

PALOMA MARTÍNEZ ABADÍA

**ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE
UNA INSTALACIÓN COMPLETA DE RED
WIFI EN UN HOSPITAL DE LA COMUNIDAD
AUTÓNOMA DE ARAGÓN**

TRABAJO FIN DE GRADO
GRADO EN INGENIERÍA DE TECNOLOGÍAS
Y SERVICIOS DE TELECOMUNICACIÓN

DIRECTOR

ÁNGEL ALONSO FORCANO

PONENTE

IGNACIO MARTÍNEZ RUIZ



**Universidad
Zaragoza**

JUNIO, 2017



DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD

(Este documento debe acompañar al Trabajo Fin de Grado (TFG)/Trabajo Fin de Máster (TFM) cuando sea depositado para su evaluación).

D./D^a. _____,

con nº de DNI _____ en aplicación de lo dispuesto en el art.

14 (Derechos de autor) del Acuerdo de 11 de septiembre de 2014, del Consejo de Gobierno, por el que se aprueba el Reglamento de los TFG y TFM de la Universidad de Zaragoza,

Declaro que el presente Trabajo de Fin de (Grado/Máster)
_____, (Título del Trabajo)

es de mi autoría y es original, no habiéndose utilizado fuente sin ser citada debidamente.

Zaragoza, _____

Fdo: _____

Agradecimientos y Dedicatorias

En primer lugar agradecer a Soluciones Tecnológicas Integradas la oportunidad que me ha dado de poder realizar este Trabajo Fin de Grado. En especial a mi director de trabajo Ángel Alonso y a mis compañeros implicados en este proyecto por la ayuda, la colaboración y el apoyo que me han dado.

Agradecer por parte de la Escuela de Ingeniería a mi Ponente Ignacio Martínez por todas las facilidades que me ha brindado durante este largo proceso.

Agradecer sobre todo a mi familia y a mi pareja Ángel la paciencia que han tenido no solo en el desarrollo de este trabajo sino durante todos los años de esfuerzo para superar esta carrera.

Y finalmente a mis amigos, a ti Elena, por confiar en que podía lograr el objetivo que me propuse.

RESUMEN DEL PROYECTO FIN DE GRADO

“Análisis, Diseño e Implementación de una instalación completa de Red WIFI en un Hospital de la Comunidad Autónoma de Aragón”

Autor: Paloma Martínez Abadía

Director: Ángel Alonso Forcano

Ponente: Ignacio Martínez Ruiz

Ahora mismo el centro hospitalario al que nos referimos en este proyecto dispone de una infraestructura de red WiFi pública muy limitada y sólo con acceso común para trabajadores, pacientes y familiares. El objetivo que se plantea con este TFG es analizar, diseñar e implementar una propuesta completa de infraestructura de red WiFi profesional para el hospital que dé servicio a los distintos perfiles de usuarios estableciendo las reglas necesarias, que permita una gestión y control total, automatizado y on-line de la red, que cubra las necesidades de cobertura y que integre tanto el amplio volumen de dispositivos del centro como la numerosa incorporación prevista de equipos para seguimiento de pacientes.

Para ello se ha realizado un estudio de las necesidades del centro así como de la infraestructura necesaria para llevar a cabo con éxito el objetivo que se plantea. Se elaboró un planteamiento de puntos de acceso en función del mapa de cobertura de éstos, un diseño de red con los equipos necesarios de infraestructura de red, direccionamiento y creación de mapa de red para integrar esta red WiFi de manera óptima.

Este TFG se ha realizado dentro de la empresa Soluciones Tecnológicas Integradas, la cual es asesora tecnológica de este centro y está llevando a cabo una remodelación tecnológica con una previsión de 5 años.

Ha sido imprescindible la colaboración de las personas responsables del área de informática y sistemas del centro hospitalario para llevar a cabo el cambio introducido con este proyecto.

Finalmente se ha dejado preparada la red WiFi para la introducción de numerosos equipos de medición de pacientes que se pretenden incorporar en el próximo año.

ESQUEMA GENERAL DE LA MEMORIA

Índice de contenidos

CAPÍTULO 1. Introducción y Objetivos.....	Página 1
1.1. Introducción.....	Página 1
1.2. Antecedentes y Motivación.....	Página 2
1.3. Objetivos.....	Página 4
1.4. Estructura de la memoria.....	Página 5
CAPÍTULO 2. Tecnologías y Metodologías.....	Página 7
CAPÍTULO 3. Análisis y Diseño.....	Página 10
3.1. Análisis del estado anterior.....	Página 12
3.2 Resultado del Análisis.....	Página 15
3.3 Diseño.....	Página 17
3.3.1 Búsqueda de soluciones en el mercado....	Página 17
3.3.2 Prueba Piloto.....	Página 23
CAPÍTULO 4. Desarrollo e implementación.....	Página 27
CAPÍTULO 5. Resultados y Evaluación.....	Página 39
CAPÍTULO 6. Conclusiones y Líneas Futuras.....	Página 43
6.1 Conclusiones.....	Página 43
6.2 Líneas futuras.....	Página 45
CAPÍTULO 7. Bibliografía.....	Página 46
Apéndices.....	Página 47

Índice de figuras.

Figura 1. Estándar IEEE 802.11

Figura 2. Modo infraestructura

Figura 3. Modo ad-hoc

Figura 4. Plano hospital planta 1 Áreas 1 y 2

Figura 5. Plano hospital planta 1 Áreas 3 y 4

Figura 6. Plano hospital planta 1 disposición APs estado anterior

Figura 7. Leyenda plano

Figura 8. Mapa de cobertura Planta 1

Figura 9. Tabla comparativa de costes

Figura 10. Características equipo Aruba

Figura 11. Características equipo Aerohive

Figura 12. Airwave

Figura 13. Hivemanager

Figura 14. Distribución electrónica de red

Figura 15. Plano hospital Planta 1 disposición APs nueva instalación

Figura 16. Tabla VLANs

Figura 17. Captura acceso control switch

Figura 18. Hivemanager configuración de red

Figura 19. Hivemanager actualización firmware

Figura 20. Tabla SSIDs

Figura 21. Hivemanager políticas de red

Figura 22. Hivemanager creación SSIDs

Figura 23. Hivemanager creación SSIDs

Figura 24. Hivemanager creación SSIDs

Figura 25. Hivemanager conexión puntos de acceso

Figura 26. Hivemanager aplicaciones

Figura 27. Hivemanager información clientes

Figura 28. Hivemanager información conexiones

Figura 29. Hospital líquido

CAPÍTULO 1. Introducción y Objetivos

1.1. Introducción

Los hospitales, las clínicas y otras instalaciones de cuidado de la salud enfrentan una enorme demanda de WiFi, ya sea para satisfacer las necesidades de más del 90% de los médicos con smartphones o para conectar la multitud de dispositivos médicos que se conectan en red cada vez más con el fin de brindar un seguimiento en tiempo real, una ubicación precisa y un soporte al paciente.

Con numerosos usuarios de dispositivos móviles, las paredes gruesas y los innumerables aparatos electrónicos, los entornos de salud son comúnmente ambientes RF hostiles. Es por eso que tantas organizaciones de cuidado de la salud en todas partes se están volcando en implantar sistemas inalámbricos adecuados para proporcionar la mejor conexión posible aún en las condiciones más difíciles.

Internet está en todos lados, es imprescindible ya prácticamente en nuestras vidas, puesto que nos la facilita en muchos sentidos. Los hospitales, lugares con elevada movilidad por parte de los trabajadores, y con mucho tiempo de espera por parte de familiares y pacientes, han sido siempre un firme candidato a necesitar conexiones de calidad y en movilidad.

El WiFi permite un acceso rápido a los registros electrónicos de pacientes, mejora la comunicación con el personal, y acelera el envío de imágenes médicas. Además, el acceso a WiFi para invitados puede extenderse a los visitantes en recepciones y salas de espera.

A pesar de que en muchos grandes hospitales de los países más desarrollados sí que es bastante habitual que ya haya redes cerradas para el personal médico (así como WiFi de pago para los pacientes), en la inmensa mayoría de los hospitales del mundo todavía es muy poco común encontrar una red inalámbrica, muchas veces ni siquiera para uso interno ni externo. Los motivos muchas veces son de presupuesto, si bien a veces también se atribuye a razones de logística o desconocimiento.

Observar dentro de los hospitales a enfermeros y/o médicos relleno a mano informes médicos, que posteriormente deben informatizar, es el denominador común aun considerándose una pérdida de tiempo y por lo tanto un descenso en la productividad.

1.2. Antecedentes y Motivación

La utilidad del WiFi en un hospital puede verse reflejada de muchas maneras; desde el familiar que visita al paciente y hasta un técnico de mantenimiento. Si en un principio a una red WiFi solían conectarse únicamente PCs y más recientemente smartphones, impresoras o tabletas, ahora lo hace cualquier tipo de dispositivo electrónico que requiera intercambiar información. Y de este tipo de dispositivos hay muchos en un hospital.

Pero ¿qué tal si el médico o enfermero en lugar de escribir sobre papel lo hace directamente en una tableta o smartphone, que se comunican vía WiFi a un centro de datos? ¿Y si en ese centro de datos se procesa la información enviada y en ese mismo momento otro usuario puede dar opinión o contestación sobre esos datos? Se habrá ahorrado mucho tiempo para todos los usuarios involucrados, pero no sólo eso; la información quedaría almacenada de manera segura (en la nube o en servidores), podría ser accedida desde cualquier lugar o incluso podría alimentar casi al instante las estadísticas de salud.

Principales aplicaciones de una red WiFi existentes en un hospital:

- Aplicaciones para el cuidado del paciente — En ésta deben incluirse dispositivos como bombas de infusión, monitores de oxígeno y toma de constantes. Estas aplicaciones son clave dentro del proceso del cuidado del paciente y reducen el riesgo para ellos.
- Aplicaciones para el desarrollo del trabajo — Aquí se ubica, por ejemplo, el acceso seguro a registros médicos electrónicos (bases de datos), visualización de registros de rayos x y diversos tipos de scanner. Estas aplicaciones permiten que personal médico y de enfermería posean movilidad flexible y puedan ubicarse en el lugar que se les necesita.
- Aplicaciones para usuarios — Implica ofrecerle al “cliente” de los hospitales (pacientes y familiares) la conectividad que necesitan para realizar diversas tareas como consultar información, ocupar las largas horas de espera, revisar sus correos electrónicos o incluso trabajar desde el hospital.

Las redes WiFi en hospitales representan la nueva generación de tecnología inalámbrica para modernizar los sistemas de salud, entre otros servicios sociales. Su utilización disminuye los costes de diseño, despliegue y ofrece una mejor experiencia en el uso de datos, voz y aplicaciones médicas críticas para cuidar de la salud de los pacientes que al final, son los más importantes.

Este Trabajo Fin de Grado se realiza dentro de un proyecto de renovación tecnológica que está llevando a cabo la empresa Soluciones Tecnológicas Integradas S.L. en este centro hospitalario de la Comunidad Autónoma de Aragón.

Este proyecto comenzó a principios de 2016 con el objetivo de llevarlo a cabo por completo en un periodo de 4-5 años.

En el momento del comienzo el Hospital dispone únicamente de una red WiFi pública, lo que si que permite que cualquier tipo de usuario acceda a internet a través de su Smartphone o Tablet pero no existe la posibilidad de que cualquier personal del centro hospitalario pueda trabajar como lo hace desde su PC conectado a la LAN.

Esta restricción supone que los trabajadores no tengan movilidad ninguna lo que conlleva una poca optimización de una red inalámbrica.

Ésta es una de las motivaciones por las que surge este proyecto junto con el objetivo que tiene el Hospital de implantar dispositivos wearables para la toma de datos de pacientes. Éste despliegue de dispositivos requiere una red inalámbrica profesional que permite el envío continuo de información.

Pero la gran motivación de este centro es mejorar tecnológicamente para aportar mayores beneficios a sus pacientes y usuarios.

1.3. Objetivos

El enfoque de este TFG, a partir de la evaluación inicial del estado actual de la red WiFi del hospital, del estudio de los problemas, carencias, limitaciones y necesidades existentes, y del análisis de alternativas tecnológicas, consistirá en diseñar y desarrollar la infraestructura de red que permita dotar al centro de una red WiFi integrada (a través de un equipamiento de puntos de acceso y sistema controlador, estudios de cobertura basados en diferentes SSIDs en función del usuario que acceda, roles/permisos de acceso, diversas funcionalidades, etc.), implantar la solución completa y validarla técnicamente para ofrecer al hospital una red WiFi profesional.

- Analizar la red WiFi existente en el centro hospitalario.
- Conocer las necesidades reales del hospital en cuanto a conexión WiFi y movilidad.
- Establecer tipos de usuario y servicios que van a utilizar esta red.
- Implantar una red profesional en la que convivan distintos SSIDs
- Permitir la movilidad del personal del centro sin perder la seguridad en la consulta de información.
- Dar un servicio de red WiFi pública adecuado para los pacientes y usuarios del centro.
- Escoger un equipamiento profesional que permita el balanceo de ancho de banda, la limitación de descargas así como el control y diferenciación de los usuarios.
- Implantar una red segura para los usuarios, teniendo en cuenta la protección de los datos al consultar las historias de los pacientes.
- Diseñar una red WiFi preparada para la incorporación de dispositivos inalámbricos para la toma de datos de los pacientes.

1.4. Estructura de la memoria

La memoria de este TFG está dividida en dos partes.

La primera parte corresponde con el desarrollo completo de este trabajo, donde se explica el análisis, diseño e implementación de los objetivos descritos anteriormente.

En la segunda parte se incluye una serie de anexos que detallan y amplían los conceptos técnicos utilizados en la primera parte de la memoria. En éstos no se comentan detalles fundamentales para el seguimiento del desarrollo pero sí que ofrecen una visión más completa del TFG.

La primera parte de la memoria está dividida en los siguientes capítulos:

- CAPÍTULO 1: Introducción y Objetivos. Se describe el entorno de la tecnología WiFi en los entornos hospitalarios junto con los antecedentes y motivación del desarrollo de este proyecto en el Hospital
- CAPÍTULO 2: Tecnologías y Metodologías. Se describe el marco tecnológico en el que se desarrolla este TFG.
- CAPÍTULO 3: Análisis y Diseño. Justifica el camino seguido para la elaboración de este proyecto así como la elaboración del diseño de la solución.
- CAPÍTULO 4: Desarrollo e Implementación. Describe de forma detallada todo el trabajo realizado para la implementación de la red.
- CAPÍTULO 5: Resultados y evaluación. Desarrollo de la situación actual del centro Hospitalario tras la implantación de la solución.
- CAPÍTULO 6: Conclusión y líneas futuras. Se realiza un análisis de los objetivos cumplidos y los beneficios que ha aportado la realización de este TFG. Incluye unas líneas futuras como posibles nuevos objetivos a desarrollar.

La segunda parte de la memoria contiene los siguientes anexos:

- Anexo 1. Planos Hospital
- Anexo 2. Distribución de APs anterior al proyecto.
- Anexo 3. Mapas de Cobertura.
- Anexo 4. Datasheet Equipos.
- Anexo 5. Datasheet Equipos Electrónica de Red.
- Anexo 6. Plano Despliegue Puntos de Acceso.
- Anexo 7. Configuración de Switches.

CAPÍTULO 2. Tecnologías y Metodologías

La especificación IEEE 802.11 es un estándar internacional que define las características de una de área local inalámbrica.

Existen distintos estándares que se han ido implementando con el paso del tiempo, con el objetivo de mejorar la conectividad y su rendimiento. Todos son mejoras y parten del inicial estándar 802.11.

Independientemente de la banda de frecuencia en que trabajan, los estándares de la familia 802.11 comparten algunas limitaciones [3]

En primer lugar, el alcance, es una de las limitaciones comunes, ya que este dato depende, en primer lugar de la ubicación y de la presencia de obstáculos en el camino entre el punto de acceso y el terminal, y en segundo lugar, de las condiciones meteorológicas y de las interferencias.

Si bien los diferentes estándares pueden alcanzar las velocidades teóricas que muestra la Figura 2.1, a causa del efecto de los protocolos necesarios para transportar la información de usuario sobre el canal, la velocidad útil es mucho menor, siendo esto una limitación común en todos ellos.

En cuanto a la calidad de servicio, no todo el tráfico tiene la misma importancia desde el punto de vista de cada usuario. Los protocolos más extendidos de WiFi, no incluyen ningún mecanismo para priorizar un tipo de tráfico sobre otro, lo cual resulta muy perjudicial cuando se mezclan flujos de tráfico con requerimientos muy diferentes, como voz y datos.

Respecto a la seguridad, las redes WiFi no presentaban mecanismos de seguridad muy sofisticados, pero con el éxito que ha ido obteniendo esta tecnología, se hizo necesario introducir mejoras en este aspecto. El 802.11i resuelve la mayoría de las debilidades originales, hasta el punto de hacerlas comparables en seguridad en las redes fijas.

En la Figura 1 se describe la evolución del estándar IEEE 802.11

IEEE 802.11

Estándar	Descripción
IEEE 802.11b	11 Mbps, cobertura de celda de 100m, opera en la banda de 2,4 Ghz.
IEEE 802.11a	Evolución del 802.11b, a mayor velocidad, 54 Mbps en la banda de 5,7 Ghz.
IEEE 802.11d	Versión del 802.11b, con translación de frecuencia para aquellos países en donde la banda 2,4 Ghz esta siendo utilizada.
IEEE 802.11e	Añade al estándar 802.11 a, b y g calidad del servicio (priorización) .
IEEE 802.11f	Añade al estándar 802.11b factores de movilidad, similares a los usados en las redes móviles .
IEEE 802.11g	Equivalente al 802.11a (velocidades hasta 54 Mbps) pero trabajando en la banda de 2,4Ghz
IEEE 802.11h	Ofrece mejoras en la potencia de transmisión y en la selección de canales en el estándar 802.11a
IEEE 802.11i	Aporta elementos de seguridad agregando nuevos métodos de encriptación y autenticación al estándar básico a, b y g.
IEEE 802.11j	Permite la coexistencia del 802.11a y el estándar europeo HiperLAN2

Figura 1

En el momento de decidir la implementación de una red WiFi se debe tener en cuenta que existe la posibilidad de aplicar dos modos: infraestructura o Ad-Hoc.

En el modo infraestructura cada estación se conecta a un punto de acceso a través de un enlace inalámbrico. Estos forman una célula y se identifican a través de un BSSID, que corresponde con la dirección MAC del punto de acceso. La limitación de este modo es al número máximo de clientes inalámbricos que se pueden conectar manteniendo una determinada calidad de servicio.

En la Figura 2 se describe la configuración del modo infraestructura.

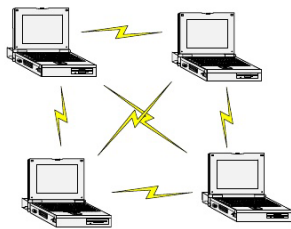


Figura 2

También existe el modo Ad-Hoc, “peer – to – peer “, es un método para que clientes inalámbricos puedan establecer una comunicación directa entre sí, no siendo necesario involucrar un punto de acceso central. Todos los nodos de esta red se pueden comunicar directamente con otros clientes. Cada cliente inalámbrico debería usar el mismo SSID y número de canal de la red.

En la Figura 3 se describe la configuración del modo infraestructura

Modo AD-Hoc



- No hay punto de acceso
- Comunicación P2P

Configuración	Nodo 1	Nodo 2
Modo	Ad hoc	
SSID	El mismo	
Canal	El mismo	
IP	IP _A (normalmente fija)	IP _B (normalmente fija)

Figura 3

CAPÍTULO 3. Análisis y Diseño

Para llegar a implantar un sistema de red WiFi como el que se propone en este TFG es necesario conocer con exactitud qué es lo que hay instalado en el momento de comenzar así como su estado.

El hospital en el que se desarrolla este proyecto dispone de 4 plantas de altura, a las que nos referiremos como Planta 0 (sótano), Planta 1 (planta calle), Planta 2 y Planta 3; y en el que deberemos diferenciar 4 áreas a partir de ahora para poder comprender con claridad la distribución del mismo.

- Área 1: zona de hospitalización y consultas compuesta por 4 plantas.
- Área 2: zona de residencia compuesta por 4 plantas aledañas a la zona de hospitalización.
- Área 3: zona de dirección, dentro de la zona de residencia, únicamente en la planta 1.
- Área 4: zona de informática, situada en el coro de la Iglesia, entre la planta 1 y 2.

Para mayor claridad las siguientes imágenes corresponden al plano de la planta 1, con cada una de las 4 áreas marcadas. En el anexo 1 se adjuntarán el resto de los planos.

Área 1 Hospitalización marcada en color rojo.

Área 2 Residencia marcada en color verde.

Área 3 Dirección marcada en color azul.

Área 4 Informática marcada en color amarillo.



Figura 4



Figura 5

3.1. Análisis del estado anterior

El primer problema que surgió al empezar este proyecto fue la falta de documentación. Por lo tanto junto con la ayuda del personal informático del hospital se realizó un descubrimiento de campo así como un análisis de cobertura de la red WiFi pública existente para conocer qué Puntos de Acceso estaban colocados y cuál era su ubicación.

Tras realizar este trabajo de campo y junto con la información que nos dio el personal informática se llegó a estas conclusiones:

- CPD localizado en el Área 4 Informática. Este punto lo trataremos más adelante ya que dentro del proyecto de remodelación tecnológica estaba previsto la instalación de un nuevo CPD que habrá que tener en cuenta para el diseño de nuestra instalación de red WiFi.
- Dos redes WiFi existentes que denominaremos Red Libre y Red Hospital.

La *Red Libre* se compone de un total de 8 puntos de Acceso distribuidos por las Áreas 1, 2 y 3. Conectados todos ellos por cable de red a un módem adsl que proporciona un ancho de banda de 6Mbps.

La *Red Hospital* se compone de 12 puntos de Acceso distribuidos en el Área 1 Hospitalización. Conectados todos ellos por fibra a un router que proporciona un ancho de banda de 20Mbps.

- Planta 0 Sótano:

Red Libre: el rack se encuentra en la parte derecha del Área 2 Residencia, situado en la primera estancia del lado izquierdo del pasillo. A ese rack están conectados los puntos de acceso por cable de categoría 5, distribuidos por el Área 2 hacia arriba. En esta planta solo hay un AP.

