UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

RED CISCO WIRELESS DE ALTA DISPONIBILIDAD PARA ROBOTS AUTOMATIZADOS DEL ALMACÉN DE UNA MEGAPLANTA DE GASEOSAS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

MIGUEL ÁNGEL GONZALES VIDAL

PROMOCIÓN
2009-II

LIMA-PERÚ
2013

RED CISCO WIRELESS DE ALTA DISPONIBILIDAD PARA ROBOTS AUTOMATIZADOS DEL ALMACÉN DE UNA MEGAPLANTA DE GASEOSAS

Mis agradecimientos a:
A mis padres Alejandro y Betty por su apoyo incondicional.
A mis hermanos Pablo y Joel.
A mi querida UNI por su formación y valores.

SUMARIO

En el presente informe se explica el diseño de una red inalámbrica Cisco de alta disponibilidad para robots automatizados del almacén de una megaplanta de gaseosas. Estos robots son montacargas no tripulados que realizan labores de carga y almacenaje de las parihuelas (pallets) sobre las cuales se depositan los paquetes de gaseosas. A este robot se le denomina LGV, siglas de Laser Guided Vehicle (Vehículo Guiado por Láser).

El LGV necesita comunicarse constantemente con la estación central de forma inalámbrica, a la espera de órdenes y el reporte de su posición, además de otras informaciones relevantes.

El diseño involucra una red inalámbrica segura, gestionable y de alta disponibilidad, ello debido a la importancia de que los procesos relacionados a los LGVs no deben verse afectados por factores externos.

El diseño de la red inalámbrica asegura una adecuada cobertura y alta disponibilidad, esto gracias a la red malla considerada.

Para el diseño de esta red malla se utiliza como herramienta el aplicativo Cisco Prime Infrastructure con el que se predice el desempeño de los puntos de acceso en el almacén. Además, esta herramienta servirá para el despliegue, operación, reporte y administración, asegurando el ciclo de vida operacional de la red.

Para esta solución, se explican las consideraciones y roles de los puntos de acceso en una red inalámbrica malla, las características y consideraciones en la selección de los puntos de acceso y controladores, las consideraciones para el diseño de los controladores, las consideraciones de puertos e interfaces en el controlador de red de área local inalámbrica, una breve definición de los aplicativos de seguridad de acceso y gestión de Cisco considerados en el diseño y finalmente los aspectos económicos así como los cronogramas estimados del proyecto.

ÍNDICE

INTRODUCCIÓN

El trabajo surge por la necesidad de una empresa embotelladora de bebidas gaseosas de contar con una red de comunicación inalámbrica para el control y supervisión de los nuevos robots automatizados.

Las tareas de los robots son críticas por ello es imprescindible que estén comunicadas permanentemente. Los montacargas no tripulados se encargan almacenar y despachar (carga y descarga) los pallets (parihuelas) de gaseosas. Estos montacargas poseen rutas preestablecidas (no rieles).

En si el diseño de la solución consiste en:

- Determinar la cantidad y ubicación de los AP a fin de asegurar la cobertura a los LGVs.- Para ello se hace uso de una aplicación de monitoreo y gestión Cisco que permite simular el escenario. Los APs cumplen con el estándar 802.11 a, b, g, n y sólo en el caso de los APs indoor, 802.11ac.
- Definir el equipamiento necesario para brindar una alta disponibilidad a la red inalámbrica a fin de asegurar las comunicaciones.- Para ello se diseña una red mesh wireless y redundancia de equipamiento activo.
- Establecer la seguridad y gestión de la red.- Determinar los aplicativos o herramientas a fin de proporcionar una adecuado control de acceso, monitoreo, etc.

Las fuentes bibliográficas utilizadas provienen principalmente de la extensa documentación desarrollada por Cisco

El presente informe de suficiencia está organizado en cuatro capítulos principales:

- Capítulo I "Planteamiento de Ingeniería del Problema".- En este capítulo se explica el problema de ingeniería y se precisan los objetivos de la tesis. También se hace una evaluación de la problemática y se establecen los alcances del proyecto desarrollado, para finalmente presentar una síntesis de la tesis realizada
- Capítulo II "Marco Teórico". En este capítulo se definirán las consideraciones operativas asociadas al despliegue de una red unificada wireless. Entre ellas se mencionan a CAPWAP (Split MAC , Túneles Basados en Capa, WLC Descubrimiento y Selección), Componentes de la Red Unificada Wireless Cisco (Cisco Wireless LAN Controlles, Access Point, Cisco Prime Infrastructure), Grupos de Movilidad, Grupos de APs, Grupos RF, Roaming (Intra Controller Roaming, Inter Controller Roaming, Inter Subnet Roaming, Auto-Anchor Mobility, Red Mesh Inalámbrica, Mobility Service Engine (Cobertura y

Movilidad), Cisco ISE.

- Capítulo III "Metodología para la Solución del Problema".- Este capítulo se enfoca a exponer las consideraciones que se tomaron para el diseño la red mesh Cisco, los equipos que involucran y como estos interaccionan y trabajan para proveer un red robusta, escalable y confiable. Se desarrolla lo siguiente: La zona de aplicación de la solución, el diagrama lógico de la red de la megaplanta, el diseño de la red mesh, las características y consideraciones de los APs mesh para el diseño y las consideraciones para el diseño de los controladores.
- Capítulo IV "Costos y Cronograma".- Se desarrollan los aspectos involucrados al análisis de costos y al cronograma de los trabajos realizados en el proyecto de ingeniería.

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

En este capítulo se explica el problema de ingeniería y se precisan los objetivos de la tesis. También se hace una evaluación de la problemática y se establecen los alcances del proyecto desarrollado, para finalmente presentar una síntesis de la tesis realizada.

1.1 Descripción del problema

Necesidad de una empresa embotelladora de bebidas gaseosas de contar con una red de comunicación inalámbrica para la comunicación de los nuevos robots automatizados.

Las tareas de los robots son críticas por ende la importancia de que estén permanentemente comunicadas. Ellos cumplen la función de almacenaje y despacho (carga y descarga) de los pallets (parihuelas) de gaseosas, además poseen rutas preestablecidas (no rieles).

1.2 Objetivos del trabajo

Diseñar una red Cisco wireless de alta disponibilidad para robots automatizados del almacén de una megaplanta de gaseosas.

Dada la importancia de los procesos, se requiere que la red inalámbrica sea segura, gestionable y de alta disponibilidad de manera que no se afecte la productividad.

1.3 Evaluación del problema

El tipo de robot a utilizar en la megaplanta de gaseosas es denominado LGV, que son siglas de Laser Guided Vehicle (Figura 1.1) o vehículo guiado por láser.

Figura 1.1 LGV - Vehículo Guiado por Láser (Fuente: Fabricante)

Los LGVs son programados para comunicarse con un administrador centralizado para asegurar que el producto se está desplazando suavemente a través del almacén, ya sea si se esté almacenando para un uso futuro o esté siendo enviado directamente a las zonas de embarque.

En la actualidad los LGVs juegan un papel importante en el diseño de nuevas fábricas y almacenes, moviendo con seguridad la mercancía a su correspondiente.

El uso de vehículos no tripulados para mover las cargas de los pallets por las áreas de almacenaje y producción se ha convertido en una mejor opción dado el gran costo beneficio que brinda. Incluso las pequeñas instalaciones pueden obtener grandes beneficios ya que las unidades casi no requieren mantenimiento, trabajan al 100% todo el tiempo, no deterioran la planta y presentan una gran ventaja respecto a tener operarios humanos [1].

La ventaja de los LGVs, sobre cualquier otro vehículo no tripulado, es que no requieren de ningún trabajo civil tal como la colocación de bandas magnéticas sobre el piso. El haz del láser, montado en la parte más alta del vehículo, triangula su posición utilizando espejos colocados a la altura del área de trabajo. El sistema continuamente compara su posición actual con la posición calculada, de tal manera que ningún error tal como una rueda sobregirada en un piso húmedo, afecte su sistema de posicionamiento y por ende se detenga hasta una asistencia manual para su reinicio.

El LGV posee unidades de detección de personal tanto en la parte frontal como posterior para detener al LGV en case de cualquier obstrucción; al eliminarse la obstrucción el LGV continua con su labor (Figura 1.2). Las rutas pueden ser cambiadas usando una PC para permitir que el sistema se expanda incluyendo más vehículos, así como estaciones de depósito y recojo de una manera fácil.

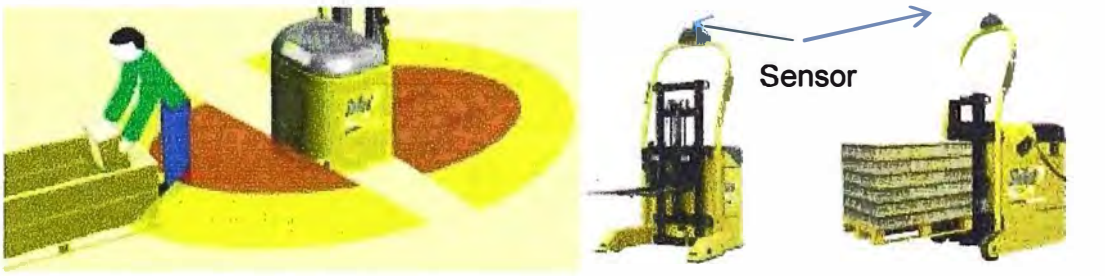

Figura 1.2 Ejemplo de haz sensor de un LGV (Fuente: Referencia [1])

Las características básicas de comunicación de cada LGV con su estación central se denominan flujo/tiempo de intercambio mensajes, como se muestra a continuación existen dos categorías:

- Mensajes de estado.
- Mensajes de administrador de tráfico.

Respecto a los mensajes de estado se tienen:

1. Peticiones de Mensajes de Estado cada 500ms del PC servidor al LGV (20bytes) (Figura 1.3).

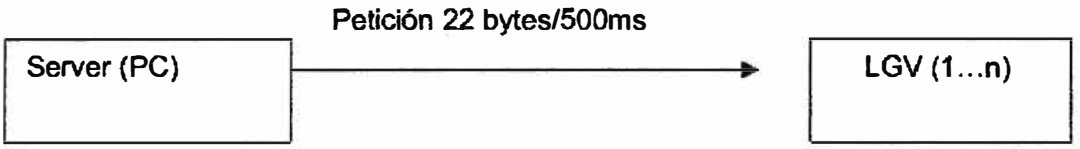

Figura 1.3 Peticiones de mensajes de estado (Fuente: referencia [2])

2. Mensajes de respuesta del LGV cada 500ms (130 bytes) (Figura 1.4).

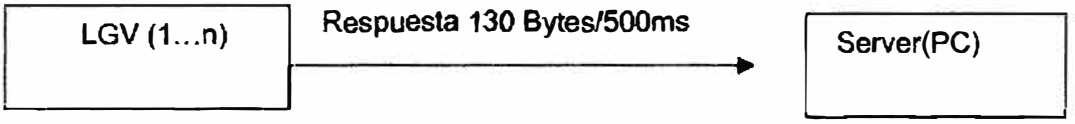

Figura 1.4 Mensajes respuesta (Fuente: referencia [2])

Respecto a los mensajes de administrador de tráfico, estos son transmitidos a cada LGV cada 1 seg (Figura 1.5).

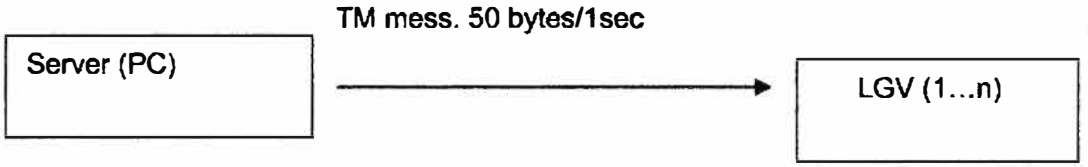

Figura 1.5 Mensajes de administrador de tráfico (Fuente: referencia [2])

Este intercambio de mensajes ocurre por cada LGV. Se considera un Timeout por pérdida de comunicación: 5 sec.

El siguiente esquema simplificado (Figura 1.6) muestra los elementos involucrados:

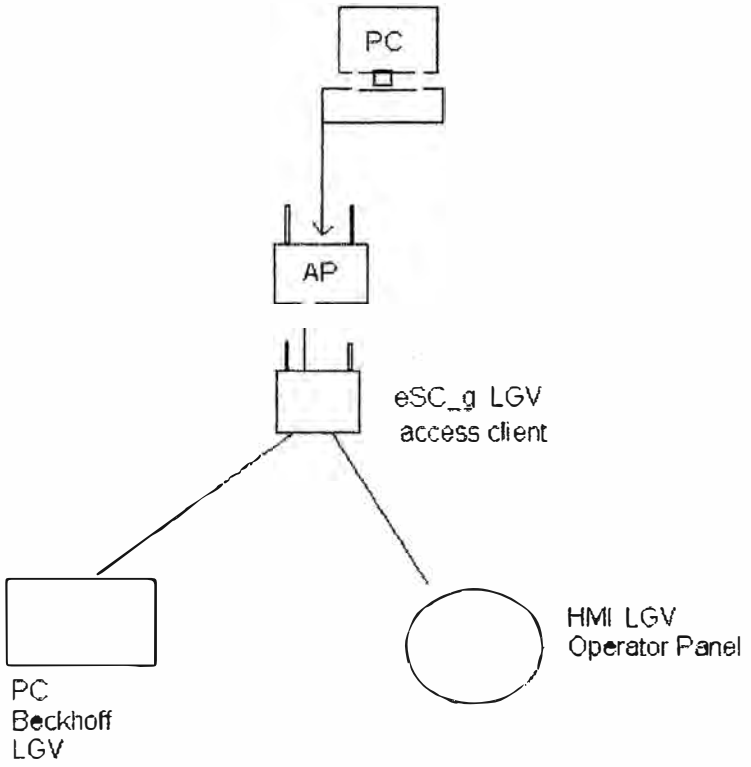

Figura 1.6 Elementos del sistema (Fuente: Referencia [2])

Por un lado están el servidor que administra una serie de Puntos de Acceso (APs). Por otro lado está el LGV que cuenta con un AP cliente, una PC interna y un panel del operador.

Dado que el LGV está orientado a desplazarse en un almacén de grandes dimensiones (altura máxima 14 metros y mínima 11), con estantes de 10 metros de altura (incluido los pallets) que contienen botellas de gaseosa, el diseño una red inalámbrica que asegure una adecuada cobertura, gestión y seguridad es sumamente importante.

1.4 Alcance del trabajo

El alcance del informe se enfoca en:

- Determinar la cantidad y ubicación de los AP a fin de asegurar la cobertura a los LGVs.- Para ello se hace uso de una aplicación de monitoreo y gestión Cisco que permite simular el escenario. Los APs cumplen con el estándar 802.11 a, b, g y n.
- Determinar el equipamiento necesario para brindar una alta disponibilidad a la red inalámbrica a fin de asegurar las comunicaciones.- Para ello se diseña una red mesh wireless y redundancia de equipamiento activo.
- Seguridad y gestión de la red.- Establecer los aplicativos o herramientas a fin de proporcionar una adecuado control de acceso, monitoreo, etc.

El informe no desarrolla la configuración para el control de acceso por ser parte de otro equipo de trabajo dentro de la empresa que provee la solución. El informe se complementa con el análisis de costos del proyecto que involucra lo antes mencionado.

CAPÍTULO II
MARCO TEÓRICO CONCEPTUAL

En este capítulo se definirán las consideraciones operativas asociadas al despliegue de una red unificada wireless.

2.1 Protocolo CAPWAP

CAPWAP (Control and Provisioning of Wireless Access Points) es el protocolo subyacente que es usado en las arquitecturas wireless de Cisco. CAPWAP provee configuración y gestión de las redes wireless LAN, además gestiona el tráfico de túnel a dos vías desde los clientes hasta los WLC (Wireless LAN Controllers) centralizados. La Figura 2.1 muestra un diagrama de alto nivel de un despliegue básico de un WLAN centralizado [3].

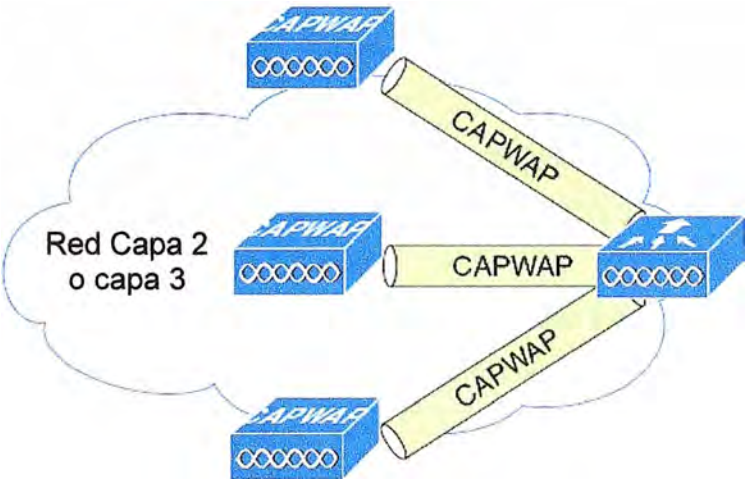

Figura 2.1 CAPWAP APs conectados a un WLC (Fuente: Referencia [3])

Las funcionalidades principales del CAPWAP incluyen:

- Split MAC Túnel
- Túneles basados en capa 3
- Procesos de descubrimiento del WLC

A continuación se definirá cada una de estas funcionalidades:

2.1.1 Funcionalidad Split MAC

Un componente clave del CAPWAP es el concepto de Split MAC, donde parte de la operación del protocolo 802.11 es manejado por el Access Point, mientras la otra parte restante es manejada por el WLC, la Figura 2.2 muestra el concepto del Split MAC [3].

El concepto de split MAC toma todas las funciones realizadas normalmente por un AP

individual y distribuye estas en dos componentes funcionales: un CAPWAP AP y un WLC. Estos dos componentes son unidos a través de la red por medio del protocolo CAPWAP y ambos proveen servicios equivalentes que un AP individual, pero de una manera en que facilita el despliegue y la gestión.

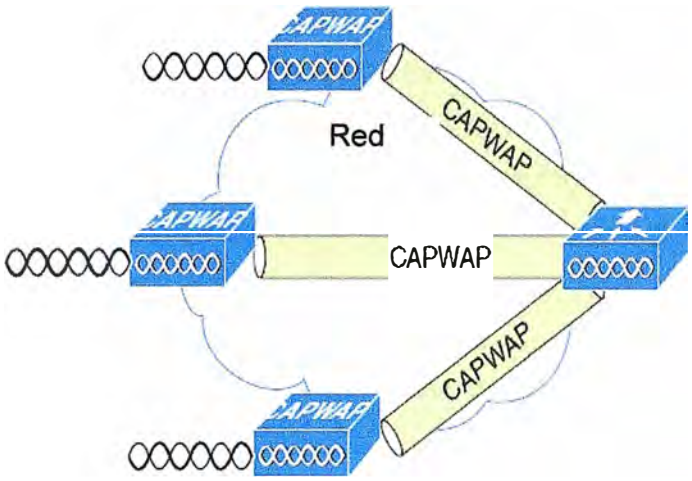

Figura 2.2 CAPWAP split-MAC ESS (Fuente: Referencia [3])

Si bien split MAC facilita la conectividad en capa 2 entre los clientes WLAN y la interface cableada del WLC, esto no significa que por el túnel CAPWAP pasará todo el tráfico. El WLC sólo envía tramas con Ethertype IP, y su comportamiento por default es no enviar tráfico multicast o broadcast.

Las operaciones simples y dependientes del tiempo son generalmente realizadas por el CAPWAP AP, mientras que las operaciones más complejas y menos dependientes del tiempo son manejadas en el WLC.

Por ejemplo las operaciones que el CAPWAP AP maneja son:

- Intercambio de tramas a tres vías entre el cliente y el AP.
- Transmisión de tramas bacon.
- Buffering y transmisión de tramas para clientes.
- Respuesta a las tramas probe requests de los clientes; estas probe requests son enviados al WLC para su procesamiento.
- Envío de notificaciones de los probe requests recibidos al WLC.
- Suministro de información en tiempo real de información de la calidad de señal con cada trama recibida.
- Monitoreo de cada canal de radio en busca de ruido, interferencia u otros WLANs.
- Monitoreo de la presencia de otros APs.
- Cifrado y descifrado de tramas 802.11.

Otras funcionalidades son realizadas por el WLC. Entre estas funciones tenemos:

- Autenticación 802.11.
- Asociación y re asociación 802.11 (movilidad).

- Traducción de tramas y bridging.
- Procesamiento 802.1X/EAP/RADIUS.

Los túneles CAPWAP soportan dos categorías de tráfico:

- Mensajes de control CAPWAP, usado para transportar información de control, configuración y gestión entre el WLC y los APs.
- Encapsulamiento de la data proveniente de los clientes wireless.

Cuando el tráfico encapsulado alcanza el WLC, este es mapeado hacia la VLAN correspondiente (interface o puerto en el WLC). Este mapeo de interfaces es definido como parte de la configuración del WLC. Generalmente este mapeo es estático, pero en base a ciertos parámetros enviados por un servidor AAA después de una exitosa autenticación EAP, este mapeo puede ser dinámico.

Además de la asignación de VLANs, otros parámetros que se pueden configurar incluyen:

- SSID.
- Estado operacional.
- Método de autenticación y seguridad.
- QoS

2.1.2 Túneles basados en capa 3

Este método usa paquetes IP UDP para facilitar la comunicación entre el CAPWAP AP y el WLC. CAPWAP capa 3 puede utilizar la fragmentación y re ensamblado de estos paquetes. Esto permite al tráfico de los clientes usar 1500 byte MTU y así no tener que ajustarse ante saturaciones del túnel [3].

2.1.3 Controlador de Red de Área Local Inalámbrica, descubrimiento y selección

En esta sección se describe el típico comportamiento de un CAPWAP AP después de ser inicializado. [3]

- Paso 1: El AP transmite un mensaje CAPWAP capa 3 de descubrimiento en la subred local. Cualquier WLC configurado en modo CAPWAP capa 3 y conectado en la misma subred verá dicho mensaje de descubrimiento. Cada WLC que reciba este mensaje, responderá con un mensaje CAPWAP de respuesta hacia el AP.
- Paso 2: El AP mantiene la dirección IP del WLC en la NVRAM. El AP envía una solicitud unicast a estas IPs de estos WLCs. Cualquier WLC que escuche esta solicitud, enviará una respuesta al AP. La información guardada en la NVRAM incluye direcciones de otros controladores aprendidas previamente y que fueron miembros de otros grupos de movilidad.
- Paso 3: Un servidor DHCP puede ser configurado para enviar la IP de un WLC usando una opción específica del DHCP. Si se programa, opción 43 es usado para publicar la

dirección de los WLCs hacia los APs. Una vez que los APs reciben la información de dirección IP, estos envían un mensaje unicast de descubrimiento hacia cada dirección de WLC aprendida mediante esta opción 43 del DHCP. Los WLCs que reciben estos mensajes de descubrimiento, envían un mensaje de respuesta unicast hacia estos APs.

- Paso 4: Sin la opción 43, el AP trata de resolver el nombre de DNS por default CISCO-CAPWAP-CONTROLLER.localdomain. El cual puede ser configurado.
- Paso 5: Si después de los pasos 1-4, no se tienen ninguna respuesta, el AP comienza nuevamente con el algoritmo de búsqueda.

Un CAPWAP AP está normalmente configurado con una lista de hasta tres WLCs que representan los preferidos, si alguno de ellos se inhabilita o tiene un exceso de APs registrados, el AP escoge otro WLC de la lista.

2.2 Componentes de la red unificada wireless Cisco

Los principales componentes que involucran la solución de red unificada wireless Cisco son: el Cisco Prime Infrastructure, oficialmente conocido como el Sistema de Control Wireless (WCS) y el sistema de control de red (NCS), los Wireless LAN Controllers (WLC), CAPWAP APs [3].

2.2.1 Controladores de área Local Inalámbrica de Cisco (WLC)

Cisco cuenta con una gran variedad de modelos a medida, los características de cada uno se ajusta a los diversos escenarios que hoy en día se cuentan, los Cisco WLCs ofrecen una gran variedad de beneficios como por ejemplo la reducción de los gastos de operación ya que simplifica el despliegue y la gestión de la red. Extiende las mismas políticas de seguridad y acceso de la red cableada y lo extiende a la red inalámbrica. Estos controladores proveen un único punto de seguridad u optimización para los clientes IPv6, oficinas remotas, desde medianas empresas hasta extensos campuses y proveedores de servicios.

