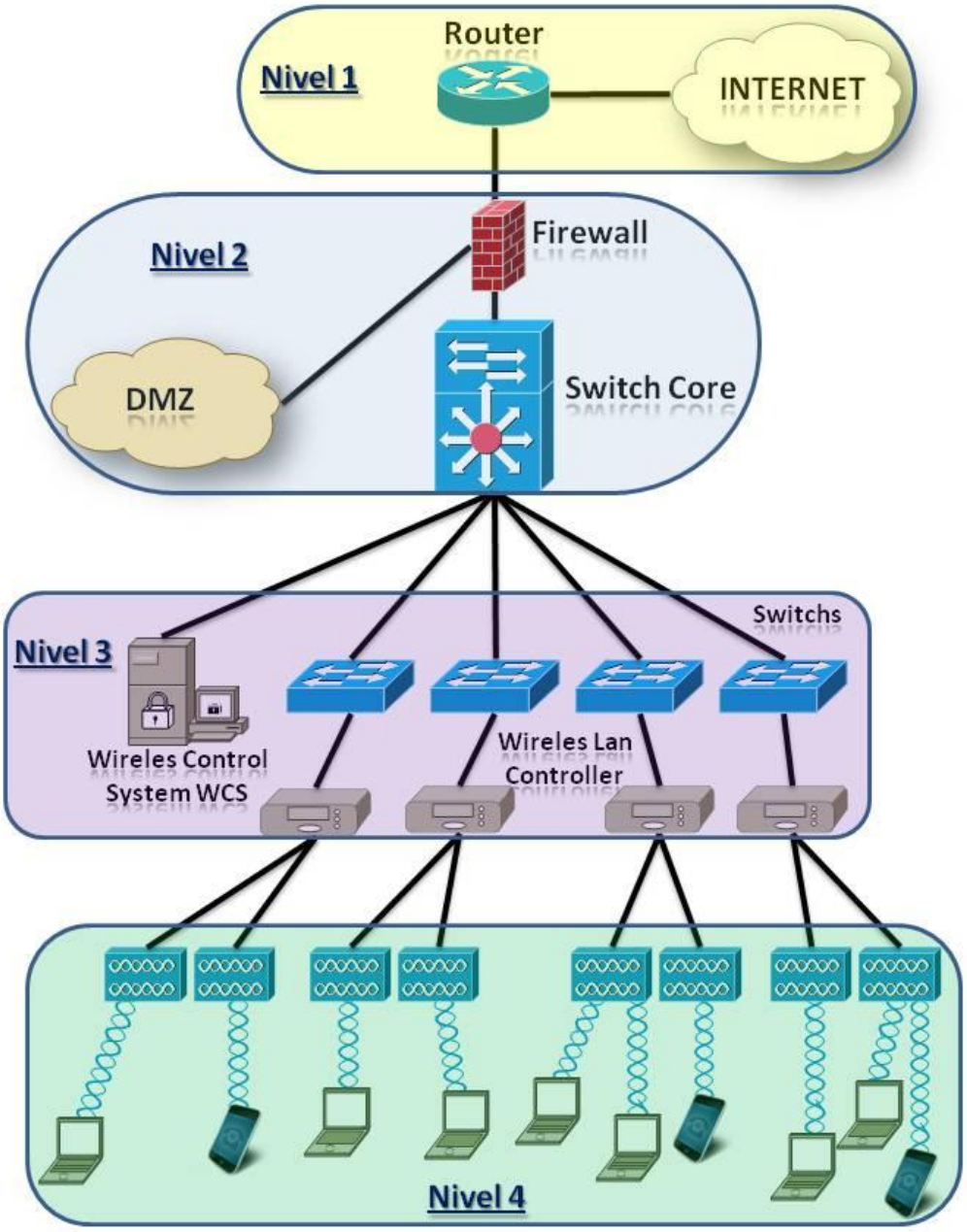


Figura 14: Modelo jerárquico implementado en la primera etapa

4.2.2. Descripción de las características de la tecnología Wifi implementada en la **primera etapa**

Los equipos AIR-LAP1252G-A-K9 que poseen la tecnología MIMO la trasmisión de datos se realiza mediante Múltiples antenas que mandan y reciben la señal. Multeple Input Multiple Output.

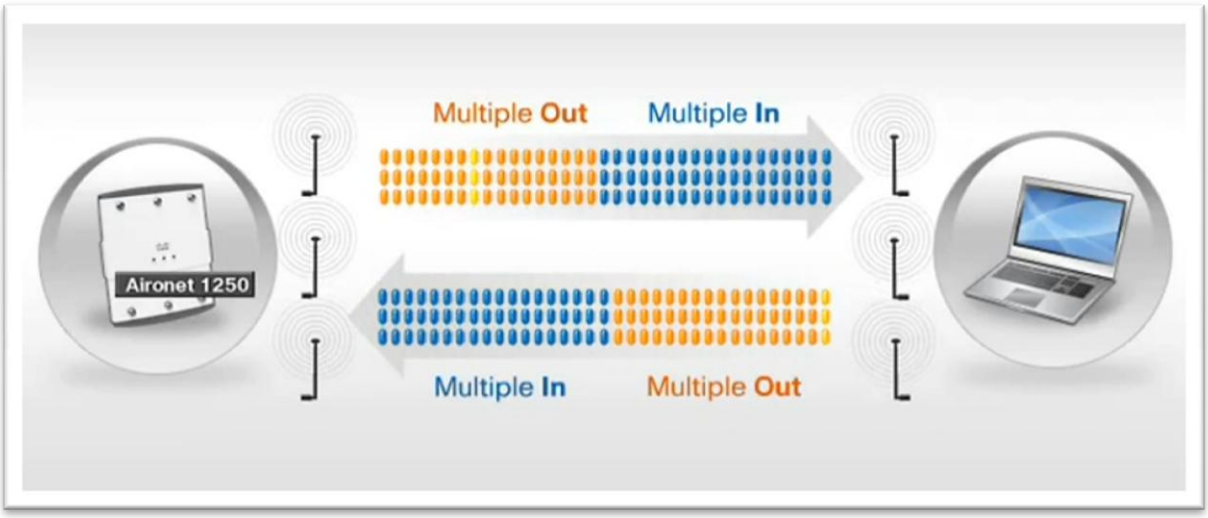


Figura 15: Tecnología MIMO

En un ambiente indoor hay distintos rebotes de señales que salen desde el access point hasta los usuarios tomando diferentes caminos y recorriendo distintas distancias llegando hasta el usuario corridos en fase uno respecto a otro (como se muestra en la figurar 40). Una de las características de los access points instalados en la UAJMS que quizá con otros equipos que tienen tecnología MIMO no podríamos llegar a conseguir, es poner en fase estas señales que llegan de RF al usuario consiguiendo de esa manera un aumento de la señal recibida y un aumento en el desempeño. Y este sistema no necesita que nuestros usuarios tengan MIMO en sus dispositivos móviles o laptops con lo que nuestros APs lo tienen basta para que el usuario conectado en banda G o banda A goce de este beneficio que se denomina Beam Forming y es desarrollado propiamente por la marca de los equipos implementados, lo cual nos brinda mayor rendimiento en la comunicación. EL proceso inverso donde las señales transmitidas desde el usuario hacia el acces point donde también se llega a conseguir poner en fase se denomina maximal ratio combining esto viene embebido dentro de lo que se denomina la tecnología M-Drive de Cisco.

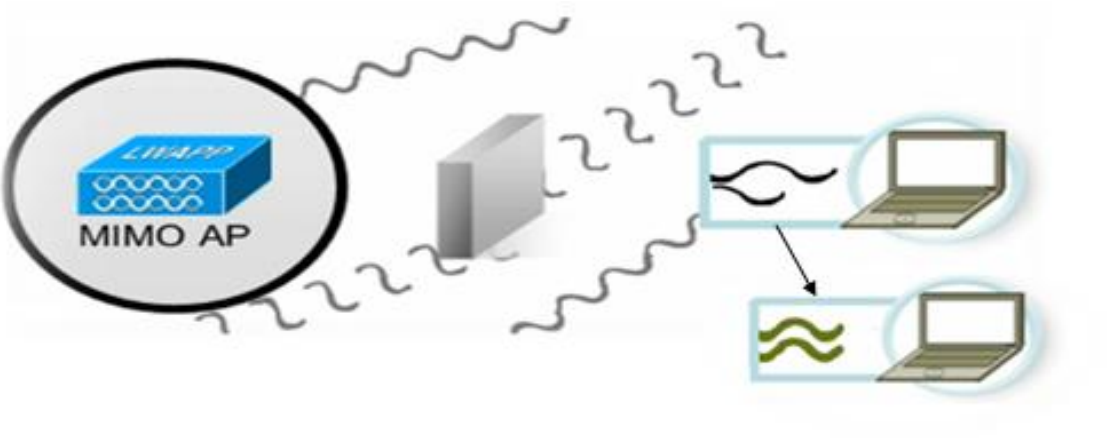


Figura 16: Transmisión de datos en ambiente indoor

Otra característica que tenemos con el protocolo 802.11n es que podemos juntar dos canales de 20 MHz y hacerlos funcionar como un solo canal de 40 MHz provocando una ganancia en el ancho de banda hasta casi 7 veces más que con dispositivos que no tienen 802.11n.

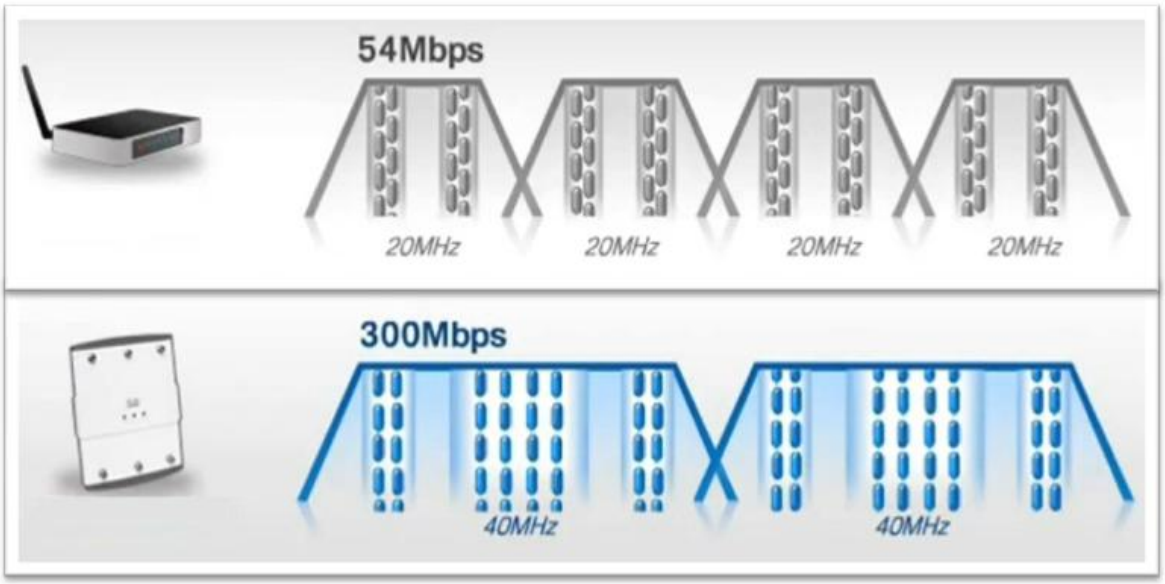


Figura 17: Unión de 2 canales de 20 MHZ

Las características anteriores del 802.11n consiguen una mejor cantidad de señal tanto del lado del access point como del lado del usuario, eso provoca que se puedan poner strings más exigentes y se puedan unificar distintos paquetes de datos para tomar la ventaja de que con un solo encabezamiento en el paquete de datos podamos pasar más información útil tanto desde el usuario hacia el AP como del AP hacia el usuario, aquí se necesita tanto el AP, como el dispositivo inalámbrico soporten 802.11n