Red Hospital: hay un rack de techo en el Área 1 Hospitalización (ver plano), donde van conectado 3 APs de ésta planta. Existe un cuarto AP en la zona de almacén situado en el Área 2, que va colgado del rack de la red libre, (existe un minirack intermedio).

- Planta 1 Calle:

Red Libre: 1 AP ubicado en el Área 3 de dirección. El cableado sube por la barandilla hacia la planta superior (planta 2). 1 AP situado en la terraza cubierta del hospital que ahora mismo han desconectado por la reforma. 1 AP ubicado en la zona del hospital, entrada principal.

Red Hospital: 3 APs distribuidos a lo largo del pasillo y un rack en la sala derecha de la entrada.

- Planta 2:

Red Libre: 2 APs en el Área 2, uno en la parte derecha y otro en la parte izquierda cuya conexión sube por la barandilla desde la planta inferior. 1 AP en el Área 1 hospital, zona de la cafetería. Enganchado al rack de la zona del hospital. *Red Hospital:* rack ubicado en la sala de espera contigua a la cafetería y 3 APs distribuidos en el pasillo. Armario de comunicaciones principal ubicado en Área 4 de informática.

- Planta 3:

Red Libre: 1 AP en el Área 2, parte izquierda junto a la bajante. En esta planta está ubicado el paso de cableado de la zona derecha a izquierda separadas en el resto de las plantas por la Iglesia en el Área 2.

Red Hospital: Área 1, 2 APs en el pasillo y un armario rack.

La Figura 6 y Figura 7 corresponden al plano y leyenda de la planta 1 con la localización de los APs instalados al comienzo del proyecto. En el anexo 2 se adjuntarán el resto de los planos.



Figura 6



Figura 7

3.2 Resultado del Análisis.

El mayor problema encontrado, es la baja intensidad de señal de los puntos de acceso. La potencia radiada por los APs es muy baja en las zonas más próximas a ellos y casi inexistente y poco estable en las zonas más alejadas.

Se ha detectado la existencia de muchas zonas de sombra donde ni siquiera llega señal suficiente para mantener una conexión.

Independientemente de la capacidad que tengan los puntos de acceso ya instalados, la cantidad de éstos es insuficiente para dar una cobertura al área total, siendo esto una necesidad para el nuevo funcionamiento del hospital.

Otro inconveniente encontrado es la imposibilidad de gestionar los puntos de acceso existentes, lo que conlleva solapamientos de canal e interferencias entre ellos, provocando una limitación en la intensidad de la señal recibida.

A esto hay que añadirle la sobrecarga de usuarios que hay en la red. La capacidad de ancho de banda disponible no es suficiente para abarcar la cantidad de conexiones que se solicitan diariamente y que tras la implantación de nuevos dispositivos en el área hospitalaria aumentará considerablemente.

Podemos señalar también la falta de hardware para realizar balanceamientos de carga entre redes. Equipamiento que ayuda a mejorar el rendimiento de la red.

En cuanto al cableado, se ha detectado un problema en la organización en cada uno de los armarios de comunicaciones y la falta de unidades libres en los racks para añadir equipamiento nuevo.

Una vez terminado el análisis se definen las siguientes acciones a plantear al Hospital:

Se procederá a la eliminación de los APs existentes debido a su limitada capacidad y a su restricción de gestionarlos y sustitución por equipos con las capacidades necesarias.

Se recomienda la instalación de una red independiente a la existente. Esto permitirá evitar cualquier conflicto con la red local del hospital, de esta manera cualquier problema que pueda surgir en cada una de ellas estará más localizado y no repercutirá en el funcionamiento de la misma.

Para ello proponemos instalar un pequeño rack en cada una de las plantas del Área 1, que llevará incluido una electrónica de red (switches gestionables) y donde estará instalado el nuevo cableado (patch panel).

En el nuevo cableado incluiríamos la colocación final de las tomas directamente a pared con cajas de superficie a las que se colocarían los APs en el techo de manera visible para optimizar su capacidad.

Cabe destacar la insuficiencia de ancho de banda contratado ahora mismo para dar servicio al elevado número de usuarios que se prevé se conecten a la nueva red WiFi. La disponibilidad actual de dos routers para la Red Libre y la Red Hospital con anchos de banda de 6MB y 20 MB no podrá dar el correcto servicio a la nueva red que se implantará por lo que se recomienda la modificación de estos contratos para obtener capacidad suficiente.

3.3 Diseño.

Una vez finalizado el descubrimiento de campo y definido las conclusiones del mismo, mantuvimos numerosas reuniones con las personas implicadas en el proyecto para definir las necesidades reales de usuarios que pudiera tener el Hospital y comenzar el diseño de la solución.

Junto con el personal responsable de informática y sistemas del centro hospitalario quedaron definidos los siguientes requerimientos.

Según las necesidades del hospital se establecerían 4 redes:

- Red Pública destinada a pacientes y familiares del centro hospitalario con capacidad aproximada para 400 conexiones simultáneas.
- Red para Personal Sanitario con 100 conexiones simultáneas.
- Red para Equipamiento Médico destinada a la subida de datos tomados por dispositivos médicos con capacidad para 1000 conexiones simultáneas.
- Red para el Área de Residencia con capacidad para 20 conexiones simultáneas.

3.3.1 Búsqueda de soluciones en el mercado.

Dentro del mercado de fabricantes de equipamiento para soluciones WiFi profesionales destacan CISCO, ARUBA y AEROHIVE. Son estas tres opciones las que en un primer momento se decidió valorar.

El comienzo del diseño de la solución pasaba por realizar un estudio de cobertura del área completa a cubrir del hospital para obtener la distribución adecuada así como número de puntos de acceso a instalar.

Para ello se seleccionaron tres puntos de acceso, uno de cada fabricante, con características similares para poder establecer valores de referencia en cuanto a capacidades del AP y así realizar un mapa de calor.

En la Figura 8 se muestra el mapa de cobertura de la Planta 1. En el anexo 3 se incluyen los mapas de cobertura completos.



Figura 8

Según el estudio realizado se recomienda la colocación de puntos de acceso según el mapa de cobertura siguiendo la disposición que se indica en los planos. Se plantea la colocación de 47 puntos de acceso para dar cobertura al área completa del centro hospitalario.

Presupuestos.

Uno de los puntos importantes a valorar era el planteamiento económico, siempre cumpliendo las condiciones y características técnicas que quedaron definidas.

Se solicitó presupuestos a tres empresas proveedoras de los tres fabricantes CISCO, ARUBA y AEROHIVE. Una vez recibidos, se tuvo que descartar la opción planteada de CISCO por ser inviable dentro de los presupuestos del Hospital.

En la Figura 9 se muestra la comparativa de costes entre ARUBA y AEROHIVE.

ARUBA

Hardware	Unidades	PVP/Unidad	PVP
AP 205	48	764,50 €	36.696,00 €
Kit montaje AP	48	27,50 €	1.320,00 €
			38.016,00 €
Software	Unidades	PVP/Unidad	PVP
Licencia y soporte por AP 1 años	48	54,00 €	2.592,00 €
Instalación Airwave	1		800,00 €
Servicios configuracion Aps	1		2.400,00 €
Puesta en Marcha	1		700,00 €
Maquina Virtual	1		780,00 €
			7.272,00 €
Instalacion	Unidades	PVP/Unidad	PVP
Electrónica de Red	6	1.713,00 €	10.278,00 €
Precio por planta	4	1.810,00 €	7.240,00 €
			17.518,00 €
Mantenimiento			
Bono 50h.			2.720,00 €

TOTAL sin descuento 65.526,00 €

Descuento Hospital 20% 13.105,20 €

TOTAL TOTAL 52.420,80 €

* Controladora virtual en Servidores

* Soporte por AP/anual. 22€

* Switches no gestionables. La electrónica de red no requiere licenciamiento

AEROHIVE

Hardware	Unidades	PVP/Unidad	PVP
AP130	48	599,00 €	28.752,00 €
			28.752,00 €
Software	Unidades	PVP/Unidad	PVP
Licencia y soporte por AP 1 año	48	70,00 €	3.360,00 €
Puesta en Marcha	1	1.775,00 €	1.775,00 €
			5.135,00 €
Instalacion	Unidades	PVP/Unidad	PVP
Electrónica de Red	6	1.599,00 €	9.594,00 €
Precio por planta	4	2.950,00 €	11.800,00 €
			21.394,00 €
Mantenimiento			
Bono 50h.			2.720,00 €

TOTAL sin descuento 58.001,00 €

Descuento Hospital 15% 8.700,15 €

TOTAL TOTAL 49.300,85 €

* Controladora en la Nube

* Licenciamiento Hive Manager y soporte por AP 3 años 140€. (46€/AP/anual)

* Licenciamiento Hive Manager y soporte por AP 5 años 210€. (42€/AP/anual)

* Switches Gestionables. Licenciamiento Hive Manager y Soporte 5 años incluido

Figura 9

La comparativa de costes se desglosa en cuatro partidas claramente diferenciadas solicitadas por el Hospital:

- Hardware. Corresponde con el coste de los puntos de acceso. 48 APs, 47 para instalación y uno de repuesto.
- Software. Esta partida incluye el licenciamiento de los puntos de acceso para su funcionamiento así como la puesta en marcha de los mismos.
- Instalación. La instalación engloba el coste del equipamiento para la electrónica de red, la colocación de los APs y el instalación de todo el cableado nuevo.
- Mantenimiento. El Hospital quiere incluir un paquete de horas para utilizar en incidencias, consultas y/o mantenimiento.

Como se ha indicado anteriormente debido al alto presupuesto que suponía la implantación del fabricante CISCO, las opciones a valorar después de la parte económica son únicamente ARUBA y AEROHIVE.

Equipos.

En cuanto a los puntos de acceso se seleccionaron de cada fabricante modelos similares en características. APs compatibles con el estándar 802.11ac, con doble antena omnidireccional interna para la banda de 2 GHz así como para la banda de 5GHz, operativo con 10/100/1000 Base-T Ethernet y PoE.

Los modelos que se plantean son los siguientes:

- IAP-205 de Aruba.

Product features		AP 204/205
Hardware scalability	Wi-Fi Standards	.11ac
	# Tx Antenna & # Rx Antenna	2x2
	# of MU-MIMO spatial streams	NA
	# of SU-MIMO spatial streams	2
	# Radios	2
	In built BLE radio	✗
External antenna option	✓	
RF Characteristics	11ac Beamforming	✓
	Airtime fairness	✓
	DFS channel support to use all available RF spectrum	✓
	Advanced Cellular Filtering for co-existence with DAS	✓
	Spectrum analysis support	✓
Interfaces	Multi-Gigabit Ethernet (2.5 and 5 Gbps)	NA
	# 10/100/1000 Base-T Ethernet autosensing link	1
	Link Aggregation (LAG)	NA
	Perfect Load Balancing on LAG	NA
	PoE on Eth 2	NA
	PoE Out	✗
Console port for the ease of installation and management	✓	
Certifications and Warranty	Wi-Fi alliance certified	✓
	Lifetime warranty	✓
Flexible deployment mode	Desktop mount	✗
	Wall Mount	✓
	Ability to use the same AP in a controller based or controller-less deployment	✓



IAP-205



Figura 10

- AP130 de Aerohive

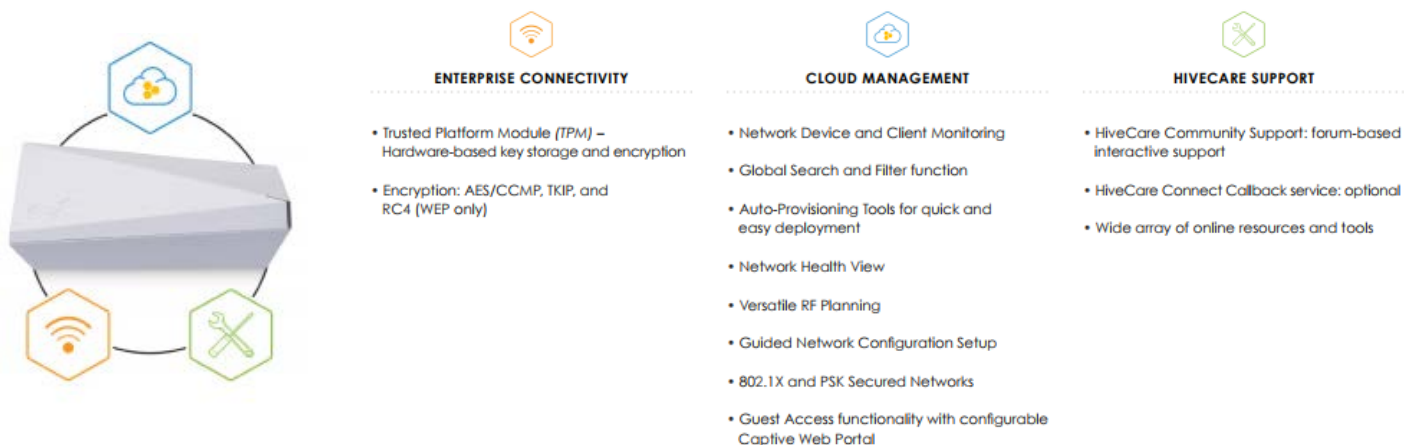


Figura 11

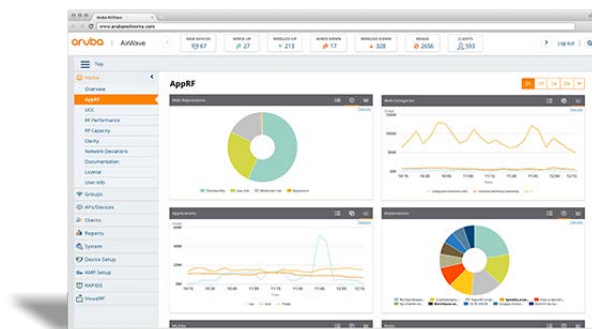
En el Anexo 4 se adjuntan los datasheet de cada uno de los equipos.

Entorno de control.

Otra de las características a tener en cuenta para la toma de decisión es el entorno de control para gestionar los puntos de acceso. Instalación, usabilidad, configuración, sencillez, gestión, reportes, avisos...son aspectos a valorar.

Como se ha introducido en el Capítulo 2 Tecnologías y metodologías, los entornos de control disponen de muchas características comunes pero una que las diferencia notablemente como es el entorno donde corren.

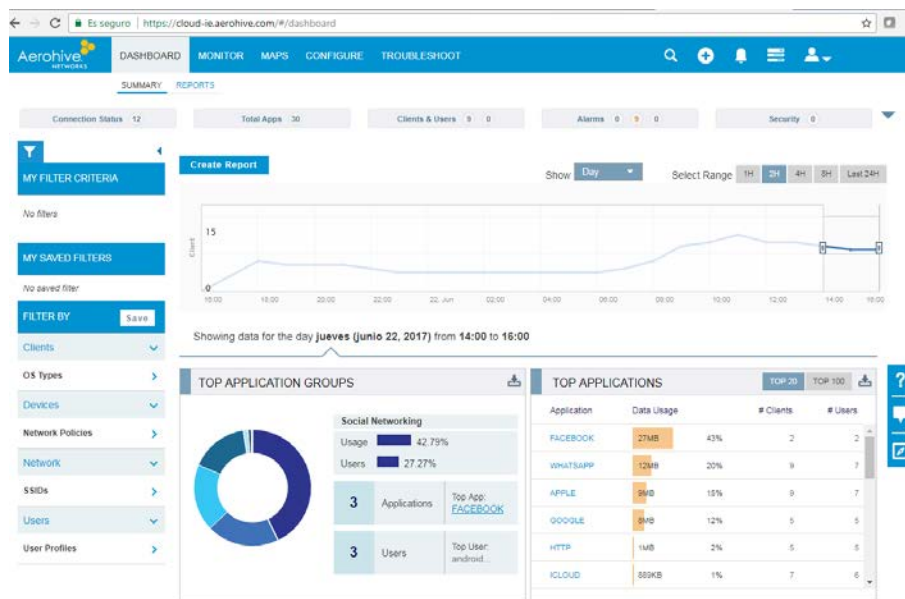
Airwave de ARUBA necesita estar instalado en una máquina virtual en la misma red de los puntos de acceso. Cierto es que existe una modalidad con coste añadido que permite gestionar puntos de acceso en diferentes localizaciones y diferentes redes pero no es el caso en el que nos encontramos.



<http://www.arubanetworks.com/es/productos/productos-de-red/gestion/gestion-de-redes/>

Figura 12
21

Sin embargo la gran ventaja que nos proporciona HiveManager de AEROHIVE es su alojamiento en la nube, lo que nos permite una monitorización y control total vía web desde cualquier red en la que nos encontremos.



<http://www.aerohive.com/products/network-management/>

Figura 13

3.3.2 Prueba Piloto.

Podemos decir que ambos fabricantes junto con CISCO ocupan los primeros puestos como líderes en el mercado, todos similares en prestaciones y cobertura haciendo que sean pequeñas características las que los diferencien.

Estamos hablando de equipamiento *enterprise* para dar cobertura y estabilidad a un entorno profesional, crítico y exigente como es un Hospital.

Esas diferencias que nos cuentan son las que queríamos ver *in situ*, en nuestro entorno, integrado dentro de la red del Hospital. Y para ello se hicieron 2 pruebas piloto, cada una con un fabricante pero simultáneamente para poder comparar “en directo”.

Las pruebas se han realizado en dos áreas diferentes del hospital, conviviendo ambos fabricantes pero en diferentes redes, uno de ellos en la Red Libre y otro en la Red Hospital.

Aerohive: las pruebas se realizaron instalando 4 puntos de acceso, dos en la zona de dirección y dos en la parte residencial. Modelo AP130*

Aruba: las pruebas se realizaron en zona de hospitalización, 4 puntos de acceso cubriendo pasillos, habitaciones y control en la parte derecha de la Planta 1. Modelo IAP-205*

Características Comunes

Se puede decir que en ambas pruebas la intensidad de señal era buena, el área de cobertura que proporcionaban era extensa y la velocidad de conexión adecuada teniendo en cuenta el ancho de banda disponible.

Un punto a destacar es la caída y recuperación de los APs. En los dos pilotos se forzó la caída de puntos de acceso para comprobar cómo afectaba a la conexión de los usuarios. Tanto en Aerohive como en Aruba si un AP se desconectaba no afectaba al usuario, inmediatamente el dispositivo móvil se conectaba al siguiente punto de acceso con buena señal si en el que estaba conectado se había producido una caída.

Otra comprobación que se realizó en este caso con Aruba fue la reacción ante la caída del punto de acceso que actuaba como controladora. Se pudo ver que en esa situación inmediatamente otro de los puntos pasaba a tener ese rol hasta que la controladora original volvía a recuperarse.

Tanto técnicamente como a nivel de usuario los dos pilotos han cubierto las necesidades y cumplido los objetivos existiendo pequeñas diferencias entre ellos a valorar.

Diferencias Existentes

Despliegue

Éste es uno de los puntos que diferencia en gran medida los dos fabricantes.

Aerohive no necesita controladora, son los propios puntos de acceso los que gestionan el tráfico por lo que su despliegue es sencillo. Dispone de alojamiento en la nube y la configuración de los APs se realiza desde su HiveManager, esto implica que solo se necesita conexión a internet para gestionar y monitorizar.

Aruba requiere una instalación inicial más compleja. En este caso necesitamos instalar en el entorno una máquina virtual para poder desplegar Airwave que será el software de gestión donde se tendrán que incluir los puntos de acceso así como determinar que uno de ellos realice la función de controladora virtual. Para gestionar y monitorizar este entorno se necesita conectarse directamente a la IP de los APs y/o la controladora. Esta controladora virtual es la que se encarga de la seguridad, entre otras cosas de la integración con el firewall y la intrusión, prevención y detección de equipos “potencialmente enemigos”

Roaming

En ambos casos el cambio de AP que realiza el dispositivo móvil es inapreciable para el usuario. La conexión es continua en movimiento.

En Aerohive el roaming entre puntos de acceso se produce en el momento en que el usuario detecta mayor señal de un AP distinto al que está conectado. Al mismo tiempo al no haber controladora y ser los puntos de acceso los que realizan el balanceo, éstos decidirán si hacer el cambio teniendo en cuenta la intensidad de señal y el número de usuarios conectados a cada AP.

Por el contrario Aruba dispone de otra política de roaming. Esto no se realizará mientras el usuario disponga de señal e intensidad suficiente en el punto de acceso al que esté conectado. Ciertamente nos permite limitar el umbral, es decir, forzar el roaming cuando esté por debajo de un determinado valor a pesar de que la señal siga siendo suficiente. En las pruebas realizabas los puntos de acceso de Aruba cubrían áreas de cobertura muy grandes y en la disposición que se colocaron aparentemente había solapamientos por ello la posibilidad de forzar el roaming.

Monitorización

Las posibilidades de controlar todos los parámetros y obtener comparativas e información es similar para ambos fabricantes. La diferencia aparece en la usabilidad del entorno de cada uno de ellos.

Como se ha indicado anteriormente para acceder al control en Aerohive únicamente se necesita una conexión a la nube, entrar a través de internet al HiveManager. El entorno es bastante intuitivo para el usuario y la monitorización y las alertas son en tiempo real.

Para la monitorización en Aruba se necesita estar en la misma red para poder acceder directamente al AP que funciona de controladora así como a la IP que contiene el Airwave. El entorno podría decirse que es menos intuitivo, un poco más complejo de manejar. La actualización de la información en el controladora es en tiempo real, se debe indicar cada cuanto se quiere refrescar la información con un mínimo de 60seg. Sin embargo los datos en Airwave no son así, tiene un retardo de 10 min lo que puede suponer un problema ante la monitorización de una incidencia.

Decisión.

Una vez finalizada la prueba piloto y el análisis de la misma se planificó una reunión para tratar todo lo ocurrido, valorar pros y contras de cada uno y tomar la decisión definitiva para poder llevar a cabo la implantación

Teniendo en cuenta la valoración económica, la diferencia entre los presupuestos no es demasiado significativa, ante igualdad de condiciones se optaría por la opción más

económica pero esto no será un condicionante si en las características técnicas existe una diferencia notable.

Los dos puntos determinantes para la elección de la solución fueron la complejidad del despliegue y la obtención de información en tiempo real.