Entre algunas funciones que los WLCs despliegan en la red tenemos:

- Flexibilidad para configurar las políticas wireless, gestión, o ajustes de seguridad vía una provisión y gestión centralizada.
- Respuesta rápida ante las necesidades de negocio a través de la gestión centralizada de la red wireless.
- Configuración de APs estandarizado por versiones.
- Capacidades de prevención de intrusos (Wireless Intrusion Prevention System).
- Capacidad de proporcionar calidad de servicio QoS para voz y video a través de la red cableada e inalámbrica.
- Políticas de seguridad centralizada para la red cableada e inalámbrica.
- Movilidad, seguridad y gestión para clientes IPv6 y dual stack.

- Los WLCs ofrecen una variedad de capacidades entre los cuales tenemos:
- Clean Air Technology: Esta funcionalidad protege el rendimiento de los estándares 802.11n y 802.11ac creando una auto-remediación y una auto-optimización de la red wireless.
- Client Link Technology: Esta funcionalidad es muy importante ya que provee de una optimización de toda la red ya que asegura que los los clientes con estándares 802.11a/g y 802.11n operen a las mejores velocidades posibles.
- Cisco Adaptive wIPS, provee de una protección robusta para toda la red wireless, incluyendo la detección, localización y mitigación de amenazas de penetración a la red y DoS.
- Punto único de gestión de políticas para la red cableada e inalámbrica, esto es posible gracias a la aplicación llamada Identity Service Engine (ISE). Cisco ISE ayuda a las compañías a lidiar con las exponenciales necesidades de crecimiento en smartphones, tablets y laptops. Cisco ISE cumple con las actuales demandas de la tendencia Bring Your Own Device (BYOD). seguridad, acceso relevante de los empleados, invitados y clientes a través de un punto de acceso centralizado [4].

2.2.2 Puntos de Acceso

Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) es un dispositivo que interconecta dispositivos de comunicación alámbrica para formar una red inalámbrica.

Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

Muchos APs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". Cisco Aironet Series APs pueden ser desplegadas en una red distribuida o centralizada de una oficina remota, campus o la gran empresa. Para proveer una experiencia privilegiada a los usuarios finales de la red inalámbrica, estos APs disponen de una variedad de capacidades entre las cuales se tiene:
- Cisco Clean Air Technology– Para auto remediación, optimización automática de red para evitar interferencia RF.
- Cisco ClientLink 3.0 –Para mejorar la confiabilidad y cobertura para los clientes ya existentes.
- Cisco BrandSelect –Para mejorar las conexiones a 5GHz en ambientes duales.
- Cisco Video Stream –Usa el multicast para mejorar las aplicaciones multimedia.

2.2.3 Cisco Prime Infrastructure 1.2

Cisco Prime Infrastructure provee de una única y completa solución integrada que

abarca todo el ciclo de vida de la gestión de una red ya sea cableado o inalámbrica de acceso de un campus, redes remotas además de dar visibilidad de los usuarios finales así como garantizar los rendimientos de las aplicaciones [5].

Cisco Prime Infrastructure acelera el despliegue de nuevos servicios, acceso seguro y gestión de dispositivos móviles haciendo que la tendencia Bring Your Own Device (BYOD) sea una realidad para las corporaciones TI.

Acoplando estrechamente el conocimiento de los clientes con la visibilidad del rendimiento de las aplicaciones y el control de la red, Cisco Prime Infrastructure ayuda a garantizar la calidad de la experiencia del usuario final. La profunda integración con el Identity Service Engine (ISE) expande la visibilidad hacia la seguridad y los problemas relacionados a las políticas, presentando una vista completa de los problemas de acceso de los usuarios proveyendo de un camino claro para resolverlos.

Cisco Prime Infrastructure está basado en un flujo de ciclo de vida (Figura 2.3 Flujo del Ciclo de Vida Operacional), este flujo incluye las tareas de alto nivel que son explicadas a continuación:

- Diseño- La fase de diseño se enfoca en el diseño general de las funcionalidades de los dispositivos o la plantilla del mismo. El área de diseño es donde se crean los patrones de diseño reutilizables como las plantillas de configuración. Cisco Prime provee de una variedad de plantillas de configuración, sin embargo se pueden personalizar las mismas. Estas plantillas y patrones están destinados para su uso en la fase de implementación del ciclo de vida.
- Implementación.- La fase de implementación se enfoca en el despliegue de diseños y plantillas, previamente definidos en la fase anterior, sobre la red. La fase de implementación permite desplegar las configuraciones de las plantillas en uno o más dispositivos.
- Operación.- El área de operación es donde se monitorea la red diariamente, así como realizar otras operaciones del día a día como el inventario de dispositivos y gestión de configuraciones. La pestaña de operación incluye tableros de trabajo, Centro de Trabajo de Dispositivos y herramientas que se necesitan para monitoreo diario, solución de problemas, mantenimiento y operaciones.
- Reporte.- Cisco Prime Infrastructure también provee de reportes que se usan para monitorear el sistema y la salud de la red así como la solución de problemas. Cisco Prime Infrastructure tableta de reportes provee el acceso a los reportes así como la programación de todos los tipos de funciones de reporte.
- Administración.- Es el área donde se establecen las configuraciones del sistema, el manejo del control de acceso y especifica los parámetros de colección de data.

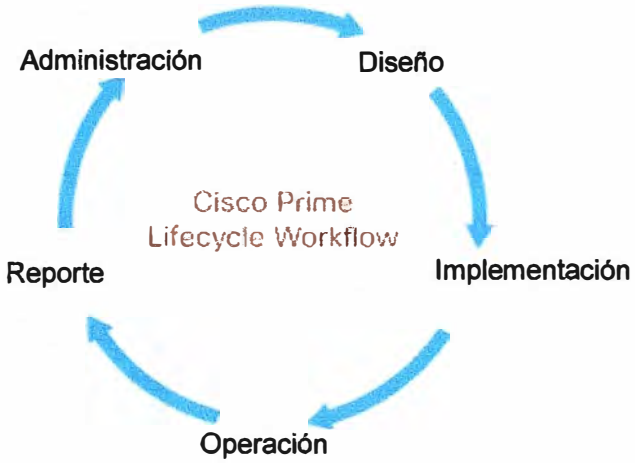

Figura 2.3 Flujo del ciclo de vida operacional (Fuente: Referencia [5])

2.3 Grupos de movilidad, de Puntos de Acceso y de radiofrecuencia

Dentro de la red unificada wireless de Cisco, hay tres importantes conceptos de grupos [3]:

- Grupos de Movilidad.
- Grupos APs.
- Grupos RF.

2.3.1 Grupos de movilidad

Un grupo de movilidad es un grupo de WLCs que en conjunto, actúan como un único WLC virtual compartiendo información esencial de clientes finales, APs y RF. Un WLC dentro de un grupo de movilidad puede tomar decisiones basadas en la data recibida desde otros miembros de todo el grupo de movilidad, esto antes de tomar estas decisiones basadas solamente en la información aprendida de sus APs y clientes directamente conectados.

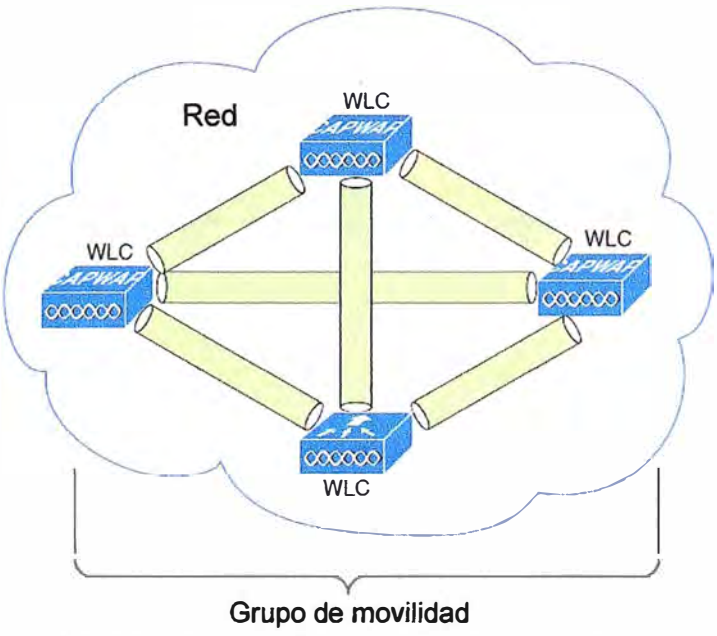

Figura 2.4 Grupo de movilidad WLC (Fuente: Referencia [3])

Un grupo de movilidad forma una malla de túneles autenticados entre los WLCs miembros, esto permite que un WLC individual se pueda comunicar con cualquier WLC dentro del grupo (Figura 2.4).

Un grupo de movilidad es usado para facilitar el roaming transparente entre APs que pertenecen a diferentes WLCs. La principal función de un grupo de movilidad es el de crear un dominio WLAN virtual (a través de múltiples WLCs) con el fin de proveer una vista completa de área de cobertura wireless.

El uso de grupos de movilidad es beneficioso cuando se hacen despliegues comprendidos por coberturas con superposición establecidos por dos o más APs conectados con diferentes WLCs. Un grupo de movilidad no tiene beneficio cuando dos APs asociados con diferentes WLCs se encuentran en ubicaciones diferentes y que no se translapan, por ejemplo el campus de una empresa y su oficina remota o dos o más infraestructuras diferentes dentro del campus.

2.3.2 Grupos de puntos de acceso

En un típico escenario de despliegue, cada WLAN esta mapeada hacia una sólo interface dinámica por WLC. Sin embargo, considerando un escenario de despliegue donde hay un WLC licenciado para soportar un máximo de 500 APs y considerando que 25 usuarios están asociados a cada AP, esto resulta en 12500 usuarios compartiendo la misma VLAN, los diseños generalmente requieren de un menor número tamaño de subred. Una forma de enfrentarse a esto es partir el WLAN en múltiples segmentos.

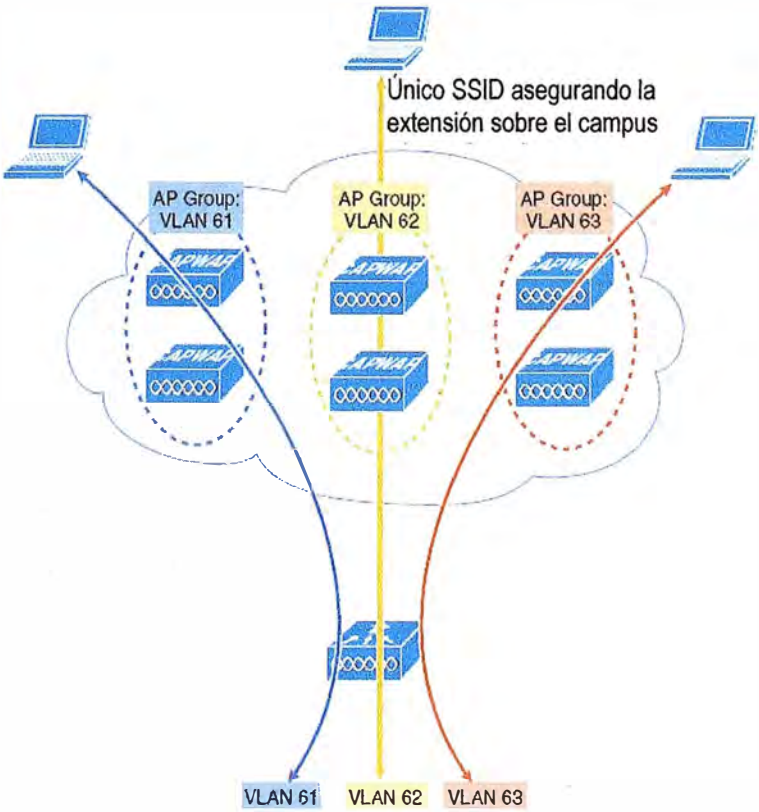

Figura 2.5 Grupo de APs y VLANs Específicas (Fuente: Referencia [3])

La funcionalidad de grupos de APs permite que la WLAN este soportada por medio de múltiples interfaces dinámicas (VLANs) en el WLC. Esto es posible tomando un grupo de APs y mapeándolos hacia una interface dinámica. La Figura 2.5 muestra este arreglo.

Como se observa en la figura, hay tres interfaces dinámicas configuradas, cada una mapeada hacia una VLAN específica (VLAN 61, 62 y 63). Cada VLAN específica y sus APs asociados están mapeados hacia un mismo WLAN SSID usando la funcionalidad de agrupamiento de APs.

2.3.3 Grupos de radiofrecuencia

Los grupos RF, también conocidos como dominios RF, representan otro tipo consideración de despliegue. Un grupo RF es un cluster de WLCs que colectivamente coordina y calcula los parámetros dinámicos del llamado Radio Resource Management (RRM) basados en el tipo de 802.11 PHY, por ejemplo, 802.11b/g y 802.11a.

Un grupo RF existe por cada tipo de 802.11 PHY. Agrupar WLCs permite a los algoritmos dinámicos de RRM escalar más allá de un solo WLC, en consecuencia, permite a un RRM de un determinado grupo RF extenderse entre pisos, edificaciones y hasta campuses.

2.4 Roaming

La movilidad ocurre cuando un cliente se traslada entre dos APs y ya que los clientes wireless se trasladan entre APs asociados a un mismo y los APs pertenecen a diferentes WLCs en una red, hay cuatro tipos de eventos de roaming que pueden ocurrir [3]:

- Intra Controller Roaming (Figura 2.6).
- Inter Controller Roaming (Figura 2.7).
- Inter Subnet Roaming (Figura 2.8).
- Auto Anchor Mobility Roaming (Figura 2.9).

La movilidad ocurre cuando un cliente se traslada entre APs asociados a un mismo WLC o entre APs que pertenecen a diferentes WLCs; estos WLCs pueden estar en una misma subred o en subredes diferentes. Hay cuatro tipos de eventos de roaming que pueden ocurrir

2.4.1 Intra Controller Roaming

Si un cliente hace roaming entre dos APs registrados en el mismo controlador, este es llamado un evento de movilidad intra controller. Este es el escenario más simple del roaming donde el WLC simplemente hace un update a la base de datos con los nuevos contextos de estado y seguridad del cliente después de que este haga el roaming desde el AP1 al AP2 (Figura 2.6).

2.4.2 Inter Controller Roaming

Este escenario ocurre cuando un cliente hace roaming entre dos APs registrados en

diferentes WLCs donde cada controlador tiene una interface a la subred del cliente, en este escenario los controladores intercambian mensajes de control a través del puerto UDP 16666 y el registro en base de datos del cliente es movido desde el controlador original hacia el nuevo controlador (Figura 2.7).

2.4.3 Inter Subnet Roaming

Este escenario se cumple cuando los clientes hacen roaming entre APs registrados en diferentes controladores y además los clientes en estos controladores están en diferentes subredes.

En esta situación, los controladores intercambian mensajes de movilidad y los cambios en la base de datos de los clientes son distintos en comparación al roaming en capa 2 descrito anteriormente, en este caso la información del cliente es copiada a la base de datos del WLC destino. En ente escenario el WLC original marca al cliente como anchor y el WLC destino marca a su nuevo cliente como foreign. Los dos controladores ahora son denominados anchor WLC y foreign WLC respectivamente (Figura 2.8).

2.4.4 Auto-Anchor Mobility

Auto ancho o auto anclaje, es cuando anclamos un cliente invitado a uno o más WLCs, esto permite direccionar el tráfico desde cualquier invitado en la WLAN hacia un anchor WLC ubicado en la DMZ (Figura 2.9).

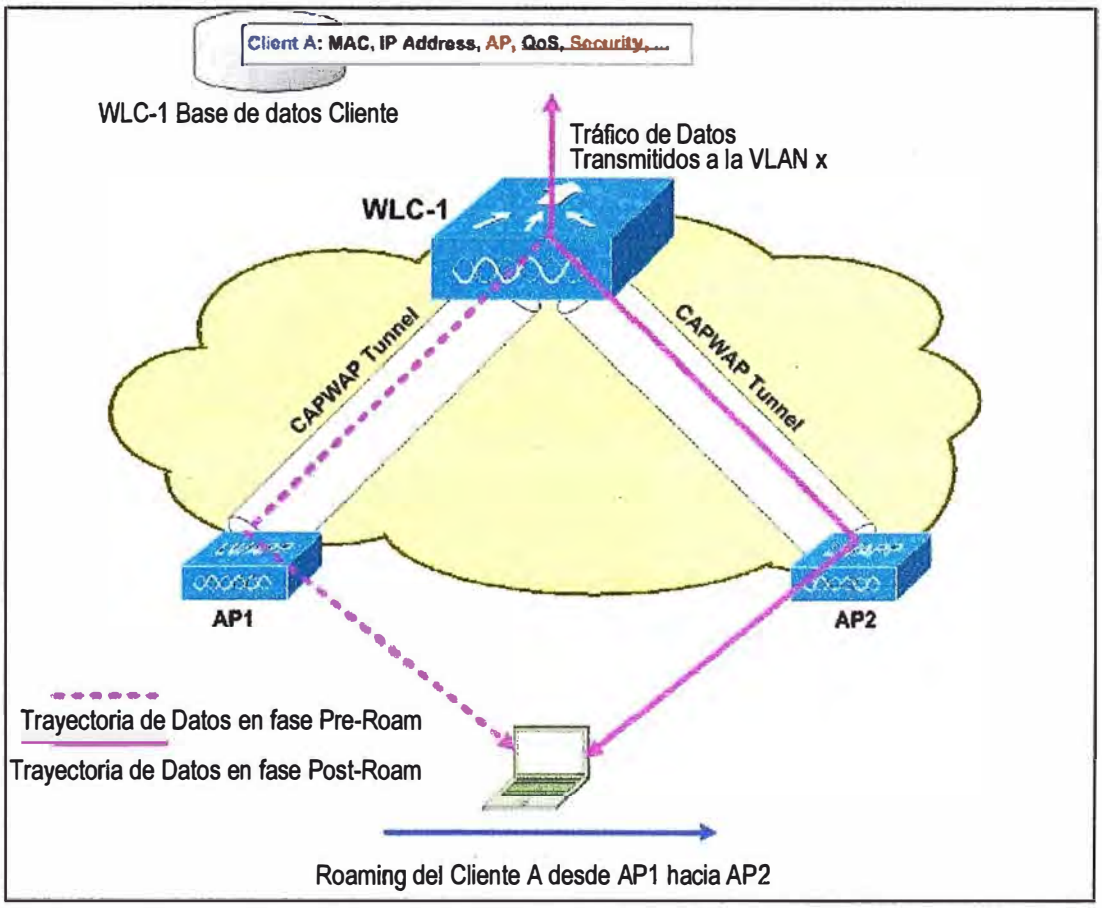

Figura 2.6 Intra-Controller Roaming (Fuente: Referencia [3])

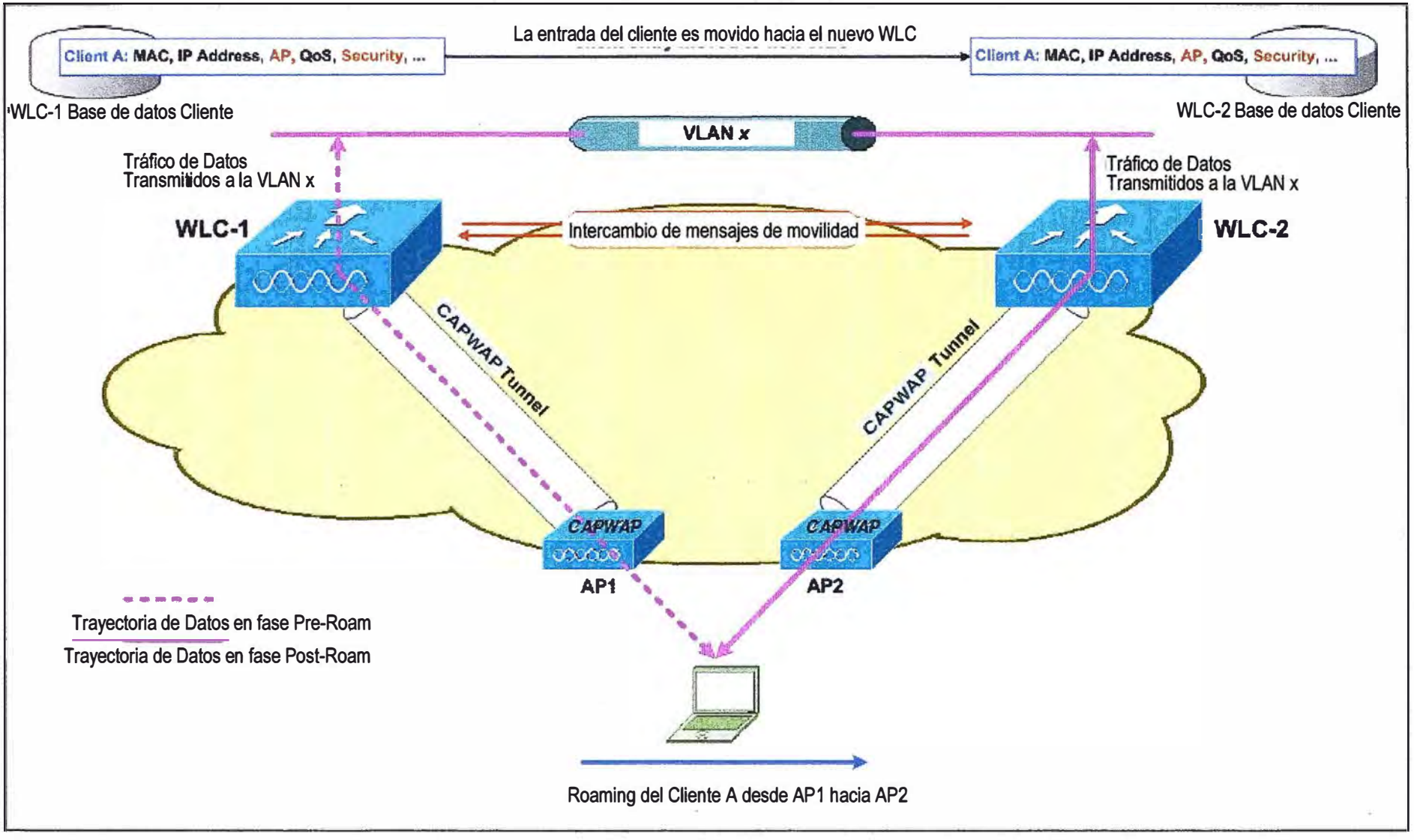

Figura 2.7 Inter-Controller Roaming (Fuente: Referencia [3])