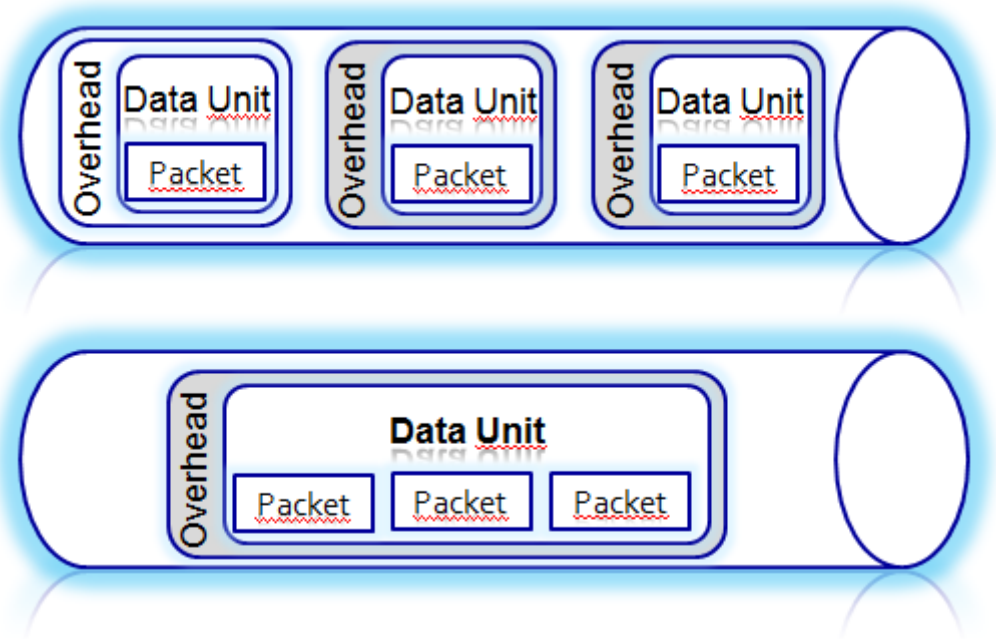


Figura 18: Unificación de paquetes de datos

Una de las necesidades es el hecho de poder contar con un sistema que opere tanto en 2,4Ghz como en 5 Ghz y en las distintas formas de transmisión tanto en 8002.11 b, g, n seleccionando de manera automática cual es la banda que conviene utilizar en ese momento.

Entonces en base al protocolo 802.11n veremos cómo se fue dando solución a nuestros requerimientos que se mostraba inicialmente antes de implementar el sistema inalámbrico dentro de nuestra institución, teníamos que:

Necesidad de más Throughput o ancho de banda en la comunicación.

Entonces con el protocolo 802.11n logramos más rapidez en la transferencia de archivos de gran tamaño por que se tiene casi 7 veces más ancho de banda con respecto a equipos que no soportan el protocolo 802.11n.

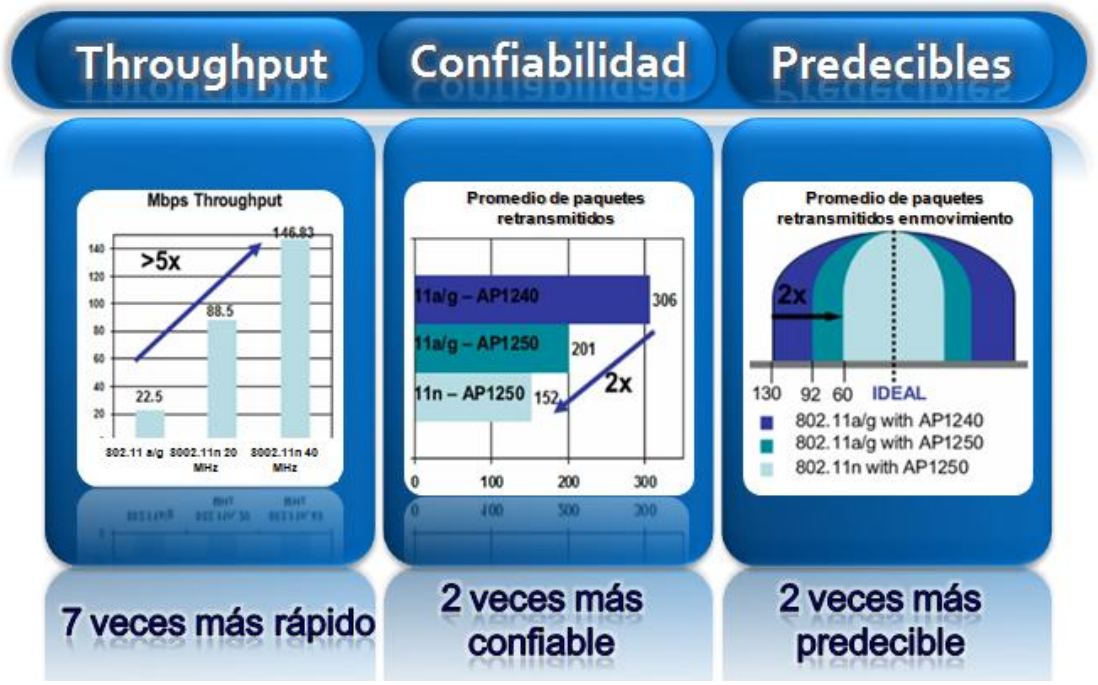


Figura 19: Requerimientos de la red inalámbrica

Otro de nuestros requerimientos era la "Confibilidad".

Lo que logramos es que el promedio de paquetes retransmitidos baje en 2 veces con respecto a equipos que no tienen el protocolo 802.11n, por ende se tiene menor latencia de las comunicaciones móviles unificadas con lo cual la confiabilidad de nuestras conexiones se incrementen en 2 veces respecto a otras soluciones.

Predicibilidad

El cubrir toda el área donde nos podamos estar moviendo con un teléfono móvil, una laptop, también logra una reducción de 2 veces en el promedio de paquetes

retransmitidos, entonces con equipos conectados y estos en movimiento gracias a la cobertura logramos que los ambientes iluminados con RF sea más predecibles.

4.2.3. Descripción de los equipos implementados en la primera etapa

A continuación se provee una descripción completa y detalla de cada uno de los equipos implementados en la primera etapa del proyecto:

NRO	DESCRIPCIÓN	CANT.
1	APs Indoor Marca Cisco Modelo: AIR-LAP1252G-A-K9.	24
2	APs Outdoor Marca Cisco Modelo: AIR-LAP1310G-A-K9	2
3	Wireless Lan Controller Marca Cisco Modelos: AIR-WLC2112-K9.	4
4	Wireless Controller System: WCS-PLUS-UPG-K9 para 50 APs.	1
5	Módulo Wireless Lan Controller Cisco Modelo: WS-SVC-WiSM-1-K9. (Proyecto intermedio entre la fase 1 y fase 2 del WiFi)	1

Figura 20: Cantidad de equipos implementados en la primera fase

4.2.3.1. Ap Indoor Marca Cisco Modelo: Air-Lap1252g-A-K9

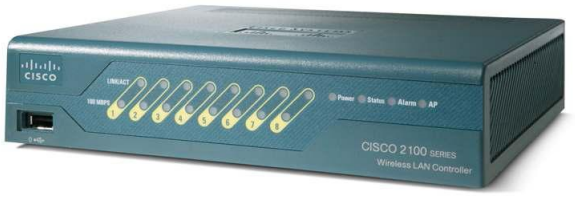
Es un punto de acceso modular dual band con antenas duales, destinado para ambientes internos en cada uno de los bloques o edificios de la UAJMS, puede trabajar en frecuencias de 2,4Ghz como en 5Ghz, soporta Power Over Ethernet (802.3af) sobre un puerto 10/100/1000BASE-T autosensing (RJ-45), puede funcionar de manera autónoma o dejarse gestionar con un controlador, incorpora tecnología M-DRIVE desarrollada netamente por la marca de estos equipos. Opera con los estándares 802.11 b/g/n. Con tres antenas que operan en 11 dBm (12.5 mW) el nivel de radiofrecuencia no supera los 50 milivatios por lo que no se requiere de licenciamiento para esta

frecuencia, ya que así lo permite según Decreto supremo 24132 en su artículo 76 de la Constitución Política del Estado.

4.2.3.2. AP Outdoor Marca Cisco Modelo: AIR-LAP1310G-A-K9

Punto de acceso para ambientes exteriores, trabaja en frecuencia de 2,4Ghz dentro de los estándares 802.11 b y g, soporta diversos tipos de antena para mejorar la cobertura de irradiación de RF o como puente en un rango de 14 millas, Con un diseño compacto este equipo soporta las temperaturas extremas de frio, calor, lluvia y estar expuesto al sol. Puede trabajar de manera autónoma o ser gestionado por un controlador. Actualmente funciona con una antena adicional de 14 dbm lo cual genera una potencia de 25 milivatios para lo cual no requiere de licencia para esta frecuencia ya que no supera los 50 milivatios establecidos en el decreto supremo 24132 en su artículo 76.

4.2.3.3. Wireless Lan Controller Marca Cisco Modelos: AIR-WLC2112-K9.



Dispositivo para Administrar de forma segura las redes WLAN, denominado WLC o Wireless Lan Controller es el que se encarga de administrar las configuraciones, políticas de seguridad y gestionar un conjunto de AP.

Inicialmente en el proyecto se adquirieron 4 de estos equipos uno para cada unidad donde se implementó el sistema inalámbrico, estos equipos adquiridos en la serie WLC-2112 pueden administrar y gestionar hasta 12 AP.

4.2.3.4. Wireless Controller System: WCS-PLUS-UPG-K9 para 50 APs.

Es un software con licencia, disponible en versiones para Windows Server y Linux RedHad, inicialmente en la UAJMS se instaló sobre la plataforma de RedHad con una licencia hasta de 50 dispositivos Access Points El Wireless Control System nos permite realizar una planificación de cómo distribuir nuestros equipos y como alcanzar la cobertura deseada en ambientes tanto INDOOR como OUTDOR atreves de Suite de herramientas de evaluación del diseño y la cobertura pudiendo integrar con lo que es googlemap para poder realizar los trabajos mencionados. También podemos generar reportes flexibles, realizar un despliegue tanto en equipos como usuarios conectados, equipos vecinos usuarios con intentos de conexión, podemos realizar un monitoreo de cada usuario y cada Acces Point, podemos realizar un TROUBLESHOOTING de manera sencilla y rápida entre otras de sus bondades. Se accede mediante un web browser. El WCS soporta hasta 1500 APs. Realiza la creación y ampliación de las políticas de seguridad por SSID y puede soportar hasta 16 SSID diferentes.