La facilidad de “plug and play” por así decirlo de Aerohive con los punto de acceso tuvo un peso determinante para el Hospital. Al realizar la implantación de la prueba piloto de ambos fabricantes al mismo tiempo quedó en evidencia la diferencia de complejidad entre ellos. El coste que supuso la instalación de la máquina virtual y el despliegue de Airwave fue llamativo en comparación a la facilidad de dar de alta los APs en la URL correspondiente a Aerohive en la que entras con Usuario y contraseña.

Por otra parte el retardo que ofrece Airwave hace que la información que ves no sea en tiempo real, característica que preocupa mucho dentro del entorno crítico que es un centro hospitalario. Era muy importante tener un control fácil y real de lo que está ocurriendo en la red WiFi mientras se visualiza.

Después de todo esto se puede concluir que la opción elegida por motivos tanto técnicos como económicos fue la del fabricante AEROHIVE.

CAPÍTULO 4. Desarrollo e implementación

A partir del análisis y diseño del capítulo anterior, la tarea principal de este trabajo fin de grado ha consistido en la gestión, supervisión, y coordinación (incluyendo el conocimiento técnico adecuado de cada una de las configuraciones, topologías, módulos, infraestructuras....) de los desarrollos técnicos que se han llevado a cabo por parte del equipo completo que realizó la implementación de la solución total.

Para el desarrollo se estableció una lista de tareas con el fin de llevar a cabo la correcta implantación de la red WiFi. Parte de estas tareas se podían realizar paralelamente, sin embargo otras muchas eran dependientes entre ellas.

Después del análisis realizado y las pruebas piloto en las que surgieron grandes problemáticas con la red existente, debimos incluir en el proyecto una auditoría de red para conocer el estado de la red completa del hospital y hacer las modificaciones necesarias para, no solo implantar una red WiFi profesional, sino definir una topología de red correcta, un direccionamiento adecuado y una infraestructura de red gestionable que soporte todo el tráfico que tiene el centro hospitalario.

A continuación se desglosa el desarrollo completo de las fases de instalación del proyecto.

- CPD y Despliegue de Fibra Óptica.

Como se indicó al principio del anterior capítulo, en el comienzo del proyecto el armario de comunicaciones se ubicaba en el Área 4 Informática, sin embargo dentro de la renovación tecnológica uno de los proyectos que se ha llevado a cabo es la creación de un nuevo CPD y la virtualización de los servidores que tenía instalados el Hospital.

Esto se debió tener en cuenta para nuestra implantación ya que cada uno de los Switches que instalaríamos en las plantas del Área 1 hospitalización del que colgarían los puntos de Acceso de cada planta debían estar conectados con el CPD, así como la electrónica de red y APs del Área 2 y Área 3 situados en el edificio anexo.

Se instaló fibra desde el nuevo CPD a cada una de las plantas para poder conectar la electrónica de red ya que ahora mismo sólo llegaba desde el armario de comunicaciones del Área 4 Informática.

- Diseño de electrónica de red.

Para el proyecto de red WiFi se diseñó la disposición y características de la nueva infraestructura de red. Al poner equipamiento nuevo se pensó en un futuro, que estos no solo fueran para la conexión de APs sino que sirvieran para sustituir también los switches no gestionables que hubiera por el hospital (plantas y CPD antiguo) con el fin de trasladar todas las máquinas a estos nuevos equipos gestionables.

En la Figura 14 se establece la disposición de la nueva infraestructura de red, incluyendo el nuevo CPD (dos CPD para tener redundancia).

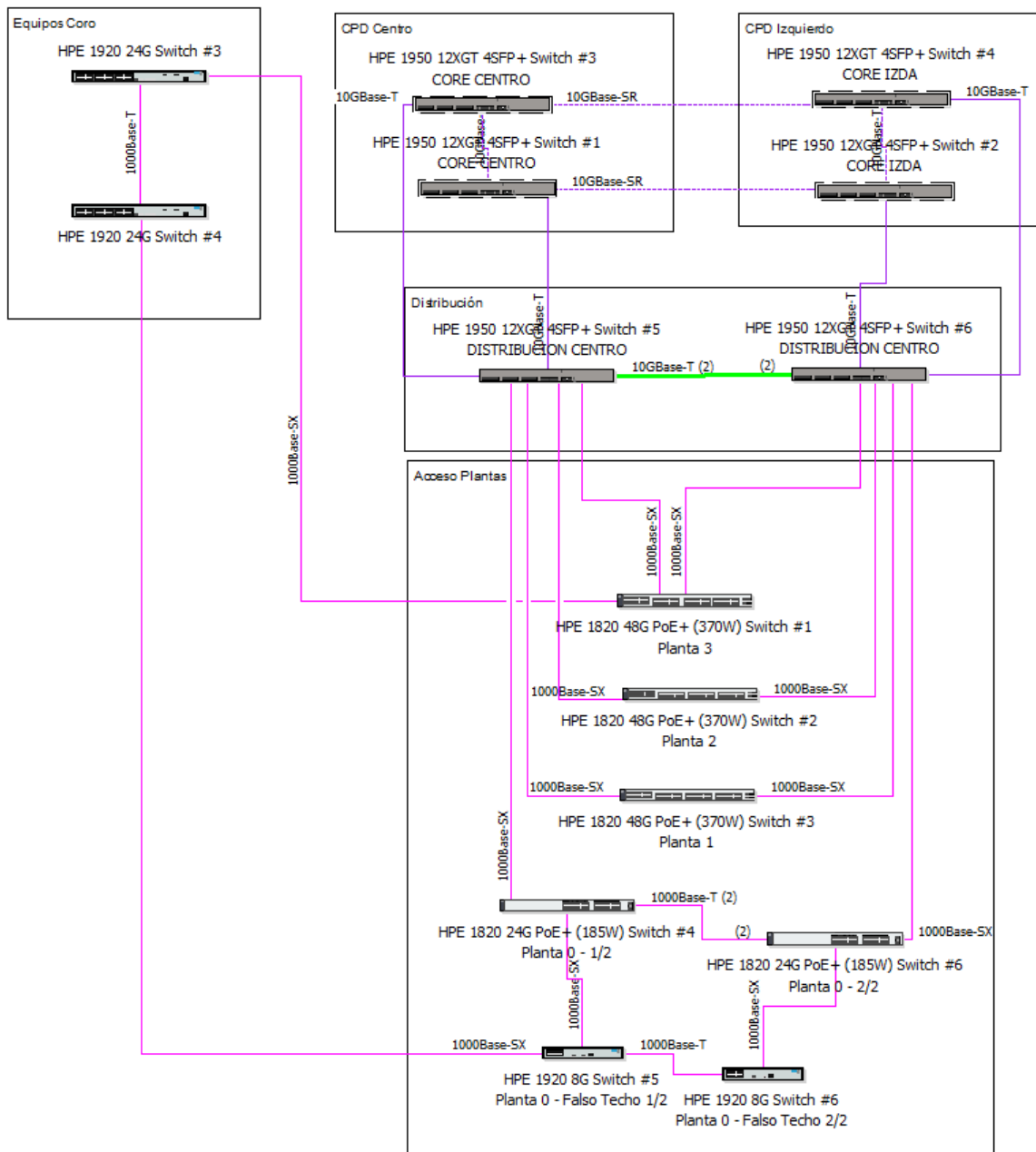


Figura 14

El equipamiento que se ha elegido para las plantas son Switches HPE 1820 de 24 o 48 puertos, de los cuales las 12 primeras bocas son POE+ destinadas a la conexión de los APs. De esta manera no necesitaremos alimentar los APs mediante inyectores.

Como se observa en la imagen, en la Planta 0 se han incluido dos equipos HPE 1920 de 8 puertos, necesarios para sustituir los switches no gestionables que había en un pequeño rack en esa planta.

En el anexo 5 se incluyen los datasheet con las características técnicas.

- Instalación de Racks y Cableado para colocación de APs.

Una de las tareas que se realizaron paralelamente a las anteriores fue la instalación de racks, patch panel y cableado para los APs, así como la colocación de los puntos de acceso.

Llegado este punto, mantuvimos una reunión con los responsables de informática para ajustar la localización de los APs.

Teniendo en cuenta el mapa de cobertura realizado, el número de puntos de acceso presupuestados y las necesidades del hospital, se estableció la siguiente disposición de puntos de Acceso.

Planta 0

Total de 11 puntos de acceso distribuidos:

Dos puntos de acceso en el Área 2 y nueve puntos distribuidos por la zona hospitalaria. A diferencia del mapa de cobertura de esta planta se han suprimido dos APs en zonas que por el momento no requieren conexión inalámbrica y se ha añadido un tercer punto en el lateral derecho del Área 1 debido a que hay una estancia independiente y diáfana en la cual no hay red LAN y se requiere un AP dedicado para cubrir ese área.

Planta 1

Total de 15 puntos de acceso distribuidos:

Dos puntos de acceso en el Área 2, dos puntos de acceso en el Área 3 y once puntos de acceso repartidos por el Área 1. En este caso respecto del mapa de cobertura inicial se ha suprimido un AP exterior de la zona de carga el cual se instalará en un futuro para el control de material de entrada y salida; se ha añadido un punto de acceso en cada uno de los laterales de Área 1, Área 2 y Área 3.

Planta 2

Total de 12 puntos de acceso distribuidos:

Dos puntos de acceso en el Área 2 y diez puntos en Área 1.

Se ha añadido un AP al mapa de cobertura para continuar con la misma distribución en los laterales que en las plantas anteriores.

Planta 3

Total de 6 puntos de acceso distribuidos:

Dos puntos en el Área 2 y cuatro puntos en el Área 1.

Esta planta es la que más cambios ha sufrido desde el primer planteamiento. El motivo surge de la interferencia que produce la señal WiFi con los equipos instalados en el servicio del lateral izquierdo de esta planta.

Finalmente se han implantado 44 puntos de acceso y se han adquirido dos más como repuesto para incidencias.

En la Figura 15 se muestra la disposición de los APs en la Planta 1. En el anexo 6 se incluyen los planos completos.

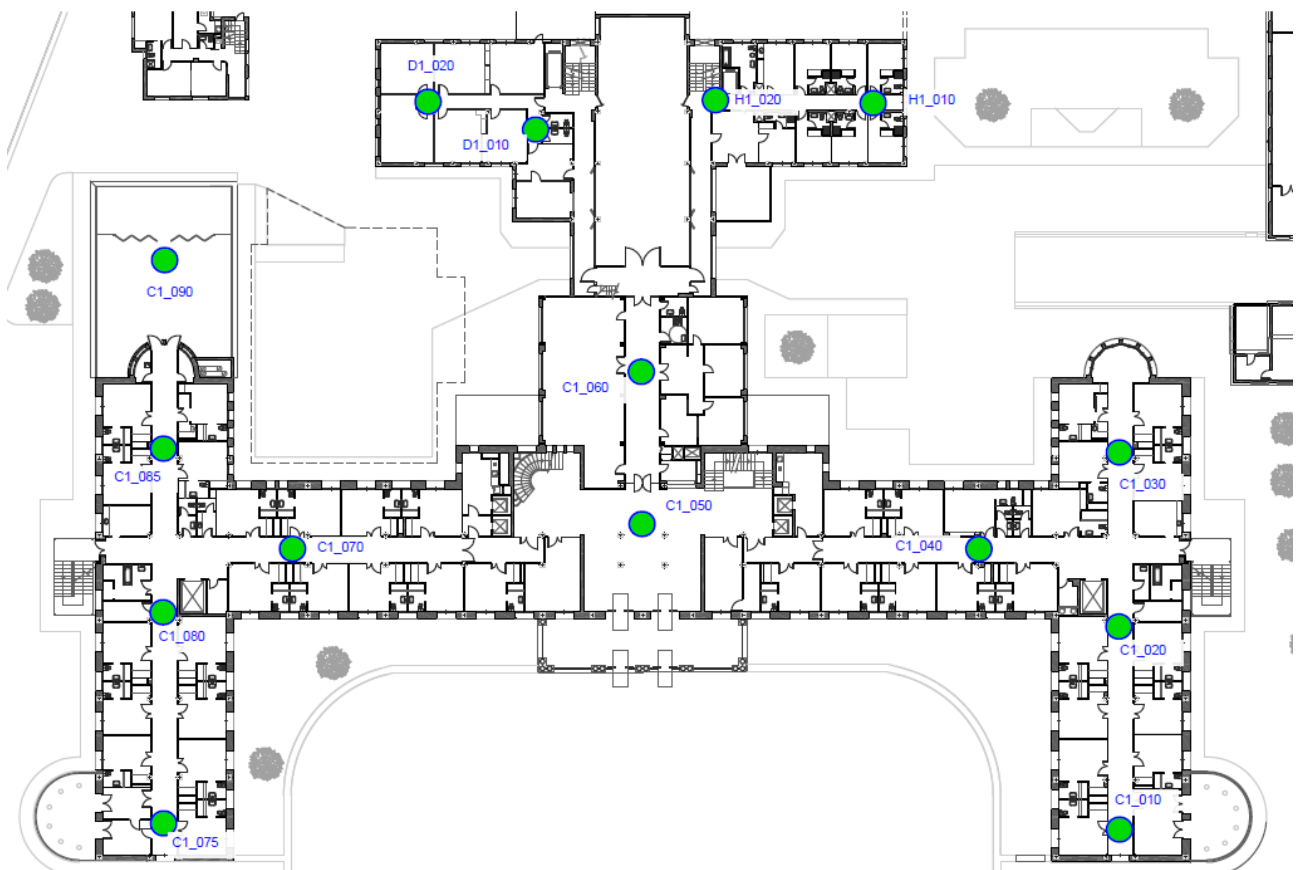


Figura 15

- Definición de VLANs red WiFi.

Según las necesidades que se indicaron anteriormente en cuanto a usuarios y diferenciación de redes se definen las siguiente VLANs que se deberán configurar en los Switches así como en los puntos de Acceso.

VLAN WIFI PÚBLICA

VLAN WIFI PRIVADA

VLAN GESTIÓN

- Auditoría de red.

Una vez realizadas todas las tareas anteriores se optó por la auditoría de red completa antes de proceder a la implantación de la nueva electrónica de red así como de la red WiFi.

1. Estudio del estado actual, relación de equipos y direccionamiento existente.

Todos los PCs, impresoras, servidores y equipos inalámbricos que se conectan a la Red Hospital obtienen una IP fija o dinámica del rango 172.29.0.1 – 172.29.15.254

2. Definición de VLANs y asignación de rangos de IPs.

Analizando todos los servicios, equipamiento y tipos de usuarios se definen las siguientes VLANs incluyendo la parte de red WiFi:

Vlan1	172.29.0.0/20	172.29.0.1 – 172.29.15.254	OLD
VLAN20	172.29.20.0/23	172.29.20.1 – 172.29.21.254	EQUIPOS
VLAN22	172.29.22.0/23	172.29.22.1 – 172.29.23.254	WIFI RED PRIVADA
VLAN24	172.29.24.0/24	172.29.24.1 – 172.29.24.254	SERVIDORES
VLAN25	172.29.25.0/24	172.29.25.1 – 172.29.25.254	SERVICIOS EXTERNOS
VLAN26	172.29.26.0/24	172.29.26.1 – 172.29.26.254	ADMINISTRACIÓN
VLAN27	172.29.27.0/24	172.29.27.1 – 172.29.27.254	IMPRESORAS
VLAN28	172.29.28.0/24	172.29.28.1 – 172.29.28.254	VPN
VLAN29	172.29.29.0/24	172.29.29.1 – 172.29.29.254	NEFRO
VLAN30	172.29.30.0/24	172.29.30.1 – 172.29.30.254	WIFI RED PUBLICA
VLAN31	172.29.31.0/24	172.29.31.1 – 172.29.31.254	RESERVA

Figura 16

- Supervisión del cambio de máscara y configuración del firewall necesarios para la convivencia de la “red antigua” con el nuevo planteamiento.

Debemos asegurarnos que al conectar algún switch al core nuevo el firewall sigue redireccionando el tráfico “de fuera de esa red”. De la misma manera se necesita que el DHCP reparta IPs a las diferentes VLANs según los rangos establecidos.

- Coordinación de la Configuración Switches.

Añadido a la electrónica de red planteada, una vez realizada la auditoría de red se consideró necesario la sustitución de 5 switches existentes que había repartidos por los diferentes despachos de las plantas de hospitalización, los cuales no eran gestionables.

Cada Switch de planta está configurado de la siguiente forma.

Se configuran las 12 primeras bocas PoE para los puntos de acceso, X número de bocas para equipos y Z número de bocas para impresoras, estas dos últimas en función del número de cada planta. El puerto 48 queda reservado para la gestión del switch.

A continuación se muestra como ejemplo la configuración de uno de los switches. En el Anexo 7 se incluye la configuración de la electrónica de red.

PLANTA 1 – 172.29.26.3

Modelo: HPE 1820 48G PoE+ (370W) Switch

Firmware instalado: PT.2.2

Conexión: HTTP

Login: XXXXX / Password YYYYYY

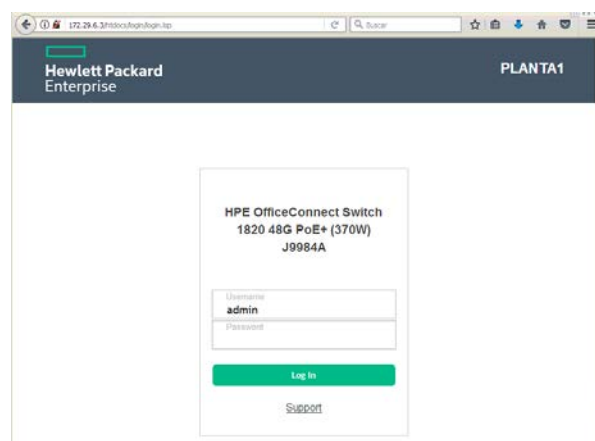


Figura 17

Configuración

- *Conexión a Distribución (fibra) Trunk 51 + 52 > tag a todas las vlan*
- *Conexión a DESPACHOS_PT1A (cobre) 13 > tag a vlans 20, 26, 27*
- *Conexión a DESPACHOS_PT1B (cobre) 14 > tag a vlans 20, 26, 27*
- *Boca de gestión (cobre) 48 > untag vlan 26*
- *Conexión a APs*
 - *VLAN 20 > bocas 1 a 12 untagged (DHCP)*
 - *VLAN 22 (WIFI_PRIVADO) > bocas 1 a 12 tagged*
 - *VLAN 50 (WIFI_PUBLICO) > bocas 1 a 12 tagged*
- *Spanning tree > Activado con configuración por defecto*

5. Cambio de IPs y máscaras a Equipos con IP estática (PCs e impresoras).

Muchos de los PCs e Impresoras tienen una IP fija, se deben identificar por plantas para posteriormente cambiar la IP y máscara correspondiente a sus VLANs

6. Cambio puerto a puerto de cables a nuevos Switches.

Esto supuso un proceso largo y en varias fases ya que se realiza en medio del servicio, se intentó minimizar el impacto de los cambios en la red.

7. Cambio servidores a su nueva VLAN.

Una vez realizado el cambio de cableado se procede a cambiar los servidores a sus nuevas VLAN y por lo tanto ubicándose en los nuevos rangos de IPs.

8. Coordinación y supervisión para deshabilitar de la “red Antigua”

172.29.7.50 – IP del CORE que modificaremos de la siguiente forma:

- a) En cuanto esté reconfigurada la Subnet Mask de 16 a 20, cambiaremos la IP a la 172.29.15.254
- b) En cuanto no haya ningún equipo en la VLAN1 esta IP y la VLAN1 se deshabilitarán completamente.

Paralelamente a las 4 últimas tareas de la auditoría de red pudimos ir avanzando con la implantación de la red WiFi.

- Conexión de los APs a los switches de planta.

Una vez configurados los switches con las VLANs según se ha comentado anteriormente, pudimos conectar los APs y comprobando que obtenían IP de su rango asignado.

En la Figura 18 se especifica la configuración de red de uno de los APs.

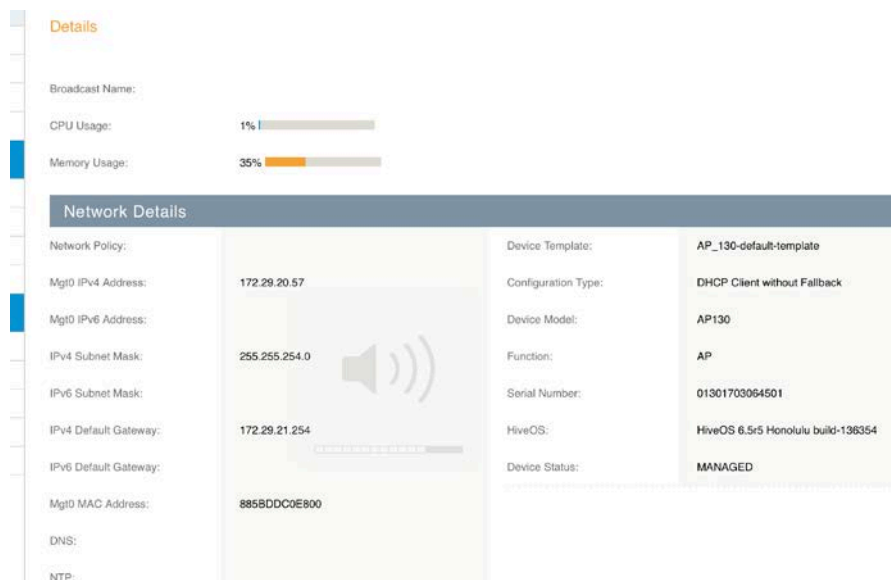


Figura 18

- Actualización de todos los puntos de acceso a sus últimas versiones de firmware. La Figura 19 muestra la manera de actualizar los APs desde el HiveManager.