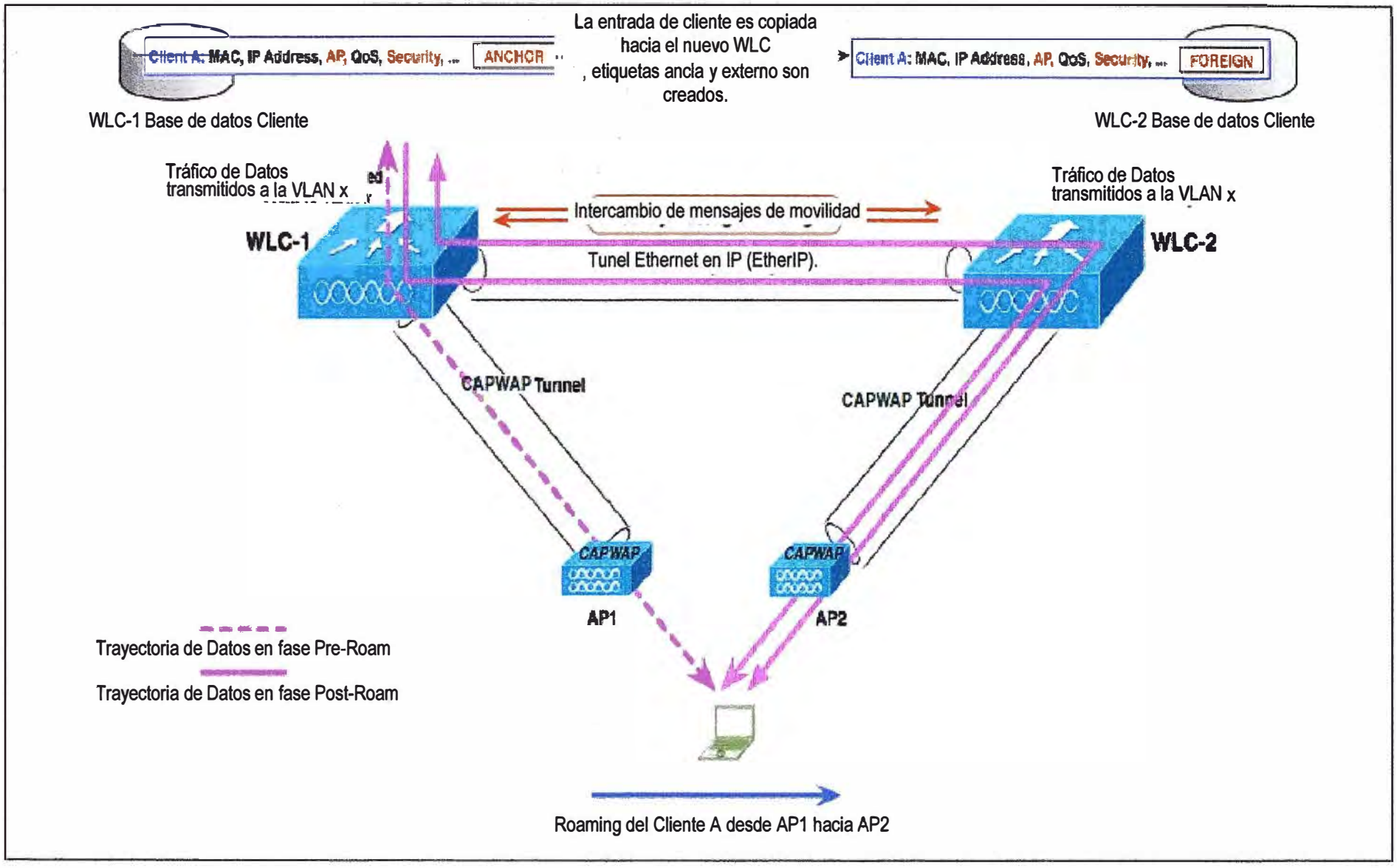

Figura 2.8 Inter Subnet Roaming (Fuente: Referencia [3])

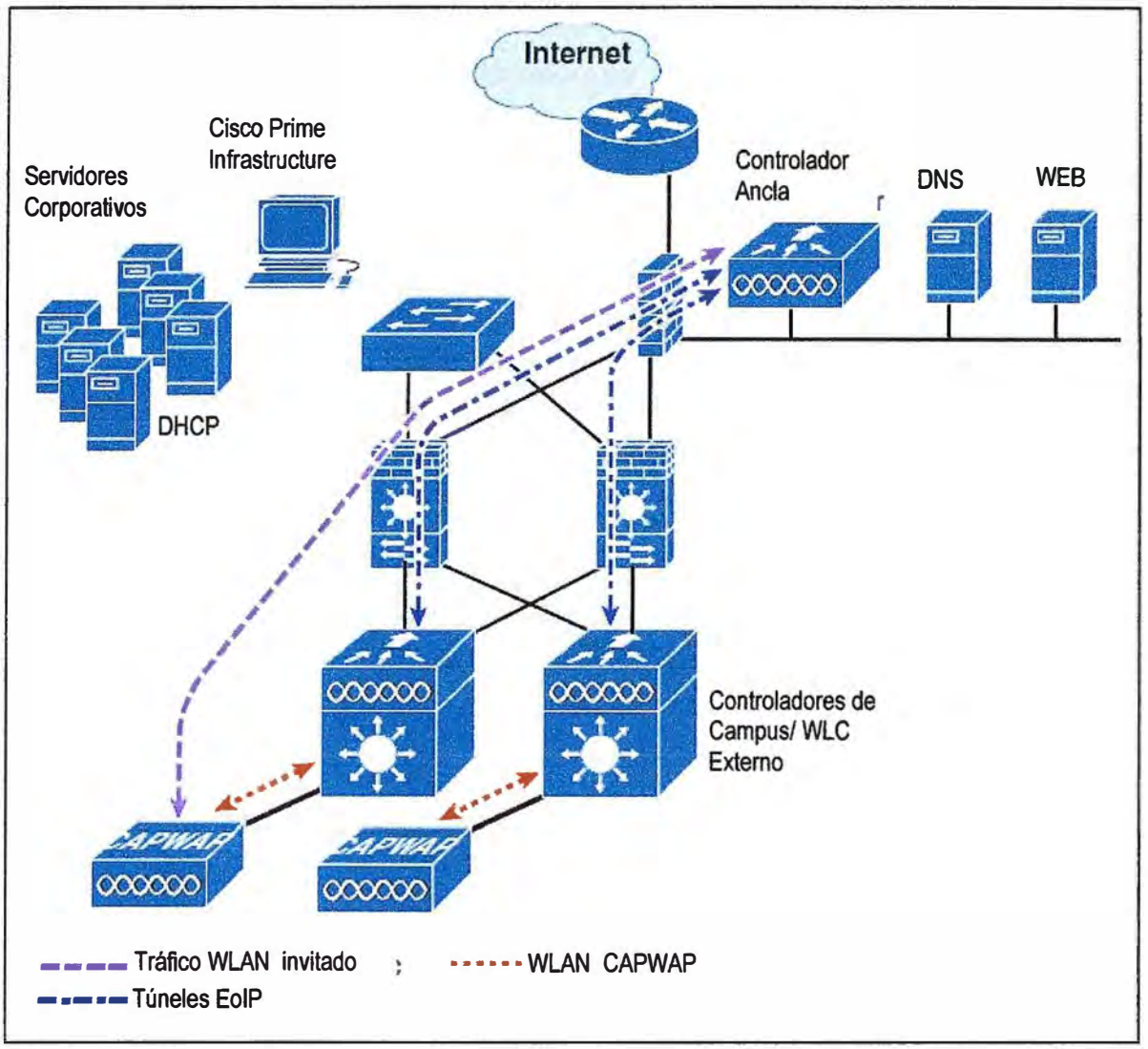

Figura 2.9 Auto Anchor EoIP Túnel (Fuente: Referencia [3])

2.5 Red mesh inalámbrica

Una red mesh es aquella que emplea outdoor mesh APs e indoor mesh APs en conjunto con el WLC para formar una zona de acceso multipunto. El protocolo Control and Provisioning Wireless Access Point (CAPWAP) gestiona las conexiones mesh de los APs en la red [6].

La seguridad punto a punto de una red mesh esta soportada por el empleo del protocolo de cifrado Advanced Encription Standard (AES) entre APs y WPA2 que protege los clientes WiFi.

Entre los roles que cumplen los APs dentro de una red mesh tenemos:

- Root AP (RAP)
- Mesh AP (MAP)

Los MAPs son los que tienen la conexión wireless con sus controladores, mientras que los RAPs tienen una conexión cableada con sus controladores. MAPs se comunican entre ellos y el RAP usando las conexiones wireless sobre el radio backhaul 802.11a/n.

MAPs usan el Cisco Adaptive Wireless Path Protocol (AWPP) para determinar la mejor ruta entre otros MAPs hacia el controlador. La Figura 2.10 muestra la relación entre MAPs y RAPs en una red mesh.

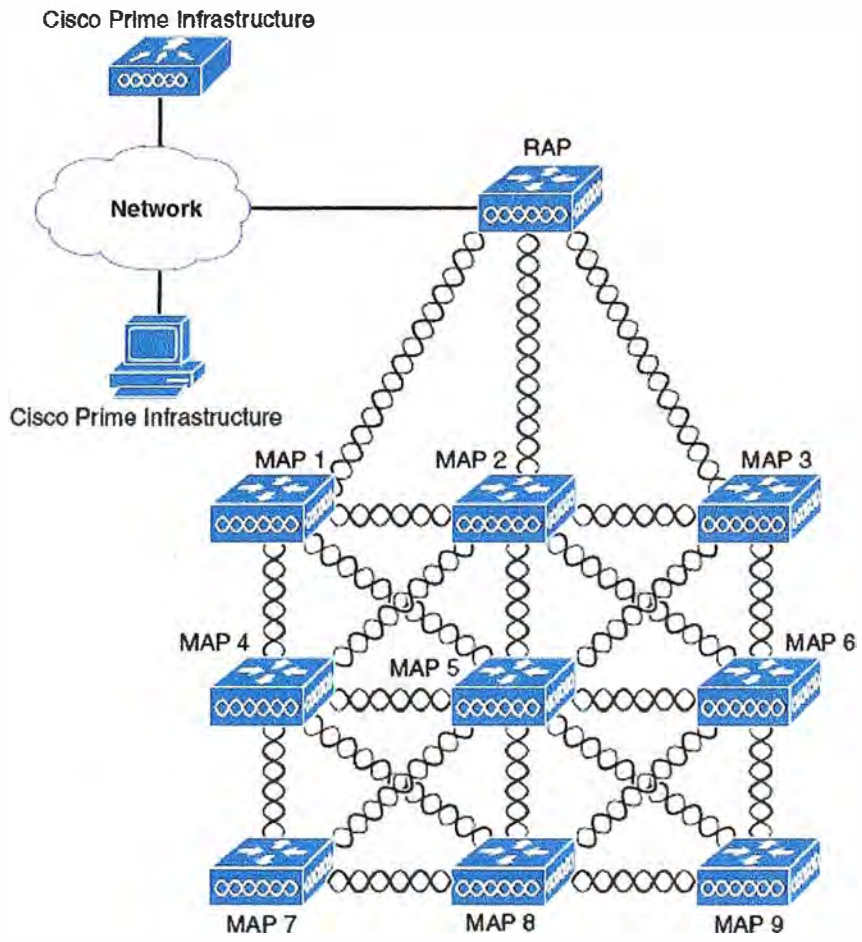

Figura 2.10 Jerarquía de una red mesh simple (Fuente: Referencia [6])

2.6 Mobility Service Engine.- Cobertura y movilidad

Mobility Service Engine (MSE) es una plataforma que soporta una suite de aplicaciones de servicios de movilidad. Diseñado como una plataforma abierta, el MSE soporta software de servicios de movilidad en forma modular y con varias opciones de configuración basados en la topología de la red y tipos de servicios requeridos. Cisco soporta varias aplicaciones entre las cuales se pueden mencionar [7]:

- Servicios de Localización Base –Incrementa la visibilidad en la red capturando y consolidando información crucial sobre el espectro RF, fuentes de interferencia RF, este aplicativo incluye una localización de servicios en tiempo real (RTLS).
- Experiencias de movilidad conectada –Connected Mobility Experience (CMX), es una plataforma WiFi que permite a las organizaciones llevar servicios de movilidad basados en localización a los usuarios finales.
- Wireless Intrusion Preventtion System –Cisco wIPS, protege la red de ataques de penetración, dispositivos wireless piratas y ataques de denegación de servicio (DoS) para

así mejorar la seguridad y cumplir con los objetivos de negocio.

2.7 Plataforma de gestión y control Cisco ISE

Cisco Identity Service Engine es una plataforma de gestión y control de las políticas de seguridad. Esta plataforma automatiza y simplifica el control de acceso y cumplimiento de seguridad tanto en la red cableada como en la red inalámbrica y conectividad VPN. Cisco ISE es principalmente usado para proporcionar un acceso seguro para diversos tipos de usuarios entre los cuales están los invitados, soporta la iniciativa BYOD y ejecuta políticas de uso de la red (Figura 2.11) [8].

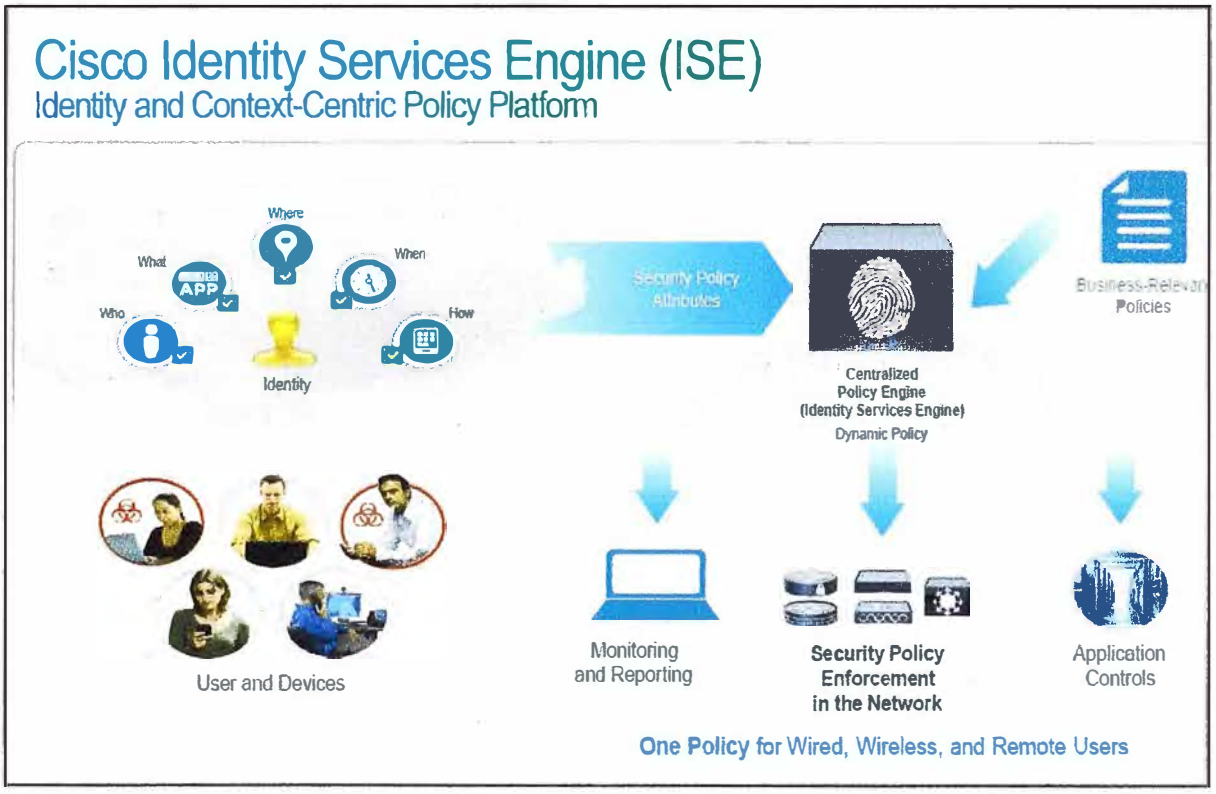

Figura 2.11 Cisco Identity Service Engine (Fuente: Cisco Borderless Network PPT)

Cisco ISE es un sistema de control de acceso basado en políticas que desarrolla las siguientes funcionalidades:

- Combina en un solo equipo el autenticación, autorización y contabilización (AAA), postura (posture), y roles (profiling).
- Proporciona una completa gestión de los invitados que ayuda en gran medida a los administradores de red.
- Aplica y provee medidas de provisión de clientes y postura de dispositivos para todos los dispositivos que acceden a la red, incluyendo entornos 802.1X.
- Provee soporte para el descubrimiento, asignación de roles, asignación de políticas basados en roles, y monitoreo de dispositivos finales.
- Provee políticas consistentes en despliegues centralizados y distribuidos que permite el envío de servicios donde son necesarios.

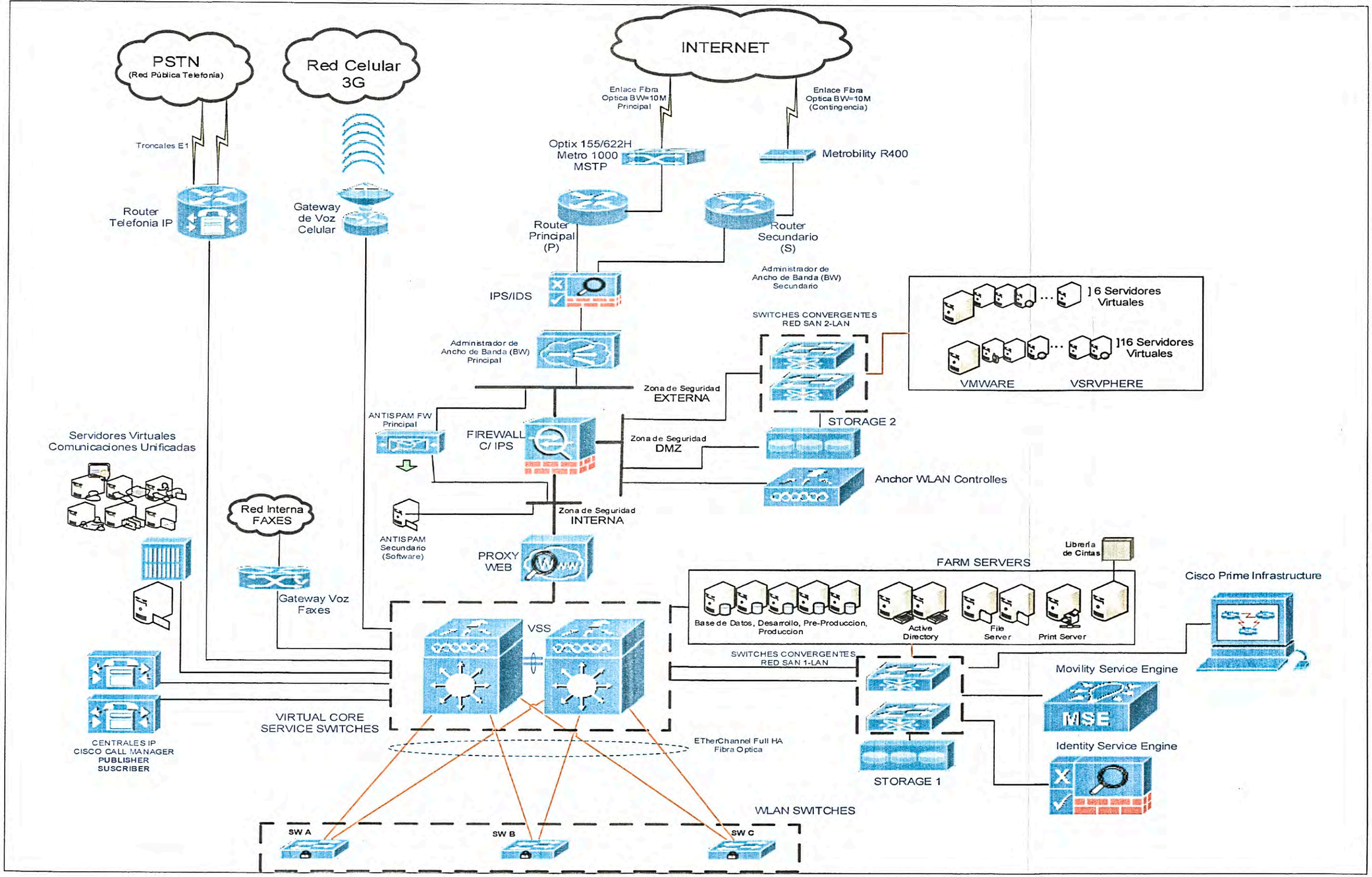

Figura 3.4 a Diagrama Lógico de La Red Completa (Fuente: Elaboración Propia)

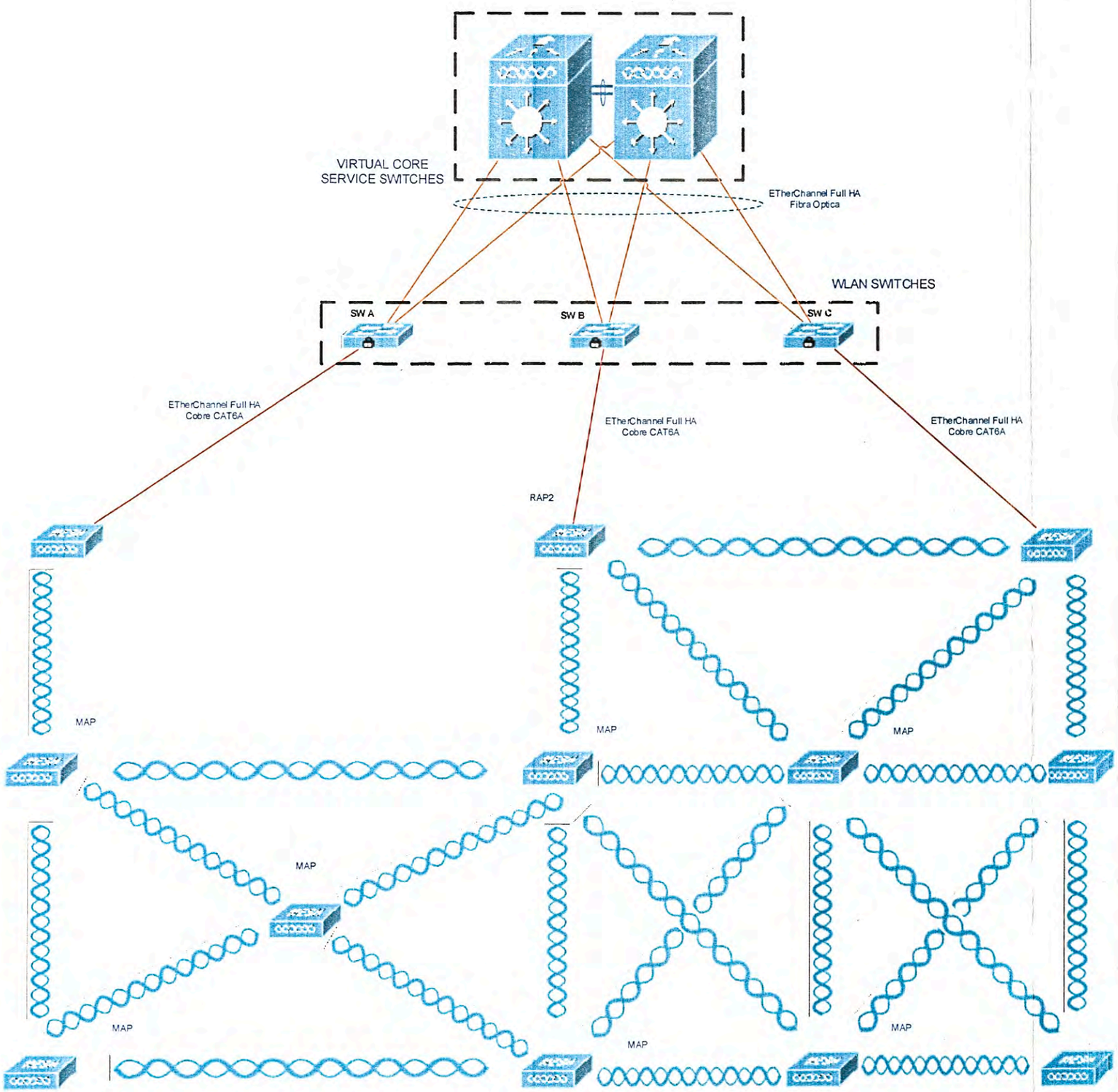

Figura 3.4 b Diagrama Lógico de La Red Completa (Fuente: Elaboración Propia)

- Provee de capacidades avanzadas como la seguridad de acceso de grupos (SGA) a través del uso de etiquetas de seguridad de grupo (SGTs) y lista de accesos basados en seguridad de grupos (SGACLs).
- Soporta la escalabilidad que permite un gran despliegue de escenarios desde pequeñas oficinas hasta grandes empresa.

CAPÍTULO III
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

Este capítulo se enfoca a exponer las consideraciones que se tomaron para el diseño la red mesh Cisco, los equipos que involucran y como estos interaccionan y trabajan para proveer un red robusta, escalable y confiable. Se desarrolla lo siguiente: La zona de aplicación de la solución, el diagrama lógico de la red de la megaplanta, el diseño de la red mesh, las características y consideraciones de los APs mesh para el diseño y las consideraciones para el diseño de los controladores.

3.1 Zona de aplicación de la solución

En esta sección se describe a la megaplanta y las zonas que deben ser iluminadas.