4.2.4. Detalle técnico de los equipos implementados en la primera etapa

4.2.4.1. Access point

AP para interiores AIR-LAP1252G-A-K9	**ESPECIFICACIONES**
Part Numbers	Access point platform with pre-installed radio modules: • AIR-AP1252AG-x-K9 802.11a/g/n 2.4/5-GHz Standalone AP; 6 RP-TNC • AIR-AP1252G-x-K9 802.11g/n 2.4-GHz Standalone AP; 3 RP-TNC

AP para interiores AIR-LAP1252G-A-K9	**ESPECIFICACIONES**
	• AIR-LAP1252AG-x-K9 802.11a/g/n 2.4/5-GHz Unified AP; 6 RP-TNC • AIR-LAP1252G-x-K9 802.11g/n 2.4-GHz Unified AP; 3 RP-TNC Individual components: • AIR-AP1250= Standalone AP Platform (no radio modules); Spare • AIR-LAP1250= Unified AP Platform (no radio modules); Spare • AIR-RM1252A-x-K9= 802.11a/n 5-GHz Radio Module; 3 RP-TNC • AIR-RM1252G-x-K9= 802.11g/n 2.4-GHz Radio Module; 3 RP-TNC • AIR-AP1250MNTGKIT= 1250 Series Ceiling, Wall Mount Bracket kit- Spare Eco-pack: • AIR-LAP1252-x-K9-5 Eco-pack 802.11a/g/n 2.4/5 GHz Unified AP-5 qty (A, E, N Reg domains only) • AIR-AP1252-N-K9-5 Eco-pack 802.11a/g/n 2.4/5 GHz Standalone AP-5 qty (N Reg domain only)
Software	• Cisco IOS® Software Release 12.4(21a)JA or later (Standalone Mode) • Cisco IOS Software Release 12.4(10b) JDD or later (Unified Mode) • Cisco Unified Wireless Network Software Release 7.0 or later.
802.11n Capabilities	• 2x3 MIMO with two spatial streams • Maximal Ratio Combining (MRC) • 20-and 40-MHz channels • PHY data rates up to 300 Mbps • Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx) • 802.11 DFS (Bin 5) • Cyclic Shift Diversity (CSD) support
Data Rates Supported	802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps
	802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps

<table>
<tr><td>AP para interiores AIR-LAP1252G-A-K9</td><td colspan="5">ESPECIFICACIONES</td></tr>
<tr><td rowspan="18"></td><td colspan="5">802.11n data rates (2.4 GHz and 5 GHz):</td></tr>
<tr><td rowspan="2">MCS Index[1]</td><td colspan="2">GI[2] = 800ns</td><td colspan="2">GI = 400ns</td></tr>
<tr><td>20-MHz Rate (Mbps)</td><td>40-MHz Rate (Mbps)</td><td>20-MHz Rate (Mbps)</td><td>40-MHz Rate (Mbps)</td></tr>
<tr><td>0</td><td>6.5</td><td>13.5</td><td>7.2</td><td>15</td></tr>
<tr><td>1</td><td>13</td><td>27</td><td>14.4</td><td>30</td></tr>
<tr><td>2</td><td>19.5</td><td>40.5</td><td>21.7</td><td>45</td></tr>
<tr><td>3</td><td>26</td><td>54</td><td>28.9</td><td>60</td></tr>
<tr><td>4</td><td>39</td><td>81</td><td>43.3</td><td>90</td></tr>
<tr><td>5</td><td>52</td><td>108</td><td>57.8</td><td>120</td></tr>
<tr><td>6</td><td>58.5</td><td>121.5</td><td>65</td><td>135</td></tr>
<tr><td>7</td><td>65</td><td>135</td><td>72.2</td><td>150</td></tr>
<tr><td>8</td><td>13</td><td>27</td><td>14.4</td><td>30</td></tr>
<tr><td>9</td><td>26</td><td>54</td><td>28.9</td><td>60</td></tr>
<tr><td>10</td><td>39</td><td>81</td><td>43.3</td><td>90</td></tr>
<tr><td>11</td><td>52</td><td>108</td><td>57.8</td><td>120</td></tr>
<tr><td>12</td><td>78</td><td>162</td><td>86.7</td><td>180</td></tr>
<tr><td>13</td><td>104</td><td>216</td><td>115.6</td><td>240</td></tr>
<tr><td>14</td><td>117</td><td>243</td><td>130</td><td>270</td></tr>
<tr><td>15</td><td>130</td><td>270</td><td>144.4</td><td>300</td></tr>
<tr><td>Frequency Band and 20-MHz Operating Channels</td><td colspan="2">A (A Regulatory Domain):
• 2.412 to 2.462 GHz; 11</td><td colspan="3">K (K Regulatory Domain):
• 2.412 to 2.472 GHz; 13 channels
• 5.180 to 5.320 GHz; 8 channels
• 5.500 to 5.620 GHz, 7 channels</td></tr>
</table>

AP para interiores AIR-LAP1252G-A-K9	**ESPECIFICACIONES**	
	channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.700 GHz, 8 channels (excludes 5.600 to 5.640 GHz) • 5.745 to 5.825 GHz; 5 channels C (C Regulatory Domain): • 2.412 to 2.472 GHz; 13 channels • 5.745 to 5.825 GHz; 5 channels E (E Reg Domain): • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.700 GHz, 8 channels I (I Regulatory Domain): • 2.412 to 2.472 GHz, 13 channels • 5.180 to 5.320 GHz; 8 channels	• 5.745 to 5.805 GHz, 4 channels N (N Regulatory Domain): • 2.412 to 2.462 GHz; 11 channels • 5.180 to 5.320 GHz; 8 channels • 5.745 to 5.825 GHz; 5 channels P (P Regulatory Domain): • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels S (S Regulatory Domain): • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels • 5.745 to 5.825 GHz; 5 channels T (T Regulatory Domain): • 2.412 to 2.462 GHz; 11 channels • 5.280 to 5.320 GHz; 3 channels • 5.500 to 5.700 GHz, 11 channels • 5.745 to 5.825 GHz; 5 channels
Note: This varies by regulatory domain. Refer to the product documentation for specific details for each regulatory domain.		
Maximum Number of Non-Overlapping Channels	2.4 GHz • 802.11b/g: • 20 MHz: 3 • 802.11n: • 20 MHz: 3	5 GHz • 802.11a: • 20 MHz: 21 • 802.11n: • 20 MHz: 21

<table>
<tr><td>AP para interiores
AIR-LAP1252G-A-K9</td><td colspan="4">ESPECIFICACIONES</td></tr>
<tr><td></td><td></td><td colspan="3">• 40 MHz: 9</td></tr>
<tr><td colspan="5">Note: This varies by regulatory domain. Refer to the product documentation for specific details for each regulatory domain.</td></tr>
<tr><td rowspan="2">Receive Sensitivity</td><td>802.11b
-90 dBm @ 1 Mb/s
-89 dBm @ 2 Mb/s
-87 dBm @ 5.5 Mb/s
-85 dBm @ 11 Mb/s</td><td>802.11g
-87 dBm @ 6 Mb/s
-86 dBm @ 9 Mb/s
-83 dBm @ 12 Mb/s
-82 dBm @ 18 Mb/s
-81 dBm @ 24 Mb/s
-80 dBm @ 36 Mb/s
-75 dBm @ 48 Mb/s
-74 dBm @ 54 Mb/s</td><td colspan="2">802.11a
-86 dBm @ 6 Mb/s
-85 dBm @ 9 Mb/s
-82 dBm @ 12 Mb/s
-81 dBm @ 18 Mb/s
-80 dBm @ 24 Mb/s
-79 dBm @ 36 Mb/s
-74 dBm @ 48 Mb/s
-73 dBm @ 54 Mb/s</td></tr>
<tr><td>2.4-GHz 802.11n (HT20)
-86 dBm @ MC0
-85 dBm @ MC1
-84 dBm @ MC2
-83 dBm @ MC3
-80 dBm @ MC4
-75 dBm @ MC5
-74 dBm @ MC6
-73 dBm @ MC7</td><td></td><td>5-GHz 802.11n (HT20)
-85 dBm @ MC0
-84 dBm @ MC1
-83 dBm @ MC2
-82 dBm @ MC3
-79 dBm @ MC4
-74 dBm @ MC5
-73 dBm @ MC6
-72 dBm @ MC7</td><td>5-GHz 802.11n (HT40)
-85 dBm @ MC0
-84 dBm @ MC1
-83 dBm @ MC2
-79 dBm @ MC3
-76 dBm @ MC4
-71 dBm @ MC5
-70 dBm @ MC6
-69 dBm @ MC7</td></tr>
</table>

AP para interiores AIR-LAP1252G-A-K9	**ESPECIFICACIONES**			
	-86 dBm @ MC8 -85 dBm @ MC9 -84 dBm @ MC10 -83 dBm @ MC11 -80 dBm @ MC12 -75 dBm @ MC13 -74 dBm @ MC14 -73 dBm @ MC15		-85 dBm @ MC8 -84 dBm @ MC9 -83 dBm @ MC10 -82 dBm @ MC11 -79 dBm @ MC12 -74 dBm @ MC13 -73 dBm @ MC14 -72 dBm @ MC15	-85 dBm @ MC8 -84 dBm @ MC9 -83 dBm @ MC10 -79 dBm @ MC11 -76 dBm @ MC12 -71 dBm @ MC13 -70 dBm @ MC14 -69 dBm @ MC15
Maximum Transmit Power	2.4GHz • 802.11b • 23 dBm with 1 antenna • 802.11g • 20 dBm with 1 antenna • 802.11n (HT20) • 17 dBm with 1 antenna • 20 dBm with 2 antennas		5GHz • 802.11a • 17 dBm with 1 antenna • 802.11n non-HT duplicate (802.11a duplicate) mode • 17 dBm with 1 antenna • 802.11n (HT20) • 17 dBm with 1 antenna • 20 dBm with 2 antennas • 802.11n (HT40**)** • 17 dBm with 1 antenna • 20 dBm with 2 antennas	
Note: The maximum power setting will vary by channel and according to individual country regulations. Refer to the product documentation for specific details.				
Available Transmit Power Settings	2.4GHz 23 dBm (200 mW) 20 dBm (100 mW) 17 dBm (50 mW) 14 dBm (25 mW) 11 dBm (12.5 mW) 8 dBm (6.25 mW)		5GHz 20 dBm (100 mW) 17 dBm (50 mW) 14 dBm (25 mW) 11 dBm (12.5 mW) 8 dBm (6.25 mW) 5 dBm (3.13 mW)	