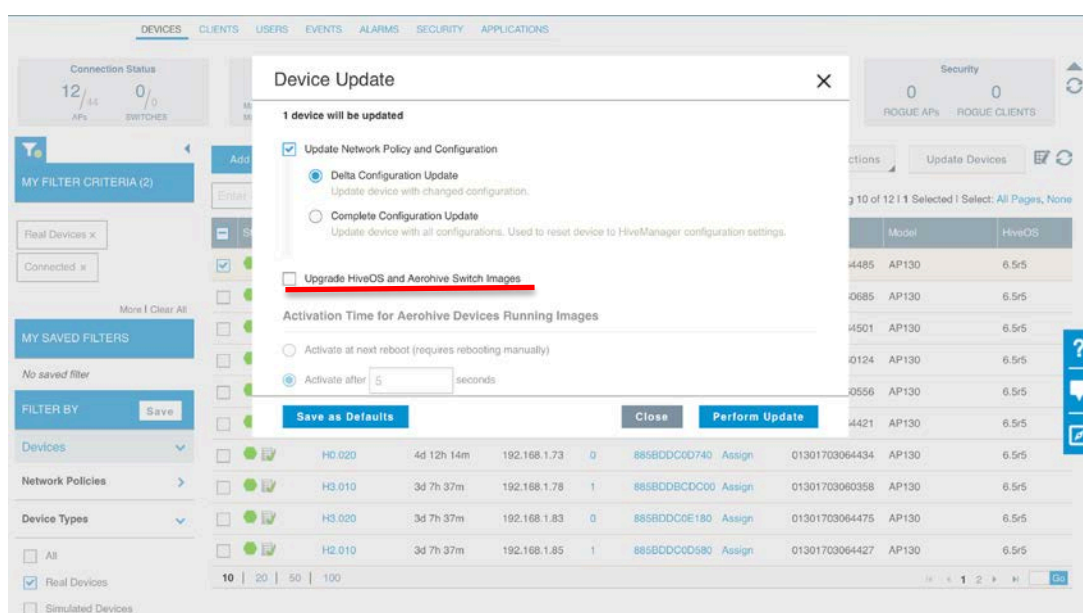


Figura 19

- Configuración de las redes en WiFi a través de HiveManager en función de lo definido.

Según las necesidades definidas en capítulos anteriores se definen 3 SSIDs a las que le aplicaremos sus correspondientes políticas.

Colectivo	Definido en APs	Red	Portal Cautivo	Tiempo Desconexión	Acceso Red HSJD	Active Directory	SSID
Área Residencia	Residencia / Dirección	Pública	No	-	No	No*	AAAAA "Residencia"
Pública	Todo	Pública	Sí	2h	No	No	BBBBB "Publica"
Dirección/ Privada / Profesional	Todo	Hospital	No	-	Sí	Sí	CCCCC "Profesional"

Figura 20

La siguiente imagen muestra cómo se configura una nueva Política de red y de SSIDs a través de HiveManager y la multitud de opciones que permite gestionar.

En la Figura 21 se puede ver la creación de la política donde se define de qué tipo es y el nombre que para identificar.

The screenshot shows the 'New Policy' configuration page in the Aerohive Networks interface. The navigation bar includes 'DASHBOARD', 'MONITOR', 'MAPS', 'CONFIGURE', and 'TROUBLESHOOT'. The 'CONFIGURE' tab is active, and the 'NETWORK POLICIES' sub-tab is selected. The page title is 'New Policy'. Below the title, there are tabs for 'Policy Details', 'Wireless Settings', 'Switch Settings', 'Additional Settings', and 'Deploy Policy'. The 'Policy Details' tab is currently active. The form asks 'What type of policy are you creating?' with two checked options: 'Wireless' and 'Switches'. Below this, it asks 'Please name your policy' and provides a text input field for 'Policy Name*' (containing 'Network Policy Name') and a larger text area for 'Description'. At the bottom of the page, there are 'Exit' and 'Next' buttons.

Figura 21

Una vez creada, se puede añadir SSIDs ya existentes en otras políticas o crear una nueva. En la Figura 22 se pueden seleccionar dos SSIDs ya creadas, de que tipo son y la VLAN que tienen asignada.

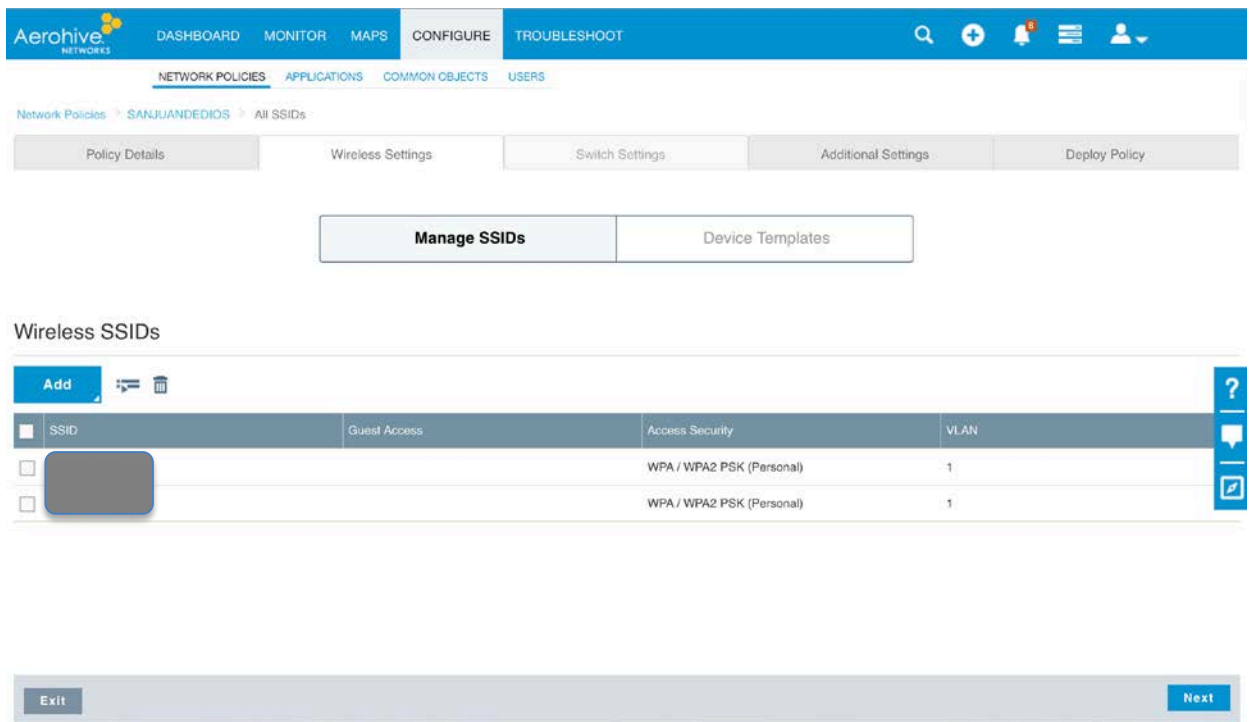


Figura 22

En la Figura 23 y Figura 24 se muestran las opciones para la creación de una nueva SSID, configuraciones de seguridad, accesos de Usuarios, etc...

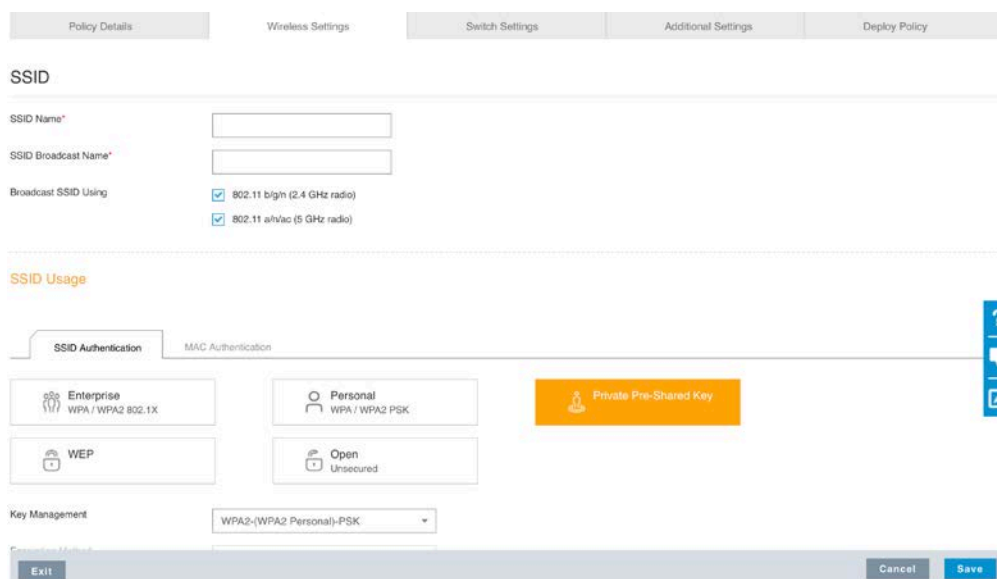


Figura 23

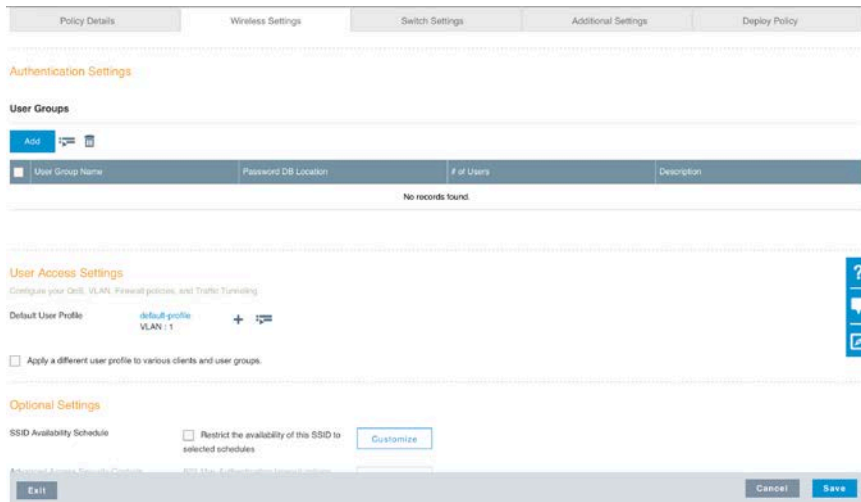


Figura 24

Deberemos tener en cuenta las siguientes configuraciones para las políticas de cada SSID:

1. Para la autenticación de Active Directory en la red interna será necesario montar el servidor RADIUS para que los Usuarios puedan identificarse contra el directorio activo de la misma manera que lo hacen en sus PCs.
2. Posibilidades WiFi publica:
 - a. Abierta con contraseña
 - b. Auto Registro (ID Manager. Solución de pago de Aerohive). Envía SMS's.
 - c. Banner Publicidad
 - d. PPSK (una clave por cada usuario)

En este caso, debido al alto volumen de usuarios y el breve tiempo de conexión se optará por una red abierta con contraseña común que se distribuirá de forma gráfica por el hospital.

- Configuración emisión informes con estadísticas de uso.
Mediante HiveManager configuraremos la emisión de reportes según interese al personal del hospital responsable del control de la red en un futuro.
Usuarios más activos, servicios más usados, puntos de acceso más saturados, etc.
- Por último se emitirá un informe con la configuración final del proyecto para incluirlo a la documentación del departamento de sistemas del Hospital.

CAPÍTULO 5. Resultados y Evaluación.

A fecha de redacción de esta memoria no está implantada la red de manera completa debido al retraso ocasionado por los imprevistos sucedidos.

Sin embargo se procederá al despliegue completo en los próximos días.

A día de hoy, de todo lo analizado, diseñado e implementado está operativo lo siguiente:

El Hospital ya dispone de un CPD nuevo, con servidores virtualizados operativo al tiempo completo. Dispone de fibra hasta cada una de las plantas tanto desde el antiguo armario de comunicaciones como desde el nuevo CPD. Este armario de comunicaciones ubicado en el Área 4 sigue en funcionamiento hasta que haya un traslado completo a la “red nueva”.

Ha quedado instalada y configurada según lo explicado en el capítulo anterior toda la electrónica de red. Ésta electrónica ya está en funcionamiento coexistiendo con la “red antigua” gracias a los cambios de configuración realizados tanto en los switches del core como en el Firewall, siendo posible así gestionar el tráfico externo e interno.

Se han instalado diferentes armarios rack consiguiendo así separar físicamente también la nueva infraestructura y cableado. Aspecto muy importante debido al mal estado en el que se encontraba el existente.

Han quedado instalados 44 puntos de acceso distribuidos por todo el Hospital según los planos adjuntados en esta memoria. Todos los puntos de acceso son visibles y ubicado en el techo.

Ahora mismo coexisten dos redes, la llamada “red antigua” no dimensionada, ubicada en el rango 172.29.0.1 – 172.29.15.254, y la nueva red definida mediante VLANs anteriormente indicadas. Gracias al enrutamiento que hace el firewall y el switch del CPD el tráfico de ambas redes puede comunicarse. Este punto ha sido crítico en el desarrollo del proyecto, ha sufrido muchas modificaciones y han sido necesarias numerosas pruebas para llegar al punto en el que todo funcione sin ninguna incidencia, siempre teniendo en cuenta que la red del Hospital no puede dejar de funcionar en ningún momento, es un entorno crítico.

Todos los equipos e impresoras han sido identificados y están conectados a la nueva electrónica de red y funcionando sin incidencias en todas las plantas. Esto ha supuesto el cambio manual de cada uno de los equipos e impresoras que tenían una IP fija configurada.

De los 44 puntos de acceso instalados, 10 están en funcionamiento pero todavía en la “red antigua”. Cabe destacar este punto.

En el momento que surgió el problema de la red existente del Hospital supuso que el proyecto de la red WiFi iba a demorarse un tiempo indeterminado. Esto no suponía daño alguno para los usuarios públicos, tampoco para el personal hospitalario ya que hasta ese momento solo disponían de una red pública con acceso limitado a internet pero sin la posibilidad de acceder a ninguna dirección interna del Hospital. Sin embargo los usuarios del Área 2 Residencia, son un colectivo que vive en esas instalaciones y su conexión depende de la red WiFi que dispusieran. No se podía permitir un retraso tan grande a estos usuarios. Se decidió en ese momento configurar los 10 puntos de acceso ubicados en esa área con una política de red de usuario y contraseña como tenían hasta ahora y en la “red antigua”.

En la Figura 25 se puede ver la conexión de los puntos de acceso todavía con IPs del rango anterior.

Status	Host Name	Uptime	IPv4	Clients	MAC	Location	Serial #	Model	HiveOS
<input type="checkbox"/>	H0.010	3d 9h 46m	192.168.1.76	0	885BDDC0E400	Assign	01301703064485	AP130	6.5r5
<input type="checkbox"/>	D1.010	3d 9h 46m	192.168.1.82	0	885BDD8D2DC0	Assign	01301703060685	AP130	6.5r5
<input type="checkbox"/>	D1.020	3d 9h 46m	192.168.1.79	0	885BDD8D0D80	Assign	01301703060556	AP130	6.5r5
<input type="checkbox"/>	H2.020	3d 9h 46m	192.168.1.86	0	885BDDC0D400	Assign	01301703064421	AP130	6.5r5
<input type="checkbox"/>	H0.020	4d 14h 23m	192.168.1.73	0	885BDDC0D740	Assign	01301703064434	AP130	6.5r5
<input type="checkbox"/>	H3.010	3d 9h 46m	192.168.1.78	1	885BDD8CDC00	Assign	01301703060358	AP130	6.5r5
<input type="checkbox"/>	H3.020	3d 9h 46m	192.168.1.83	0	885BDDC0E180	Assign	01301703064475	AP130	6.5r5
<input type="checkbox"/>	H2.010	3d 9h 46m	192.168.1.85	2	885BDDC0D580	Assign	01301703064427	AP130	6.5r5
<input type="checkbox"/>	H1.020	3d 9h 46m	192.168.1.80	2	885BDD8CCE480	Assign	01301703060392	AP130	6.5r5
<input type="checkbox"/>	H1.010	3d 9h 46m	192.168.1.77	0	885BDD8CCA40	Assign	01301703060287	AP130	6.5r5

Figura 25

En la Figura 26 tenemos una visión global de las aplicaciones visitadas en el periodo de tiempo seleccionado.

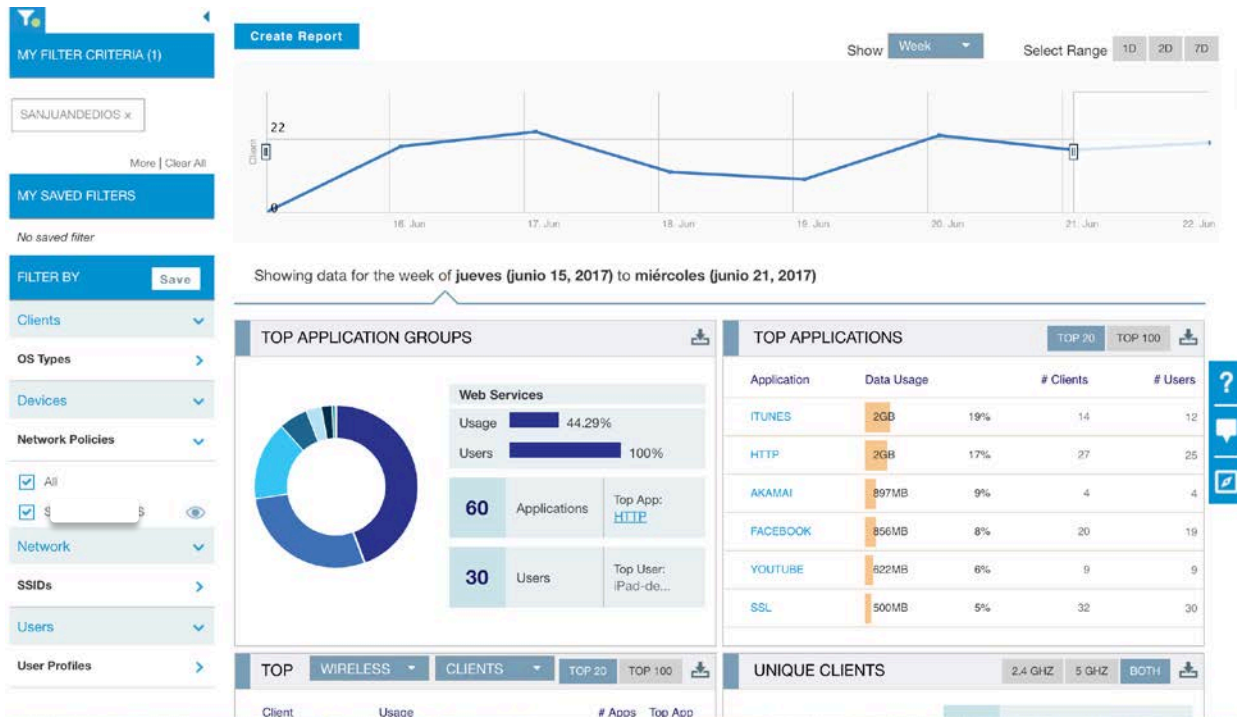


Figura 26

La Figura 27 y Figura 28 muestran información de los clientes conectados y características de sus conexiones y dispositivos.



Figura 27



Figura 28

Han quedado definidas las 3 SSIDs que se enviarán a los puntos de acceso en la puesta en marcha completa de la red WiFi que se llevará a cabo en los próximos días

Queda pendiente la migración de servidores a las nuevas IPs, que se realizará en 3 fases para minimizar el impacto en el hospital. Una vez obtengan las IPs correspondientes a su VLAN y se compruebe el funcionamiento completo de todos los servicios se hará lo mismo con el CPD principal y por lo tanto se podrá realizar la supresión de la VLAN1 y con ello la "red antigua".

CAPÍTULO 6. Conclusiones y Líneas Futuras

6.1 Conclusiones

El objetivo de este TFG era el análisis, diseño e implementación de una red WiFi profesional en un centro hospitalario.

Debido al estado de la red existentes los cambios sufridos han sido mucho mayores.

La infraestructura de red que había así como la topología de red no eran las adecuadas para la implantación de la red WiFi por lo que se ha tenido que ampliar el objetivo en medio del desarrollo del proyecto.

Finalmente el trabajo ha sido el diseño de una red completa así como la incorporación de una red WiFi profesional.

Según los objetivos planteados:

- Se ha analizado la red WiFi existente del Hospital antes del comienzo del proyecto.
- Mediante diversas reuniones e intercambios de información se han determinado las necesidades reales del Hospital en cuando a red WiFi y movilidad.
- Se han establecido los tipos de usuarios y servicios que debe soportar la red WiFi.
- Se han definido las redes o SSIDs necesarios a implantar para establecer las políticas de grupo adecuadas para los diferentes usuarios.
- Se ha configurado la red de manera que permita una movilidad total al personal del centro hospitalario, situación que anteriormente era imposible
- Con la limitación de ancho de banda que todavía existe se ha proporcionado a los usuarios una red WiFi pública como servicio añadido en el hospital.
- A través de una valoración técnica y económica se ha instalado un equipamiento profesional que cumple las especificaciones técnicas y de seguridad que se planteaban como objetivo.
- Se ha diseñado una red WiFi profesional preparada para soportar la incorporación de dispositivos de toma de constantes en paciente con envío inalámbrico.

Debido a las circunstancias surgidas durante el proyecto se han alcanzado objetivos que no estaban planteados en un inicio como es el cambio de topología de red, la implantación de nueva electrónica de red, creación de VLANs y direccionamiento de red.

6.1.1 Beneficios Personales del Trabajo.

Los conocimientos adquiridos tras este trabajo son de gran valor para mi formación.

He podido comprobar que el trabajo que uno va a realizar nunca es aislado, y menos en el entorno tecnológico en el que nos movemos.

- Trabajo en grupo con los beneficios y las responsabilidades que ello conlleva. Tu trabajo repercute en las tareas de otros y viceversa.
- Responsabilidad y empatía queda demostrado que son dos puntos clave en la relación laboral que se establece con el cliente.
- La capacidad de adaptación ante diferentes problemas y modificaciones que pueden surgir es de vital importancia para llevar a cabo con éxito el objetivo planteado.
- La continua formación reflejada en el constante aprendizaje de nuevas tecnologías, protocolos y configuraciones.
- Cambio experimentado al pasar del entorno educativo de la Universidad al ámbito profesional conlleva tomas de decisiones y con ello responsabilidades de las que anteriormente estábamos exentos.

6.2 Líneas futuras

El fin de la implantación de esta red WiFi profesional quedaba englobada en un proyecto de renovación tecnológica completa.

Éste fin era el de dar servicio a los distintos usuarios del Centro Hospitalario y establecer un entorno profesional para la llegada de numerosos dispositivos de tomas de datos.