En la Figura 3.1 se observa en detalle las dimensiones del estante (rack) de 5 niveles que se encuentra distribuido en todo el almacén. Cada Pallet incluida su carga tiene una altura de 1.8 metros y una profundidad de 1.4 metros. La altura total entonces es de 9.760 metros y el espesor del estante (considerando ambos lados) de 2.95 metros

En la Figura 3.2 se resaltan los recorridos de los LGVs, las dimensiones de los del almacén que es 205x63 metros. Las líneas blancas continuas y punteadas son las trayectorias que recorrerán los LGVs.

En la Figura 3.3 se muestra el perfil derecho del almacén de la megaplanta que cuenta con 11 metros en su parte más baja y 14 metros en su parte más alta.

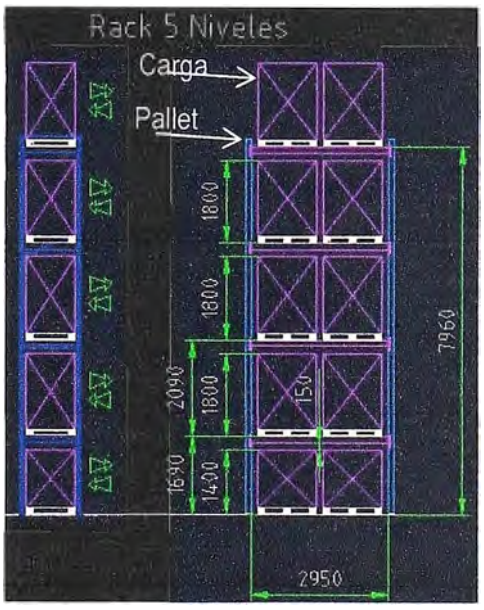

Figura 3.1 Perfil de Estructura de Estantes (Fuente: Elettric80)

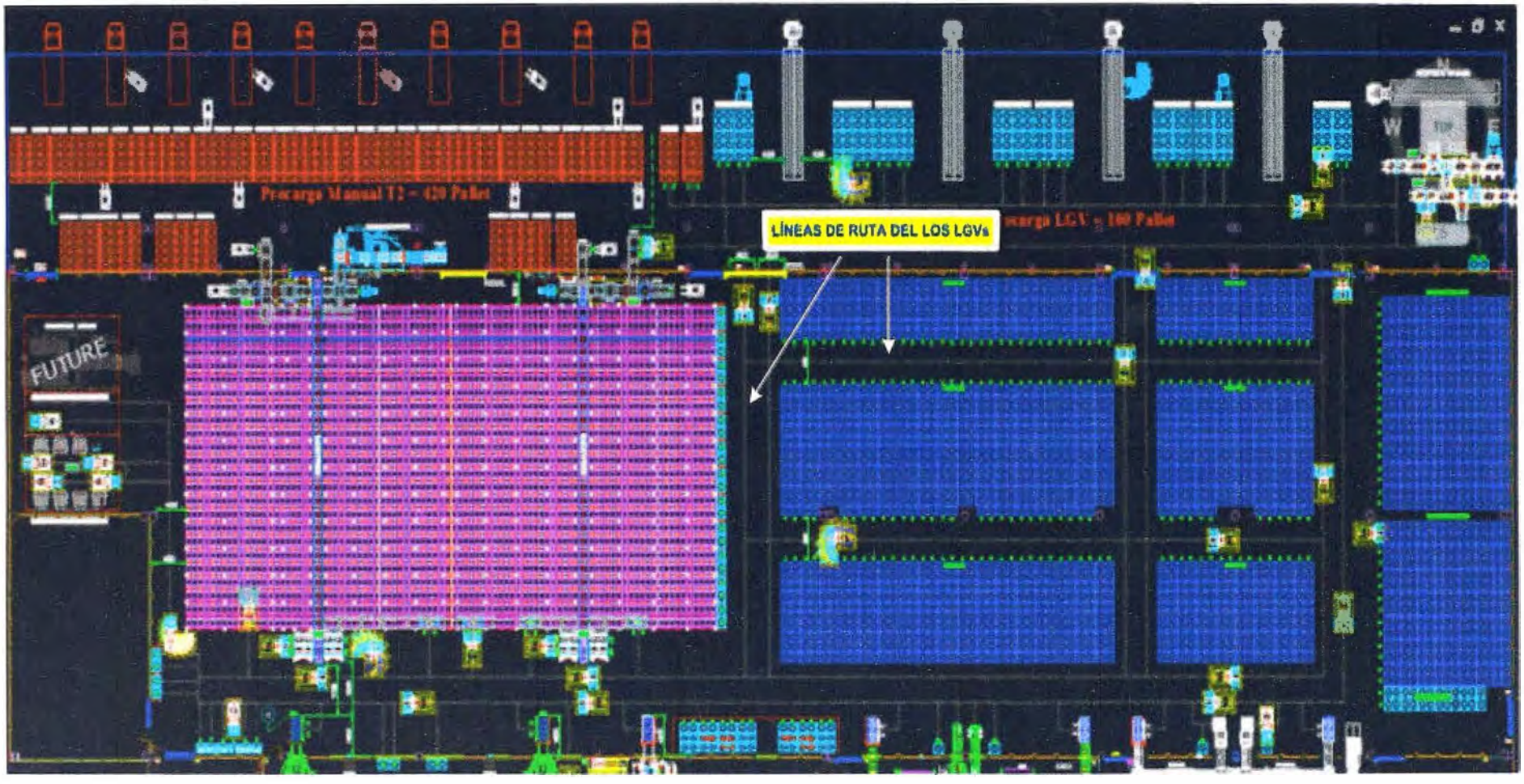

Figura 3.2 Línea de Ruta de los LGVs (Fuente: Elettric80)

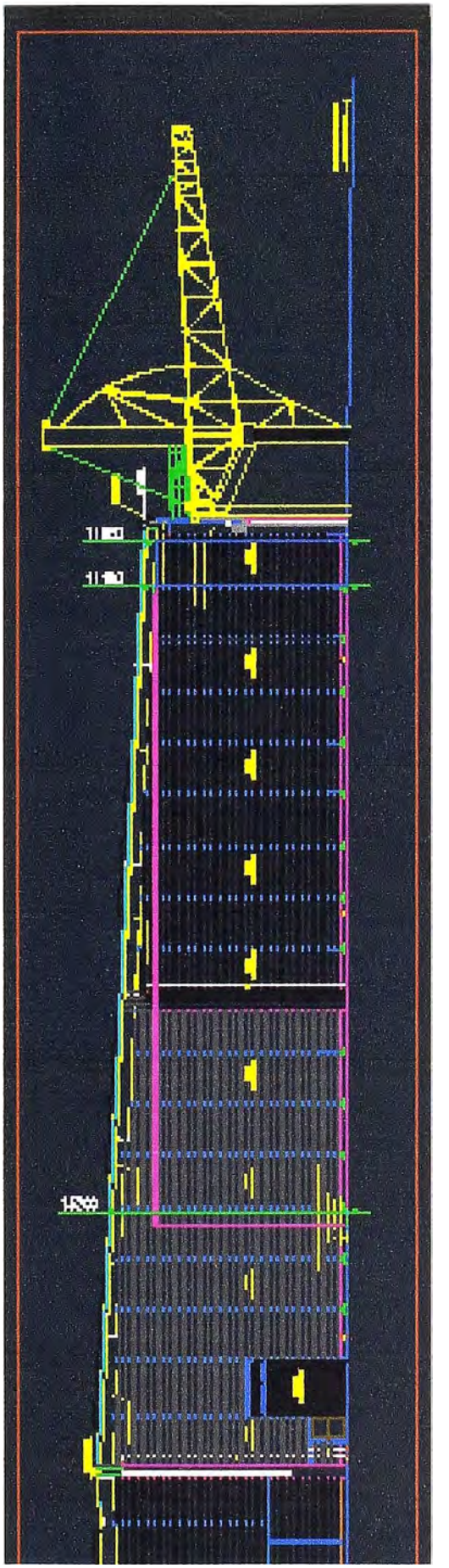

Figura 3.3 Vista de Perfil del Almacén (Fuente: Elettric80)

3.2 Diagrama lógico de la red de la megaplanta

En la Figura 3.4 a y Figura 3.4 b se muestra el diagrama lógico de la red de la megaplanta donde se está incorporando los siguientes componentes que involucran el proyecto:

a. Cisco Prime Infrastructure.

El aplicativo permitirá el diseño, despliegue, operación, reporte y administración de toda la red Cisco. Todos los dispositivos se registrarán a este aplicativo mediante licencias que serán adquiridas en este proyecto. Este aplicativo estará virtualizado en un servidor Cisco UCS. Este servidor virtual estará configurado para un despliegue mediano. Este servidor estará ubicado en el data center de la megaplanta y se conectarán a switches de datacenter convergentes que la megaplanta cuenta.

b. Cisco Identity Service Engine.

El aplicativo permitirá una verificación rigurosa de la identidad de los clientes. Para tal fin se definirán las políticas de acceso en conjunto con los objetivos de seguridad que el cliente. Este aplicativo estará virtualizado en un servidor Cisco UCS. Este servidor virtual estará configurado para un despliegue mediano. Este servidor estará ubicado en el data center de la megaplanta y se conectarán a switches de data center convergentes que la megaplanta cuenta.

c. Cisco Mobility Service Engine.

Este aplicativo estará virtualizado en un servidor Cisco UCS. Este servidor virtual estará configurado para un despliegue mediano. Este servidor estará ubicado en el data center de la megaplanta y se conectarán a switches de data center convergentes que la megaplanta cuenta

d. Dos switches de core tipo chasis de la serie 4500.

Propiedad del cliente, ambos en modo virtual con supervisora 8E el cual viene con capacidad de controlador con soporte de hasta 50 APs y 2000 clientes wireless cada uno. Se aprovechará la capacidad de controlador de estos switches por lo que sólo se activarán licencias por cada AP considerado para cada switch de core. Estos controladores estarán en modo Mobility Controller que centralizará el Radio Resource Management (RRM). Adicionalmente este permitirá un rápido roaming de clientes.

e. Tres switches Cisco de la serie 3800.

Con controlador incorporado y con capacidad de soportar 50 APs y 2000 clientes wireless cada uno, estos controladores estarán en modo mobility agent y pertenecerán a un mismo switch peer group (SPG) que es un grupo lógico de mobility agents dirigidos por el mobility controller, este limita el tráfico de roaming de los clientes dentro de este grupo, dentro de este grupo los switches formarán entre ellos una red mesh de túneles

CAPWAP, los roamings dentro del SPG no necesitan la intervención del movility controller en el switch de core, sin embargo si el cliente tuviera que salir a otros SPGs, en este caso sí necesitaría la intervención del mobility controller

f. Diez APs de la serie 3600.

Para usarlos en modo mesh indoor. Estos APs se desplegarán en iluminando todos los pasadizos del almacén interno de la megaplanta. Estos APs formarán una red mesh de alta disponibilidad de forma que si un AP dejara de funcionar, otro tomará su cobertura de forma transparente sin perjudicar el correcto funcionamiento y transmisión de data desde los clientes wireless.

g. Dos APs de la serie 1500 para usarlos en modo outdoor.

Estos APs se ubicarán en la zona externa por donde transitarán los LGVs para cargar la cajas de gaseosas en los camiones distribuidores. Además al igual que los APs indoor considerados, serán parte de la red mesh que se diseña e iluminará de forma redundante la zona externa del área de trabajo de los LGVs así como de los operarios.

h. Un controlador de la serie 5500.

Será el controlador anchor o ancla y estará ubicado en la DMZ para los clientes guest. Este controlador pertenecerá a un grupo de movilidad diferente al de los controladores embebidos en los switches 3850 y 4500.

Cada vez que un cliente quiera salir a la red insegura, este establecerá relación con el controlador ancla ubicado en la DMZ y será por ahí que cualquier cliente guest saldrá a la red de forma segura, esta arquitectura será importante ya que mejora los niveles de seguridad exigidos en la red interna así como evitará tener espacios exclusivos para los invitados, ya que la red se extenderá por todas las áreas que abarque. La arquitectura propuesta y la existente.

i. Cableado estructurado.

- En FO monomodo 10G de los switches de core hacia los switches de acceso vía Interchassis Etherchannel (ICE) que permitirá tener los dos enlaces hacia cada chasis activos, mejorando así el ancho de banda del enlace a la vez que se mantiene la redundancia.
- Categoría 6A de los switches de acceso a los Root APs que trasladarán el todo el tráfico de la red mesh hacia la red cableada.

j. Todo el accesorio de rackeo y montaje.

Además tres gabinetes de pared para los switches de acceso que se colocarán en forma estratégica por cada switch de acceso. Complementariamente los trabajos de instalación y configuración, que involucra la instalación de los APs en los techos del almacén interno así como en los techos de la parte externa.

3.3 Diseño de la red mesh

En esta sección brindan los detalles relacionados al diseño de la red mesh: Consideraciones y roles de los APs en una red mesh, Cisco Prime Infrastructure, el descubrimiento en una red mesh vía CAPWAP, Adaptive Wireless Path Protocol, flujo de tráfico, vecinos, padres e hijos mesh.

3.3.1 Consideraciones y roles de los APs en una red mesh

Los APs en una red mesh operan en uno de los siguientes dos modos:

- Root Access Point (RAP).
- Mesh Access Point (MAP).

Todos los APs Cisco vienen pre configurado como mesh APs, para usarlos en modo root habrá que configurarlos. Mientras los RAPs tienen conexión cableada hacia los controladores, los MAPs tienen conexión wireless hacia los controladores. Los MAPs se comunican entre ellos y con el RAP usando conexiones wireless a través de 802.11n a/n radio. Los MAPs usan el protocolo Cisco Adaptive Wireless Path Control (AWPP) para determinar el mejor camino a través de los MAPs hacia los controladores. Este protocolo Cisco permite que cada MAP identifique a sus vecinos e inteligentemente escoja el mejor camino hacia la red cableada calculando el costo de cada camino en términos de la calidad de señal y número de saltos requeridos para llegar al controlador.

En la Figura 3.5 se muestra la relación entre RAPs y MAPs

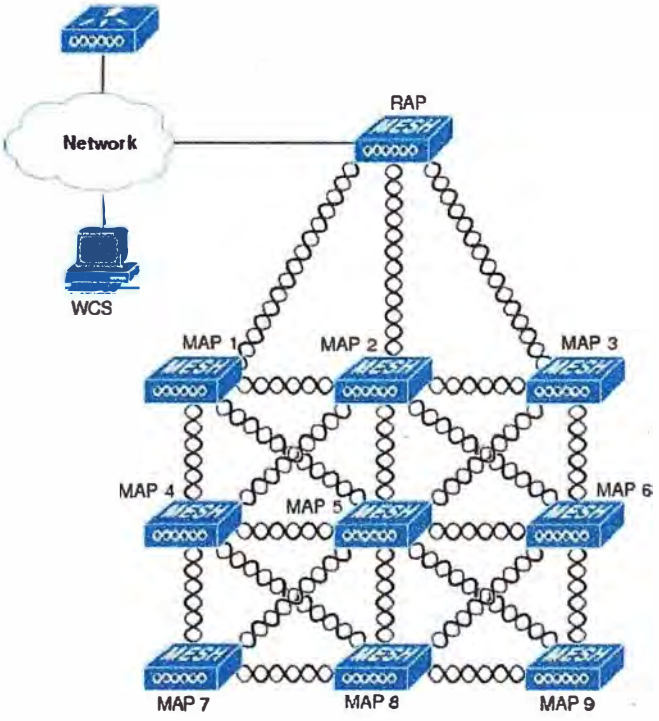

Figura 3.5 Jerarquía en Una Red Mesh Simple (Fuente: Referencia [6])

La red wireless mesh transmite dos tipos de tráfico:

- Tráfico de los clientes wireless LAN

- Tráfico de los puertos Ethernet MAP

El tráfico de los clientes wireless termina en los controladores, mientras el tráfico de los puertos termina en los puertos Ethernet de los MAPs

La autenticación de la red mesh para los MAPs se hacen a través del Cisco Identity Service Engine.

3.3.2 Cisco Prime Infrastructure

El Cisco Prime Infrastructure es la plataforma gráfica que permitió planear, configurar y gestionar la red mesh. En el caso de estudio ayudó a diseñar, controlar y monitorear de la red wireless mesh de forma centralizada.

Con el Cisco Prime se logró en el laboratorio diseñar la red, sin embargo una vez implementada, esta herramienta permitió obtener predicciones de RF, políticas de provisión, optimización de la red, solución de problemas, seguimiento de usuarios, monitoreo de la seguridad y gestión de la red wireless LAN. Interfaces gráficas hacen del despliegue de la red WLAN y las operaciones simples y rentables. Tendencias detalladas y análisis de reportes hacen de esta herramienta algo vital para las operaciones relativas a la red wireless.

El Cisco Prime corre en una plataforma de servidor con base de datos embebido, que provee escalabilidad tanto para los controladores como para los APs. Esta plataforma se usó para el diseño de la cobertura de la red mesh tal como se muestra en las Figuras 3.6 al 3.12. (La Figura 3.7 muestra el entorno Cisco Prime donde se hacen las simulaciones).

Una vez ya realizada todas las simulaciones y hecho el site survey respectivo para verificar los resultados obtenidos en el Cisco Prime Infrastructure se procede a ubicar los APs en sus posiciones tal como lo indica la Figura 3.13.

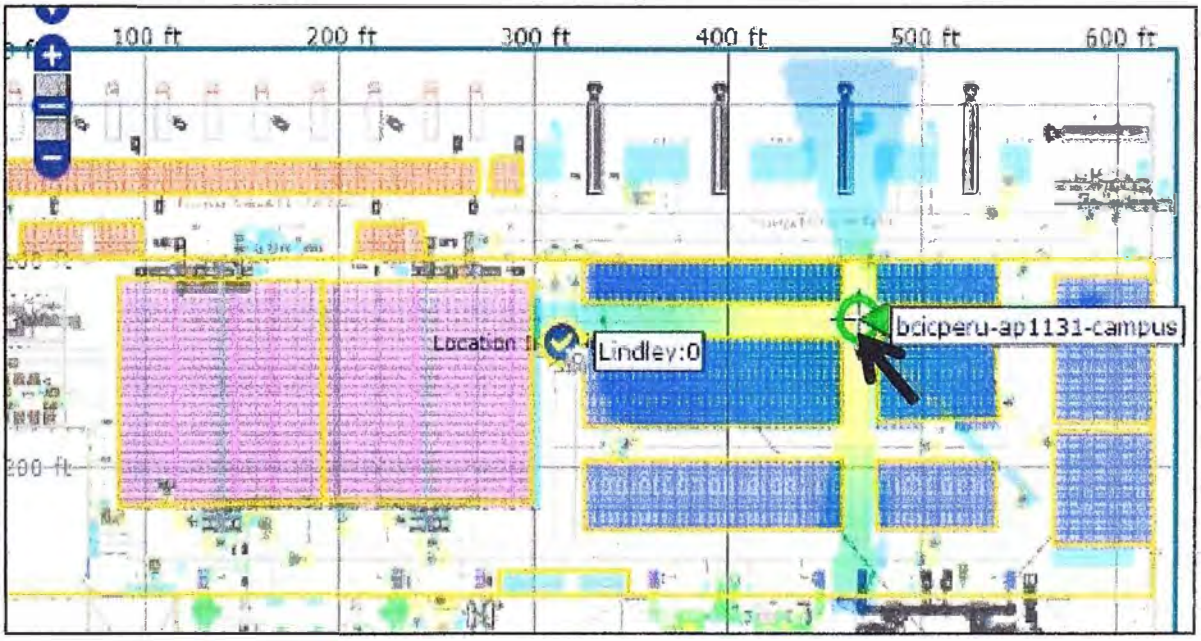

Figura 3.6 Posición y Cobertura del MAP 5 (Fuente: Elaboración Propia)

Figura 3.7 Posición y Cobertura del MAP 7 (Fuente: Elaboración Propia)

Figura 3.8 Posición y Cobertura del MAP 4 (Fuente: Elaboración Propia)

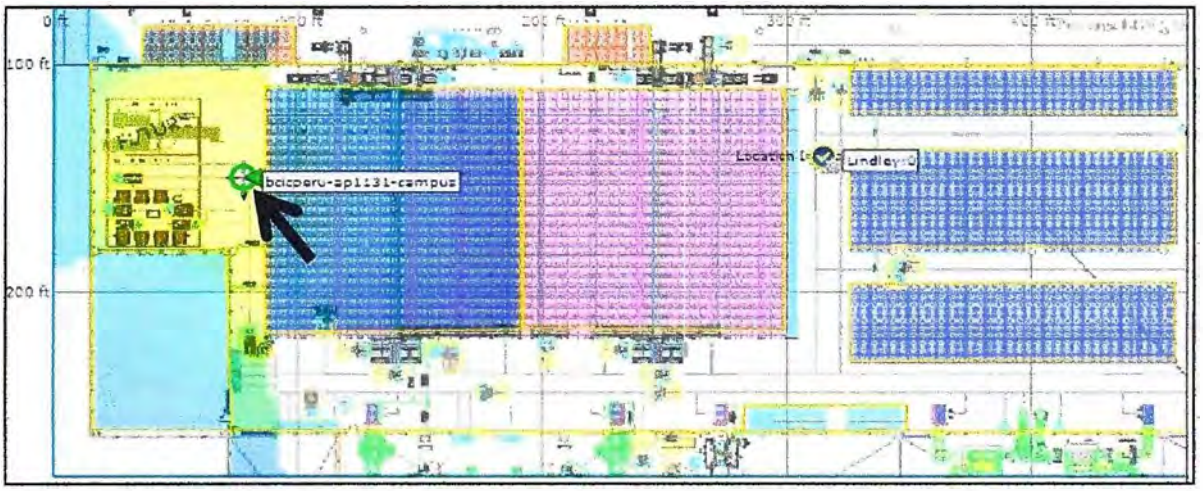

Figura 3.9 Posición y Cobertura del RAP 1 (Fuente: Elaboración Propia)

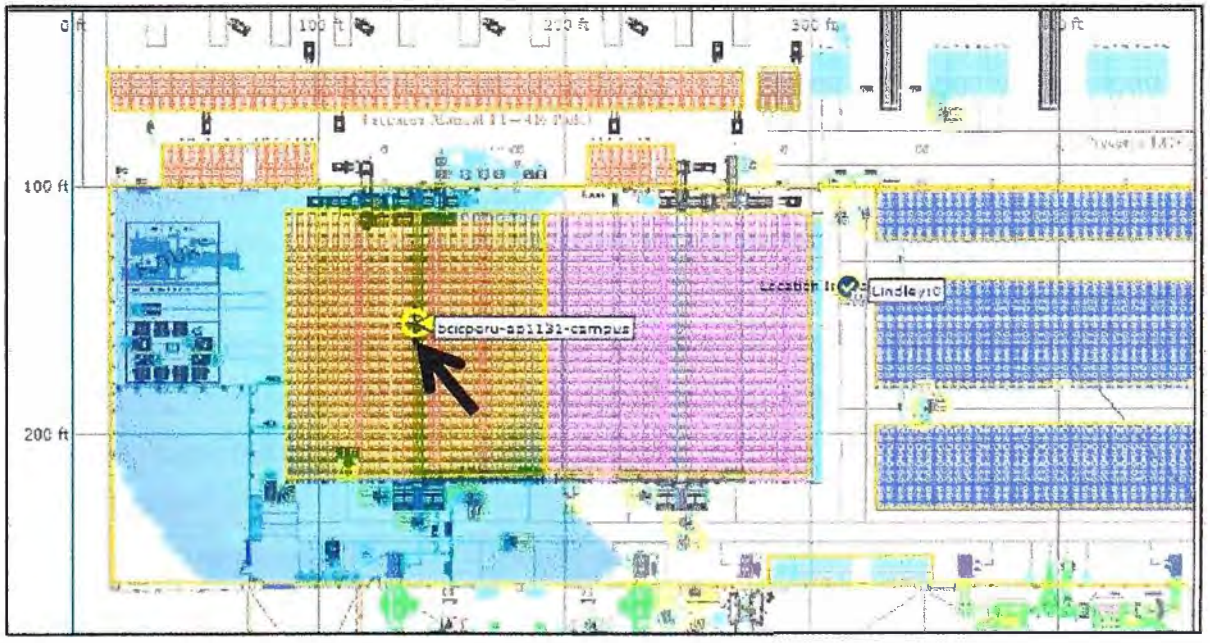

Figura 3.10 Posición y Cobertura del MAP 1 (Fuente: Elaboración Propia)

Figura 3.11 Posición y Cobertura del MAP 2 (Fuente: Elaboración Propia)

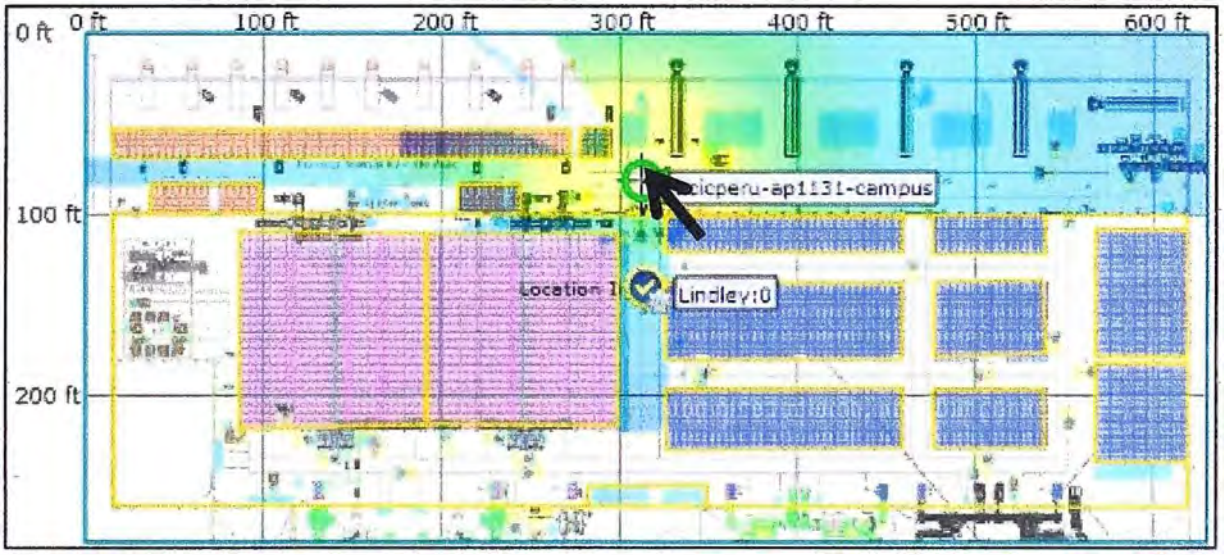

Figura 3.12 Posición y Cobertura del MAP 9 (Fuente: Elaboración Propia)

La simulación consiste en cargar el mapa en CAD para así tener la visibilidad del ambiente de trabajo real. Luego se insertan los niveles de atenuación que se pueden calcular del site survey preliminar y se va posicionando el AP en los puntos convenientes para así cubrir todo el ambiente de trabajo. Finalmente, una vez esté desplegado, con esta herramienta en producción, se obtienen los valores reales de atenuaciones y fuentes de interferencia del ambiente de trabajo, ya que tanto el AP como el controlador cuentan con tecnologías para la detección y mitigación de los mismos, tecnologías para el uso eficiente y conveniente de los canales en 2.4 GHz y 5 GHz así como decisión en el tipo de modulación y por lo tanto la velocidad de las conexiones de los clientes según conveniencia del escenario en un momento dado.