<table>
<tr><td>AP para interiores
AIR-LAP1252G-A-K9</td><td colspan="3">ESPECIFICACIONES</td></tr>
<tr><td></td><td>5 dBm (3.13 mW)
2 dBm (1.56 mW)
-1 dBm (0.78 mW)</td><td colspan="2">2 dBm (1.56 mW)
-1 dBm (0.78 mW)</td></tr>
<tr><td colspan="4">Note: The maximum power setting will vary by channel and according to individual country regulations. Refer to the product documentation for specific details.</td></tr>
<tr><td>Antenna Connectors</td><td colspan="3">• 2.4-GHz: 3 RP-TNC connectors
• 5-GHz: 3 RP-TNC connectors</td></tr>
<tr><td>Interfaces</td><td colspan="3">• 10/100/1000BASE-T autosensing (RJ-45)
• Management console port (RJ45)</td></tr>
<tr><td>Indicators</td><td colspan="3">• Status LED indicates operating state, association status, error/warning condition, boot sequence, and maintenance status.
• Ethernet LED indicates activity over the Ethernet, status.
• Radio LED indicates activity over the radio, status.</td></tr>
<tr><td rowspan="4">Modularity</td><td colspan="3">• Number of radio module slots: 2
• Available radio modules</td></tr>
<tr><td>Part Number</td><td>Description</td><td>Maximum per AP1250 platform</td></tr>
<tr><td>AIR-RM1252A-x-K9</td><td>2.4 802.11a/n-d2.0 5-GHz Radio Module; 3 RP-TNC</td><td>1</td></tr>
<tr><td>AIR-RM1252G-x-K9</td><td>802.11g/n-d2.0 2.4-GHz Radio Module; 3 RP-TNC</td><td>1</td></tr>
<tr><td>Dimensions (W x L x H)</td><td colspan="3">• AP (without mounting bracket): 8.12 x 9.52 x 2.35 in. (20.62 x 24.18 x 5.97 cm)
• AP (with mounting bracket): 8.12 x 9.52 x 2.75 in. (20.62 x 24.18 x 6.99 cm)</td></tr>
</table>

AP para interiores AIR-LAP1252G-A-K9	**ESPECIFICACIONES**
Weight	• AP with 2 radios installed: 5.1 lbs (2.31 kg) • AP chassis: 2.1 lbs (0.95 kg) • 2.4 GHz radio: 1.5 lbs (0.68 kg) • 5 GHz radio: 1.5 lbs (0.68 kg)
Environmental	**Nonoperating (storage) temperature:** -40 to 185°F (-40 to 85°C) **Operating temperature:** -4 to +131°F (-20 to +55°C) **Operating humidity:** 10 to 90 percent (noncondensing)
System Memory	• 64 MB DRAM • 32 MB flash
Input Power Requirements	• AP1250: 36 to 57 VDC • Power Supply and Power Injector: 100 to 240 VAC; 50 to 60 Hz
Powering Options	• Cisco Catalyst switch port capable of sourcing 20W or greater • Cisco AP1250 Power Injector (AIR-PWRINJ4) • Cisco AP1250 Local Power Supply (AIR-PWR-SPLY1) • 802.3af switch (AP1250 with single radio only)
Power Draw	• AP1250 with two RM1252 radio modules installed: 18.5W • AP1250 with one RM1252 radio module installed: 12.95W **Note:** For a 1250 Series Access Point with two radios, 18.5W is the maximum power required at the access point (powered device). When deployed using PoE, the power drawn from the power sourcing equipment will be higher by some amount dependent on the length of the interconnecting cable. This additional power may be as high as 1.5W, bringing the total system power draw (access point + cabling) to 20W. A similar consideration applies for a 1250 Series Access Point with one radio.
Warranty	Limited Lifetime Hardware Warranty
Compliance	Standards • **Safety:** • UL 60950-1

AP para interiores AIR-LAP1252G-A-K9	**ESPECIFICACIONES**
	• CAN/CSA-C22.2 No. 60950-1 • UL 2043 • IEC 60950-1 • EN 60950-1 • **Radio approvals:** • FCC Part 15.247, 15.407 • RSS-210 (Canada) • EN 300.328, EN 301.893 (Europe) • ARIB-STD 33 (Japan) • ARIB-STD 66 (Japan) • ARIB-STD T71 (Japan) • AS/NZS 4268.2003 (Australia and New Zealand) • EMI and susceptibility (Class B) • FCC Part 15.107 and 15.109 • ICES-003 (Canada) • VCCI (Japan) • EN 301.489-1 and -17 (Europe) • EN 60601-1-2 EMC requirements for the Medical Directive 93/42/EEC • **IEEE Standard** • IEEE 802.11a/b/g, IEEE 802.11n, IEEE 802.11h, IEEE 802.11d • **Security:** • 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA • 802.1X • Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP) • **EAP Type(s):** • Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) • EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) • Protected EAP (PEAP) v0 or EAP-MSCHAPv2 • Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) • PEAPv1 or EAP-Generic Token Card (GTC) • EAP-Subscriber Identity Module (SIM) • **Multimedia:** • Wi-Fi Multimedia (WMM™) • **Other:**

AP para interiores AIR-LAP1252G-A-K9	**ESPECIFICACIONES**
	• FCC Bulletin OET-65C • RSS-102
Calculated Mean Time Between Failure (MTBF)	380,000 hours

4.2.4.2. Access Point outdoor

AP para exteriores (Outdoor) AIR-LAP1310G-A-K9	**ESPECIFICACIONES**
Cantidad	Treinta (30)
Descripción	Access Point Outdoor o Bridge (para exteriores) con cable de antena integrado
LEDs de estado	4 LEDs: Instalación, Radio, Estado, y Ethernet
Puertos	Dos conectores coaxiales para full-duplex Ethernet Puerto de consola full-duplex tipo RS232
Accesorios	Deberá incluir: • Fuente de poder para el inyector. Alimentacion de 100 a 240 VAC • Power injector de 48 VDC • Cable coaxial dual del tipo RG-6 con un largo no menor a 30ms. • Accesorios para montar en el techo o pared
Compatibilidad	Por motivos de darle continuidad a la actual estructura de red y al ser esta licitación una segunda etapa con equipos que actualmente se tienen en producción en la UAJMS, estos equipos deberán ser 100% compatible con: Wireles Controler Chasis WS-SVC-WiSM-1-k9 Wireles LAN Controler AIR-WLC2112-k9
Tomas de tierra	Debe incluir como mínimo dos tomas de tierra para protección contra rayos.
Interfase de Antena	Antena direccional integrada Dos conectores para antenas externas (Opcionales)
Estándar de Interfase aérea	IEEE 802.11b y IEEE 802.11g
Frecuencia de Banda	● 2.412 a 2.462 GHz (FCC)

AP para exteriores (Outdoor) AIR-LAP1310G-A-K9	**ESPECIFICACIONES**
Modulación Wireless	802.11b ● DSSS (Direct Sequence Spread Spectrum): DBPSK a 1 Mbps DQPSK a 2 Mbps CCK a 5.5 y 11 Mbps 802.11g ● OFDM (Orthogonal Frequency Divisional Multiplexing): BPSK a 6 y 9 Mbps QPSK a 12 y 18 Mbps 16-quadrature amplitude modulation (QAM) a 24 y 36 Mbps 64-QAM a 48 y 54 Mbps
Protocolo de acceso a medio	Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)
Protocolo para administración centralizada	Protocolo LAP para administración centralizada
Canales de Operación	802.11b/g 11 canales
Canales no sobrepuestos	3
Seguridad en el rol de Bridge	Autenticación soporte 802.1X que incluye LEAP para autenticación mutual y dinámica por usuario y llaves de encriptación por sesión Encriptación ● TKIP o WPA TKIP; key hashing (per-packet keying), Message Integrity Check (MIC) y broadcast key rotation ● AES (802.11i)
Seguridad en el rol de Access Point	Soporte de WPA y WPA2 que incluye: Autenticación ● 802.1X que incluye LEAP, Protected EAP-Generic Token Card (PEAP-GTC), PEAPMicrosoft Challenge Authentication Protocol Version 2 (MSCHAPv2), EAP Message Digest 5 (EAPMD5), EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (EAP-TTLS), EAP-Subscriber Identity Module (EAP-SIM), y

AP para exteriores (Outdoor) AIR-LAP1310G-A-K9	**ESPECIFICACIONES**
	EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) Encriptación ● WPA: TKIP o WPA TKIP; key hashing (per-packet keying), MIC y broadcast key rotation ● WPA2: AES (802.11i)
SNMP	Versiones 1 y 2
Memoria	● 8 MB de Memoria Flash interna ● 2Gb o superior de memoria Flash externa de tipo USB compatible 1.0 y/o 2.1
Valores disponibles para potencia de transmisión.	802.11b: • 100 mW (20 dBm) • 50 mW (17 dBm) • 30 mW (15 dBm) • 20 mW (13 dBm) • 10 mW (10 dBm) • 5 mW (7 dBm) • 1 mW (0 dBm) 802.11g: • 30 mW (15 dBm) • 20 mW (13 dBm) • 10 mW (10 dBm) • 5 mW (7 dBm) • 1 mW (0 dBm)
Nivel maximo de recepción operacional	-20 dBm
Sensibilidad de Recepción	• 1 Mbps: -94 dBm • 2 Mbps: -91 dBm

AP para exteriores (Outdoor) AIR-LAP1310G-A-K9	**ESPECIFICACIONES**
	• 5.5 Mbps: -89 dBm • 11 Mbps: -85 dBm • 6 Mbps: -90 dBm • 9 Mbps: -89 dBm • 12 Mbps: -86 dBm • 18 Mbps: -84 dBm • 24 Mbps: -81 dBm • 36 Mbps: -77 dBm • 48 Mbps: -73 dBm • 54 Mbps: -72 dBm
Rango externo (como AP)	• 350 feet (105 metros) a 54 Mbps • 1410 feet (430 metros) a 11 Mbps
Rango Punto a punto (como Bridge)	• 4.5 miles (7 km) a 54 Mbps • 14 miles (23 km) a 11 Mbps
Rango Punto a multipunto (como Bridge)	• 2.0 miles (3.3 km) a 54 Mbps • 10 miles (16 km) a 11 Mbps

4.2.4.3. Wireless LAN CONTROLLER

Controladro de red Wireless AIR-WLC2112-K9	Especificaciones
Wireless Standards	IEEE 802.11a, 802.11b, 802.11g, 802.11d, 802.11h, 802.11n
Wired/Switching/Routing	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, and IEEE 802.1Q VLAN tagging
Data RFCs	• RFC 768 UDP • RFC 791 IP • RFC 792 ICMP • RFC 793 TCP • RFC 826 ARP • RFC 1122 Requirements for Internet Hosts • RFC 1519 CIDR • RFC 1542 BOOTP • RFC 2131 DHCP

Controladro de red Wireless AIR-WLC2112-K9	Especificaciones
Security Standards	• Wi-Fi Protected Access (WPA) • IEEE 802.11i (WPA2, RSN) • RFC 1321 MD5 Message-Digest Algorithm • RFC 2104 HMAC: Keyed Hashing for Message Authentication • RFC 2246 TLS Protocol Version 1.0 • RFC 3280 X.509 PKI Certificate and CRL Profile
Encryption	• WEP and Temporal Key Integrity Protocol-Message Integrity Check (TKIP-MIC): RC4 40, 104 and 128 bits (both static and shared keys) • Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024- and 2048-bit • Advanced Encryption Standard (AES): CCM, Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
Authentication, Authorization, -and Accounting (AAA)	• IEEE 802.1X • RFC 2548 Microsoft Vendor-Specific RADIUS Attributes • RFC 2716 PPP EAP-TLS • RFC 2865 RADIUS Authentication • RFC 2866 RADIUS Accounting • RFC 2867 RADIUS Tunnel Accounting • RFC 2869 RADIUS Extensions • RFC 3576 Dynamic Authorization Extensions to RADIUS • RFC 3579 RADIUS Support for EAP • RFC 3580 IEEE 802.1X RADIUS Guidelines • RFC 3748 Extensible Authentication Protocol • Web-based authentication
Management	• SNMP v1, v2c, v3 • RFC 854 Telnet • RFC 1155 Management Information for TCP/IP-Based Internets • RFC 1156 MIB • RFC 1157 SNMP • RFC 1213 SNMP MIB II • RFC 1350 TFTP • RFC 1643 Ethernet MIB