Ésta es la línea futura más inmediata que se plantea. La gestión y control, no sólo de usuarios, sino de dispositivos que dan información en tiempo real de los pacientes del Hospital.

Podríamos plantear la creación de un nuevo SSID en la red hospitalaria para el acceso al almacenamiento de toda esta información que sería consultada de manera continua por multitud de usuario y que conllevaría un tráfico muy alto. La optimización de la gestión de este tráfico mediante las herramientas de HiveManager sería un objetivo a corto plazo que poder plantear.

Otra línea a desarrollar podría ser un proyecto de innovación después de implantar la infraestructura de red adecuada. Estudiar aportaciones innovadoras que implicaran utilizar dispositivos de bajo consumo, redes inteligentes, llevar a la realidad Internet de las Cosas; y con ello dar un valor añadido como Hospital Tecnológico.

Siguiendo esta última línea el objetivo final sería convertir en un Hospital Líquido. Un hospital “líquido” es un nuevo concepto que define a aquel hospital que va más allá de las paredes del centro y que busca implicar a pacientes y familiares, profesionales y sociedad en la creación de este nuevo concepto. Un hospital que aprovecha la Red y los caminos que marcan la Web social o 2.0.

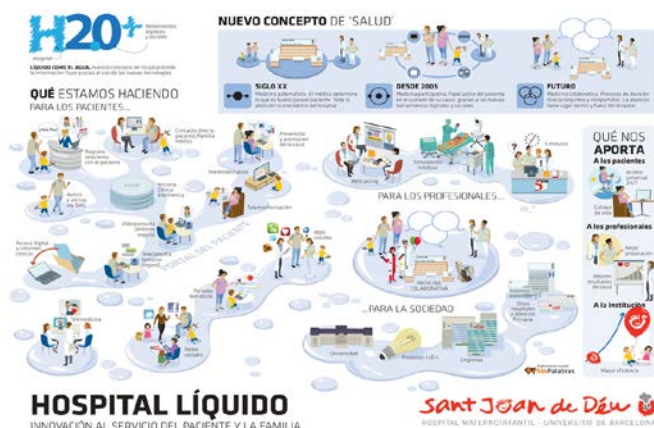


Figura 29

CAPÍTULO 7. Bibliografía

Estándar 802.11.

https://es.wikipedia.org/wiki/IEEE_802.11

<http://www.redes-wifi.es/tecnologia/ventajas-802-11n>

Aerohive

<http://www.aerohive.com/products/network-management/>

Aiwwave

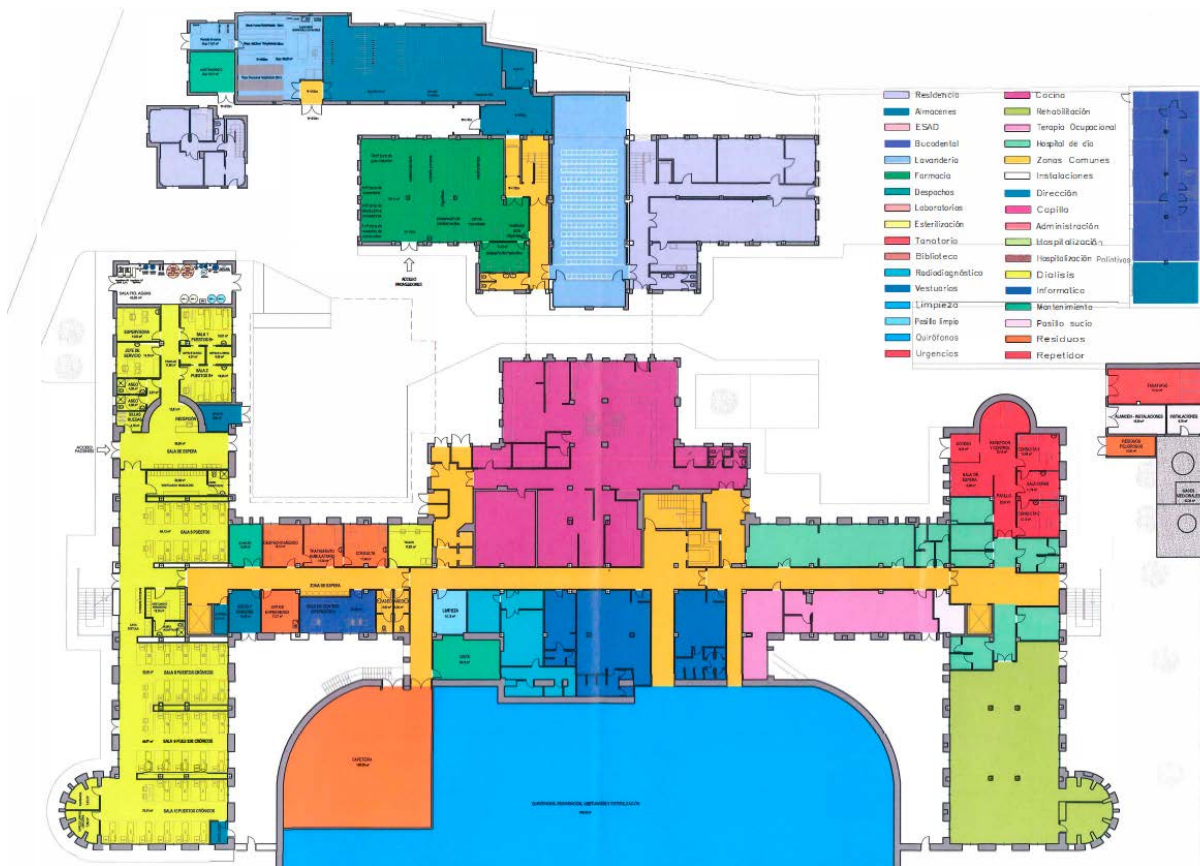
<http://www.arubanetworks.com/es/productos/productos-de-red/gestion/gestion-de-redes/>

Tecnología y Hospitales

<https://www.sjdhospitalbarcelona.org/es/innovacion>

Apéndices

Anexo 1. Planos Hospital



Planta 0



Planta 1

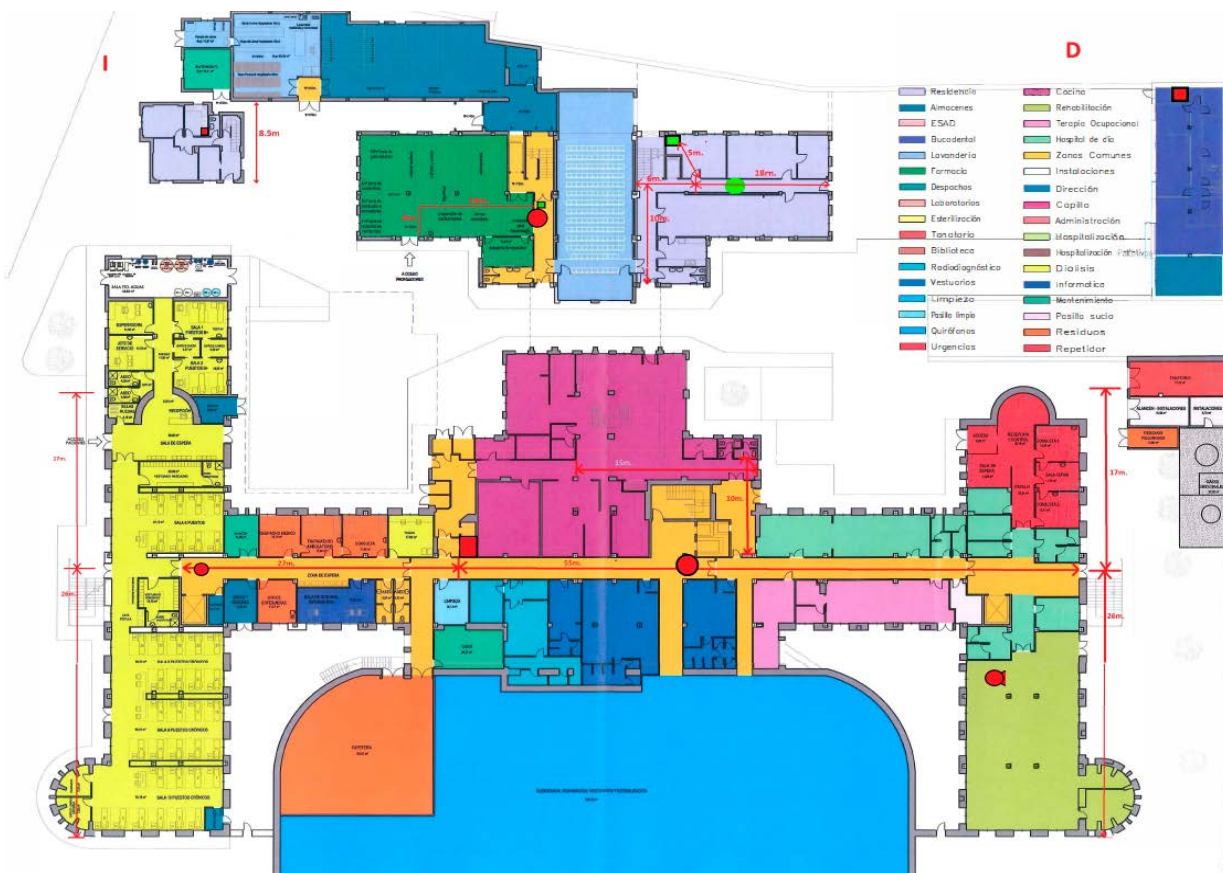


Planta 2



Planta 3

Anexo 2. Distribución de APs anterior al proyecto.



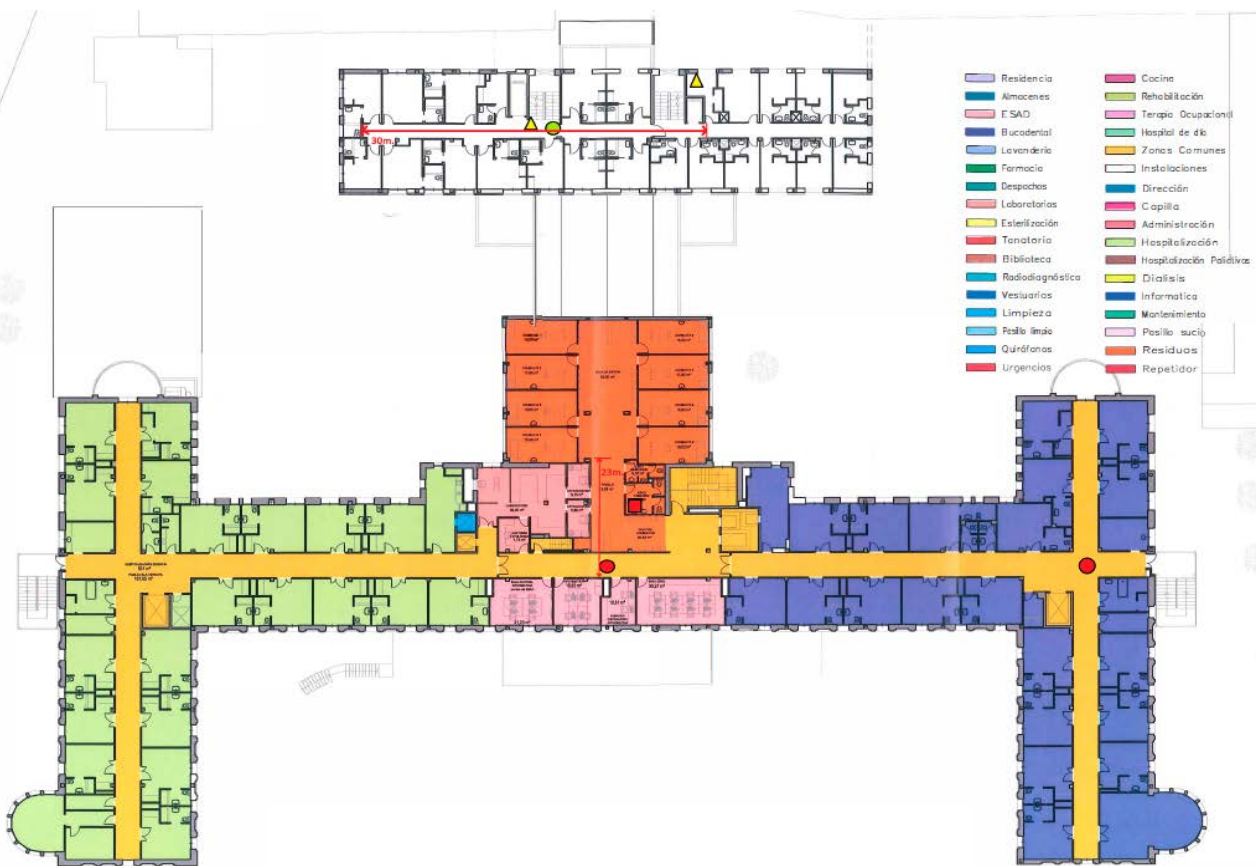
Planta 0



Planta 1

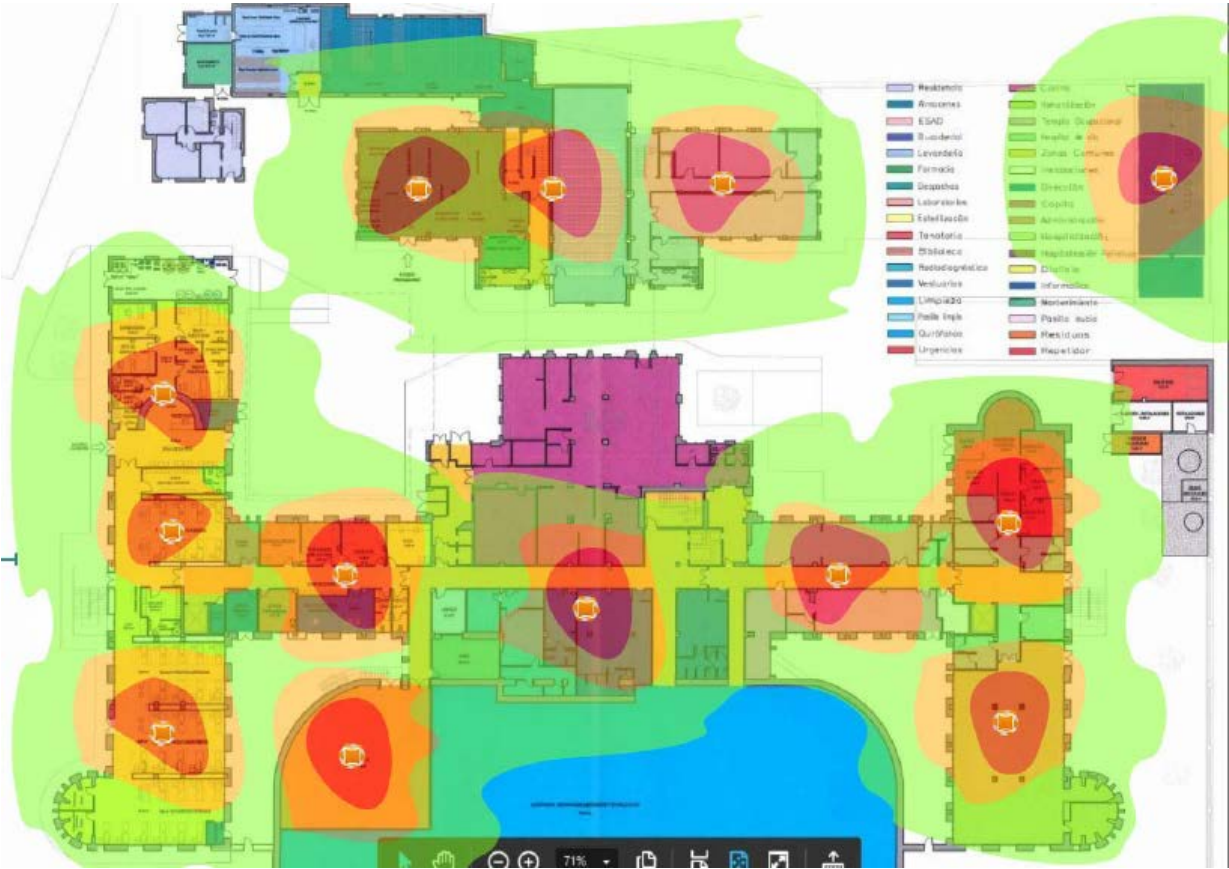


Planta 2

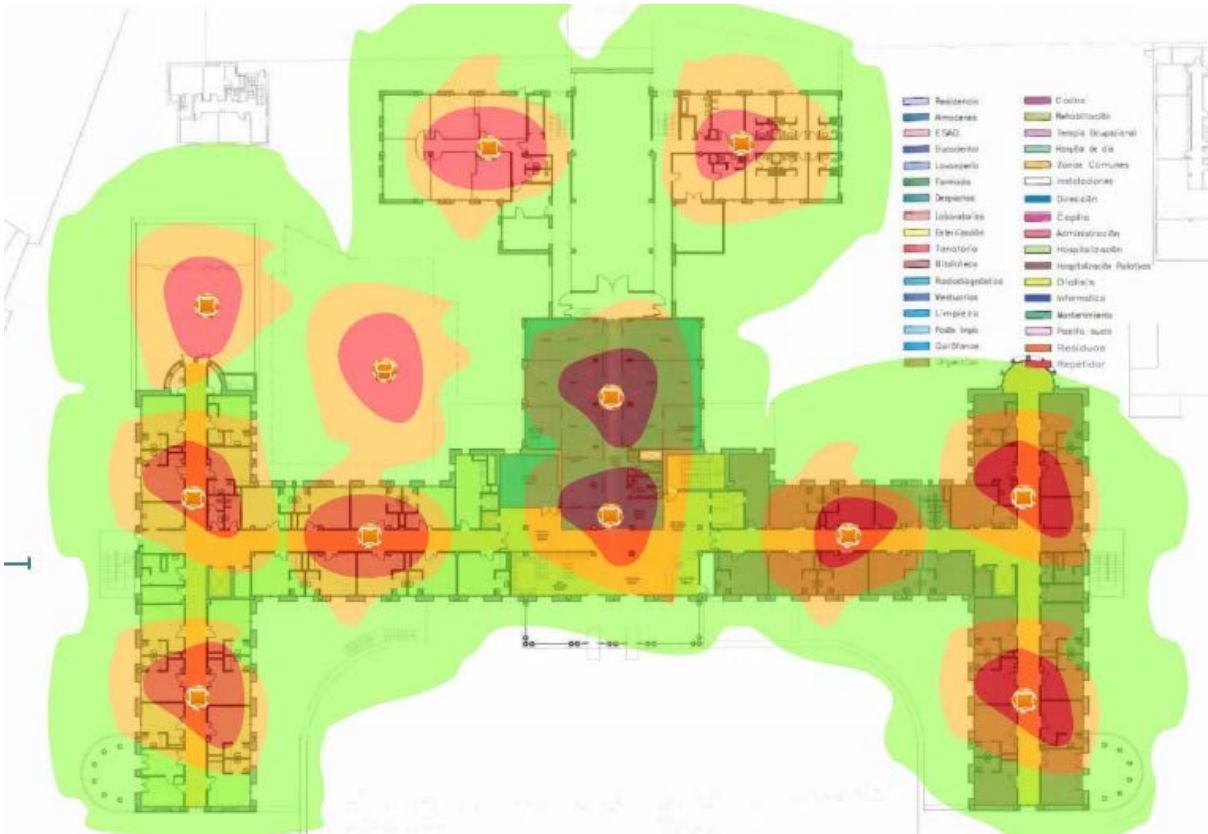


Planta 3

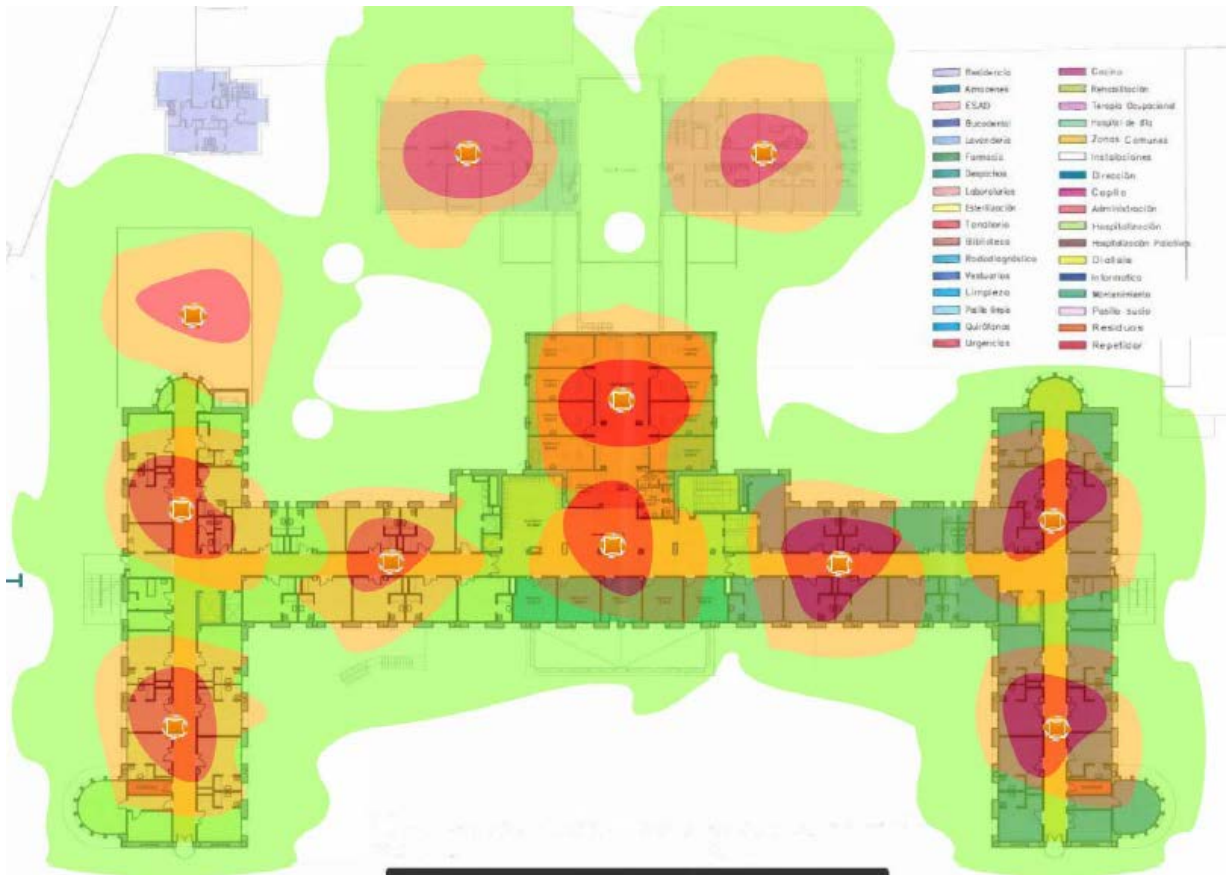
Anexo 3. Mapas de Cobertura.