Una vez ya realizada todas las simulaciones y hecho el site survey respectivo se procede a ubicar los APs en sus posiciones tal como lo indica la Figura 3.13.

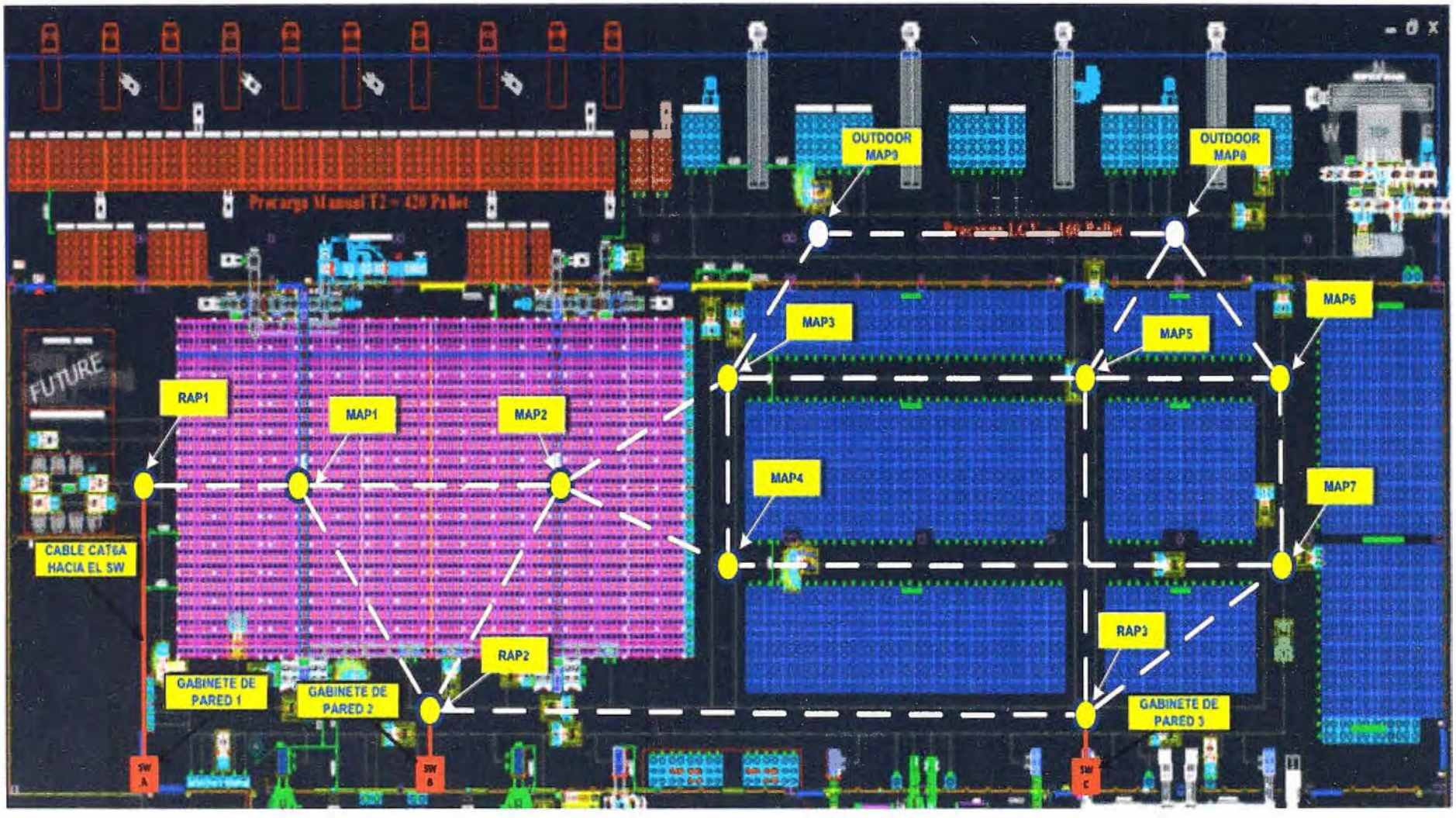

Figura 3.13 Despliegue de los APs de la Red Mesh (Fuente: Elaboración Propia)

3.3.3 Descubrimiento en una red mesh vía protocolo CAPWAP

CAPWAP (Control and Provision Wireless Access Points) es el protocolo usado por el controlador para gestionar los APs ya sean mesh o no mesh en la red.

El proceso de descubrimiento CAPWAP en la red mesh es como se detalla a continuación:

1. El AP mesh establece un link antes de empezar el descubrimiento CAPWAP.
2. El AP mesh inicia el descubrimiento CAPWAP usando una IP estática para el AP mesh en una red capa 3 o busca en la red su controlador primario, secundario o terciario si lo hubiera. Un máximo de 10 intentos son realizados para conectarse.

Nota: El AP la lista de controladores configurados en el AP al momento de la configuración inicial.

3. Si el paso 2 falla, después de 10 intentos, el AP mesh cambia a modo DHCP y realiza 10 intentos para obtener información del controlador.
4. Si tanto el paso 2 como el paso 3 fallan y no hay una conexión CAPWAP exitosa, luego el AP mesh se cambia al protocolo LWAPP.
5. Si no se logra el descubrimiento después de intentar los pasos 2,3, y 4, el AP mesh intenta el siguiente link.

3.3.4 Protocolo AWPP (Adaptive Wireless Path Protocol)

Adaptive Wireless Path Protocol (AWPP), está diseñado específicamente para una red mesh y provee de forma sencilla el despliegue, convergencia veloz y un mínimo consumo de recursos.

AWPP permite a un AP remoto a dinámicamente encontrar el mejor camino hacia en RAP por cada MAP que es parte del grupo, RAP Bridge Group Name (BGN). En comparación con otros protocolos, AWPP toma en cuenta los detalles de la RF, el costo de cada camino es determinado por el número de saltos y la fuerza de la señal. Después de que una ruta es escogida, AWPP constantemente monitorea las condiciones y cambia las rutas de ser necesario.

3.3.5 Flujo de tráfico

El flujo de tráfico dentro de un wireless mesh puede dividirse en tres componentes:

1. Tráfico CAPWAP que fluye dentro de un despliegue estándar de APs CAPWAP; esto es, tráfico CAPWAP entre un AP CAPWAP y un controlador CAPWAP.
2. Flujo de trama de datos wireless mesh.
3. Intercambios AWPP.

3.3.6 Vecinos, padres e hijos mesh

La relación entre APs mesh son padre, hijo, o vecino. Un AP padre ofrece la mejor ruta hacia el RAP basado en ciertos valores. Un padre puede ser un RAP o MAP.

Estos valores son calculados usando SNR salto de enlace en cada vecino. Teniendo varias opciones el AP con el máximo valor es seleccionado. Un AP hijo escoge su AP padre como su mejor ruta hacia el RAP. Un AP vecino está en el rango RF de otros APs pero no son seleccionados como APs padres debido a que sus valores calculados son menores que el AP padre.

3.4 Características y consideraciones de los AP mesh para el diseño

Se detalla lo relacionado a los equipos: AP 3.4.1 Cisco Indoor Mesh AP Serie 3600 y el Cisco Outdoor Access Point 1552 Series.

3.4.1 Cisco indoor mesh AP serie 3600

En la Figura 3.14 se muestra el AP de la serie 3600

Figura 3.14 AP Indoor Mesh Serie 3600 (Fuente: [9])

Estos APs serán utilizados para iluminar el área interna del almacén vía una red mesh, entre las características resaltantes que cuenta esta serie de APs tenemos:

- Este AP está preparado para soportar altas tazas te transmisión.
- 802.11n con 4X4 MIMO y tres spatial-stream que es capaz de sostener 450 Mbps a través de una gran cobertura.
- Tecnología Cisco ClientLink 3.0 que mejora el desempeño de subida y bajada de todos los clientes móviles que se conecten a la red incluyendo dispositivos de uno, dos, y tres spatial-streams en 802.11n. Esta funcionalidad es importante para la red ya que habrá una gran variedad de clientes que se conectarán a la red, estos pueden ser IEEE 802.11a, 802.11g, 802.11n, y el nuevo estándar, 802.11ac. Sin embargo, estándares poco usados como los 802.a/g siempre obstruyen la habilidad de la red de tomar ventaja de las ganancias en desempeño de los estándares recientes como 802.11ac.La tecnología Cisco ClientLink 3.0 se enfoca en redes donde residen este mix de clientes asegurando de que trabajen a las mejores tazas posibles, especialmente cuando estos se encuentran en las fronteras de una celda.
- Tecnología Cisco CleanAir que provee un espectro de alta velocidad inteligente para combatir problemas de desempeño producto de interferencia wireless.

La posición de los APs indoor mesh se muestran en la Figura 3.15.

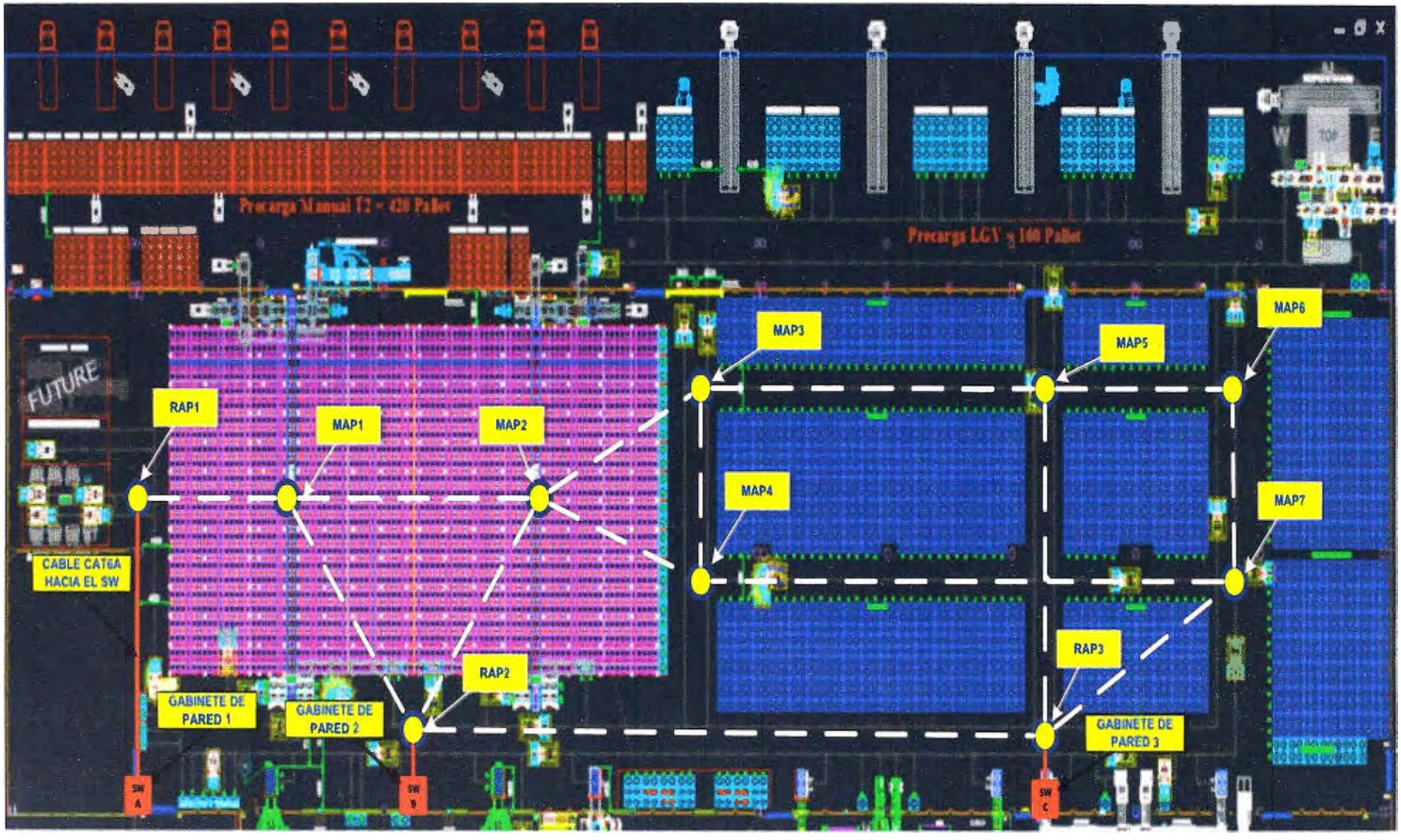

Figura 3.15 Posicionamiento de los APs Indoor Mesh (Fuente: Elaboración Propia)

Entre las características más resaltantes se tienen:

- AP controlado de doble banda que soporta 802.11a/g/n/ac
- Soporta el 802.11ac al incluir un módulo adicional con las siguientes características (futuros escenarios):
  - o Soporta 3X3:3SS (spatial streams), 80MHz de canales amplios, 256 QAM, transmisión de data de hasta 1.3Gbps (IEEE 802.11ac Wave 1).
  - o Certificación Wifi
  - o Cisco 3G Small Cell Module
  - o 3GPP Banda 1 (2100 MHz), 16 usuarios, voz (R99), paquete de datos (HSPA/HSDPA+)
  - o Capacidades 802.11n:
  - o 4x4 multiple-input multiple-output (MIMO) con tres spatial streams
  - o Máxima Relación de Combinación (MRC).
  - o 802.11n y 802.11a/g beamforming
  - o Canales 20- y 40-MHz
  - o PHY data rates hasta 450 Mbps (40-MHz con 5 Ghz)
  - o Agregación de Paquetes: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
  - o 802.11 selección dinámica de frecuencia (DFS)
  - o Soporte de cambio cíclico de diversidad (CSD)
  - o Velocidades soportadas:
  - o 802.11a: 6, 9, 12, 18, 24, 36, 48, y 54 Mbps
  - o 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, y 54 Mbps
  - o 802.11n velocidades soportadas (2.4 GHz y 5 GHz)

En la Figura 3.16 se muestra el gráfico de los canales mencionados para la banda de 2.4 GHz así como los canales sin traslape:

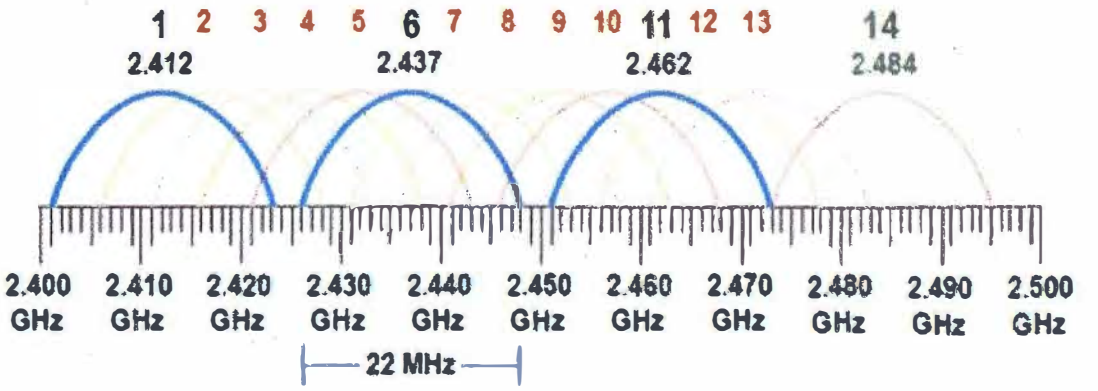

Figura 3.16 Canales para 2.4GHz (22 MHz) (Fuente [11])

En la Figura 3.17 se muestra el gráfico de los canales en 2.4 GHz para el acceso de clientes recomendados de acuerdo al site survey realizado:

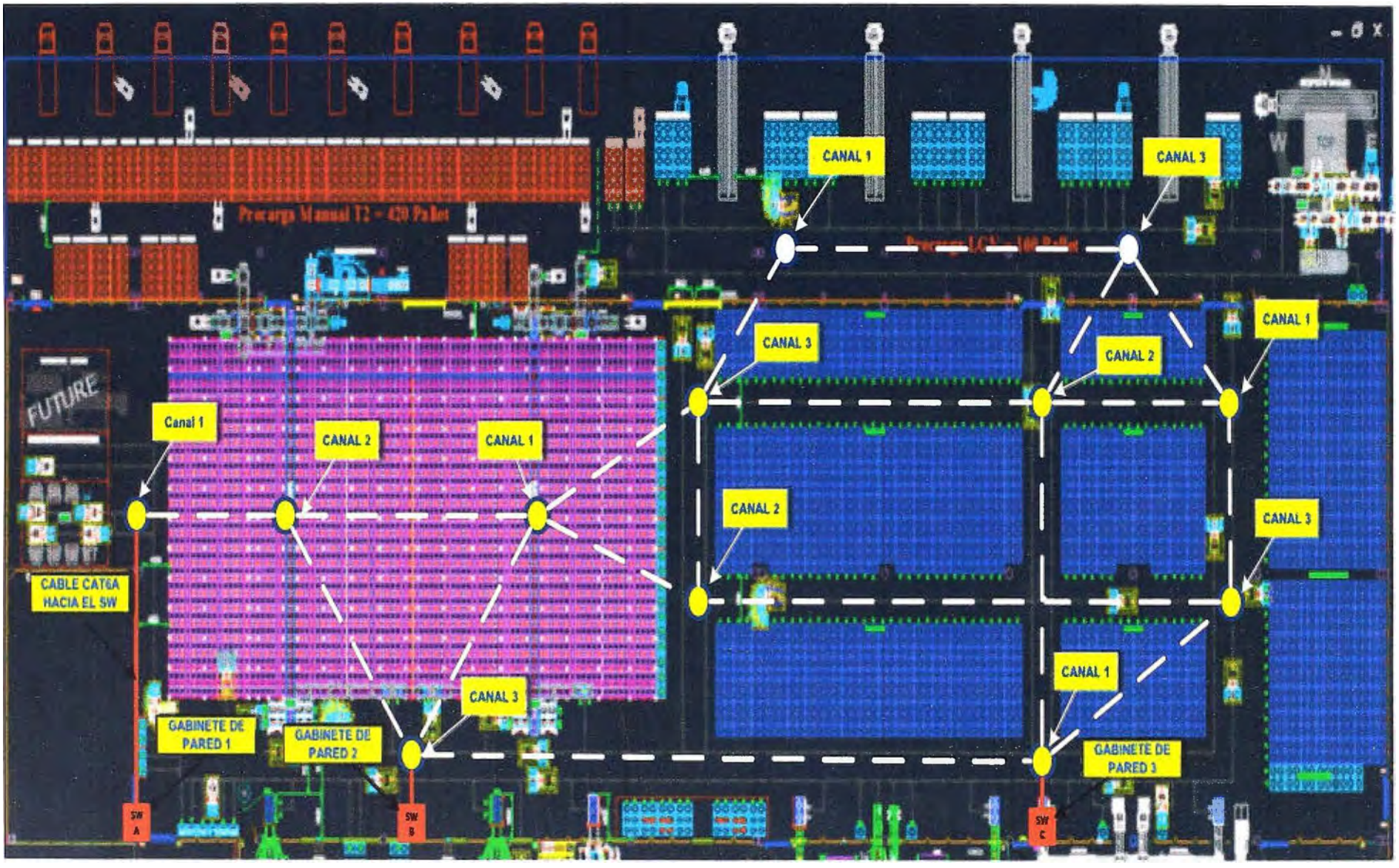

Figura 3.17 Despliegue de Canales Recomendados en 2.4 GHz (Fuente: Elaboración Propia)

En la Figura 3.18 se muestra el gráfico de los canales mencionados para la banda de 5 GHz. Para este caso no habrá problemas ya que el AP de la serie 3600 cuenta con 21 canales disponibles en 20 MHz y 9 canales disponibles en 40MHz tanto para el acceso de clientes wireless así como el backhaul hacia la red cableada y controladores:

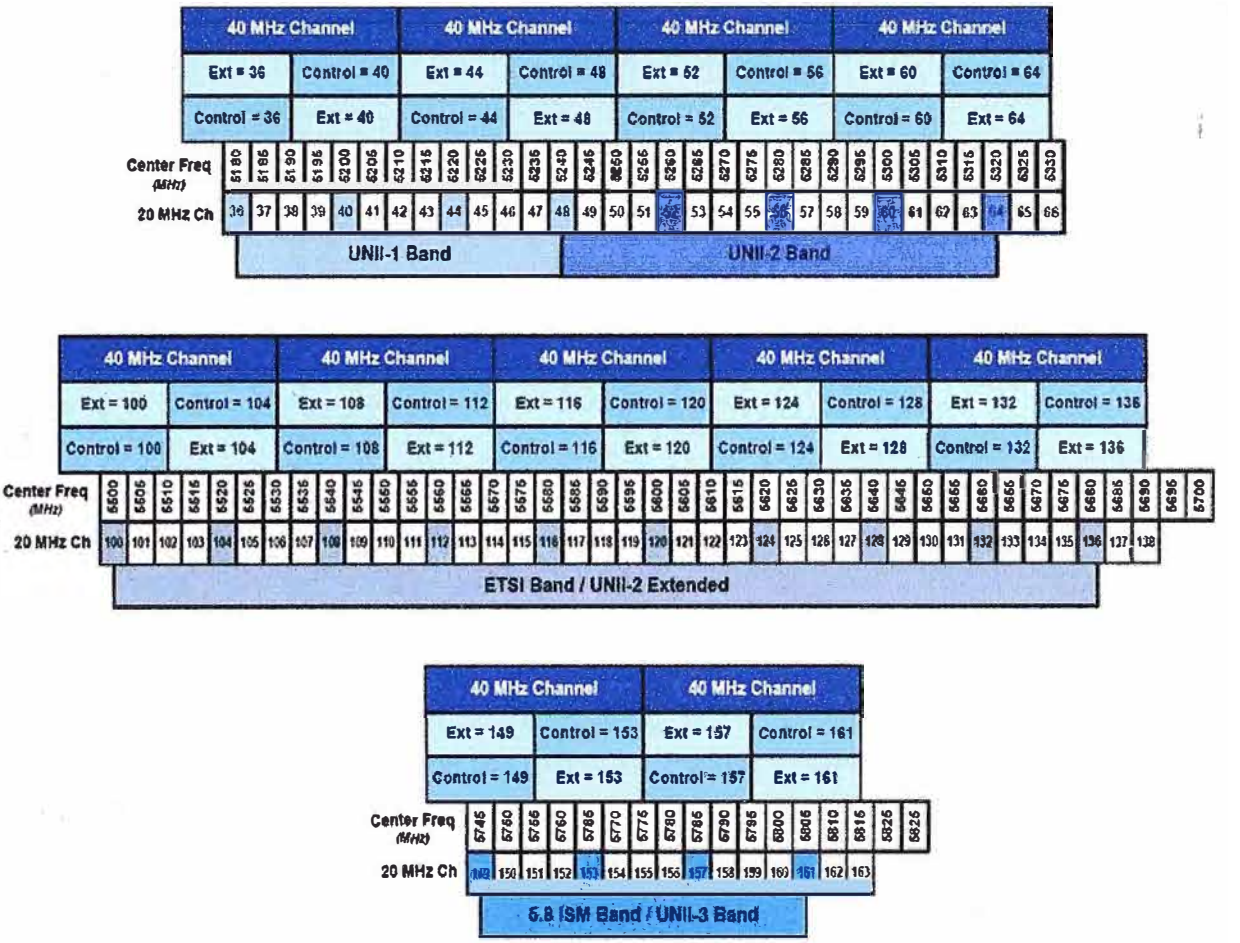

Figura 3.18 Canales Disponibles en 5GHz (20MHz y 40MHz) (Fuente [12])

a. Antenas externas:

Se consideran dos tipos de antenas, antenas omnidireccionales y antenas direccionales de gran ganancia. Se utilizarán 4 antenas externas Aironet dipolo de doble banda compatible con el AP 3600 por cada AP considerado, en la Figura 3.19 se muestra dicha antena:

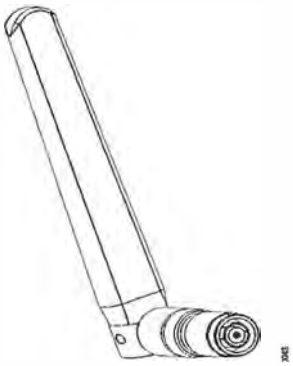

Figura 3.19 Antena Omnidireccional Cisco Aironet Dual-Band (Fuente [13])

Ganancias de la antena:

- 2.4GHz: 2dBi
- 5 GHz: 4dBi

En la Figura 3.20 se muestra el patrón de radiación de la antena:

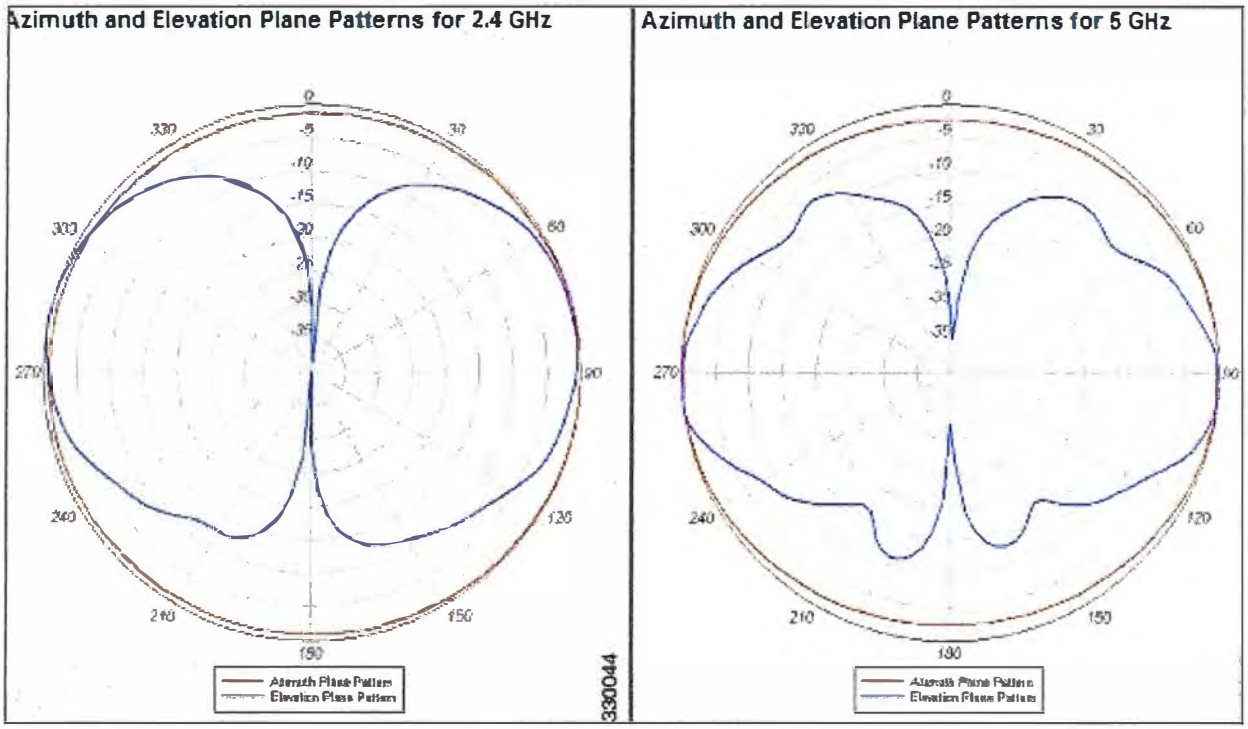

Figura 3.20 Patrón de Radiación en 2.4GHz y 5GHz (Fuente [13])

b. Instalación de los Puntos de Acceso

Los APs indoor estarán dentro de cajas NEMA como se aprecia en la Figura 3.21 y estos estarán instalados por medio de un Mount Kit que se acoplará a varillas que se fijarán a 10 m del piso tal como se muestra en las Figuras 3.22 y 3.23.

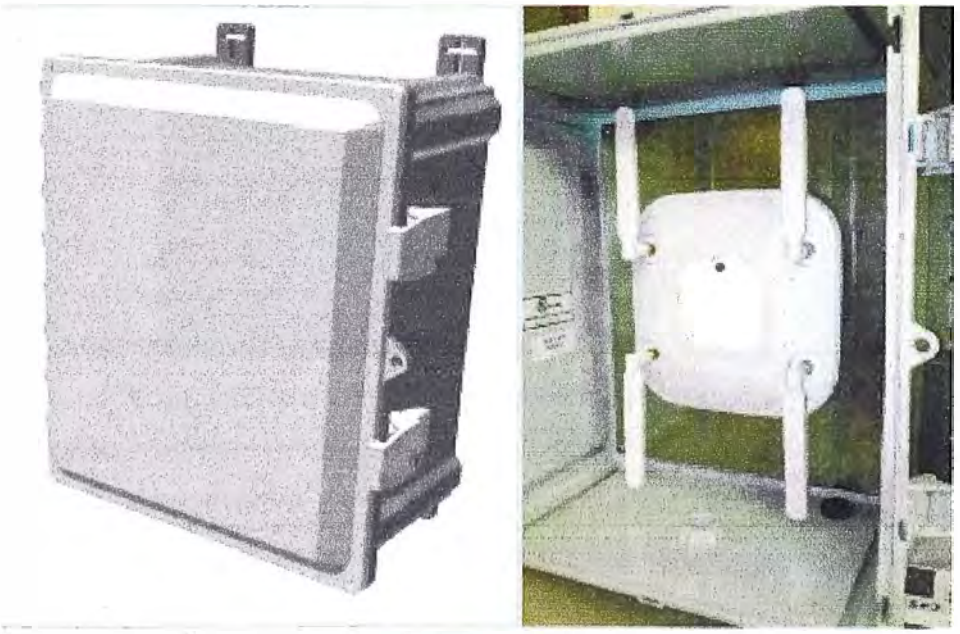

Figura 3.21 Cajas NEMA donde se Instalarán los APs (Fuente [14])

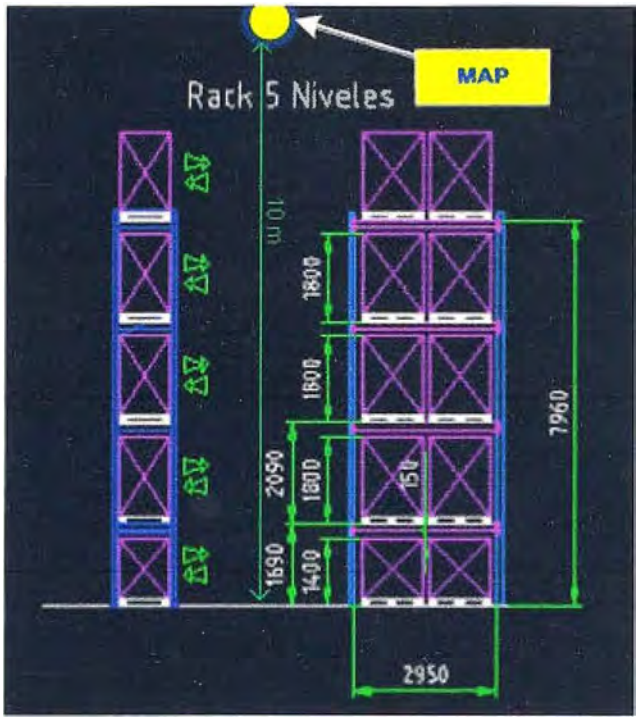

Figura 3.22 Instalación de los APs Indoor (Fuente: Elaboración Propia)

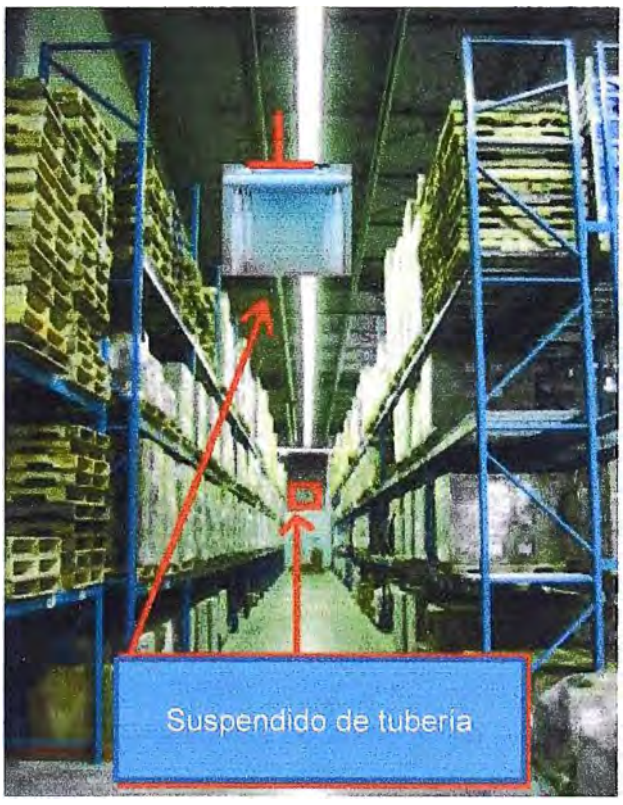

Figura 3.23 Instalación de los APs Indoor (Fuente [14])

3.4.2 Cisco outdoor access point de la serie 1552

En la Figura 3.24 se muestra los APs outdoor de la serie 1500 a utilizar.

El Cisco Aironet 1552 outdoor mesh AP, es un wireless mesh AP diseñado para el uso en una red mesh. Este AP será colocado en las afueras del almacén dando cobertura a los LGVs que trabajarán en esa zona, además de los operarios con sus dispositivos

tablets y teléfonos wireless que podrán acceder a la red de forma segura.

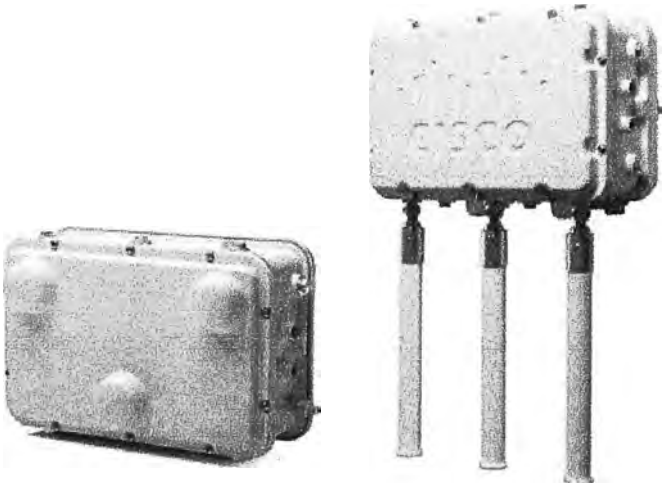

Figura 3.24 APs Outdoor de la Serie 1500 (Fuente [15])

Este AP soporta el esquema punto-multipunto y punto-punto que serán usados según conveniencia. Soporta el protocolo Adaptive Wireless Path Control que será el modo en que la red inteligentemente buscará la mejor ruta hacia los controladores vía los MAPs mesh indoor.

Este AP consiste en el esquema Multiple Input Multiple Output (MIMO) Radio WLAN. Además ofrece 2x3 MIMO con dos spatial-streams, beamforming e inteligencia de espectro integrada (Cisco ClientLink) suficiente para el área y tas tazas de transferencia de misión crítica que se planea en esta área externa.

El CleanAir en este tipo de antenas, proveerá un performance full en 802.11n mientras que a su vez, detectará, localizará clasificará y mitigará interferencias de radiofrecuencia para proveer la mejor experiencia en los clientes así como la confiabilidad e integridad en la transmisión de datos críticos a través de la red.

La tecnología CleanAir permitirá mitigar interferencias wifi o no-wifi en los radios 2.4GHz.

Estos APs son duales y usarán dos radios: 2.4GHz y 5 GHz MIMO radios. Mientras que los radios de 2.4GHz son usados principalmente para el acceso local de clientes wireless, los radios de 5GHz son usados para dos propósitos, el acceso local de clientes así como las redes de retorno o backhaul de la red mesh.

Estos APs además cuentan con una batería de backup.

Velocidades soportadas:

- 802.11a: 6, 9, 12, 18, 24, 36, 48, y 54 Mbps
- 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, y 54 Mbps
- 802.11n velocidades soportadas (2.4 GHz y 5 GHz) según la tabla 3.2:

A continuación se desarrolla lo relacionado a las antenas externas y a la instalación de los APs. En la Figura 3.25 se muestra la ubicación de estos APs Outdoor.

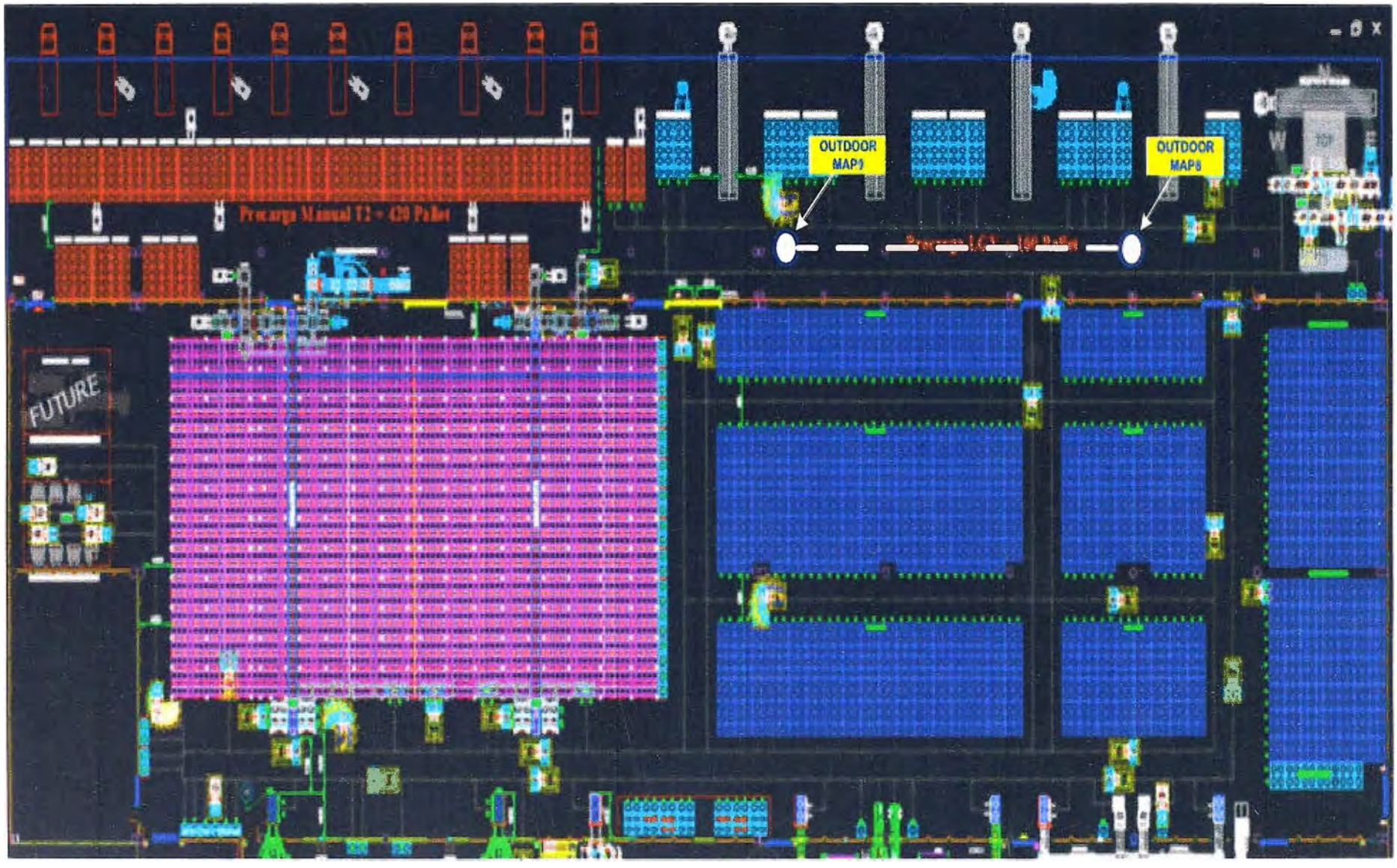

Figura 3.25 Ubicación de los APs Outdoor (Fuente: Elaboración Propia)

a. Antenas externas

Se consideran antenas omnidireccionales

En la Figura 3.26 Se utilizarán 3 antenas Aironet dipolo de doble banda compatible con el AP 1500, dos para transmisión y los tres para recepción:

- 2.4GHz: 4dBi
- 5 GHz: 7dBi

Figura 3.26 Antena Omnidireccional Cisco Aironet Dual-Band (Fuente [16])

En la Figura 3.27 se muestra el patrón de radiación de esta antena:

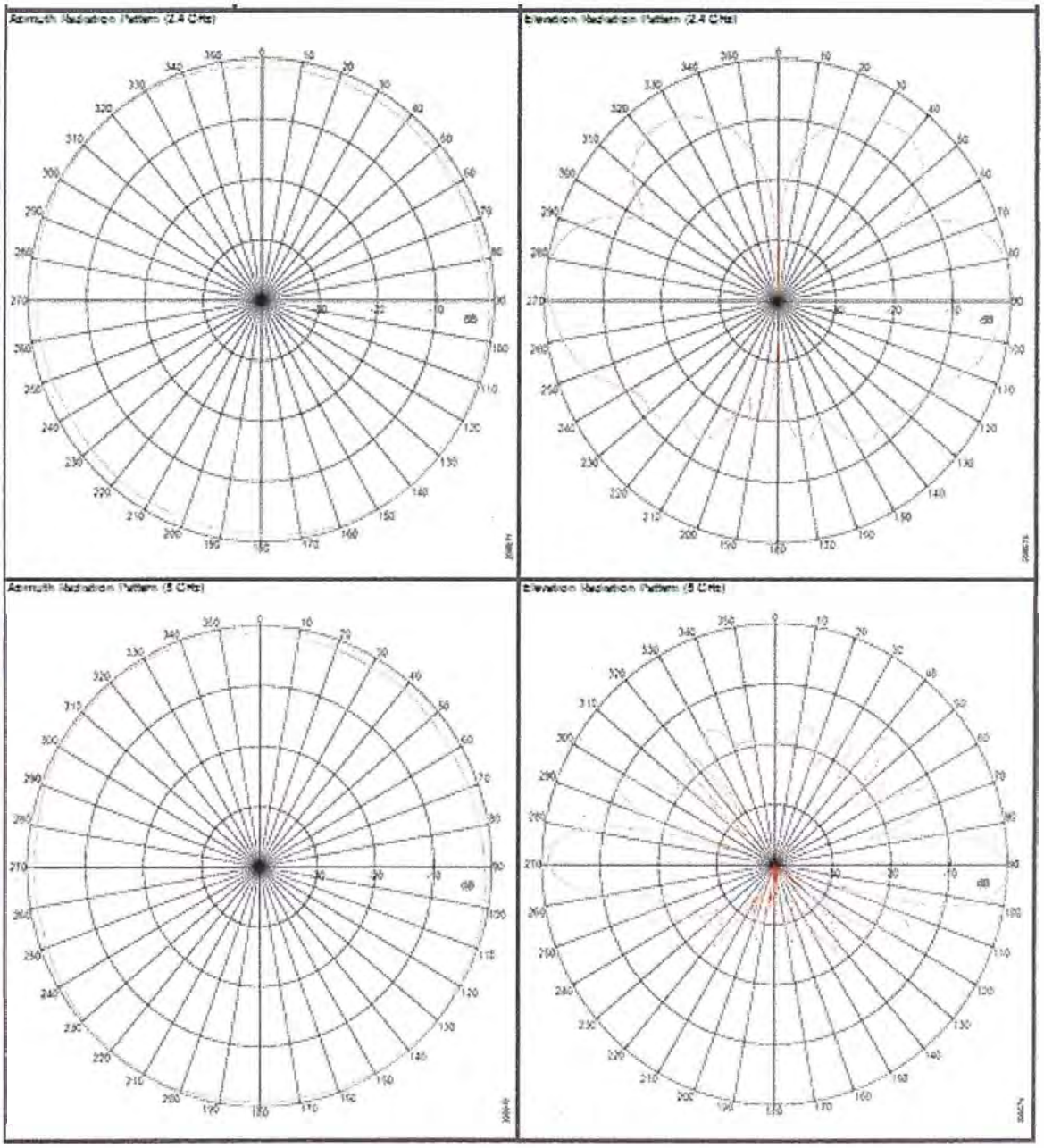

Figura 3.27 Patrón de Radiación en 2.4 GHz y 5 GHz (Fuente [16])

b. Instalación de Puntos de Acceso

La instalación de los APs outdoor se realizarán por medio del Cisco Pole Mount Kit que se acoplará a varillas que se fijarán a 10 m del piso y amarrados a tubos fijados en el techo como se muestra en la Figura 3.28 y 3.29.