Controladro de red Wireless AIR-WLC2112-K9	Especificaciones
	• RFC 2030 SNTP • RFC 2616 HTTP • RFC 2665 Ethernet-Like Interface types MIB • RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions • RFC 2819 RMON MIB • RFC 2863 Interfaces Group MIB • RFC 3164 Syslog • RFC 3414 User-Based Security Model (USM) for SNMPv3 • RFC 3418 MIB for SNMP • RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs • Cisco private MIBs
Management Interfaces	• Designed for use with Cisco Wireless Control System • Web-based: HTTP/HTTPS individual device manager • Command-line interface: Telnet, SSH, serial port
Interfaces and Indicators	• Console port: RS-232 (DB-9 male/RJ-45 connector included) • Network: Eight 10/100 Mbps Ethernet (RJ-45) including two 802.3af or Cisco PoE ports rated for use with Cisco Aironet lightweight access points • LED indicators: Link Activity (each 10/100 port), Power, Status, Alarm, Access Point Joined
Physical and Environmental	• Dimensions: 1.75 x 7.89 x 6.87 in. (4.45 x 20.04 x 17.45 cm) • Weight: 4.0 lbs (with power supply) • Temperature: • Operating: 32 to 104°F (0 to 40°C) • Storage: -13 to 158°F (-25 to 70°C) • Humidity: • Operating humidity: 10 to 95 percent, noncondensing • Storage humidity: Up to 95 percent • Power adapter: Input power: 100 to 240 VAC; 50/60 Hz

Controladro de red Wireless AIR-WLC2112-K9	Especificaciones
	• Heat Dissipation: 72 BTU/hour
Regulatory Compliance	• CE Mark • Safety: • UL 60950-1:2003 • EN 60950:2000 • EMI and susceptibility (Class B): • U.S.: FCC Part 15.107 and 15.109 • Canada: ICES-003 • Japan: VCCI • Europe: EN 55022, EN 55024

4.2.4.4. Wireless Control System.

WCS-PLUS-UPG-K9 para 50 APs.	Especificaciones
REPORTES	
Inventario	Deberá proporcionar informes del inventario para los equipos Wireless desplegados dentro de la red (puntos de acceso, controladores, y aplicaciones de la localización) se deberá poder generar para cada categoría del hardware o como un informe combinado para todas las categorías. Los informes deberán soportar la inclusión del tipo del hardware, la revisión del software, y la localización por el edificio o el piso.
Seguridad	La información de seguridad se deberá poder transferir como informe así como el número de dispositivos intrusos detectados por cada Access Point. Deberá contar con un sistema de reportes para la detección de intrusos (IDS) que despliegue de forma grafica o en lista los dispositivos intrusos y los ad hoc.
Compatibilidad	Deberá ser 100% compatible con los access points del ítem 1 y 3, y controladores Wireless del ítem 4, ofertados para la solución requerida en esta licitación y los equipos actualmente en producción.
Reporte detallado del cliente	Deberá poder proporcionar informes con el historial de todos los clientes, de los clientes de

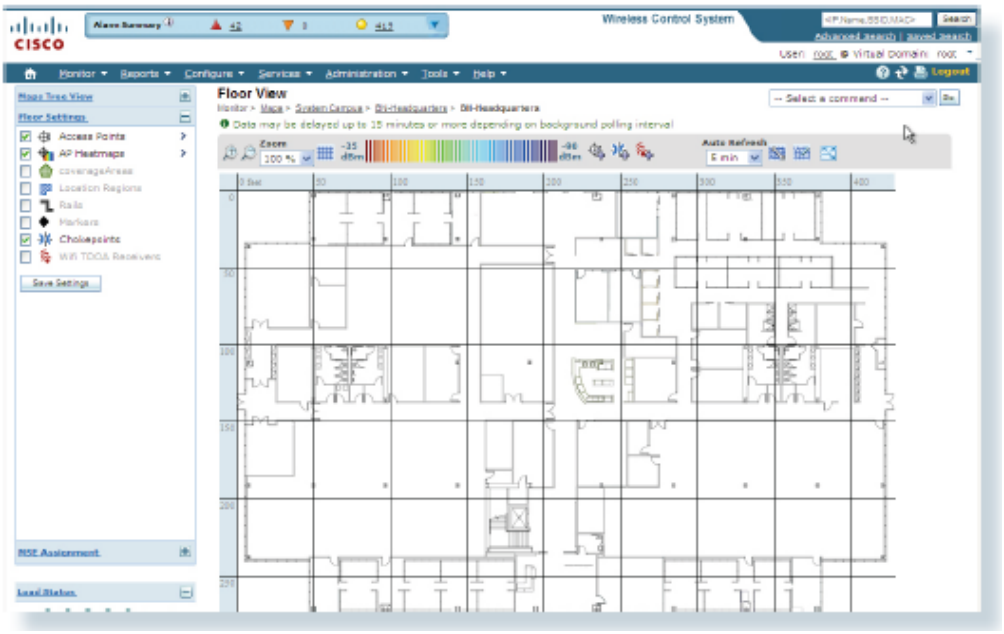
WCS-PLUS-UPG-K9 para 50 APs.	Especificaciones
	mayor saturación y de clientes exclusivos que tuvieron acceso a un área específica mediante la WLAN durante un tiempo específico. Deberá proporcionar estadísticas de clientes incluyendo MAC address, Access Point asociado, la transmisión/recepción en todas partes, RSSI. Los informes deberán generarse basados en una variedad de criterios incluyendo superficie cubierta, controladores, Access Point, e identificadores determinados del servicio (SSIDs).
CARACTEÍSTICAS	
GUI intuitivo y simplificado de fácil uso	Deberá proveer un sistema de fácil administración para configurar, supervisar, y localizar averías fácilmente.
Mapas Jerarquicos	Deberá proveer un acceso rápido a diversos sitios geográficos, campus, edificios y pisos para una mejor visibilidad y control.
Planillas de administración de políticas	Administración de políticas para QoS, Seguridad, y RF.
Seguridad robusta para Wireless y protección de red	Administración y monitoreo de seguridad a través de la red wireless. Deberá soportar detección de intrusos built-in, localización Adaptive Wireless IPS y políticas de seguridad robusta.
Protección completa contra intrusiones para la red Wireless LAN	Detección intrusiones no autorizadas y ataques RF con alarmas automatizadas que permitan una respuesta rápida para atenuar el riesgo.
Acceso Seguro	Autenticación y autorización segura con SNMP version 3 y TACACS+ para acceso de los administradores al software de gestion.
Información integrada del tipo Context-Aware de alta precisión	Deberá soportar la entrega de información contextual en tiempo real sobre usuarios y dispositivos móviles, así como también la ubicación, temperatura, disponibilidad, y aplicaciones en uso.
Voz sobre WLAN	Debe soportar la inclusión de una variedad de herramientas avanzadas para planear, desplegar, supervisar y optimizar la WLAN para utilizar VoWLAN, incluyendo las herramientas de localización de averías de la voz, de intervención de la voz y de la preparación de la voz.

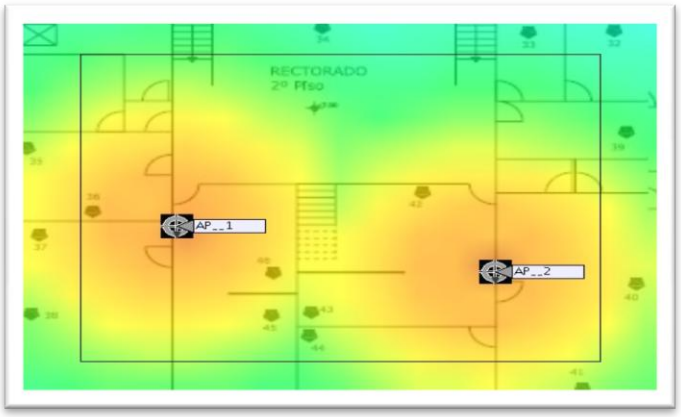
WCS-PLUS-UPG-K9 para 50 APs.	Especificaciones
Herramientas de planificación para Wireless LAN	Deberá contar con herramientas para el planeamiento Wireless y el diseño LAN para aumentar la eficacia de la predicción del RF. Deberá soportar formatos tales como JPEG, pdf, y Autocad.
Monitoreo y migración simplificada para Access Point independientes.	Deberá soportar una herramienta para facilitar el proceso de migrar Access Point independientes (autónomos) para funcionar como Access Points lightwight administrados por el controlador correspondiente.
Iniciativas verdes	Deberá permitir la reducción de costos de energía mediante el encendido y apagado de los access point en base a intervalos programados.

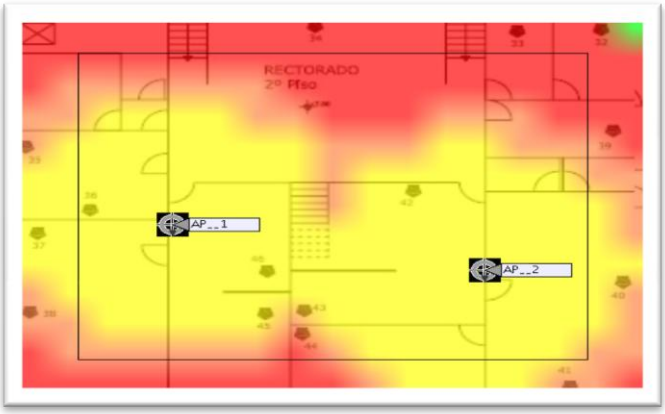
4.3. Descripción General de la Implementación de la red Inalámbrica (Segunda Etapa)

En base a la implementación de la primera fase, esta sirvió como una prueba piloto orientada a la implementación de la segunda fase. Los equipos adquiridos en la primera etapa sirvieron para dimensionar de mejor manera y lo más importante poder realizar una planificación de coberturas tanto dentro de los edificios como áreas externas potencialmente utilizables para brindar conexión inalámbrica.

Para encarar la segunda fase el software WCS brindó una gran ayuda al momento de dimensionar la cantidad de equipos a utilizar. Haciendo uso de sus herramientas de planificación de coberturas donde cargando planos de los bloques o edificios nos brida en base a mapas de calor la simulación del comportamiento de la cobertura según el modelo de Access Poit a implementar.