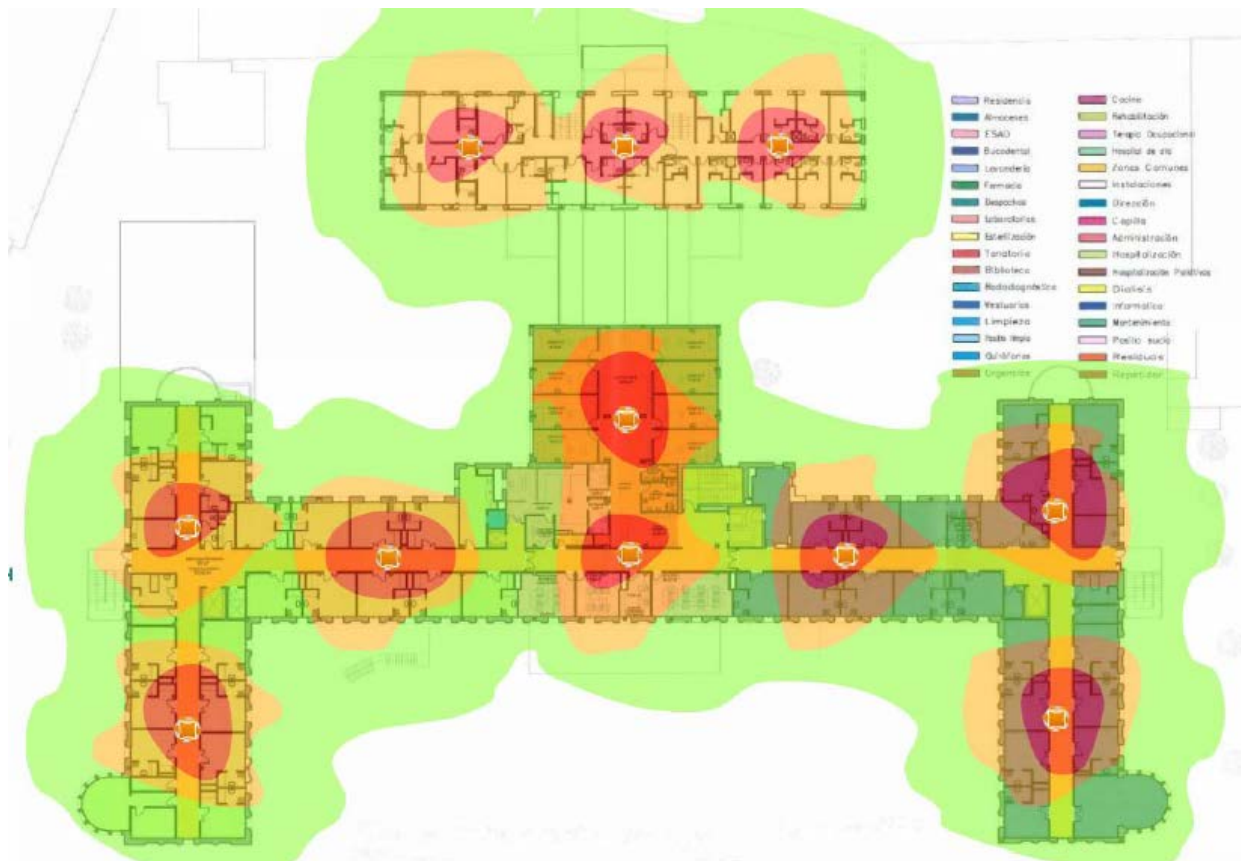
Planta 0



Planta 1



Planta 2



Planta 3

Anexo 4. Datasheet Equipos.

DATA SHEET

ARUBA INSTANT 205/ HP 205 INSTANT ACCESS POINT

Bringing 802.11ac to the masses



Multifunctional and affordable Instant 205 802.11ac wireless APs maximize mobile device performance in medium-density enterprise Wi-Fi environments.

These compact and cost-effective dual-radio APs deliver wireless data rates of up to 867 Mbps to 5-GHz devices with 802.11ac technology leveraging two spatial MIMO streams while simultaneously supporting 2.4-GHz 802.11n clients with data rates of up to 300 Mbps.

IAP-205 features four integrated omni-directional downtilt antennas.

UNIQUE BENEFITS

- Wi-Fi client optimization
 - To eliminate sticky client behavior while users roam, IAP-205 features patented ClientMatch™ technology, which continuously gathers session performance metrics from mobile devices.
 - If a mobile device moves away from an AP or if RF interference impedes performance, ClientMatch automatically steers the device to a better AP.
- Advanced Cellular Coexistence (ACC)
 - ACC lets WLANs perform at peak efficiency by minimizing interference from 3G/4G LTE networks, distributed antenna systems and commercial small cell/femtocell equipment.
- Quality of service for unified communication apps
 - IAP-205 supports priority handling and policy enforcement for unified communication apps, including Microsoft Lync with encrypted videoconferencing, voice, chat and desktop sharing.
- A single AP automatically distributes the network configuration to other Instant APs in the WLAN. Simply power-up one Instant AP, configure it over the air, and plug in the other APs – the entire process takes about five minutes.

SPECIFICATIONS

- 2.4-GHz (300 Mbps max rate) and 5-GHz (867 Mbps max rate) radios, each with 2x2 MIMO and four integrated omni-directional downtilt antennas.

ADVANCED FEATURES

- RF management
 - Adaptive Radio Management™ (ARM) technology automatically assigns channel and power settings, provides airtime fairness and ensures that APs stay clear of all sources of RF interference to deliver reliable, high-performance WLANs.
 - IAP-205 can be configured to provide part-time or dedicated air monitoring for spectrum analysis and wireless intrusion protection, VPN tunnels to extend remote locations to corporate resources, and wireless mesh connections where Ethernet drops are not available.
- Spectrum analysis
 - Capable of part-time or dedicated air monitoring, the spectrum analyzer remotely scans the 2.4-GHz and 5-GHz radio bands to identify sources of RF interference.
- Security
 - Integrated Trusted Platform Module (TPM) for secure storage of credentials and keys
 - SecureJack-capable for secure tunneling of wired Ethernet traffic.

OPERATING MODES

- Aruba Instant AP
- Air monitor (AM) for wireless IDS, rogue detection and containment
- Spectrum analyzer, dedicated or hybrid
- Secure enterprise mesh

WIRELESS RADIO SPECIFICATIONS

- AP type: Indoor, dual radio, 5-GHz 802.11ac and 2.4-GHz 802.11n 2x2:2
- Software-configurable dual radio supports 5 GHz (Radio 0) and 2.4 GHz (Radio 1)
- 2x2 MIMO with two spatial streams and up to 867 Mbps wireless data rate
- Support for up to 255 associated client devices per radio, and up to 16 BSSIDs per radio
- Supported frequency bands (country-specific restrictions apply):
 - 2.4000 GHz to 2.4835 GHz
 - 5.150 to 5.250 GHz
 - 5.250 to 5.350 GHz
 - 5.470 to 5.725 GHz
 - 5.725 to 5.850 GHz
- Available channels: Dependent on configured regulatory domain
- Dynamic frequency selection (DFS) optimizes the use of available RF spectrum
- Supported radio technologies:
 - 802.11b: Direct-sequence spread-spectrum (DSSS)
 - 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM)
- Supported modulation types:
 - 802.11b: BPSK, QPSK, CCK
 - 802.11a/g/n/ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
- Transmit power: Configurable in increments of 0.5 dBm
- Maximum (aggregate, conducted total) transmit power (limited by local regulatory requirements):
 - 2.4-GHz band: +21 dBm (18 dBm per chain)
 - 5-GHz band: +21 dBm (18 dBm per chain)
- Advanced Cellular Coexistence (ACC) minimizes interference from cellular networks
- Maximum ratio combining (MRC) for improved receiver performance
- Cyclic delay/shift diversity (CDD/CSD) for improved downlink RF performance
- Short guard interval for 20-MHz, 40-MHz and 80-MHz channels

- Space-time block coding (STBC) for increased range and improved reception
- Low-density parity check (LDPC) for high-efficiency error correction and increased throughput
- Transmit beamforming (TxBF) for increased reliability in signal delivery
- Supported data rates (Mbps):
 - 802.11b: 1, 2, 5.5, 11
 - 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
 - 802.11n: 6.5 to 300 (MCS0 to MCS15)
 - 802.11ac: 6.5 to 867 (MCS0 to MCS9, NSS = 1 to 2)
- 802.11n high-throughput (HT) support: HT 20/40
- 802.11ac very high throughput (VHT) support: VHT 20/40/80
- 802.11n/ac packet aggregation: A-MPDU, A-MSDU

ANTENNAS

Four integrated downtilt omni-directional antennas for 2x2 MIMO with maximum antenna gain of 4.0 dBi in 2.4 GHz and 6.0 dBi in 5 GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. The downtilt angle for maximum gain is approximately 30 degrees.

OTHER INTERFACES

- 10/100/1000BASE-T Ethernet network interface (RJ-45)
 - Auto-sensing link speed and MDI/MDX
 - 802.3az Energy Efficient Ethernet (EEE)
 - PoE-PD: 48 Vdc (nominal) 802.3af PoE
- DC power interface, accepts 1.7/4.0-mm center-positive circular plug with 9.5-mm length
- Visual indicators (LEDs):
 - Power/system status
 - Ethernet link status (ENET)
 - Radio status (two: RAD0, RAD1)
- Reset button: factory reset (during device power up)
- Serial console interface (RJ-45)
- Kensington security slot

POWER

- Maximum (worst-case) power consumption: 12.5 watts (PoE) or 11.7 watts (DC)
- Maximum (worst-case) power consumption in idle mode: 8.4 watts (PoE) or 7.7 watts (DC)
- Direct DC source: 12 Vdc nominal, +/- 5%
- Power over Ethernet (PoE): 48 Vdc (nominal) 802.3af-compliant source

- Power sources sold separately
- When both power sources are available, DC power takes priority

MOUNTING

- Included with AP:
 - Mounting brackets (2) for attaching to 9/16-inch or 15/16-inch T-bar drop-tile ceiling

MECHANICAL

- Dimensions/weight (unit, excluding mount accessories):
 - 150 mm x 150 mm x 41.5 mm (W x D x H)
 - 380 g
- Dimensions/weight (shipping):
 - 190 mm x 187 mm x 57 mm (W x D x H)
 - 550 g

ENVIRONMENTAL

- Operating:
 - Temperature: 0° C to +40° C (+32° F to +104° F)
 - Humidity: 5% to 95% non-condensing
- Storage and transportation:
 - Temperature: -40° C to +70° C (-40° F to +158° F)

REGULATORY

- FCC/Industry of Canada
- CE Marked
- R&TTE Directive 1995/5/EC
- Low Voltage Directive 72/23/EEC
- EN 300 328
- EN 301 489
- EN 301 893
- UL/IEC/EN 60950
- EN 60601-1-1 and EN 60601-1-2

For more country-specific regulatory information and approvals, please see your Aruba representative.

RELIABILITY

MTBF: 711,187 hours (81.2 years) at +25° C operating temperature

REGULATORY MODEL NUMBER

- APIN0205

CERTIFICATIONS

- CB Scheme Safety, cTUVus
- UL2043 plenum rating
- Wi-Fi Alliance (WFA) certified 802.11a/b/g/n/ac

WARRANTY

- Aruba limited lifetime warranty

MINIMUM SOFTWARE VERSIONS

- Aruba InstantOS™ 4.1.1.0

RF PERFORMANCE TABLE		
	Maximum transmit power (dBm) per transmit chain	Receiver sensitivity (dBm) per receive chain
2.4 GHz		
802.11b		
1 Mbps	18.0	-95.0
11 Mbps	18.0	-88.0
802.11g		
6 Mbps	18.0	-92.0
54 Mbps	16.0	-74.0
802.11n HT20		
MCS0/8	18.0	-91.0
MCS7/15	16.0	-71.0
802.11n HT40		
MCS0/8	18.0	-88.0
MCS7/15	16.0	-68.0
5 GHz		
802.11a		
6 Mbps	18.0	-93.0
54 Mbps	16.0	-75.0
802.11n HT20		
MCS0/8	18.0	-91.0
MCS7/15	15.0	-71.0
802.11n HT40		
MCS0/8	18.0	-88.0
MCS7/15	15.0	-68.0
802.11ac VHT20		
MCS0	18.0	-91.0
MCS9	12.0	-64.0
802.11ac VHT40		
MCS0	18.0	-88.0
MCS9	12.0	-61.0
802.11ac VHT80		
MCS0	18.0	-85.0
MCS9	12.0	-58.0

Maximum capability of the hardware provided. Maximum transmit power is limited by local regulatory settings.

Aerohive AP130

802.11ac Dual-Radio 2x2:2 access point with internal antennas designed for ultra-high density environments



The AP130 is an enterprise-grade, two radio (2x2) two stream MIMO 802.11ac Access Point, engineered with uncompromising performance for high capacity environments

AEROHIVE NETWORKS AP130 Enterprise access points provide a seamless transition to 802.11ac. With more users, more devices, more things, more applications, and strained infrastructure and budget, the AP130 is a powerful option to meet those challenges. Aerohive has built an AP for pervasive Wi-Fi prepared for ultra-high density environments, powerful enough to provide all the services needed for an enterprise network, and inexpensive enough to deploy for ultra-high capacity networks. The AP130 combines 2x2, 2-stream, 802.11ac Wi-Fi technology and advanced security and device lifecycle management together into a cost-optimized solution that allows you to deploy high speed Wi-Fi into every office or classroom.

Combining Aerohive innovative distributed Cooperative Control architecture with the powerful HiveOS operating system, coupled with the ability to provide full functionality on legacy PoE infrastructure, the AP130 maintains the Aerohive standard for cost-effective solution pricing that allows enterprises of all sizes to deploy capacity-oriented Wi-Fi networks. The AP130 provides an enterprise-class experience for all types of mobile devices, including legacy Wi-Fi types.

The AP130 provides high-performance data rates up to 876Mbps in the 5-GHz band. It supports dual concurrent 2.4GHz 802.11b/g/n and 5GHz 802.11a/n/ac radios.

Key Features and Benefits

Engineered for ultra-high density

Pervasive access – thousands of new devices, used in more places, storing more data, on new device types- BYOD, Consumerization of IT, wearables and IoT, high performance Wi-Fi, very-high client density, industry and government regulations, advanced applications and services – are no longer the exclusive domain of the large enterprise and are pretty much required by every organization. Companies of all sizes must accommodate every user laptop, personal devices, and in the very near future lighting, security, air conditioning, and other connected devices. The AP130 with the latest HiveOS incorporates the advanced software features required by every organization, including an integrated RADIUS server, DHCP server, Captive Web Portal, and automatic mesh for wireless network redundancy. Add the simplified management experience with Aerohive HiveManager, including auto-discovery and AP130 auto-provisioning experience, flexible network policies and AP-specific configurations and you get a powerful solution for any enterprise that's simple enough for any deployment.

Future-proof deployment

Upgrading your network to 802.11ac DOES NOT require you to upgrade your existing PoE infrastructure. Our advancements in energy efficiency allow the AP130 full 2-stream 802.11ac performance while using existing 802.3af PoE infrastructure. Improvements to the radio management protocol allow adding more access points to the network, such as an AP in every classroom for schools. AP130 features a thin, lightweight, sleek design for a very clean install. A TPM chip (Trusted Platform Module) provides hardware-based key and configuration encryption for added security.

Enterprise-Class Services

The AP130 supports granular location tracking for devices and a complete Application Visibility and Control functionality, including reporting, stateful firewall, and powerful Aerohive Quality of Service (QoS) which assures prioritization of the data traffic and data rate limits for different users, groups of users, and devices. The Aerohive Mobility Suite featuring Client Management, ID Manager, and Social Login applications take advantage of Aerohive's HiveOS that runs on the AP130 and extends management and control with simplified onboarding, management, and troubleshooting with context-based visibility, policies, and enforcement for the entire spectrum of client devices.

Warranty and Support

Every Aerohive Networks device is backed by a limited lifetime hardware warranty. Extended product and technical support may be purchased separately and can include next day advanced replacement, 24x7 or 8x5 technical support, web and email support access, and software updates. For complete support terms go to www.aerohive.com/support

Contact us today to learn how your organization can benefit from an Aerohive wireless LAN architecture.



Aerohive Networks, Inc.
330 Gibraltar Drive
Sunnyvale, California 94089 USA
phone 408.510.6100
toll-free 866.918.9918
fax 408.510.6199
www.aerohive.com

DS_AP130_0415_D1-5

Product Specifications

Radio Specifications—802.11a

- 5.150-5.950 GHz Operating Frequency
- Orthogonal Frequency Division Multiplexing (OFDM) Modulation
- Rates (Mbps): 54, 48, 36, 24, 18, 12, 9, 6 w/ auto fallback

Radio Specifications—802.11b

- 2.4-2.5 GHz Operating Frequency
- Direct-Sequence Spread-Spectrum (DSSS) Modulation
- Rates (Mbps): 11, 5.5, 2, 1 w/ auto fallback Rates (Mbps): 54, 48, 36, 24, 18, 12, 9, 6 w/ auto fallback

Radio Specifications—802.11g

- 2.4-2.5 GHz Operating Frequency
- Orthogonal Frequency Division Multiplexing (OFDM) Modulation
- Rates (Mbps): 54, 48, 36, 24, 18, 12, 9, 6 w/ auto fallback

Radio Specifications—802.11n

- 2.4-2.5 GHz & 5.150-5.950 GHz Operating Frequency
- 802.11n Modulation
- Rates (Mbps): MCS0 - MCS15 (6.5Mbps - 300Mbps)
- 2x2 Multiple-In, Multiple-Out (MIMO) Radio
- HT20 and HT40 High-Throughput (HT) Support
- A-MPDU and A-MSDU Frame Aggregation

Radio Specifications—802.11ac

- 5.150-5.950 GHz Operating Frequency
- 802.11ac Modulation (256-QAM)
- Rates (Mbps): MCS0 - MCS9 (6.5Mbps - 867 Mbps), NSS = 1-2
- 2x2.2 Stream Multiple-In, Multiple-Out (MIMO) Radio • VHT20/ VHT40/VHT80 support

Antennas

- 4x internal antennas (2x2.4GHz and 2x5GHz)

Interfaces

- Autosensing 10/100/1000 Base-T Ethernet PoE (Power over Ethernet 802.3af) Port

Physical

- LxWxH 147X147X42 mm (5.79x5.79x1.65in); w/b mounting brackets
- 51kg (113 lbs) w/b brackets

Environmental

- Operating: 0 to +40°C, Storage: -40 to +70°C
- Humidity: 95%

Environmental Compliance

- UL2043

Power Specifications

- IEEE 802.3af PoE Power

Power Options

- 802.3af Power over Ethernet (PoE) capable Gigabit Ethernet port (RJ-45 power input pins: Wires 4,5,7,8 or 1,2,3,6)
- 802.3af Power over Ethernet injector

Mounting

- Desktop
- Wall Mount included as part of AP
- Built-in slot for Kensington type locks
- Ceiling Tile flush 15/16" and Wall Mount locking accessory included with AP

Accessories Sold Separately

- Ceiling Tile Recessed 15/16", 3/8", 9/16" sold as an accessory
- Ceiling Tile flush 3/8", 9/16" sold as an accessory
- Suspend Mount sold as an accessory
- Plenum Mount sold as an accessory

SKU

Ambiwi Access Point	
AH-AP-130-AC-FCC	AP130, indoor rated, 2 radio 2x2 802.11a/b/g/n/ac, 1 10/100/1000, FCC regulatory domain, without POE injector
AH-AP-130-AC-W	AP130, indoor rated, 2 radio 2x2 802.11a/b/g/n/ac, 1 10/100/1000, configurable regulatory domain, without POE injector

Features & Benefits

Flexible Hardware Platform

- Small, light weight intuitive design.
- Two radios provide concurrent 802.11a/n/ac and 802.11b/g/n connections with no degradation in performance
- Automatic or dedicated mesh backup
- Full 802.11ac performance with IEEE 802.3af power

Advanced Features

- Integrated application visibility and control (AVC)
- On-device RADIUS Switch directory support, Captive, Web Portal, DHCP server, and spectrum analysis - Max 256 concurrent RADIUS authenticated users
- Max 512 DHCP clients per AP

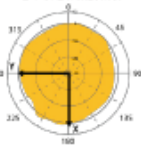
Hardware Assisted Features

Security

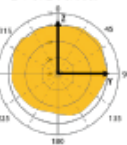
- Trusted Platform Module (TPM)—Hardware-based key storage and encryption
- Wireless privacy & authentication Wi-Fi CERTIFIED WPA and WPA2, 802.11i, WEP, 802.1x, PSK
- Granular user profile-based management defines QoS, mobility policies, and security policies for each user that enters the network
- Encryption: AES-CCMP, TKIP, and RC4 (WEP only)
- Marking and policing—WMM (802.11e) for wireless
- 802.1p and/or DiffServ
- Wi-Fi CERTIFIED WMM
- WMM power save (U-APSD)

RF Coverage Maps

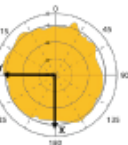
2.4 GHz Horizontal



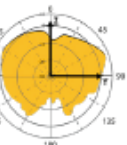
2.4 GHz Vertical



5 GHz Horizontal



5 GHz Vertical



Power & Sensitivity Table

Power shown is per transmit chain and is a maximum power that the radio is capable of, power limits will be limited by local radio regulations.