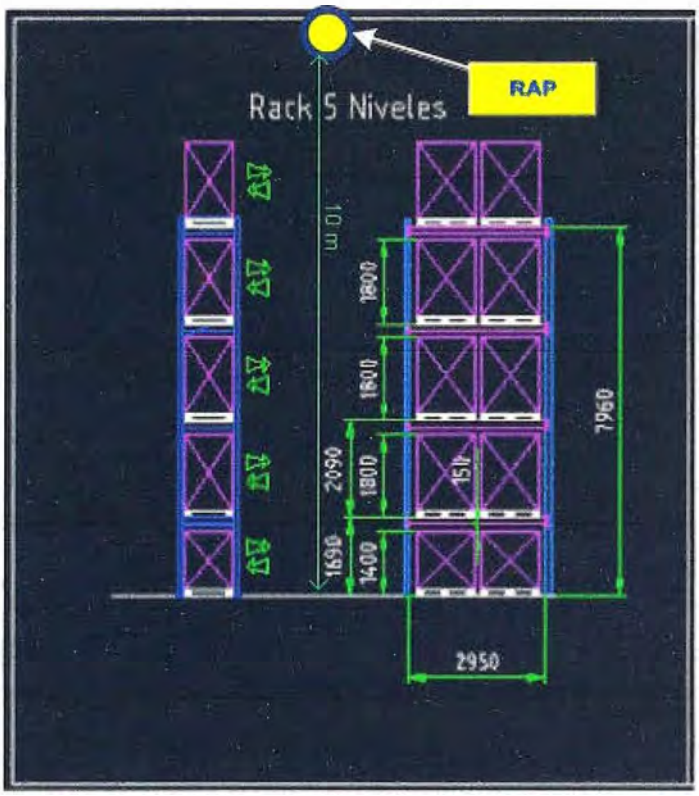

Figura 3.28 Instalación de los APs Outdoor (Fuente: Elaboración Propia)

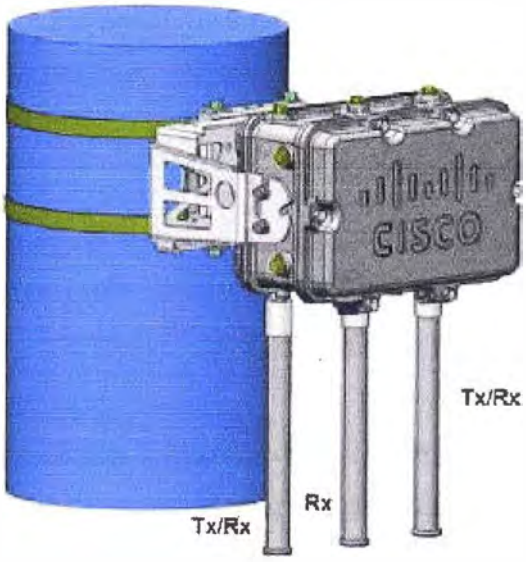

Figura 3.29 APs Outdoor (Fuente [6])

3.5 Consideraciones para el diseño de los controladores

Esta sección está desarrolla lo siguiente: Consideraciones preliminares de diseño, consideraciones de puertos e interfaces en el WLC, consideraciones sobre el grupo de

movilidad, uso de grupos de APs y uso de grupos de RF.

3.5.1 Consideraciones preliminares de diseño

Si el firewall está configurado para enviar tráfico sólo de APs que usan LWAPP, hay que cambiar las reglas del firewall para que estos puedan enviar tráfico de APs que usan CAPWAP.

Se deben asegurar que los puertos 5246 y 5247 (similar a los puertos 12222 y 12223 del LWAPP) estén habilitados y que ningún dispositivo intermedio impida la comunicación.

Si algún ACL está en la vía de control entre el controlador y el AP, se necesitará abrir los nuevos puertos de los protocolos para que el AP no se quede varado.

Aunque el Split MAC facilita la conectividad capa 2 entre los clientes WLAN y la interface cableada del WLC, esto no quiere decir que el túnel CAPWAP pasará todo el tráfico. El WLC reenvía las tramas IP EtherType, y el comportamiento por defecto es de no reenviar el tráfico broadcast y multicast. Esto es importante tenerlo en cuenta al considerar el reenvío del tráfico broadcast y multicast en un despliegue WLAN.

Cuando el tráfico encapsulado de los clientes alcanza el WLC, este es mapeado a su correspondiente LAN (WLAN) esto en la interface o puerto del WLC. Este mapeo está definido como parte de la configuración del WLC. El mapeo de interface es estático, pero se podría configurar para hacerlo dinámico por medio de parámetros enviados desde un servidor AAA una vez se produzca una autenticación exitosa vía EAP. Otros parámetros a configurar incluyen:

- SSID.
- Estado operacional.
- Método de autenticación y seguridad.
- QoS.

CAPWAP capa 3 es capaz de hacer la fragmentación y reensamble de los paquetes del túnel. Esto permite al tráfico del cliente usar 1500 byte MTU. Con el fin de optimizar el proceso de fragmentación y el reensamble, el número de fragmentos que el AP así como el WLC esperan recibir es limitado.

3.5.2 Consideraciones de puertos e interfaces en el controlador WLC

Algunos conceptos se deben tener en cuenta de cómo el WLC se conecta a la red cableada: puertos, interfaces y WLANs.

a. Acerca de los puertos

Un puerto es una entidad física que es usado para las conexiones en la plataforma controladora. Los controladores cuentan con dos tipos de puertos: puertos de sistema de distribución y puertos de servicio. En la Figura 3.30 se muestra como ejemplo el

controlador que se usará en modo ancla y servirá para el acceso a Internet de los clientes tanto de la red mesh considerada en el proyecto así como los clientes wireless de toda la empresa. Sin embargo la red que se implementará consiste principalmente en una red convergente donde los controladores residen dentro de los switches tanto de core como de acceso para la red wireless mesh.

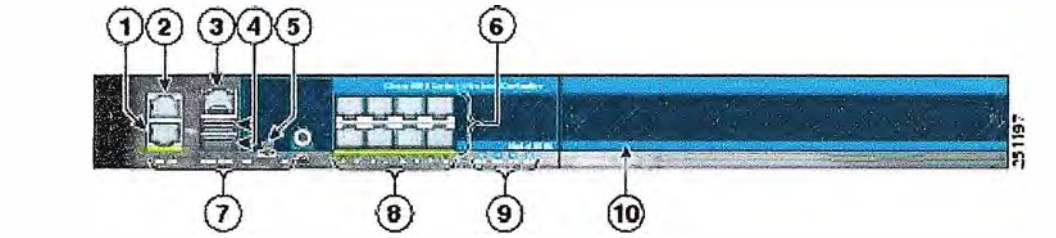

Figura 3.30 Controlador Serie 5500 (Fuente [17])

1. Puerto redundante (RJ-45)
2. Puerto de servicio (RJ-45)
3. Puerto de consola (RJ-45)
4. USB puerto 0 y 1 (Tipo A)
5. Puerto de consola (Mini USB Tipo B)
6. Puertos de sistemas de distribución SFP 1-8
7. Puertos de Gestión LEDs
8. Puertos de distribución SFP Link and Activity LEDs
9. Fuentes de poder (PS1 and PS2), System (SYS), y Alarm (ALM) LEDs
10. Slot para módulo de expansión

Nota: Sólo se puede usar un puerto de consola (RJ-45 o mini USB). Cuando uno se conecta a un puerto de consola la otra se deshabilita automáticamente.

b. Acerca de los puertos del sistema de distribución

Los puertos de sistema de distribución conectan al controlador hacia los switches vecinos y servidores.

El controlador cuenta con 8 puertos de sistema de distribución Gigabit Ethernet, estos WLCs soportan un total de 12, 25, 50, 100, ó 250 access points. Cisco 5508 no tiene restricciones en el número de access points por puerto, sin embargo es recomendable para el diseño usar el link aggregation (LAG) o configurar interfaces dinámicas de gestión de APs en cada puerto Gigabit Ethernet para balancear la carga automáticamente.

Los puertos del sistema de distribución están configurados como puertos VLAN trunk 802.1Q.

c. Acerca de los puertos de servicio

El controlador propuesto además cuenta con un puerto de servicio Ethernet 10/100/1000 en cobre, el puerto de servicio está controlado por la interface de puerto de

servicio y está reservado para la gestión remota del controlador, recuperación y mantenimiento del sistema en caso de fallas. Este puerto no es capaz de cargar etiquetas 802.1Q, por eso este debe ir conectado a un puerto de acceso en el switch vecino. El uso del puerto de servicio será opcional. No se configurarán los clientes wireless en la misma subred o VLAN que el puerto de servicio ya que esto impediría el acceso a la interface de gestión.

d. Acerca de las interfaces

Una interface es una entidad lógica del controlador. Una interface cuenta con varios parámetros asociados, los cuales incluyen una dirección IP, Gateway por default (para la subred), puerto físico primario, puerto físico secundario, identificador de VLAN, servidor DHCP.

Estos tipos de interfaces están disponibles en el controlador, cuatro de las cuales son estáticos y están configurados al momento de la configuración inicial:

- Interface de gestión (Estático y configurado al momento inicial, obligatorio)
- Interface AP-manager (Estático y configurado al momento inicial, obligatorio)
- Interface virtual (Estático y configurado al momento inicial, obligatorio)
- Interface de puerto de servicio (Estático y configurado al momento inicial, opcional)
- Interface dinámica (definido por el usuario).

Cuando LAG está deshabilitado, cada interface estará mapeado a por lo menos un puerto primario, y algunas interfaces (dinámico y gestión) pueden ser mapeados a un puerto secundario o backup. Adicionalmente múltiples interfaces pueden ser mapeados a un solo puerto del controlador.

La interface de gestión es la interface por default para la gestión en línea del controlador y la conectividad a los servicios Enterprise como los servidores AAA. Es también el utilizado para la comunicación entre el controlador y el AP.

Para CAPWAP, el controlador requiere una interface de gestión para controlar todas las comunicaciones internas del controlador y una interface AP-manager para controlar todas las comunicaciones controlador-AP, esto sin importar el número de puertos.

Para prevenir o bloquear el acceso de los usuarios de la red cableada o inalámbrica hacia la red de gestión, se utilizarán ACLs o un firewall entre la interface dinámica del cliente y la red de gestión.

No se deberá mapear la interface de Management a un cliente WLAN invitado, ya que si el túnel EoIP entre el WLC y el WLC ancla se rompe por algún motivo, el cliente podría obtener una IP de la subred de Management.

e. Acerca de los WLANs

Un WLAN asocia una interface con un Service Set Identifier (SSID) o con una

interface de grupo. Este es configurado tomando en cuenta la seguridad, calidad de servicio (QoS), políticas de radio y otros parámetros de red wireless. Hasta 512 WLANs se pueden configurar en un controlador.

Cada puerto de conexión del controlador es un trunk 802.1Q y será configurado así en el switch vecino. En switches son Cisco, la VLAN nativa de un trunk 802.1Q es la VLAN sin etiquetas. Hay que estar seguros de que al configurar la VLAN nativa en el switch, la interface del controlador debe estar en modo no etiquetado.

Se recomienda que se utilicen el etiquetado de VLANs en el controlador, además que se permitan sólo las VLANs relevantes en el puerto trunk 802.1Q. Todas las otra VLANs deberán ser deshabilitadas o utilizar el VLAN prunning en la configuración del puerto trunk del switch. Esta práctica será realizada para el desempeño óptimo del controlador.

Se recomienda el uso de un grupo de VLANs para los WLANs y diferentes grupos de VLANs para las interfaces de gestión para asegurar que el controlador enrute el tráfico de VLANs.

3.5.3 Consideraciones sobre el grupo de movilidad

Todas las versiones del software de los controladores son los mismos dentro del grupo de movilidad, esto como requisito y las buenas practicas que Cisco recomienda.

El grupo de movilidad requiere que todos los controladores usen la misma dirección IP virtual.

Cada controlador debe usar el mismo número de dominio de movilidad (nombre de grupo).

Para el correcto roaming de clientes, los WLAN SSID y las configuraciones de seguridad estarán configurados de forma idéntica en todos los controladores que comprende el grupo de movilidad.

El motivo principal de crear un grupo de movilidad es el de crear un dominio WLAN virtual a través de múltiples controladores con el fin de dar visibilidad del área de cobertura. Esto es beneficioso considerando que el despliegue de los APs que tendrán cobertura contigua overlapping ya que esto permitirá el roamming de los clientes en el grupo de movilidad.

De acuerdo al diseño planteado, los dos switches miembros del Virtual Core Switch planteado así como los Wireless LAN Switches que dan acceso a los Access Points pertenecerán a un grupo de movilidad para proporcionar el roaming transparente entre los clientes. En la Figura 3.31 se muestra los controladores que serán parte de un mismo grupo de movilidad en el diseño planteado.

Se considera usar un controlador ancla en cual requiere un túnel de movilidad estático entre los controladores de la red y el controlador ancla, esto para los servicios de acceso

de invitados. Los controladores remotos no pueden establecer relaciones de movilidad entre sí. El controlador ancla deberá contar con un miembro de grupo de movilidad estático por cada controlador remoto donde es necesario un túnel estático, este requerimiento es el mismo para el controlador remoto. En la figura 3.33 se muestra el funcionamiento del controlador ancla y en la Figura 3.34 se muestra la ubicación en el diseño considerado.

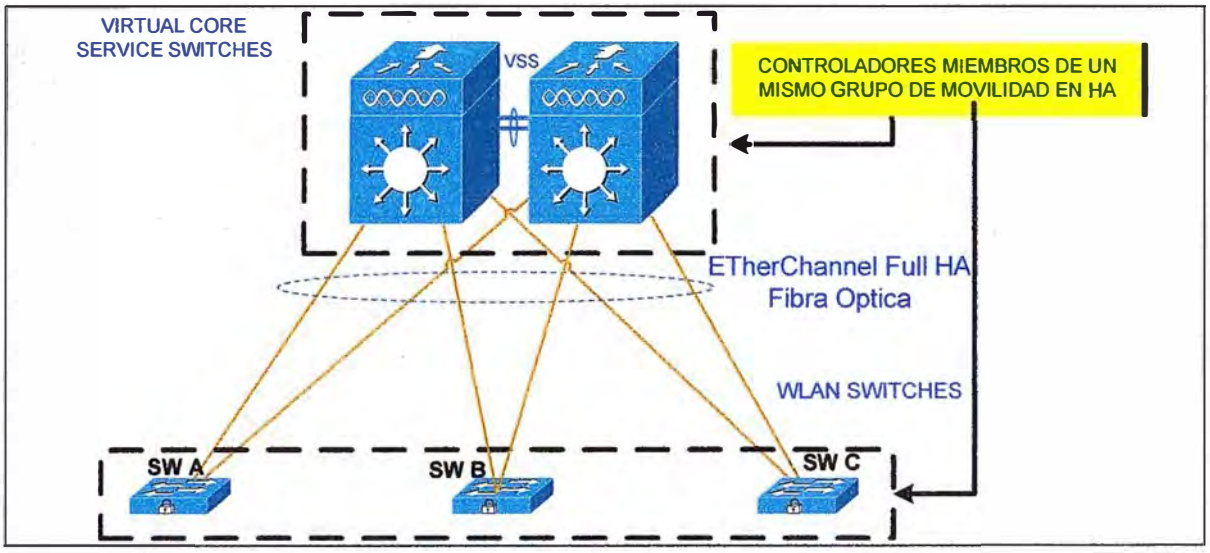

Figura 3.32 Controladores del Grupo Movilidad (Fuente: Elaboración Propia)

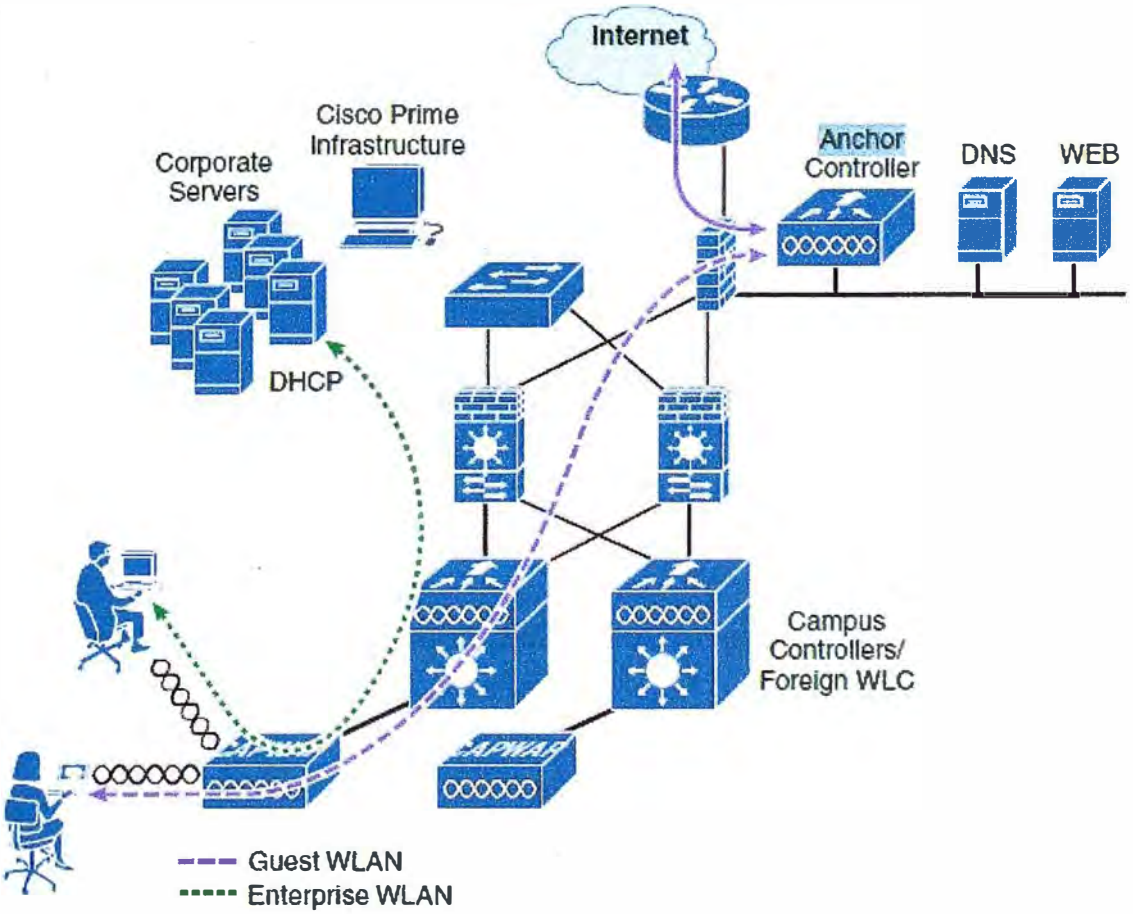

Figura 3.33 Flujo al Controlador Ancla (Fuente [3])

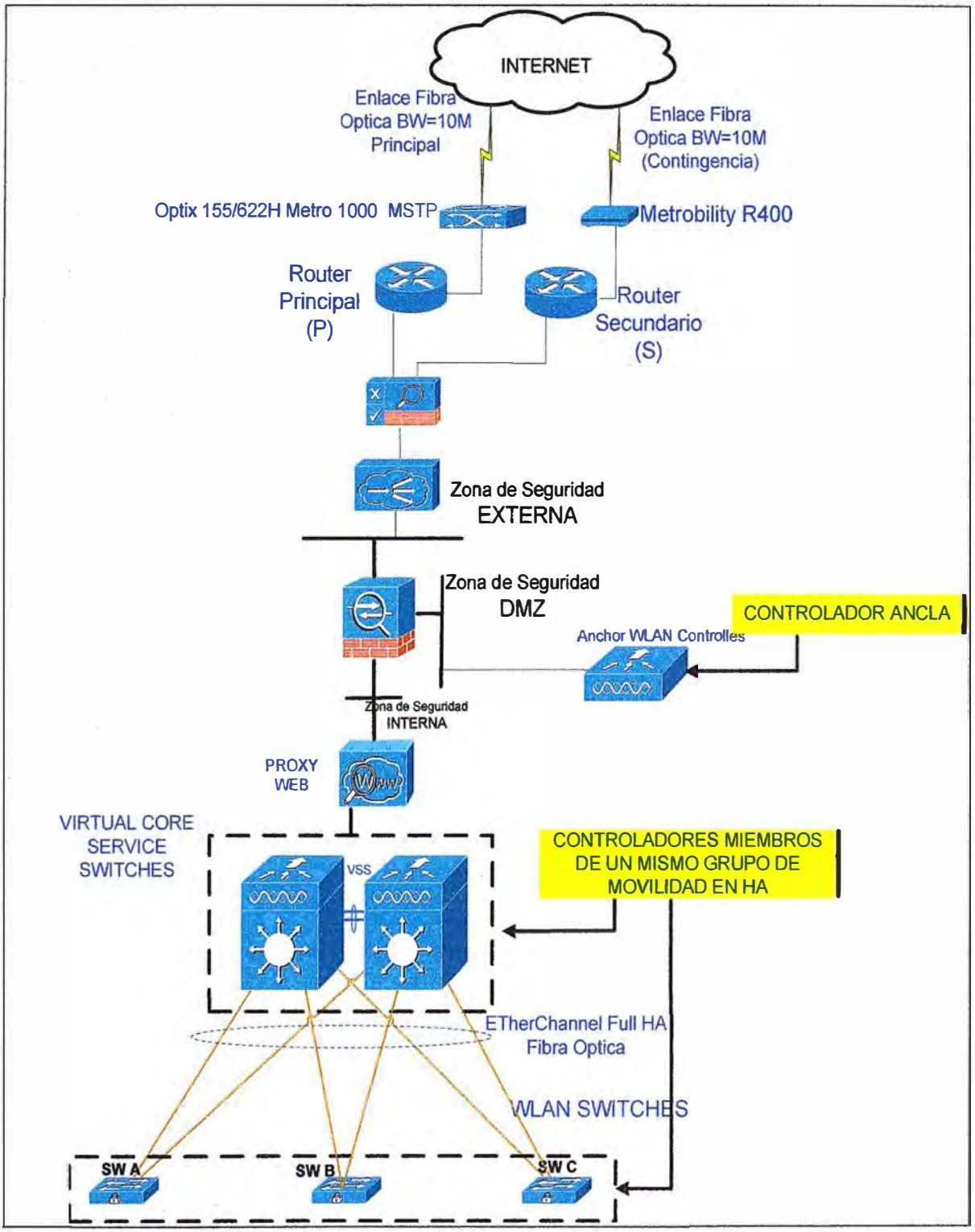

Figura 3.34 Ubicación del Controlador Ancla (Fuente: Elaboración Propia)

3.5.4 Uso de grupos de Puntos de Acceso

El uso del grupo de APs será importante ya que permitirá segmentar un WLAN en varias VLANs para no extender el dominio de broadcast. La funcionalidad de grupos de APs permite que un WLAN pueda ser soportado a través de varias interfaces dinámicas (VLANs) en un controlador. Esto es posible tomando un grupo de APs y mapeándolos a una interface dinámica específica. Estos APs pueden ser agrupados lógicamente por tipo

de trabajo o ubicación física. Cada VLAN específica y sus APs asociados estarán al mismo WLAN SSID usando la funcionalidad de grupos de APs

La característica de este funcionamiento será que si un usuario corporativo se asocia a un WLAN en un AP que corresponde a un grupo correspondiente a una VLAN determinada, a este se la asigna una dirección IP correspondiente a la subred de la VLAN determinada. El roaming entre VLANs es realizado internamente por el controlador como un roaming capa 3, así este cliente mantendrá su dirección IP original.

3.5.5 Uso de grupos de Radiofrecuencia

El uso de grupos de RF o dominios de RF representa una importante consideración al desplegar la solución. Un grupo de RF es un cluster de controladores que coordinarán y calcularán los recursos de gestión de radio (RRM) basados en la capa física del 802.11 (por ejemplo el 802.11b/g y 802.11a).

La funcionalidad que un grupo de RF tendrá será la siguiente:

Un CAPWAP envía mensajes periódicos al aire que incluye la dirección IP del controlador y un check de integridad de mensaje (MIC) derivados del tiempo de ocurrencia y el BSSID del AP.

El algoritmo de hashing utiliza una llave secreta (el nombre de grupo RF) que es configurado en el WLC enviado por cada AP. Los APs que comparten la misma llave secreta pueden validar los mensajes entre ellos usando MIC. Cuando APs que pertenecen a otros controladores escuchan los mensajes validados con una intensidad de -80 dBm a más, sus controladores automáticamente se convertirán en miembro del grupo RF.