Wireless Control System
Floor View
Access Points
AP Heatmaps
Chokepoints


RECTORADO
2º Piso
AP_1
AP_2



En esta segunda etapa por el tiempo transcurrido y por el cambio tecnológico que avanza de manera muy rápida, los Access Points implementados en la primera fase se descontinuaron y fueron reemplazados por otros con mejores prestaciones y mayores rendimientos. Previo a la segunda etapa dentro de un proyecto que encaró el DTIC a nivel institucional **"Comunicación y Conectividad para la Universidad Autónoma Juan Misael Saracho – Segunda Fase"** se adquirió un nuevo Switch Modular para el Core de red de la UAJMS en este caso se incorporó un módulo controlador de red inalámbrica WLC además de otros módulos para la conectividad general de la red en la UAJMS. Con este nuevo equipo el cual permite tener un mayor rendimiento en el CORE y una administración centralizada con mejores y mayores servicios, el modelo jerárquico una vez implementado la segunda etapa quedó de la siguiente manera:

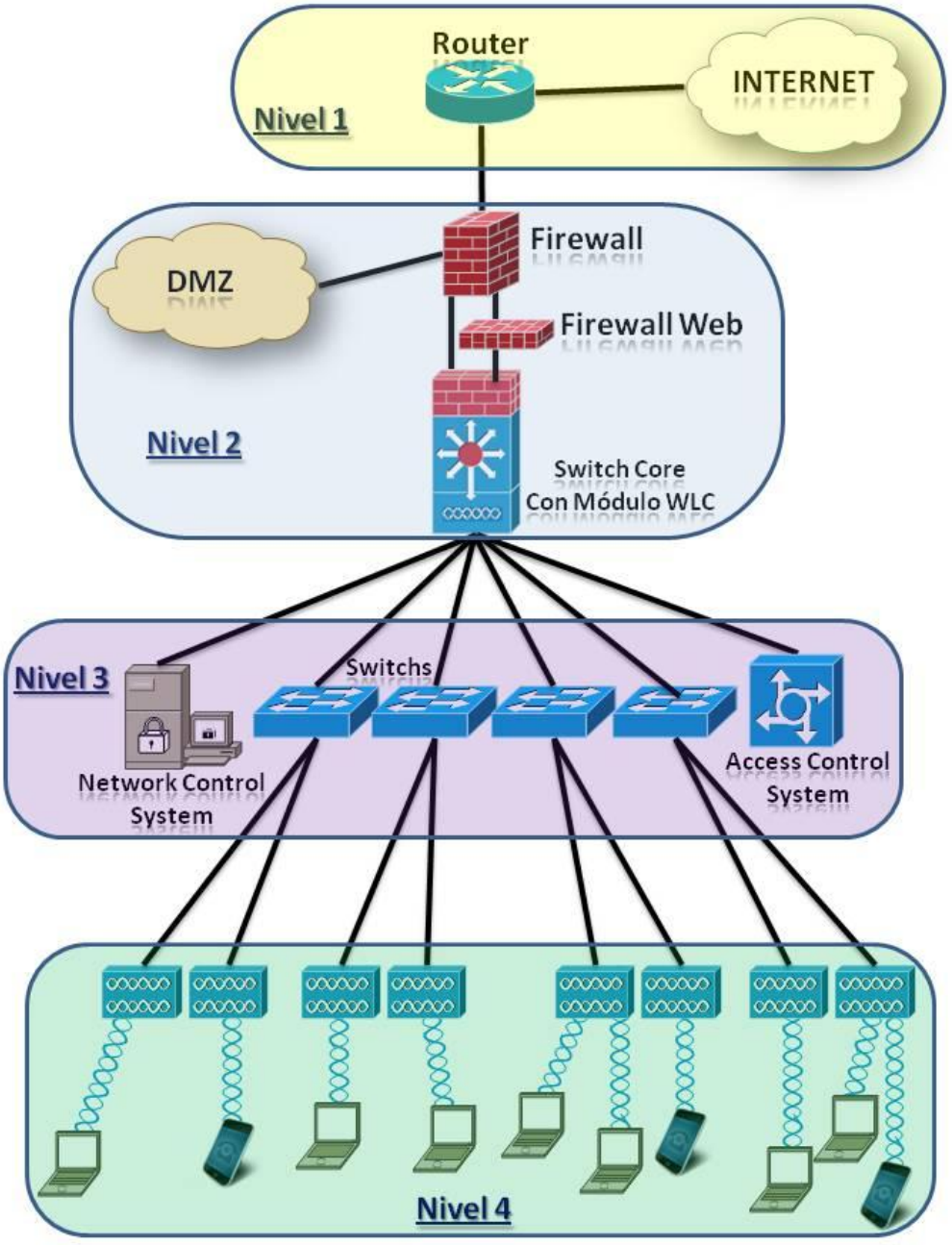


Figura 21: Modelo jerárquico una vez implementado la segunda etapa

4.3.1. Modelo Jerárquico Implementado en La Segunda Etapa

El diseño de WLAN de la red en la segunda fase de la UAJMS, se describe de acuerdo al modelo inicial implementado en la primer etapa, sigue adoptando un modelo de niveles de jerarquía pero en la segunda fase del proyecto el modelo centraliza la administración de toda la red inalámbrica mediante el módulo Wireless Lan Controller, con este equipo se seguirá pudiendo transformar o poder configurar la red para permitir la escalabilidad, redundancia, incremento de usuarios, fácil detección de errores y la adaptación a cambios tecnológicos que permita incorporar nuevos servicios a toda la red.

Nivel 1

No se realiza ningún cambio ya que este nivel sigue ofreciendo una conexión rápida entre los puntos de distribución y el proveedor de servicios ISP.

Nivel 2

El tráfico en la red es dirigido a través de cada uno de los servicios mediante un Switch de Core multicapa con un módulo firewall que segmenta la red de los usuarios que desean salir hacia Internet y los usuarios que deseen ingresar a los servicios de la UAJMS alojados dentro de la DMZ. Los usuarios que salen al Internet se encuentran previo al Firewall perimetral con otro firewall que es dedicado a la detección de malware, realiza un filtrado de contenidos, filtrado web y anlaiza las conexiones dedicadas para descargas tipo P2P pudiendo permitir, restringir o denegar estos servicios. Sigue permitiendo alternativas de poder segmentar los dominios de colisión y broadcast, para evitar las congestiones en la red principal. Es en este Switch Core se incorpora en un módulo el Wireless Lan Controller para la red inalámbrica y ahora forma parte del backbone principal de la red (NIVEL 2) que a diferencia de la primera fase en se dividía en 4 WLC que se ubicaban en el Nivel 3 instalados en los edificios que tenían inicialmente comunicación inalámbrica. El Core permite la comunicación de los edificios que existen en el campus universitario y los edificios

externos al campus como Rectorado Posgrado y Odontología mediante la utilización de fibra óptica monomodo. Además sigue manejando el control al borde de la red con servicios de red inteligentes, incluye calidad de servicio (QoS), clasificación y priorización de tráfico.

Nivel 3

En este nivel desaparecen los dispositivos WLC que permitían la administración y concentración de un grupo de puntos de acceso para acceder a cada unos de los servicios de la red. Los switches siguen manejando una conmutación de paquetes a nivel de capa 3 y 2 del modelo OSI. Sigue incorporando este nivel la funcionalidad de administración de los diferentes sectores que conforma la red, a través de dispositivos específicos para el monitoreo y gestión de redes inalámbricas, como el servidor tipo RADIUS (802.1X). El Wireless Control System (WCS) plataforma que permite direccionar la planificación LAN Wireless, configuración, administración y movilidad de servicios es actualizada a la versión del Network Control System que además de poder ver todo lo que pasa en la red inalámbrica ahora este sistema suma los equipos activos de la red cableada como Switches capa 3 y 2, usuarios conectados a cada uno de los puntos de acceso tanto de la red inalámbrica como de la red cableada Provee un recurso poderoso que permite que el administrador diseñe, controle y monitoree las redes Wireless desde una ubicación centralizada simplificando las operaciones.

Nivel 4

Es la capa de acceso de los usuarios a los distintos servicios ofrecidos por la red, la cual se encarga de distribuir los diferentes enlaces inalámbricos hasta el nivel del usuario. No sufre ninguna alteración en la segunda fase por lo tanto se encuentran ubicados los puntos de acceso con sus respectivas configuraciones dependiendo de la capacidad del número de usuarios finales y la cobertura de cada celda emitida por el Access Point. Los dispositivos finales de comunicación se encuentran accediendo a cada aplicación de red, a través de los puntos de acceso ya que corresponden a la

arquitectura de la red Inalámbrica de la UAJMS. Estos pueden ser equipos portátiles o de escritorio, así como cualquier otro dispositivo que embeba la tecnología Wi-Fi.

4.3.2. Descripción de los nuevos equipos utilizados en la implementación de la segunda etapa

4.3.2.1. Wireless Integrated Services Module (WiSM)

Este modulo es parte del Switch Core 65009-E instalado en el centro de datos de la UAJMS, es el que reemplaza a los 4 controladores inicialmente adquiridos en la primera fase del proyecto WiFi, a diferencia de los controladores pequeños que podían administrar hasta 12 APs, este módulo permite la administración de forma centralizada hasta de 300 APs. En el modelo jerárquico implementado en la segunda fase se sitúa en el nivel 2. Interactúa con los APs de tecnología CleaAir para optimizar y garantizar una conexión confiable y segura.

El Wireless LAN Controller trabaja en conjunto con el AP, comunicándose con éste por medio de LWAPP, es el responsable de implementar una política centralizada de QoS, seguridad y manejo de RF (Radio Frecuencia). El Wireless LAN Controller agrega inteligencia al manejo de RF brindando las siguientes funcionalidades:

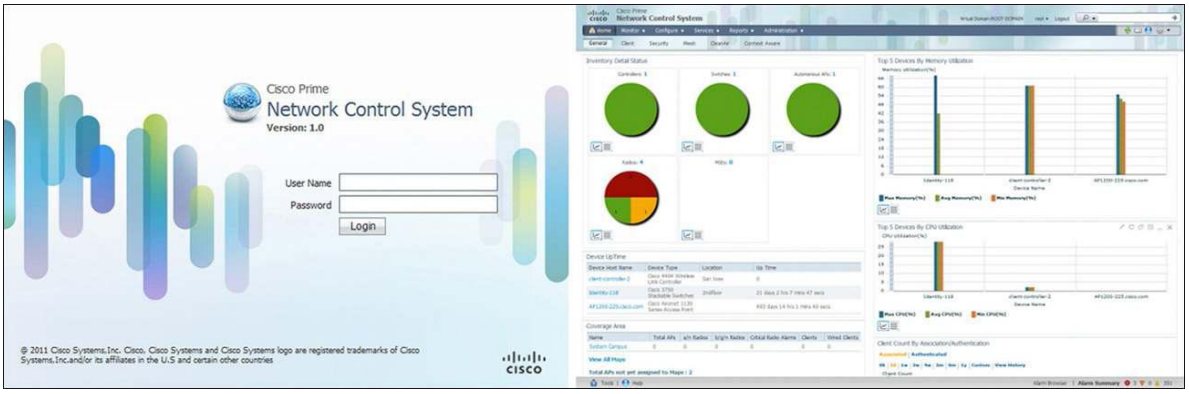
- Asignación dinámica de los canales sin solapamiento a cada AP.
- Detección de interferencias. El LAN Controller detecta interferencias y reconfigura los parámetros de RF para evitarlos.
- Balanceo de carga entre APs.
- Detección de zonas sin cobertura; incrementa la potencia de los APs aledaños para cubrir dichas zonas.

- Se encarga de aplicar las políticas de seguridad.

4.3.2.2. Cisco Aironet 3500e

Este Access Point incorpora la tecnología CleanAir desarrollada por la marca del equipo y de uso exclusivo para la línea de estos equipos el cual realiza una auto optimización de la red inalámbrica que mejora la calidad del espectro en el aire mediante la detección de interferencias de radio frecuencias para optimizar la cobertura inalámbrica. Estos puntos de acceso innovadores proporcionan conectividad en 802.11n conservando también toda la tecnología M-Drive descrita en la implementación de la Primera Fase del proyecto. Soportan el estándar 802.3af (PoE), pueden funcionar en frecuencias de 2,4Ghz y 5Ghz al igual que los anteriores Access Points descritos en la primera fase.