Rate	2.4GHz		5GHz		Rate	2.4GHz		5GHz	
	TX Power	RX Sensitivity	TX Power	RX Sensitivity		TX Power	RX Sensitivity	TX Power	RX Sensitivity
802.11a					802.11ac VHT40				
6 Mbps - 24 Mbps			19	-94, -86	MCS 0	20	-94	19	-93
36 Mbps			18	-82	MCS 1	20	-91	19	-89
48 Mbps			17	-78	MCS 2	20	-89	19	-87
54 Mbps			16	-77	MCS 3	20	-86	19	-84
802.11b					MCS 4				
1 Mbps	21	-99			MCS 5	20	-78	18	-76
2 Mbps	21	-97			MCS 6	18	-76	16	-75
5.5 Mbps	21	-94			MCS 7	17	-73	15	-73
11 Mbps	21	-91			MCS 8	16	-70	13	-69
802.11g					MCS 9				
6 Mbps - 24 Mbps	20	-95, -86			802.11ac VHT40				
36 Mbps	18	-82			MCS 0	20	-91	19	-90
48 Mbps	17	-78			MCS 1	20	-88	19	-87
54 Mbps	16	-77			MCS 2	20	-85	19	-85
802.11n HT20					MCS 3				
MCS 0, 1, 2, 3, 4, 8, 9, 10, 11, 12	20	-94, -81	19	-93, -81	MCS 4	20	-79	19	-78
MCS 5, 13	18	-77	18	-76	MCS 5	20	-75	18	-74
MCS 6, 14	17	-74	17	-75	MCS 6	18	-73	16	-72
MCS 7, 15	16	-74	16	-73	MCS 7	17	-72	15	-71
802.11n HT40					MCS 8				
MCS 0			19	-93	MCS 9	13	-65	12	-64
MCS 1			19	-90	802.11ac VHT80				
MCS 2			19	-88	MCS 0			19	-87
MCS 3			19	-84	MCS 1			19	-84
MCS 4			18	-81	MCS 2			19	-81
MCS 5			17	-77	MCS 3			19	-78
MCS 6			16	-75	MCS 4			19	-75
MCS 7			14	-74	MCS 5			18	-70
MCS 8			19	-90	MCS 6			16	-69
MCS 9			19	-87	MCS 7			15	-68
MCS 10			19	-85	MCS 8			13	-63
MCS 11			19	-81	MCS 9			12	-61
MCS 12			18	-78					
MCS 13			17	-74					
MCS 14			16	-72					
MCS 15			14	-71					

Anexo 5. Datasheet Equipos Electrónica de Red.

Data sheet

HP 1820 Switch Series



Key features

- Customized operation using intuitive Web interface
- Flexible deployment options including wall, under table, and desktop mounting
- 24- and 48-port models include SFP ports
- 8-, 24- and 48-port non-PoE+ models are fanless for quiet operation
- Limited Lifetime Warranty 2.0

Product overview

HP 1820 Switch Series devices are basic, smart-managed, fixed-configuration Gigabit Ethernet Layer 2 switches designed for small businesses looking for key features in an easy-to-administer solution.

The series consists of six switches including 8-, 24- and 48-port Gigabit Ethernet switches and 8-, 24-, and 48-port Gigabit PoE+ models each providing non-blocking Gigabit per port performance. Some models include SFP ports for fiber connectivity and some are fanless, making them ideal for office deployments. All 1820 Switches support flexible installation options, including mounting on wall, under table, or on desktop. The 8-port Gigabit Ethernet model can be powered by an upstream Power over Ethernet (PoE) switch for environments where no line power is available.

These Gigabit switches are plug-and-play out of the box, yet network operation can be fine-tuned through features available from a simple Web browser-based GUI, if necessary. Customizable features include VLANs, Rapid Spanning Tree, IGMP Snooping, link aggregation trunking, and DSCP QoS policies. All models include the latest energy-saving capabilities, including Energy Efficient Ethernet (EEE) and idle-port power down.

Features and benefits Management

- Simple Web management

Allows for easy management of the switch—even by nontechnical users—through an intuitive Web GUI; supports HTTP and HTTP Secure (HTTPS)

- SNMPv1, v2c

Enable devices to be discovered and monitored from an SNMP management station

- Port mirroring

Enables traffic on a port to be simultaneously sent to a network analyzer for monitoring

- Dual flash images

Provide independent primary and secondary operating system files for backup while upgrading

- Network Time Protocol (NTP)

Synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network

- Manual network time configuration

Manually set the date and time on the switch in the absence of an NTP server

- Default DHCP client mode

Allows the switch to be directly connected to a network, enabling plug-and-play operation; in the absence of a DHCP server on the network, the switch falls back to a default, fixed IP address

Quality of service (QoS)

- Traffic prioritization

Provides time-sensitive packets (like VoIP and video) with priority over other traffic based on DSCP or IEEE 802.1p classification; packets are mapped to eight hardware queues for more effective throughput

- Broadcast control

Allows limiting of broadcast traffic rate to reduce unwanted network broadcast traffic

- IEEE 802.1p/Q

Delivers data to devices based on the priority and type of traffic; supports IEEE 802.1Q

Connectivity

- Auto-MDI/MDIX

Automatically adjusts for straight through or crossover cables on all ports

- IEEE 802.3X Flow Control

Provides a flow throttling mechanism propagated through the network to prevent packet loss at a congested node

- Loop protection

If the switch detects a loop, it disables the source port from forwarding data packets originating from the switch to avoid broadcast storms

- SFP ports for fiber connectivity

Provides fiber connections for uplinks and other connections across longer distances than copper cabling can support; SFP ports are in addition to available copper Ethernet ports, providing a higher total number of available ports. SFP ports available on 24- and 48 port models

- IEEE 802.3af PoE-powered device option

Obtains power provided by a standard PoE device connected to port 1; deploy the switch wherever an Ethernet cable can reach as a power outlet is not needed (8-port GbE non-PoE+ model only)

- IEEE 802.3at Power over Ethernet (PoE+)

Provides up to 30 W per port, which allows support of the latest PoE+-capable devices such as IP phones, wireless access points, and security cameras, as well as any IEEE 802.3af-compliant end device; lowers the cost of additional electrical cabling and circuits that would otherwise be necessary in IP phone and WLAN deployments

- PoE+ port availability

Ports 1–4 provide PoE+ on the HP 1820-8G-PoE+ (65W) switch; ports 1–12 provide PoE+ on the HP 1820-24G-PoE+ (180W) switch; ports 1–24 provide PoE+ on the HP 1820-48G-PoE+ (370W) switch

- Auto-PoE power configuration

The switch automatically assigns the required power to a port for a PD device based on Link Layer Discovery Protocol (LLDP). Optionally, the switch permits manual, per port, PoE power configuration

- PoE shutdown mode

A PoE scheduler provides the ability to define the hours of PoE power being supplied to a group of switch ports based on a 24-hour day. The scheduler enables the flexibility to select individual days of a week as well as reoccurrence on a weekly basis with a start and end date.

- Energy Efficient Ethernet

Compliant with IEEE 802.3az standard requirements to save energy during periods of low data activity

- Auto-port shutdown

The switch saves power by automatically shutting down power to inactive ports. Power is restored on a port upon link detection

- Energy savings status

The switch provides an estimated cumulative energy savings due to green Ethernet features being enabled

Security

- Secure Sockets Layer (SSL)

Encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch

- Automatic denial-of-service protection

Monitors nine types of malicious attacks and protects the network by blocking these attacks.

- Management password

Provides security so that only authorized access to the Web browser interface is allowed

Performance

- Half-/full-duplex auto-negotiating capability on every port doubles the throughput of every port

- IGMP snooping

Improves network performance through multicast filtering, instead of flooding traffic to all ports

Layer 2 switching

- VLAN support and tagging

Supports up to 64 port-based VLANs and dynamic configuration of IEEE 802.1Q VLAN tagging, providing security between workgroups

- Jumbo packet support

Improves the performance of large data transfers; supports frame size of up to 9,220 bytes

HP 1820 Switch Series

Specifications (continued)



	HP 1820-24G-PoE+ (185W) Switch (J9983A)	HP 1820-48G Switch (J9981A)	HP 1820-48G-PoE+ (370W) Switch (J9984A)
I/O ports and slots	12 RJ-45 autosensing 10/100/1000 PoE+ ports; Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 12 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 2 SFP 100/1000 Mbps ports (IEEE 802.3z Type 100BASE-X, IEEE 802.3u Type 100BASE-FX) Supports a maximum of 24 autosensing 10/100/1000 ports plus 2 SFP ports	48 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 4 SFP 100/1000 Mbps ports (IEEE 802.3z Type 100BASE-X, IEEE 802.3u Type 100BASE-FX) Supports a maximum of 48 autosensing 10/100/1000 ports plus 4 SFP ports	24 RJ-45 autosensing 10/100/1000 PoE+ ports; Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 24 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 4 SFP 100/1000 Mbps ports (IEEE 802.3z Type 100BASE-X, IEEE 802.3u Type 100BASE-FX) Supports a maximum of 48 autosensing 10/100/1000 ports plus 4 SFP ports
Physical characteristics			
Dimensions	17.42(w) x 9.69(d) x 1.73(h) in (44.25 x 24.61 x 4.39 cm) (1U height)	17.42(w) x 9.69(d) x 1.73(h) in (44.25 x 24.61 x 4.39 cm) (1U height)	17.42(w) x 12.7(d) x 1.73(h) in (44.25 x 32.26 x 4.39 cm) (1U height)
Weight	7.3 lb (3.31 kg)	7.3 lb (3.31 kg)	9.7 lb (4.4 kg)
Memory and processor	ARM Cortex-A9 @ 400 MHz, 128 MB SDRAM, 16 MB flash; packet buffer size: 1.5 MB	ARM Cortex-A9 @ 400 MHz, 128 MB SDRAM, 16 MB flash; packet buffer size: 1.5 MB	ARM Cortex-A9 @ 400 MHz, 128 MB SDRAM, 16 MB flash; packet buffer size: 1.5 MB
Performance			
100 Mb Latency	< 7 μs (LIFO 64-byte packets)	< 7 μs (LIFO 64-byte packets)	< 7 μs (LIFO 64-byte packets)
1000 Mb Latency	< 2 μs (LIFO 64-byte packets)	< 2 μs (LIFO 64-byte packets)	< 2 μs (LIFO 64-byte packets)
Throughput	up to 38.6 Mpps (64-byte packets)	up to 77.3 Mpps (64-byte packets)	up to 77.3 Mpps (64-byte packets)
Switching capacity	52 Gbps	104 Gbps	104 Gbps
MAC address table size	8000 entries	16000 entries	16000 entries
Reliability			
MTBF (years)	64.52	61.73	45.05
Environment			
Operating temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Operating relative humidity	15% to 95% @ 104°F (40°C)	15% to 95% @ 104°F (40°C)	15% to 95% @ 104°F (40°C)
Nonoperating/Storage temperature	-40°F to 70°F (-40°C to 21.1°C)	-40°F to 158°F (-40°C to 70°C)	-40°F to 158°F (-40°C to 70°C)
Nonoperating/Storage relative humidity	15% to 95% @ 140°F (60°C)	15% to 95% @ 140°F (60°C)	15% to 95% @ 140°F (60°C)
Altitude	up to 9,842 ft (3 km)	up to 9,842 ft (3 km)	up to 9,842 ft (3 km)
Acoustic	Power: 0 dB no fan	Power: 0 dB no fan	Power: 45 dB



HPE OfficeConnect 1920 Switch Series



Key features

- Customized operation using intuitive Web Interface
- Layer 3 static routing with 32 routes for network segmentation and expansion
- Access control lists for granular security control
- Spanning Tree Protocol: STP, RSTP, and MSTP
- HPE Limited Lifetime warranty

Product overview

The HPE OfficeConnect 1920 Switch Series consists of advanced smart-managed fixed-configuration Gigabit switches designed for small businesses in an easy-to-administer solution. By utilizing the latest design in silicon technology, this series is one of the most power efficient in the market.

The series has 9 switches: four non-PoE models and five PoE+ models. All models are equipped with additional Gigabit SFP ports for fiber connectivity. The 8-, 24- and 48-port PoE+ models are available with PoE or without PoE.

The series is part of the OfficeConnect portfolio of Hewlett Packard Enterprise small business networking products. These switches provide a great value, and includes features to satisfy even the most advanced small business networks. All models support rack mounting or desktop operation. Customizable features include basic Layer 2 features like VLANs and link

aggregation, as well as advanced features such as Layer 3 static routing, IPv6, ACLs, and Spanning Tree Protocols. HPE OfficeConnect 1920 Switch Series includes a Limited Lifetime Warranty. This warranty provides advance hardware replacement with next business day shipment in most countries, limited 24x7 telephone support available from HPE for the first 90 days, and limited electronic and business hours telephone support is available from HPE for the entire warranty period.

Features and benefits

Management

- Simple Web management
 - Allows for easy management of the switch—even by nontechnical users—through an intuitive Web GUI; supports HTTP and HTTP Secure (HTTPS)
- Single IP management
 - Enables management of up to 32 HPE OfficeConnect 1920 switches using a single Web Interface; simplifies management of multiple devices
- SNMPv1, v2c, and v3
 - Facilitate management of the switch, as the device can be discovered and monitored from an SNMP management station
- Complete session logging
 - Provides detailed information for problem identification and resolution
- Port mirroring
 - Enables traffic on a port to be simultaneously sent to a network analyzer for monitoring
- Dual flash images
 - Provide independent primary and secondary operating system files for backup while upgrading
- Management security
 - Restricts access to critical configuration commands; offers multiple privilege levels with password protection; ACLs provide TELNET and SNMP access; local and remote syslog capabilities allow logging of all access
- Network Time Protocol (NTP)
 - Synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so that the devices can provide diverse applications based on the consistent time
- Limited CLI
 - Enables users to quickly deploy and troubleshoot devices in the network
- Default DHCP client mode
 - Allows the switch to be directly connected to a network, enabling plug-and-play operation; in absence of a DHCP server on the network, the switch will fall back to a unique static address determined by the switch's MAC address
- FTP, TFTP, and SFTP support
 - Offer different mechanisms for configuration updates; FTP allows bidirectional transfers over a TCP/IP network; trivial FTP (TFTP) is a simpler method using User Datagram Protocol (UDP); Secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security
- Remote monitoring (RMON)
 - Uses standard SNMP to monitor essential network functions; supports events, alarm, history, and statistics group plus a private alarm extension group

Quality of service (QoS)

- Traffic prioritization
Provides time-sensitive packets (like VoIP and video) with priority over other traffic based on DSCP or IEEE 802.1p classification; packets are mapped to eight hardware queues for more effective throughput
- IEEE 802.1p/Q VLAN tagging
Delivers data to devices based on the priority and type of traffic; supports IEEE 802.1Q
- Advanced classifier based QoS
Classifies traffic using multiple match criteria based on Layer 2, 3, and 4 information; applies QoS policies such as setting priority level and rate limit to selected traffic on a per-port basis
- Broadcast control
Allows limitation of broadcast traffic rate to cut down on unwanted network broadcast traffic
- Rate limiting
Sets per-port ingress enforced maximums and per-port, per-queue minimums
- Class of Service (CoS)
Sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ
- Powerful QoS feature
Supports the following congestion actions: strict priority queuing (SP), weighted round robin (WRR) queuing, and SP+WRR

Connectivity

- IPv6
 - IPv6 host
Enables switches to be managed and deployed at the IPv6 network's edge
 - IPv6 routing
Supports IPv6 static routes
 - MLD snooping
Forwards IPv6 multicast traffic to the appropriate interface, preventing traffic flooding
 - IPv6 ACL/QoS
Supports ACL and QoS for IPv6 network traffic
- IEEE 802.3X Flow Control
Provides a flow throttling mechanism propagated through the network to prevent packet loss at a congested node
- IEEE 802.3at Power over Ethernet (PoE+)
Provides up to 30 W per port, which allows support of the latest PoE+ capable devices such as IP phones, wireless access points, and security cameras, as well as any IEEE 802.3af-compliant end device; mitigates the cost of additional electrical cabling and circuits that would otherwise be necessary in IP phone and WLAN deployments
- Cable diagnostics
Detects cable issues remotely using a browser-based tool
- Flow Control
Provides back pressure using standard IEEE 802.3x, reducing congestion in heavy traffic situations
- Auto MDI/MDI-X
Adjusts automatically for straight-through or crossover cables on all 10/100/1000 ports

Security

- **Advanced access control lists (ACLs)**
Enables network traffic filtering and enhances network control using MAC- and IP-based ACLs; time-based ACLs allow for greater flexibility with managing network access
- **IEEE 802.1X and RADIUS network logins**
Controls port-based access for authentication and accountability
- **Secure Sockets Layer (SSL)**
Encrypts all HTTP traffic, allowing safe access to the browser-based management GUI in the switch
- **Port Isolation**
The port Isolation feature isolates Layer 2 traffic for data privacy and security without using VLANs. This feature can also be used to isolate the hosts in a VLAN from one another
- **Port security**
Combines and extends IEEE 802.1X and MAC authentication to provide MAC-based network access control
- **ARP attack protection**
The ARP detection feature enables access devices to block ARP packets from unauthorized clients to prevent user spoofing and gateway spoofing attacks
- **Automatic VLAN assignment**
Assigns users automatically to the appropriate VLAN based on their identity, location, and time of day
- **STP BPDU port protection**
Blocks Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks
- **STP root guard**
Protects the root bridge from malicious attacks or configuration mistakes
- **Automatic denial-of-service protection**
Monitors for malicious attacks and protects the network by blocking the attacks
- **Management password**
Provides security so that only authorized access to the Web browser interface is allowed

Performance

- **Half- and full-duplex auto-negotiating capability** on every port doubles the throughput of every port
- **Selectable queue configurations**
Allows for increased performance by selecting the number of queues and associated memory buffering that best meet the requirements of the network applications
- **IGMP snooping**
Improves network performance through multicast filtering, instead of flooding traffic on all ports
- **Fiber uplink**
Provides greater distance connectivity using Gigabit Ethernet fiber uplinks

Layer 2 switching

- **Spanning Tree Protocol (STP)**
Supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- **BPDU filtering**
Drops BPDU packets when STP is enabled globally but disabled on a specific port

- Jumbo frame support
Supports up to 10 kilobyte frame size to improve the performance of large data transfers
- VLAN support and tagging
Support IEEE 802.1Q with 4,094 simultaneous VLAN IDs

Layer 3 services

- Address Resolution Protocol (ARP)
Determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network
- DHCP Relay
Simplifies management of DHCP addresses in networks with multiple subnets

Layer 3 routing

- Static IPv4/IPv6 routing
Provides basic routing (supporting up to 32 static routes and 8 virtual VLAN interfaces); allows manual routing configuration

Resiliency and high availability

- Available redundant power supply
Provides additional PoE of up to 795 W for high-power applications like PTZ IP cameras, video IP phones; the HPE RPS1600 Redundant Power System (JG136A), which is sold separately, is for use with the HPE OfficeConnect 1920 24G PoE+ (370W) switch and HPE OfficeConnect 1920 48G PoE+ Switch (370W) switch models.
- Link aggregation
Groups together multiple ports up to a maximum of eight ports per trunk either automatically using Link Aggregation Control Protocol (LACP), or manually, to form an ultra-high-bandwidth connection to the network backbone; help prevent traffic bottlenecks. The 8 port models support 4 trunks, 16 and 24 port models support 8 trunks, 48 port models support 16 trunks.