Los miembros de un grupo de RF elegirán un líder de dominio RF quien colectará data en tiempo real para mantener una potencia master y un esquema de canales para el grupo de RF.

Las funciones del algoritmo RRM serán las siguientes:

- Alcanzar una señal uniforme de -65dB a través de todos los APs.
- Evitar la interferencia co-canal y contención.
- Evitar interferencias externas al 802.11.

El algoritmo RRM utiliza cálculos de amortiguación para minimizar los cambios dinámicos del sistema. El resultado es calculado dinámicamente resultando en la potencia óptima y el plan de canales que es una respuesta ante un cambio en el ambiente de RF.

CAPÍTULO IV
COSTOS Y CRONOGRAMA

En el presente capítulo se tocan los temas involucrados al presupuesto y al cronograma del proyecto de ingeniería.

4.1 Aspectos económicos del proyecto

El proyecto tiene un costo de 196,328.44 dólares americanos. En la Tabla 4.1 se muestra el cuadro de costos y los componentes y servicios involucrados en este proyecto.

Tabla 4.1 Análisis de Costos

Número de Línea	Producto	Descripción	Cantidad	Tiempo de Entrega	Precio Total de Venta del Partner
Productos					
Servidor Cisco UCS 220M3 Para Virtualizar el Prime, MSE e ISE					
1.0	**UCSC-C220-M3S**	UCS C220 M3 SFF w/o CPU mem HDD PCIe PSU w/ rail kit	1	55 días	1,859.00
1.1	UCS-CPU-E5-2650	2.00 GHz E5-2650/95W 8C/20MB Cache/DDR3 1600MHz	2	55 días	4,186.00
1.2	UCS-MR-1X082RY-A	8GB DDR3-1600-MHz RDIMM/PC3-12800/dual rank/1.35v	12	55 días	2,644.20
1.3	A03-D1TBSATA	1TB 6Gb SATA 7.2K RPM SFF HDD/hot plug/drive sled mounted	2	55 días	1,266.20
1.4	UCSC-CMA1	Reversible Cable Management Arm for C220C22C24 servers	1	55 días	120.25
1.5	CAB-C13-CBN	Cabinet Jumper Power Cord 250 VAC 10A C14-C13 Connectors	2	55 días	0.00
1.6	UCSC-PSU-450W	450W power supply for C-series rack servers	2	55 días	728.00
1.7	N2XX-AIPCI01	Intel X520 Dual Port 10Gb SFP+ Adapter	1	55 días	1,217.45
1.8	N20-BBLKD	UCS 2.5 inch HDD blanking panel	6	55 días	0.00
1.9	UCSC-HS-C220M3	Heat Sink for UCS C220 M3 Rack Server	2	55 días	0.00
1.10	UCSC-PCIF-01F	Full height PCIe filler for C-Series	1	55 días	0.00
1.11	UCSC-RAIL1	Rail Kit for C220 C22 C24 rack servers	1	55 días	0.00
1.12	VMW-VS5-STD-3A	VMware vSphere 5 Standard (1 CPU) 3yr Support Required	2	55 días	2,425.80
Cisco Prime Infrastructure					
2.0	**R-PI-1.1-K9**	Cisco Prime Infrastructure 1.1	1	55 días	0.00
2.1	L-PILMS42-50	Prime Infrastructure LMS 4.2 - 50 Device Base Lic	1	55 días	0.00

2.2	L-PINCS11-50	Prime Infrastructure NCS 1.1 - 50 Device Base Lic	1	55 días	0.00
2.3	L-PINCSW11-50	Prime Infrastructure NCS WAN 1.1 - 50 Device Base Lic	1	55 días	0.00
2.4	R-PI-1.1-50-K9	Prime Infrastructure 1.1 Software - 50 Device Base Lic	1	55 días	3,441.75
Mobility Service Engine					
3.0	**L-MSE-7.0-K9**	MSE Virtual Appliance (Please select L-MSE-PAK for MSE Lic)	1	55 días	3,246.75
4.0	**AIR-CAS-1KT-K9=**	Context Aware License For 1K Tags(RSSI Chokeponts and TDOA)	1	55 días	3,575.00
Identity Service Engine					
5.0	**ISE-VM-K9=**	Cisco Identity Services Engine VM	1	55 días	3,893.50
6.0	**L-ISE-AD3Y-W-100=**	Cisco ISE 100 Endpoint 3 Year Wireless Subscription License	1	55 días	2,600.00
Cisco WLAN Controller					
7.0	**AIR-CT5508-25-K9**	Cisco 5508 Series Wireless Controller for up to 25 APs	1	55 días	10,396.75
7.1	SWC5500K9-72	Cisco Unified Wireless Controller SW Release 7.2	1	55 días	0.00
7.2	AIR-PWR-CORD-NA	AIR Line Cord North America	2	55 días	0.00
7.3	LIC-CT5508-25	25 AP Base license	1	55 días	0.00
7.4	LIC-CT5508-BASE	Base Software License	1	55 días	0.00
7.5	AIR-PWR-5500-AC	Cisco 5500 Series Wireless Controller Redundant Power Supply	1	55 días	971.75
7.6	PI-MSE-PRMO-INSRT	Insert Packout - PI-MSE	1	55 días	0.00
8.0	**GLC-T=**	1000BASE-T SFP	8	55 días	2,054.00
Cisco Outdoor Access Point					
9.0	**AIR-CAP1552E-A-K9**	802.11N Outdoor Mesh Access Point Ext. Ant. A Reg. Domain	2	55 días	5,843.50
9.1	SWAP1500-BTIMGE-K9	Cisco 1520/1550 Series Boot Image - Unified SW	2	55 días	0.00
9.2	AIR-ANT2547V-N	2.4 GHz 4dBi/5 GHz 7dBi Dual Band Omni Antenna N connector	6	55 días	1,166.10
9.3	AIR-1520-BATT-6AH	1520 Series Battery Backup	2	55 días	1,038.70
10.0	**AIR-CORD-R3P-40NA=**	1520 Series AC Power Cord 40 ft. N. Amer Plug	2	55 días	388.70
11.0	**AIR-ACCPMK1550=**	1550 Series Pole-Mount Kit	2	55 días	440.70
Cisco Indoor Access Point					
12.0	**AIR-CAP3602E-A-K9**	802.11n CAP w/CleanAir; 4x4:3SS; Mod; Ext Ant; A Reg Domain	10	55 días	10,367.50
12.1	AIR-AP-BRACKET-1	802.11n AP Low Profile Mounting Bracket (Default)	10	55 días	0.00
12.2	AIR-AP-T-RAIL-F	Ceiling Grid Clip for Aironet APs - Flush Mount	10	55 días	0.00
12.3	AIR-AP-T-RAIL-R	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	10	55 días	0.00
12.4	SWLAP3600E-MESH-K9	Enterprise Wireless Mesh - AP3600e Controller-based SW Image	10	55 días	0.00
12.5	AIR-	2.4 GHz 3dBi/5 GHz 5dBi Low Profile	40	55 días	1,534.00

	ANT2535SDW-R	Antenna White RP-TNC			
Cisco WLAN Switch Convergente					
13.0	**WS-C3850-24P-S**	Cisco Catalyst 3850 24 Port PoE IP Base	3	55 días	14,235.00
13.1	CAB-TA-NA	North America AC Type A Power Cable	6	55 días	0.00
13.2	PWR-C1-715WAC/2	715W AC Config 1 Secondary Power Supply	3	55 días	1,950.00
13.3	C3850-NM-2-10G	Cisco Catalyst 3850 2 x 10GE Network Module	3	55 días	4,875.00
13.4	S3850UK9-33SE	CAT3850 Universal k9 image	3	55 días	0.00
13.5	LIC-CTIOS-1A	AP adder license for IOS based Wireless LAN Controllers	36	55 días	4,680.00
13.6	STACK-T1-50CM	50CM Type 1 Stacking Cable	3	55 días	0.00
13.7	CAB-SPWR-30CM	Catalyst 3750X Stack Power Cable 30 CM	3	55 días	0.00
13.8	PWR-C1-715WAC	715W AC Config 1 Power Supply	3	55 días	0.00
14.0	**SFP-10G-SR=**	10GBASE-SR SFP Module	12	55 días	7,761.00
				SUBTOTAL	**$98,906.60**
Garantías Extendidas de la Marca Cisco por 3 Años					
1.0.1	CON-SNTP-C220M3SF	SMARTNET 24X7X4 UCS C220 M3 SFF w/o	1	55 días	1,061.78
1.12.0.1	CON-ISV1-VS5STD3A	ISV 24X7 VMware vSphere Standard List Price is ANNUAL	2	55 días	1,601.50
2.0.1	CON-SAU-PI11K9B	SW APP SUPP + UPGR NULL SKU-No line item services included	1	55 días	0.00
2.4.0.1	CON-SAU-PI1150	SW APP SUPP + UPGR PI 1.1 Software - 50 Device Base Lic	1	55 días	2,065.05
3.0.1	CON-SAU-LMSE7K	SW APP SUPP + UPGR MSE Virtual Appliance	1	55 días	8,769.15
5.0.1	CON-SAU-ISEVM	SW APP SUPP + UPGR Cisco Identity Services Engine Virtual M	1	55 días	2,336.10
7.0.1	CON-SNTP-CT0825	SMARTNET 24X7X4 Cisco 5508 Series	1	55 días	8,917.84
9.0.1	CON-SNTP-C1552EA	SMARTNET 24X7X4 802.11N External Antenna Mesh Access Poi	2	55 dias	1,544.40
12.0.1	CON-SNTP-C362EA	SMARTNET 24X7X4 802.11n CAP w/CleanAir; 4x4:3SS; Mod; Ex	10	55 días	2,734.88
13.0.1	CON-SNTP-WS-C384PS	SMARTNET 24X7X4 Cisco Catalyst 3850 24 Port PoE IP Base	3	55 días	5,638.70
13.5.0.1	CON-SNTP-LCTIOS1A	SMARTNET 24X7X4 AP adder license for	36	55 días	4,054.05
				SUBTOTAL	**$38,723.43**
Servicios de la Empresa Partner de Cisco que Venderá la Solución					
15.0	VS5-STD-3P-SSS-C	Production Support/Subscription for VMware vSphere 5 Standard for 1 processor for 3 years Technical Support, 24 Hour Sev 1 Support -- 7 days a week.	1	55 días	1,875.00
16.0	Despacho	Despacho y entrega de hardware (Trujillo)	1	1 días	1,250.00
17.0	Instalación: Networking	Instalación del equipamiento involucrado en la propuesta -NO incluye bandejas porta equipos -NO incluye kit de rackeo de NO figurar la propuesta	1	10 días	6,250.00

		-NO incluye cables de conexión tipo patch-cord o jumpers de fibra			
18.0	CONFIG: Networking	Configuración lógica de la solución propuesta, WL Controller, Servidor UCS, Aps, Switches, Software de control y acceso ofertados, Software de Monitoreo.	1	03 días	12,500.00
19.0	Puesta en Marcha	Prueba total de red e interconexión	1	01 días	1,250.00
20.0	Mesa de Ayuda HelpDesk (36 meses)	Soporte (mesa de ayuda) 24x7x365 -- Procesos normados vía **ISO 9000** (vigente) -- Soporte remoto de la solución implementada -- SLA menor a 3 horas remoto en atención y 10 horas Onsite para problemas críticos. -- 02 visitas anuales para inspección, mantenimiento preventivo de la solución implementada.	1	55 días	5,625.00
				SUBTOTAL	**$28,750.00**
		TOTAL: VENTA sin IGV			**$166,380.03**
				IGV 18%	**18%**
		TOTAL: VENTA incluido IGV			**$196,328.44**

4.2 Cronograma

En la Figura 4.1 y 4.2 se muestra el cronograma Gantt del ciclo de vida del proyecto que se estima comience el 15 de Enero y culmine el 13 de Abril, 77 días.

Id	Nombre de tarea	Duració	Comienzo	Fin
1	CRONOGRAMA ESTIMADO PROYECTO: RED WIRELESS MESH	77 días	mar 15/01/13	sáb 13/04/13
2	TRABAJOS PRELIMINARES	9 días	mar 15/01/13	jue 24/01/13
3	Inicio del servicio (Recepción de OC)	1 día	mar 15/01/13	mar 15/01/13
4	Elaboración del programa de suministro	1 día	mié 16/01/13	mié 16/01/13
5	Elaboración del programa de instalación	1 día	jue 17/01/13	jue 17/01/13
6	Elaboración del programa de configuración	1 día	vie 18/01/13	vie 18/01/13
7	Elaboración del programa de pruebas	1 día	lun 21/01/13	lun 21/01/13
8	Elaboración del programa de certificación, conformidad y puesta en servicio	1 día	mar 22/01/13	mar 22/01/13
9	Elaboración del programa de mantenimiento preventivo	1 día	mié 23/01/13	mié 23/01/13
10	Elaboración de programa de capacitaciones	1 día	jue 24/01/13	jue 24/01/13
11	Puesta de órdenes de compra a proveedores	1 día	mié 16/01/13	mié 16/01/13
12	ENTREGA DEL EQUIPAMIENTO (HARDWARE Y SOFTWARE) POR PARTE DE LOS MAYORISTAS	55 días	jue 17/01/13	jue 21/03/13
13	IMPLEMENTACIÓN EQUIPAMIENTO CISCO	14 días	vie 22/03/13	sáb 06/04/13
14	Instalación	10 días	vie 22/03/13	mar 02/04/13
15	Configuración	3 días	mié 03/04/13	vie 05/04/13
16	Puesta en marcha	1 día	sáb 06/04/13	sáb 06/04/13
17	CIERRE DEL PROYECTO	6 días	lun 08/04/13	sáb 13/04/13
18	Pruebas de funcionamiento integrales	2 días	lun 08/04/13	mar 09/04/13
19	Documentación final, incluye Plan de capacitación y mantenimiento preventivo correctivo	3 días	mié 10/04/13	vie 12/04/13
20	Cierre del Proyecto	1 día	sáb 13/04/13	sáb 13/04/13
21	FIN	0 días	sáb 13/04/13	sáb 13/04/13

Figura 4.1 Tabla Gantt del Ciclo de Vida del Proyecto (Fuente: Elaboración Propia)

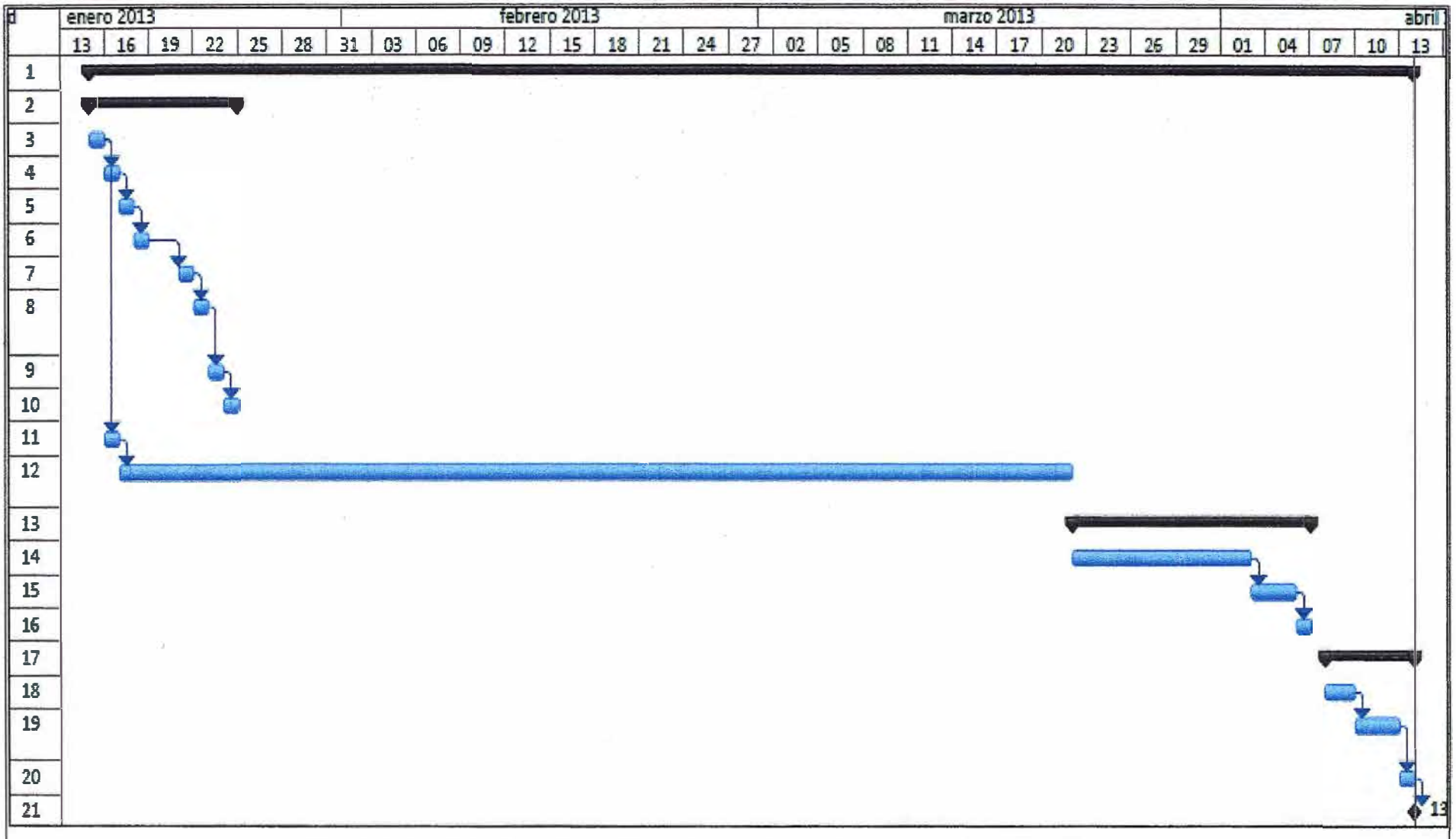

Figura 4.2 Diagrama Gantt del Ciclo de Vida del Proyecto (Fuente: Elaboración Propia)

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Se logró diseñar una red Cisco wireless segura, gestionable y de alta disponiblidad de manera que no se vea afectada la productividad de la planta megaplanta de gaseosas para sus procesos en los que intervienen robots (motacargas) automatizados, satisfaciendo así la necesidad de la empresa.

2. Los LGVs involucran movimiento y requieren la conexión permanente a la red, es pues que la arquitectura implementada, aparte de manejar la red mesh de la solución, está preparada para soportar la integración con otras redes wireless que cuenta el cliente, estos simplemente se integrarían a futuro mediante la red WAN.

3. La calidad de servicio aplicada ha sido provechosa para los LGVs, ya que cuentan con prioridad exclusiva del tráfico que intercambian con sus servidores de monitoreo y de aplicación. La segunda prioridad el resto de accesos con las restricciones pertinentes ya que así se asegura que la producción no se vea afectada.

4. La implementación de los APs fue sencilla y al contar con el Cisco Prime Infrastructure, además de monitorear el despliegue de APs, es posible con la misma aplicación poder configurar de manera remota y gráfica estos. Sólo bastaría colocar el AP en la posición deseada, el resto es muy sencillo.

Recomendaciones

1. Es recomendable siempre realizar un site survey que ayude a determinar las áreas de cobertura RF y así escoger en número de APs necesarios para la solución. Esto ayuda a superar los problemas de las redes wireless (distorsión multitrayecto, nodos escondidos), descubriendo regiones donde la interferencia multitrayecto puede ocurrir, áreas donde la interferencia RF es muy alta y encontrar soluciones para eliminar estos problemas.

2. Es altamente recomendable usar antenas omnidireccionales en todos los ambientes de la megaplanta, ya que una direccional podría dejar áreas sin cobertura debido a la forma de los patrones de radiación característica de estas antenas, esta recomendación viene producto de las pruebas que se hicieron con dicho tipo de antena.

3. Para tener una idea de la capacidad de tráfico (velocidad de comunicación) que se

puede tener por cliente, se recomienda tomar la tasa más alta que puede soportar el AP, dividirlo entre dos y luego a ese resultado dividirlo entre el número de clientes promedio que se enlazarán al AP en un instante dado, esto será la capacidad promedio por cliente que la celda podrá soportar.

ANEXO A
GLOSARIO DE TÉRMINOS

AAA	Autenticación, Autorización y Contabilización
AES	Advanced Encription Standard
ALM	Alarma (Alarm)
AWPP	Cisco Adaptive Wireless Path Protocol
BGN	Bridge Group Name
BYOD	Trae tu Propio Dispositivo (Bring Your Own Device)
CAPWAP	Control and Provision Wireless Access Points
CMX	Connected Mobility Experience
CSD	Cambio Cíclico de Diversidad (Cyclic Shift Diversity)
DFS	Selección Dinámica de Frecuencia (Dynamic Frequency Selection)
DoS	Denegación de Servicio (Denial of Service)
ICE	Interchassis Etherchannel
ISE	Identity Service Engine
LAG	Agregación de Enlace (Link Aggregation)
MAP	Puntos de Acceso Malla (Mesh Access Point)
MCS	Esquema de Modulación y Codificación (Modulation and Coding Scheme)
MIC	Check de Integridad de Mensaje (Message Integrity Check)
MIMO	Multiple-input Multiple-output
MRC	Máxima Relación de Combinación (Maximal Radio Combining)
MSE	Mobility Service Engine
NCS	Sistema de Control de Red (Network Control System)
QoS	Calidad de Servicio (Quality of Service)
RAP	Root Access Point
RRM	Recursos de Gestión de Radio (Radio Resource Management)
RTLS	Servicios de Localización en Tiempo Real (Real Time Localization Service)
SGA	Seguridad de Acceso de Grupos (Secure Group Access)
SGACLs	Seguridad de Grupos (Security Group Access Lists)
SGTs	Etiquetas de Seguridad de Grupo (Security Group Tags)
SPG	Switch Peer Group
SSID	Service Set Identifier
SYS	Sistema (System)
WAP	Punto de Acceso Inalámbrico (Wireless Access Point)
WCS	Sistema de Control Wireless (Wireless Control System)
wIPS	Sistema de Prevención de Intrusos Inalámbrico (Wireless Intrusion Prevention System)
WLC	Wireless LAN Controllers

BIBLIOGRAFÍA

[1] Atlanta Packaging "Laser Guided Vehicles (AGV's)". http://www.atlantapackaging.co.uk/laser-guided-vehicles

[2] Eletricc80, "Wlan para sistemas LGV – Especificaciones_2_Espanol" , 2010

[3] Cisco Mobile Design 7.1

[4] Cisco, "Cisco Wireless Controllers", http://www.cisco.com/en/US/prod/collateral/modules/ps2706/at_a_glance_c45-652653.pdf

[5] Cisco Press "Cisco Prime Infrastructure 1.2 Data Sheet" http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps12239/data_sheet_c78-715144.html

[6] Cisco Wireless Mesh Access Points, Design and Deployment Guide, Release 7.4

[7] Cisco Press, "Cisco Mobility Services Engine Data Sheet" http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c78-475378.html

[8] Cisco, "Overview of Cisco ISE" http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_overview.html

[9] Cisco, "Aironet 3600 Series Access Point Datasheet".

[10] "Modulation and Coding Scheme - MCS Index Table", http://mcsindex.com/

[11] The Hive Mind blog, "Wi-Fi Back to Basics – 2.4 GHz Channel Planning" http://blogs.aerohive.com/blog/the-wireless-lan-training-blog/wifi-back-to-basics-24-ghz-channel-planning

[12] Cisco 1140 Series Access Point Deployment Guide

[13] Cisco Aironet Dual-band Dipole Antenna (AIR-ANT2524DB-R, AIR-ANT2524DG-R, and AIR-ANT2524DW-R)

[14] Cisco Aironet 1600/2600/3600 Series Access Point Deployment Guide

[15] Cisco Aironet 1550 Series Outdoor Access Point Datasheet

[16] Cisco Aironet Dual-Band Omnidirectional Antenna (AIR-ANT2547V-N)

[17] Cisco 5500 Series Wireless Controller Installation Guide

[18] Cisco Wireless LAN Controller Configuration Guide, Release 7.5