4.3.2.3. Network Control System



El Network Control System (NCS) es una actualización realizada al Wireless Control System (WCS) el cual además de de poder realizar todas las tareas que realiza el WCS en la administración, monitoreo y detección rápida de errores en los equipos de la red inalámbrica, el NCS extiende algunas características a los a los equipos desplegados en toda la red cableada.

4.3.3. Especificaciones Técnicas de los Equipos Utilizados en la Segunda Etapa

4.3.3.1. Product Specifications for the Cisco WiSM

Wireless Integrated Services Module (WISM)	Especificaciones
Wireless	IEEE 802.11a, 802.11b, 802.11g, 802.11d, 802.11h, 802.11n
Wired/Switching	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, IEEE 802.1Q VLAN tagging, and IEEE 802.1D Spanning Tree Protocol
Data RFCs	• RFC 768 UDP • RFC 791 IP • RFC 792 ICMP • RFC 793 TCP • RFC 826 ARP • RFC 1122 Requirements for Internet Hosts • RFC 1519 CIDR • RFC 1542 BOOTP • RFC 2131 DHCP
Security Standards	• NAC • WPA • IEEE 802.11i (WPA2, RSN) • RFC 1321 MD5 Message-Digest Algorithm • RFC 1851 The ESP Triple DES Transform • RFC 2104 HMAC: Keyed Hashing for Message Authentication • RFC 2246 TLS Protocol Version 1.0 • RFC 2401 Security Architecture for the Internet Protocol • RFC 2403 HMAC-MD5-96 within ESP and AH • RFC 2404 HMAC-SHA-1-96 within ESP and AH • RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV • RFC 2406 IPSec • RFC 2407 Interpretation for ISAKMP • RFC 2408 ISAKMP • RFC 2409 IKE • RFC 2451 ESP CBC-Mode Cipher Algorithms

Wireless Integrated Services Module (WISM)	Especificaciones
	• RFC 2661 L2TP • RFC 3280 Internet X.509 PKI Certificate and CRL Profile • RFC 3602 The AES-CBC Cipher Algorithm and its use with IPSec • RFC 3686 Using AES Counter Mode with IPSec ESP
Encryption	• WEP and TKIP-MIC: RC4 40, 104 and 128 bits (both static and shared keys) • Secure Sockets Layer (SSL) and TLS: RC4 128-bit and RSA 1024- and 2048-bit • AES: CCM, CCMP
AAA	• IEEE 802.1X • RFC 2548 Microsoft Vendor-Specific RADIUS Attributes • RFC 2716 PPP EAP-TLS • RFC 2865 RADIUS Authentication • RFC 2866 RADIUS Accounting • RFC 2867 RADIUS Tunnel Accounting • RFC 2869 RADIUS Extensions • RFC 3576 Dynamic Authorization Extensions to RADIUS • RFC 3579 RADIUS Support for EAP • RFC 3580 IEEE 802.1X RADIUS Guidelines • RFC 3748 Extensible Authentication Protocol • Web-based authentication
Management	• Simple Network Management Protocol (SNMP) v1, v2c, v3 • RFC 854 Telnet • RFC 1155 Management Information for TCP/IP-Based Internets • RFC 1156 MIB • RFC 1157 SNMP • RFC 1213 SNMP MIB II • RFC 1350 TFTP • RFC 1643 Ethernet MIB • RFC 2030 SNTP • RFC 2616 HTTP

Wireless Integrated Services Module (WISM)	Especificaciones
	• RFC 2665 Ethernet-Like Interface Types MIB • RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions • RFC 2819 RMON MIB • RFC 2863 Interfaces Group MIB • RFC 3164 Syslog • RFC 3414 User-Based Security Model (USM) for SNMPv3 • RFC 3418 MIB for SNMP • RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs • Cisco private MIBs
Management Interfaces	• Web-based: HTTP/HTTPS • Command-line interface: Telnet, Secure Shell (SSH), serial port
Interfaces and Indicators	• Console port: RS-232 (DB-9 male, DTE interface) • Status LED: Normal sequence, fault during initialization, environmental monitoring • Disk LED
Physical and Environmental	• Dimensions (W x D x H): 1.6 x 15.3 x 16.3 in. (4.1 x 38.9 x 41.4 cm) • Weight: 11 lbs (5 kg) • Temperature: • Operating: 32 to 104°F (0 to 40°C) • Storage: -40 to 167°F (-40 to 75°C) • Humidity: • Operating humidity: 10 to 95 percent, noncondensing • Storage humidity: Up to 95 percent • Power • 164 watts • 6.07 Amps at 42V
Regulatory Compliance	• CE Mark • Safety: • UL 60950-1:2003

Wireless Integrated Services Module (WISM)	Especificaciones
	• EN 60950:2000 • EMI and susceptibility (Class A): • U.S.: FCC Part 15.107 and 15.109 • Canada: ICES-003 • Japan: VCCI • Europe: EN 55022, EN 55024

4.3.3.2. Cisco Aironet 3500e

Aironet 3501E	Especificaciones
Part Numbers	• AIR-CAP3501E-x-K9 - Single-band controller-based 802.11g/n SMARTnet Services for the Cisco Aironet 3500e model with external antennas • CON-SNT-CAP3502x - SMARTnet 8x5xNBD 3500e access point (dual-band 802.11 a/g/n) Cisco Wireless LAN Services • AS-WLAN-CNSLT - Cisco Wireless LAN Network Planning and Design Service • AS-WLAN-CNSLT - Cisco Wireless LAN 802.11n Migration Service • AS-WLAN-CNSLT - Cisco Wireless LAN Performance and Security Assessment Service Regulatory domains: (x = regulatory domain) Customers are responsible for verifying approval for use in their individual countries. To verify approval and to identify the regulatory domain that corresponds to a particular country, please visit http://www.cisco.com/go/aironet/compliance. Not all regulatory domains have been approved. As they are approved, the part numbers will be available

<table>
<tr><th>Aironet 3501E</th><th colspan="5">Especificaciones</th></tr>
<tr><td></td><td colspan="5">on the Global Price List.</td></tr>
<tr><td>Software</td><td colspan="5">Cisco Unified Wireless Network Software Release 7.0 or later (autonomous IOS not supported)</td></tr>
<tr><td>802.11n Version 2.0 (and Related) Capabilities</td><td colspan="5">• 2x3 multiple-input multiple-output (MIMO) with two spatial streams
• Maximal ratio combining (MRC)
• Legacy beamforming
• 20- and 40-MHz channels
• PHY data rates up to 300 Mbps
• Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
• 802.11 dynamic frequency selection (DFS)
• Cyclic shift diversity (CSD) support</td></tr>
<tr><td rowspan="11">Data Rates Supported</td><td colspan="5">802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps</td></tr>
<tr><td colspan="5">802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps</td></tr>
<tr><td colspan="5">802.11n data rates (2.4 GHz and 5 GHz):</td></tr>
<tr><td rowspan="2">MCS Index[1]</td><td colspan="2">GI[2] = 800ns</td><td colspan="2">GI = 400ns</td></tr>
<tr><td>20-MHz Rate (Mbps)</td><td>40-MHz Rate (Mbps)</td><td>20-MHz Rate (Mbps)</td><td>40-MHz Rate (Mbps)</td></tr>
<tr><td>0</td><td>6.5</td><td>13.5</td><td>7.2</td><td>15</td></tr>
<tr><td>1</td><td>13</td><td>27</td><td>14.4</td><td>30</td></tr>
<tr><td>2</td><td>19.5</td><td>40.5</td><td>21.7</td><td>45</td></tr>
<tr><td>3</td><td>26</td><td>54</td><td>28.9</td><td>60</td></tr>
<tr><td>4</td><td>39</td><td>81</td><td>43.3</td><td>90</td></tr>
<tr><td>5</td><td>52</td><td>108</td><td>57.8</td><td>120</td></tr>
<tr><td>6</td><td>58.5</td><td>121.5</td><td>65</td><td>135</td></tr>
<tr><td>7</td><td>65</td><td>135</td><td>72.2</td><td>150</td></tr>
</table>

Aironet 3501E	Especificaciones				
	8	13	27	14.4	30
	9	26	54	28.9	60
	10	39	81	43.3	90
	11	52	108	57.8	120
	12	78	162	86.7	180
	13	104	216	115.6	240
	14	117	243	130	270
	15	130	270	144.4	300
Frequency Band and 20-MHz Operating Channels	A (A regulatory domain): • 2.412 to 2.462 GHz; 11 channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.700 GHz, 8 channels (excludes 5.600 to 5.640 GHz) • 5.745 to 5.825 GHz; 5 channels C (C regulatory domain): • 2.412 to 2.472 GHz; 13 channels • 5.745 to 5.825 GHz; 5 channels E (E regulatory domain): • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.700 GHz, 8 channels			N (N regulatory domain): • 2.412 to 2.462 GHz; 11 channels • 5.180 to 5.320 GHz; 8 channels • 5.745 to 5.825 GHz; 5 channels Q (Q regulatory domain): • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.700 GHz; 11 channels S (S regulatory domain): • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels • 5.745 to 5.825 GHz; 5 channels	

Aironet 3501E	Especificaciones	
	(excludes 5.600 to 5.640 GHz) I (I regulatory domain): • 2.412 to 2.472 GHz, 13 channels • 5.180 to 5.320 GHz; 8 channels K (K regulatory domain): • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.620 GHz, 7 channels • 5.745 to 5.805 GHz, 4 channels	T (T regulatory domain): • 2.412 to 2.462 GHz; 11 channels • 5.280 to 5.320 GHz; 3 channels • 5.500 to 5.700 GHz, 11 channels • 5.745 to 5.825 GHz; 5 channels
Note: Customers are responsible for verifying approval for use in their individual countries. To verify approval and to identify the regulatory domain that corresponds to a particular country, please visit http://www.cisco.com/go/aironet/compliance.		
Maximum Number of Nonoverlapping Channels	2.4 GHz • 802.11b/g: • 20 MHz: 3 • 802.11n: • 20 MHz: 3	5 GHz • 802.11a: • 20 MHz: 21 • 802.11n: • 20 MHz: 21 • 40 MHz: 9
Note: This varies by regulatory domain. Refer to the product documentation for specific details for each regulatory domain.		
Receive Sensitivity	802.11b (CCK) -101 dBm @ 1 Mb/s -98 dBm @ 2	802.11g (non HT20) -92 dBm @	802.11a (non HT20) -93 dBm @ 6 Mb/s -93 dBm @ 9 Mb/s

Aironet 3501E	Especificaciones			
	Mb/s -92 dBm @ 5.5 Mb/s -89 dBm @ 11 Mb/s	6 Mb/s -92 dBm @ 9 Mb/s -92 dBm @ 12 Mb/s -90 dBm @ 18 Mb/s -86 dBm @ 24 Mb/s -84 dBm @ 36 Mb/s -79 dBm @ 48 Mb/s -78 dBm @ 54 Mb/s	-92 dBm @ 12 Mb/s -90 dBm @ 18 Mb/s -87 dBm @ 24 Mb/s -84 dBm @ 36 Mb/s -79 dBm @ 48 Mb/s -79 dBm @ 54 Mb/s	
	2.4-GHz 802.11n (HT20) -92 dBm @		5-GHz 802.11n (HT20) -93 dBm	5-GHz 802.11n (HT40) -91 dBm