Convergence

- LLDP-MED (Media Endpoint Discovery)
Defines a standard extension of LLDP that stores values for parameters such as QoS and VLAN to configure network devices such as IP phones automatically
- PoE allocations
Support multiple methods (automatic, IEEE 802.3af class, LLDP-MED, or user-specified) to allocate PoE power for more efficient energy savings
- Auto-voice VLAN
Recognizes IP phones and automatically assigns voice traffic to dedicated VLAN for IP phones

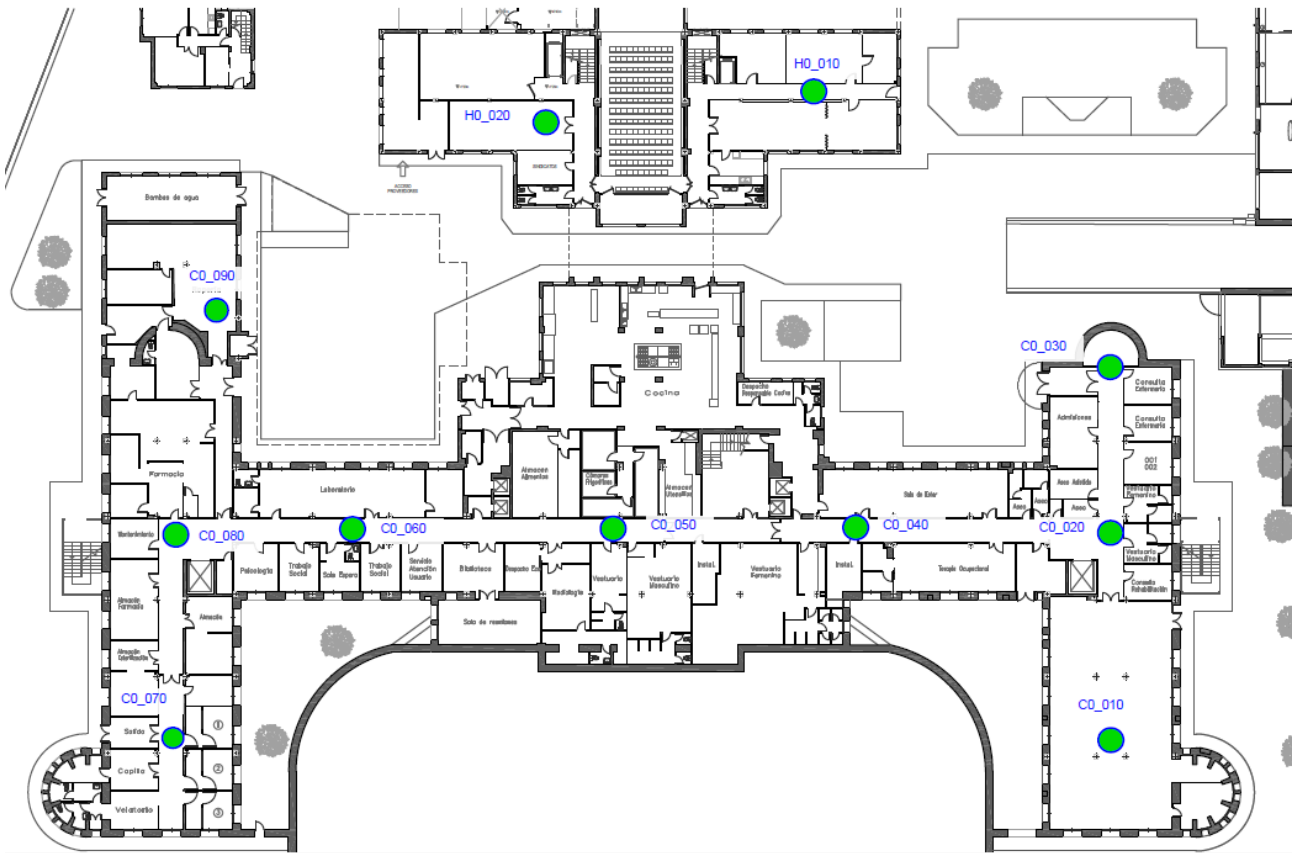
Additional information

- Green Initiative support
Provides support for RoHS and WEEE regulations
- Green IT and power
Improves energy efficiency through the use of the latest advances in silicon development; shuts off unused ports and utilizes variable-speed fans, reducing energy costs
- Energy Efficient Ethernet
Compliant with IEEE 802.3az standard requirements to save energy during periods of low data activity

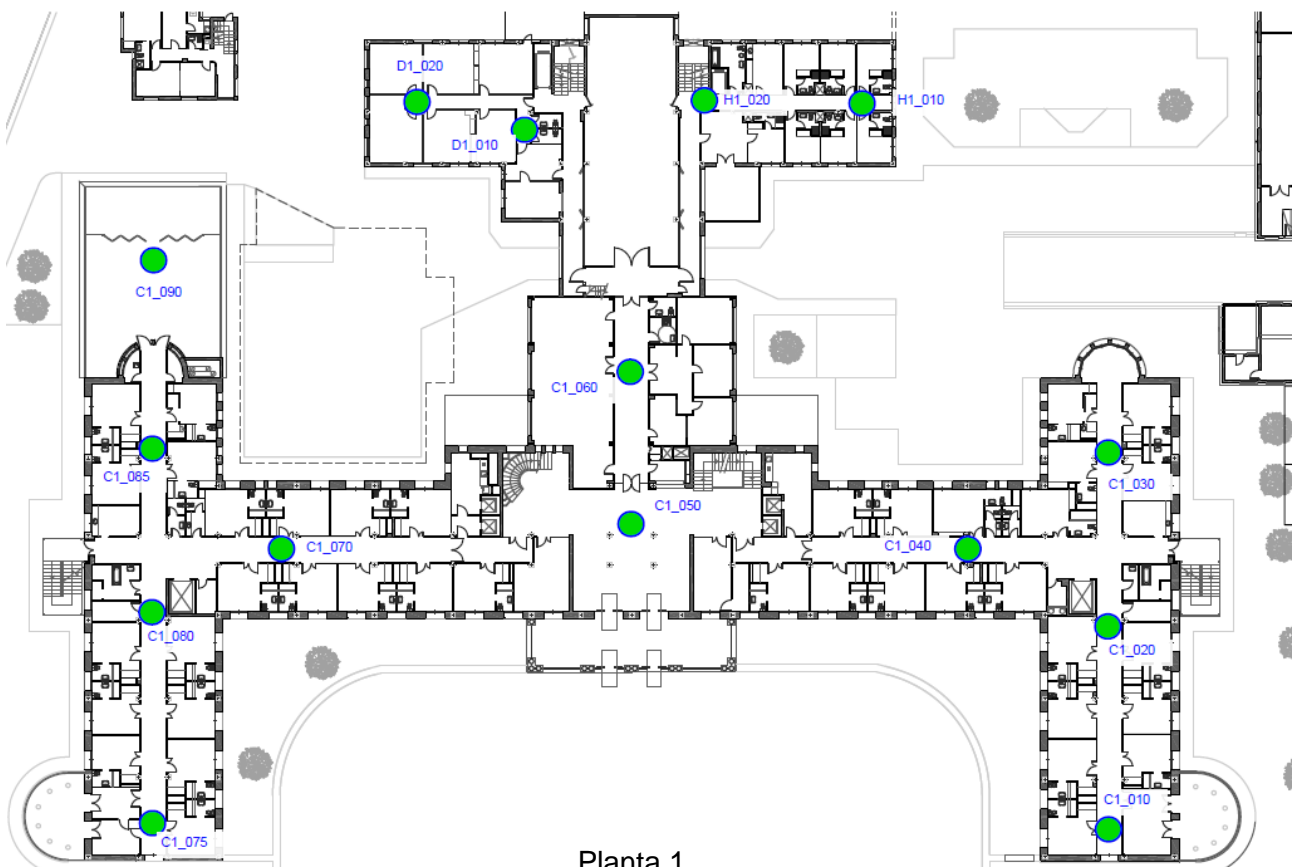
Specifications	HPE OfficeConnect 1920 8G Switch (JG920A)	HPE OfficeConnect 1920 8G PoE+ (65W) Switch (JG921A)	HPE OfficeConnect 1920 8G PoE+ (180W) Switch (JG922A)
Environment			
Operating temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Operating relative humidity	10% to 90%, noncondensing	10% to 90%, noncondensing	10% to 90%, noncondensing
Nonoperating/Storage temperature	-40°F to 158°F (-40°C to 70°C)	-40°F to 158°F (-40°C to 70°C)	-40°F to 158°F (-40°C to 70°C)
Nonoperating/Storage relative humidity	10% to 95%, noncondensing	10% to 95%, noncondensing	10% to 95%, noncondensing
Altitude	up to 16,404 ft (5 km)	up to 16,404 ft (5 km)	up to 16,404 ft (5 km)
Acoustic	Pressure: 0 dB No Fan	Pressure: 0 dB No Fan	Low-speed fan: 43.6 dB, High-speed fan: 51.5 dB; ISO 7779
Electrical characteristics			
Frequency	50/60 Hz	50/60 Hz	50/60 Hz
AC voltage	100 - 240 VAC	100 - 240 VAC	100 - 240 VAC
Maximum power rating	9 W	94 W	235 W
PoE power		65 W PoE+	180 W PoE+
	Notes Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the Infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.	Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the Infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated. PoE power is the power supplied by the internal power supply. It is dependent on the type and quantity of power supplies.	Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the Infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated. PoE power is the power supplied by the internal power supply. It is dependent on the type and quantity of power supplies.
Safety	UL 60950; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1-03	UL 60950; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1-03	UL 60950; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1-03
Emissions	FCC part 15 Class A; VCCI Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; EN 61000-3-2 2000, 61000-3-3; ICES-003 Class A	FCC part 15 Class A; VCCI Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; EN 61000-3-2 2000, 61000-3-3; ICES-003 Class A	FCC part 15 Class A; VCCI Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; EN 61000-3-2 2000, 61000-3-3; ICES-003 Class A
Management	IMC—Intelligent Management Center; limited command-line interface; Web browser; SNMP Manager; IEEE 802.3 Ethernet MIB	IMC—Intelligent Management Center; limited command-line interface; Web browser; SNMP Manager; IEEE 802.3 Ethernet MIB	IMC—Intelligent Management Center; limited command-line interface; Web browser; SNMP Manager; IEEE 802.3 Ethernet MIB
Notes	SFP port and copper ports work simultaneously, independent of each other, to provide a total of 10 Gigabit switching ports.	SFP port and copper ports work simultaneously, independent of each other, to provide a total of 10 Gigabit switching ports.	SFP port and copper ports work simultaneously, independent of each other, to provide a total of 10 Gigabit switching ports.
Services	Refer to the Hewlett Packard Enterprise website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.	Refer to the Hewlett Packard Enterprise website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.	Refer to the Hewlett Packard Enterprise website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.

Specifications	HPE OfficeConnect 1920 8G Switch (JG920A)	HPE OfficeConnect 1920 8G PoE+ (65W) Switch (JG921A)	HPE OfficeConnect 1920 8G PoE+ (180W) Switch (JG922A)
Environment			
Operating temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Operating relative humidity	10% to 90%, noncondensing	10% to 90%, noncondensing	10% to 90%, noncondensing
Nonoperating/Storage temperature	-40°F to 158°F (-40°C to 70°C)	-40°F to 158°F (-40°C to 70°C)	-40°F to 158°F (-40°C to 70°C)
Nonoperating/Storage relative humidity	10% to 95%, noncondensing	10% to 95%, noncondensing	10% to 95%, noncondensing
Altitude	up to 16,404 ft (5 km)	up to 16,404 ft (5 km)	up to 16,404 ft (5 km)
Acoustic	Pressure: 0 dB No Fan	Pressure: 0 dB No Fan	Low-speed fan: 43.6 dB, High-speed fan: 51.5 dB, ISO 7779
Electrical characteristics			
Frequency	50/60 Hz	50/60 Hz	50/60 Hz
AC voltage	100 - 240 VAC	100 - 240 VAC	100 - 240 VAC
Maximum power rating	9 W	94 W	235 W
PoE power		65 W PoE+	180 W PoE+
	Notes Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.	Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated. PoE power is the power supplied by the internal power supply. It is dependent on the type and quantity of power supplies.	Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated. PoE power is the power supplied by the internal power supply. It is dependent on the type and quantity of power supplies.
Safety	UL 60950; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1-03	UL 60950; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1-03	UL 60950; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1-03
Emissions	FCC part 15 Class A; VCCI Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; EN 61000-3-2 2000, 61000-3-3; ICES-003 Class A	FCC part 15 Class A; VCCI Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; EN 61000-3-2 2000, 61000-3-3; ICES-003 Class A	FCC part 15 Class A; VCCI Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; EN 61000-3-2 2000, 61000-3-3; ICES-003 Class A
Management	IMC—Intelligent Management Center; limited command-line interface; Web browser; SNMP Manager; IEEE 802.3 Ethernet MIB	IMC—Intelligent Management Center; limited command-line interface; Web browser; SNMP Manager; IEEE 802.3 Ethernet MIB	IMC—Intelligent Management Center; limited command-line interface; Web browser; SNMP Manager; IEEE 802.3 Ethernet MIB
Notes	SFP port and copper ports work simultaneously, independent of each other, to provide a total of 10 Gigabit switching ports.	SFP port and copper ports work simultaneously, independent of each other, to provide a total of 10 Gigabit switching ports.	SFP port and copper ports work simultaneously, independent of each other, to provide a total of 10 Gigabit switching ports.
Services	Refer to the Hewlett Packard Enterprise website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.	Refer to the Hewlett Packard Enterprise website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.	Refer to the Hewlett Packard Enterprise website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.

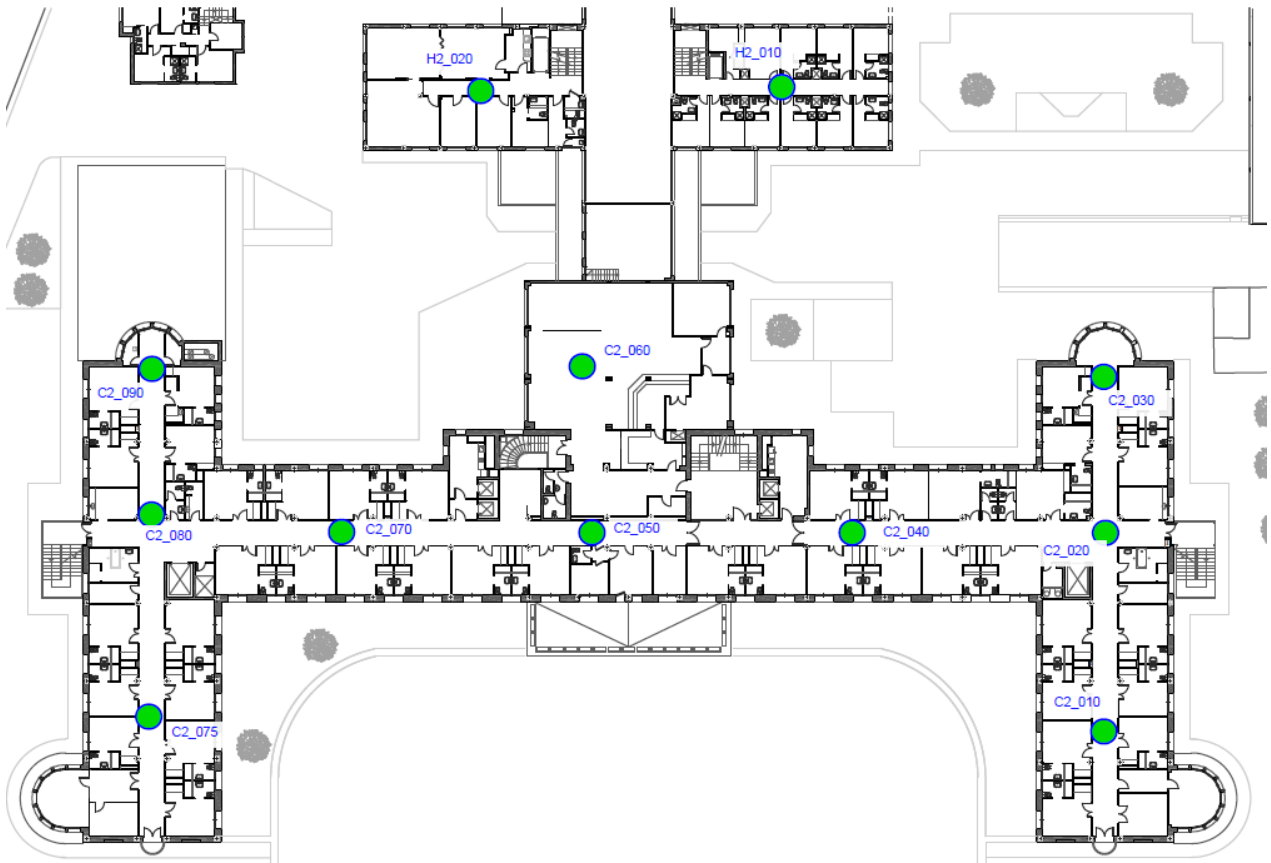
Anexo 6. Plano Despliegue Puntos de Acceso.



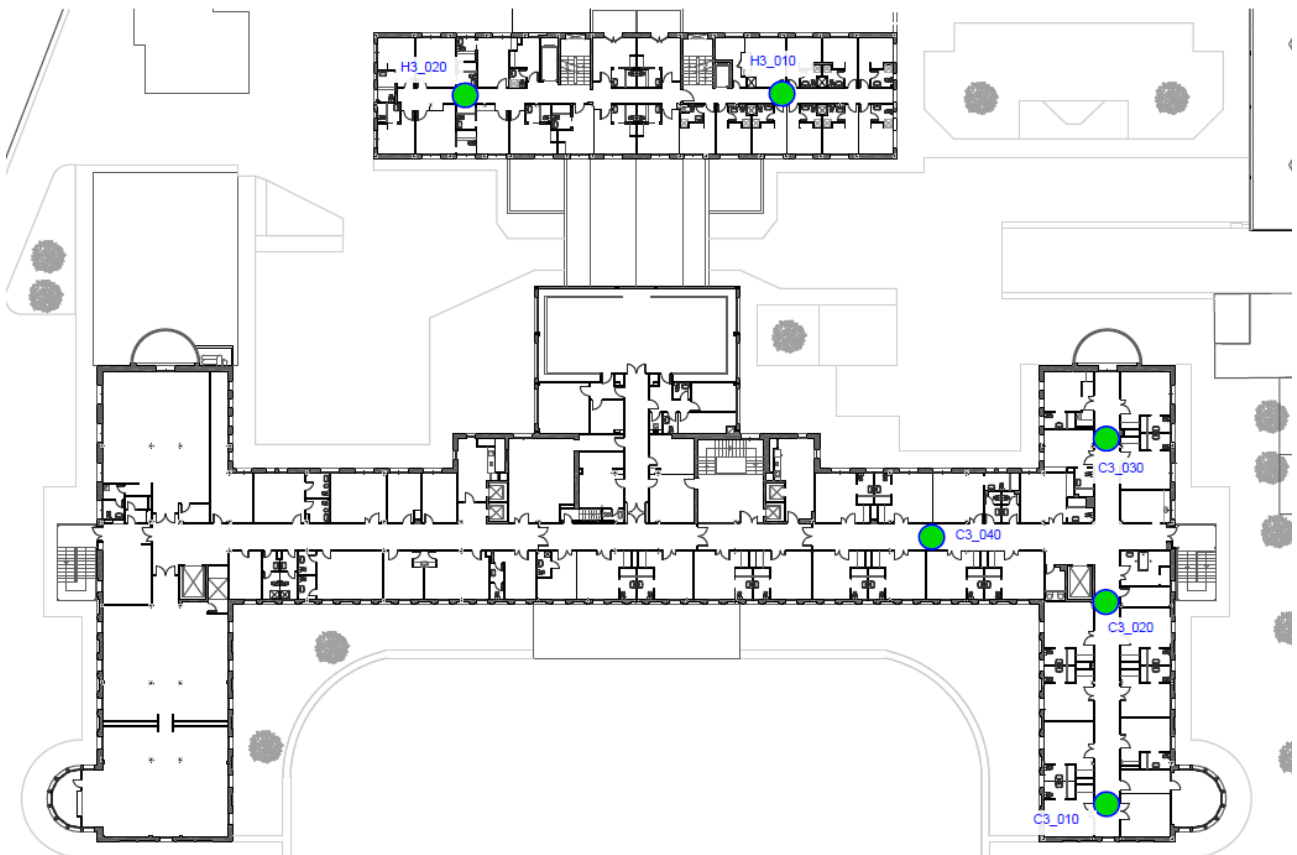
Planta 0



Planta 1



Planta 2



Planta 3

Anexo 7. Configuración de Switches.

PLANTA3 – 172.29.26.X

- Modelo: HPE 1820 48G PoE+ (370W) Switch
- Firmware instalado: PT.2.2
- Conexión: HTTP
- Login: xxxx / Password: yyyy
- Configuración
 - Conexión a Distribución (fibra) 51 + 52 > tag a todas las vlan
 - Conexión a CORO1 (fibra) 50 > tag a todas las vlan
 - Boca de gestión (cobre) 48 > untag vlan 26
 - Conexión a APs
 - VLAN 20 > bocas 1 a 6 untagged (DHCP)
 - VLAN 22 (WIFI_PRIVADO) > bocas 1 a 6 tagged
 - VLAN 50 (WIFI_PUBLICO) > bocas 1 a 6 tagged
 - Spanning tree > Activado con configuración por defecto

PLANTA2 – 172.29.26.X

- Modelo: HPE 1820 48G PoE+ (370W) Switch
- Firmware instalado: PT.2.2
- Conexión: HTTP
- Login: xxxx / Password: yyyy
- Configuración
 - Conexión a Distribución (fibra) Trunk 51 + 52 > tag a todas las vlan
 - Boca de gestión (cobre) 48 > untag vlan 26
 - Conexión a APs
 - VLAN 20 > bocas 1 a 12 untagged (DHCP)
 - VLAN 22 (WIFI_PRIVADO) > bocas 1 a 12 tagged
 - VLAN 50 (WIFI_PUBLICO) > bocas 1 a 12 tagged
 - Spanning tree > Activado con configuración por defecto

PLANTA1 – 172.29.26.X

- Modelo: HPE 1820 48G PoE+ (370W) Switch
- Firmware instalado: PT.2.2
- Conexión: HTTP
- Login: xxxx / Password: yyyy
- Configuración
 - Conexión a Distribución (fibra) Trunk 51 + 52 > tag a todas las vlan
 - Boca de gestión (cobre) 48 > untag vlan 26
 - Conexión a APs

- VLAN 20 > bocas 1 a 12 untagged (DHCP)
- VLAN 22 (WIFI_PRIVADO) > bocas 1 a 12 tagged
- VLAN 50 (WIFI_PUBLICO) > bocas 1 a 12 tagged
- Spanning tree > Activado con configuración por defecto

PLANTA0_1 – 172.29.26.X

- Modelo: HPE 1820 24G PoE+ (185W) Switch
- Firmware instalado: PT.2.2
- Conexión: HTTP
- Login: xxxx / Password: yyyy
- Configuración
 - Conexiones a Distribución (fibra) 26 > tag a todas las vlan
 - Conexiones a FALSO_TECHO1 (fibra) 25 > tag a todas las vlan
 - Conexión a PLANTA0_2 boca 23 (cobre) > tag a todas las vlan
 - Boca de gestión 24 > untag a vlan 26
 - Conexión a APs
 - VLAN 20 > bocas 1 a 10 untagged (DHCP)
 - VLAN 22 (WIFI_PRIVADO) > bocas 1 a 10 tagged
 - VLAN 50 (WIFI_PUBLICO) > bocas 1 a 10 tagged
 - Spanning tree > Activado con configuración por defecto

PLANTA0_2 – 172.29.26.X

- Modelo: HPE 1820 24G PoE+ (185W) Switch
- Firmware instalado: PT.2.2
- Conexión: HTTP
- Login: xxxx / Password: yyyy
- Configuración
 - Conexiones a Distribución (fibra) 26 > tag a todas las vlan
 - Conexiones a FALSO_TECHO2 (fibra) 25 > tag a todas las vlan
 - Conexión a PLANTA0_1 boca 23 (cobre) > tag a todas las vlan
 - Boca de gestión 24 > untag a vlan 26
 - Spanning tree > Activado con configuración por defecto

FALSO_TECHO1 – 172.29.26.X

- Modelo: HPE 1920 8G Switch
- Firmware instalado: 5.20 R1115
- Conexión: HTTP
- Login: xxxx / Password: yyyy

- Configuración
 - Conexión a PLANTA0_1 (fibra) 10 > tag a todas las vlan
 - Conexión a CORO2 (fibra) 9 > tag a todas las vlan
 - Conexión a FALSO_TECHO2 7 > tag a todas las vlan
 - Boca de gestión 8 > untag vlan 26

FALSO_TECHO 2 – 172.29.26.X

- Modelo: HPE 1920 8G Switch
- Firmware instalado: 5.20 R1115
- Conexión: HTTP
- Login: xxxx / Password: yyyy
- Configuración
 - Conexión a PLANTA0_1 (fibra) 10 > tag a todas las vlan
 - Conexión a FALSO_TECHO1 (cobre) 7 > tag a todas las vlan
 - Boca de gestión (cobre) 8 > untag vlan 26