Aironet 3501E	Especificaciones			
	MCS0 -90 dBm @ MCS1 -88 dBm @ MCS2 -85 dBm @ MCS3 -82 dBm @ MCS4 -77 dBm @ MCS5 -76 dBm @ MCS6 -74 dBm @ MCS7 -92 dBm @ MCS8 -90 dBm @ MCS9 -87 dBm @ MCS10 -85 dBm @ MCS11 -82 dBm @ MCS12 -77 dBm @ MCS13 -75 dBm @		@ MCS0 -91 dBm @ MCS1 -89 dBm @ MCS2 -86 dBm @ MCS3 -83 dBm @ MCS4 -78 dBm @ MCS5 -77 dBm @ MCS6 -75 dBm @ MCS7 -87 dBm @ MCS8 -87 dBm @ MCS9 -85 dBm @ MCS10 -83 dBm @ MCS11 -79 dBm @ MCS12 -75 dBm @ MCS13 -73 dBm	@ MCS0 -89 dBm @ MCS1 -87 dBm @ MCS2 -83 dBm @ MCS3 -80 dBm @ MCS4 -75 dBm @ MCS5 -74 dBm @ MCS6 -72 dBm @ MCS7 -86 dBm @ MCS8 -85 dBm @ MCS9 -84 dBm @ MCS10 -80 dBm @ MCS11 -77 dBm @ MCS12 -72 dBm @ MCS13 -71 dBm

Aironet 3501E	Especificaciones			
	MCS14 -74 dBm @ MCS15		@ MCS14 -72 dBm @ MCS15	@ MCS14 -70 dBm @ MCS15
Maximum Transmit Power	2.4 GHz • 802.11b • 23 dBm with 2 antennas • 802.11g • 20 dBm with 2 antennas • 802.11n (non-HT duplicate mode) • 20 dBm with 2 antennas • 802.11n (HT20) • 20 dBm with 2 antennas		5 GHz • 802.11a • 20 dBm with 2 antennas • 802.11n non-HT duplicate mode • 20 dBm with 2 antennas • 802.11n (HT20) • 20 dBm with 2 antennas • 802.11n (HT40) • 20 dBm with 2 antennas	
Note: The maximum power setting will vary by channel and according to individual country regulations. Refer to the product documentation for specific details.				
Available Transmit Power Settings	2.4 GHz 23 dBm (200 mW) CCK Only 20 dBm (100 mW) 17 dBm (50 mW) 14 dBm (25 mW) 11 dBm (12.5 mW) 8 dBm (6.25 mW) 5 dBm (3.13 mW)		5 GHz 20 dBm (100 mW) 17 dBm (50 mW) 14 dBm (25 mW) 11 dBm (12.5 mW) 8 dBm (6.25 mW) 5 dBm (3.13 mW) 2 dBm (1.56 mW) -1 dBm (0.78 mW)	

Aironet 3501E	Especificaciones	
	2 dBm (1.56 mW) -1 dBm (0.78 mW)	
Note: The maximum power setting will vary by channel and according to individual country regulations. Refer to the product documentation for specific details.		
Integrated Antenna	• 2.4 GHz, Gain 4 dBi, internal Omni, horizontal beamwidth 360° • 5 GHz, Gain 3 dBi, internal Omni, horizontal beamwidth 360°	
External Antenna (sold separately)	• Cisco offers the industry's broadest selection of 802.11n antennas delivering optimal coverage for a variety of deployment scenarios • Connectors: 3 RP-TNC (2.4GHz), 3 RP-TNC (5-GHz)	
Interfaces	• 10/100/1000BASE-T autosensing (RJ-45) • Management console port (RJ-45)	
Indicators	• Status LED indicates boot loader status, association status, operating status, boot loader warnings, boot loader errors	
Dimensions (W x L x H)	• Access point (without mounting bracket): 8.7 x 8.7 x 1.84 in. (22.1 x 22.1 x 4.7 cm)	
Weight	• 2.3 lbs (1.04 kg)	
Environmental	Cisco Aironet 3500i • Nonoperating (storage) temperature: -22 to 185°F (-30 to 85°C) • Operating temperature: 32 to 104°F (0 to 40°C) • Operating humidity: 10 to 90% percent (noncondensing) Cisco Aironet 3500e • Nonoperating (storage) temperature: -40 to 185°F (-40 to 85°C) • Operating temperature: -4 to +131°F (-20 to	

Aironet 3501E	Especificaciones
	+55°C) • Operating humidity: 10 to 90 percent (noncondensing)
System Memory	• 128 MB DRAM • 32 MB flash
Input Power Requirements	• AP3500: 44 to 57 VDC • Power Supply and Power Injector: 100 to 240 VAC; 50 to 60 Hz
Powering Options	• 802.3af Ethernet Switch • Cisco AP3500 Power Injectors (AIR-PWRINJ4=) • Cisco AP3500 Local Power Supply (AIR-PWR-B=)
Power Draw	• AP3500: 12.95 W **Note:** When deployed using Power over Ethernet (PoE), the power drawn from the power sourcing equipment will be higher by some amount dependent on the length of the interconnecting cable. This additional power may be as high as 2.45W, bringing the total system power draw (access point + cabling) to 15.4W.
Warranty	Limited Lifetime Hardware Warranty
Compliance Standards	• Safety: • UL 60950-1 • CAN/CSA-C22.2 No. 60950-1 • UL 2043 • IEC 60950-1 • EN 60950-1 • Radio approvals: • FCC Part 15.247, 15.407 • RSS-210 (Canada) • EN 300.328, EN 301.893 (Europe) • ARIB-STD 33 (Japan) • ARIB-STD 66 (Japan) • ARIB-STD T71 (Japan) • EMI and susceptibility (Class B) • FCC Part 15.107 and 15.109

Aironet 3501E	Especificaciones
	• ICES-003 (Canada) • VCCI (Japan) • EN 301.489-1 and -17 (Europe) • EN 60601-1-2 EMC requirements for the Medical Directive 93/42/EEC • IEEE Standard: • IEEE 802.11a/b/g, IEEE 802.11n 2.0, IEEE 802.11h, IEEE 802.11d • Security: • 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA • 802.1X • Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP) • EAP Type(s): • Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) • EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) • Protected EAP (PEAP) v0 or EAP-MSCHAPv2 • Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) • PEAPv1 or EAP-Generic Token Card (GTC) • EAP-Subscriber Identity Module (SIM) • Multimedia: • Wi-Fi Multimedia (WMM™) • Other: • FCC Bulletin OET-65C • RSS-102

4.3.3.3. Network Control System.

Network Control System	Specification
VMware ESX and ESXi Versions (Virtual Appliance on a Customer-Supplied Server)	If deploying Cisco Prime NCS as a virtual appliance, on a customer-supplied server, one of the following versions of VMware ESX or ESXi may be used: • VMWare ESX or VMWare ESXi version 4.1
Minimum Server Requirements for Deploying Virtual Appliances	Cisco Prime NCS High-End Virtual Appliance: • 15,000 lightweight access points; 5000 standalone access points; 1200 wireless LAN controllers and

Network Control System	Specification
	5000 switches • Minimum RAM: 16GB • Minimum Hard disk space allocation: 400GB • Processors: 8, at 2.93GHz or better
	Cisco Prime NCS Standard Virtual Appliance: • 7500 lightweight access points; 2500 standalone access points; 600 wireless LAN controllers and 2500 switches • Minimum RAM: 12GB • Minimum Hard disk space allocation: 300GB • Processors: 4, at 2.93GHz or better
	Cisco Prime NCS Low-End Virtual Appliance: • 3000 lightweight access points; 1000 standalone access points; 240 wireless LAN controllers and 1000 switches • Minimum RAM: 8GB • Minimum Hard disk space allocation: 200GB • Processors: 2, at 2.93GHz or better
	Deploying Cisco Prime NCS Virtual Appliance on CiscoWorks Wireless LAN Solution Engine (WLSE) models 1130-19 or 1133 • Cisco Prime NCS is not supported on the Cisco WLSE hardware
Minimum Client Requirements	Internet Explorer 8.0 or later and Mozilla Firefox 3.6 or later
Management and Security	SNMP v1, v2c, v3 and Cisco Terminal Access Controller Access-Control System Plus (TACACS+) PNG, JPEG, and AutoCAD (DXF and DWG) import file types supported
Managed Devices	Cisco 2100, 2500, 4400, 5500 and Flex 7500 Series Wireless LAN Controllers; Cisco Catalyst 6500 Series Wireless Services Modules (WiSM/WiSM2) and Cisco Wireless LAN Controller Module on SRE 2; Cisco Catalyst 3750G Integrated Wireless LAN Controller; Cisco Wireless LAN Controller Module (WLCM and WLCM-E) for Integrated Services Routers; Cisco Aironet access points with CleanAir technology, Cisco Aironet lightweight access points, Cisco Aironet lightweight outdoor mesh access points, Cisco OfficeExtend 600 Access Point, Cisco Aironet

Network Control System	Specification
	1240AG and 1130AG Series Access Points, Cisco 3300 Series Mobility Services Engine (MSE), Cisco Wireless Location Appliance, Cisco Spectrum Expert Wi-Fi, Cisco Context-Aware Software, and Cisco Adaptive wIPS Software. Monitoring and migration of selected Cisco Aironet standalone (autonomous) access points. Monitoring of the standalone access points of Cisco 800, -1800, 2800, and 3800 Series Integrated Services Routers. Monitoring of Cisco Catalyst 2960, 2975 Switches [IOS12.2(50)SE], Cisco Catalyst 3560 Switches [IOS12.2(50)SE], Cisco Catalyst 3750 Switches [IOS12.2(50)SE], Cisco Catalyst 4500 Switches [IOS12.2(50)SG], Cisco Catalyst 6500 Switches [IOS12.2(33)SXI].

CONCLUSIONES Y RECOMENDACIONES

Una vez culminado el presente proyecto es posible realizar las siguientes conclusiones y recomendaciones:

5.1. Conclusiones

El desarrollo del presente proyecto significa un aporte para la comunidad universitaria y para la población en general que esté interesada en profundizar en la tecnología WiFi, ya que provee información general y a detalle que describen aspectos más importantes sobre la utilización e implantación de redes inalámbricas.

Las redes inalámbricas basadas en el estándar IEEE 802.11 son una tecnología que aporta beneficios considerables en términos de flexibilidad, escalabilidad y movilidad, pero que tiene un gran impacto en la infraestructura, operaciones y Seguridad de la Información de las organizaciones.

La clave para un correcto y eficaz despliegue y explotación de este tipo de redes está en comprender los riesgos que entrañan, además de conocer las posibilidades de la tecnología con la que contamos en la actualidad para mitigarlos.

A pesar del alto costo de las redes inalámbricas en comparación con las redes cableadas, se puede observar que esto es relativo, dado que la flexibilidad y versatilidad de las redes inalámbricas representa un ahorro significativo en cuanto a mantenimiento, reubicación de nodos y ampliación de la red.

5.2. Recomendaciones

Establecer políticas de seguridad dentro de la red es una alternativa que debe tener muy en cuenta en la UAJMS, de manera que se informe a cada usuario de los riesgos que implicarían para el bienestar de la Universidad violar estos acuerdos.

Se debe capacitar al personal encargado de administrar y gestionar la red de la UAJMS, así como brindar información a los usuarios de la red inalámbrica, informando de todas las implicaciones que tendría el uso indebido de la misma.

Existirá un incremento tanto lineal como exponencial de usuarios y será necesario dimensionar la red para una demanda máxima tanto de los usuarios estudiantiles como de usuarios administrativos, docentes.