FACULTAD DE INGENIERÍAS Y CIENCIAS AGROPECUARIAS

SOLUCIÓN DE RED INALÁMBRICA CON ADMINISTRACIÓN DE POLÍTICAS Y PERFILES DE USUARIO PARA EL “HOTEL FINLANDIA” EN LA CIUDAD DE QUITO.

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniera en Redes y Telecomunicaciones

Profesor Guía

MSc. Marcelo Ricardo Filián Narváez

Autora

Tnlgo. Sandra Elizabeth Toasa Criollo

Año

2016

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de las reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los trabajos de titulación”

_____

Marcelo Ricardo Filián Narváez
Magister en Conectividad y Redes de Telecomunicaciones
CI: 060288863-8

DECLARACIÓN DEL ESTUDIANTE

“Declaro que este trabajo es original y de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

Sandra Elizabeth Toasa Criollo

Tecnòloga en Electrónica y Telecomunicaciones

CI: 180390254-1

AGRADECIMIENTOS

Agradezco a Dios por permitirme este logro. A mis padres y hermanas. A mi esposo Alexis por su apoyo incondicional y ayuda en todo lo que represento la realización de este proyecto.

A mi profesor guía por su valiosa colaboración y aporte en este trabajo y a todos quienes me han apoyado.

DEDICATORIA

Quiero dedicar este trabajo a Dios y a mi familia, de manera especial a mi esposo por ser mi fortaleza y apoyo constante y a mi hija Sarahi por ser mi razón de ser y motivación para luchar cada día.

RESUMEN

La solución de red inalámbrica que se propone para el Hotel Finlandia permitirá a los huéspedes así como a los propios empleados del hotel contar con un servicio de cobertura Wi-Fi fiable, seguro y de calidad mediante la administración de políticas y perfiles de usuario.

En el primer capítulo se incluye información teórica sobre conceptos asociados a las redes inalámbricas y su funcionamiento. Además se incluirá conceptos técnicos de los componentes y elementos que intervienen en la solución de red inalámbrica.

En el segundo capítulo se presenta el análisis de la red inalámbrica actual del hotel previo al diseño de la misma.

En el tercer capítulo se presenta el diseño de la solución de red inalámbrica, los equipos a utilizar y la configuración de las políticas y perfiles de usuario. Se realiza la simulación del diseño y pruebas de funcionamiento.

Finalmente en el cuarto capítulo se presentan las conclusiones y recomendaciones de éste proyecto.

ABSTRACT

The solution of wireless network that one proposes for the Finlandia Hotel will allow the guests as well as the own employees of the hotel to possess a service of coverage trustworthy, sure Wi-Fi and of quality by means of the administration of policies and user's profiles.

In the first chapter there is included theoretical information about concepts associated with the wireless networks and his functioning. In addition there will be included technical concepts of the components and elements that intervene in the solution of wireless network.

In the second chapter one presents the analysis of the wireless current network of the hotel before the design of the same one.

In the third chapter one presents the design of the solution of wireless network, the equipments to using and the configuration of the policies and user's profiles. There are realized the simulation of the design and tests of functioning.

Finally in the fourth chapter they present the conclusions and recommendations of this one I project.

ÌNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Hoy en día los huéspedes de los hoteles están acostumbrados a utilizar varios dispositivos móviles y esperan poder conectarse a internet en cualquier lugar y en cualquier momento. Según la encuesta de Hotels.com el Wi-Fi gratuito es uno de los servicios más solicitado y más importante para los huéspedes en el hotel. (Hotels, 2012).

El 80% de los viajeros a nivel mundial le concede gran importancia que los alojamientos ofrezca Wi-Fi gratis. De hecho, no disponer de ello supone un gran impacto en la reserva, al igual que si no se ofrece desayuno gratuito y artículos de cuidado personal, otros dos elementos muy requeridos entre los clientes. (Web 2.0, 2013).

Actualmente el Hotel Finlandia ubicado en el sector centro norte de Quito se ha visto en la necesidad de ampliar y mejorar la infraestructura de red existente debido a que ha construido una nueva torre para ampliar sus instalaciones.

La solución de red inalámbrica que se propone deberá cubrir toda el área del edificio actual del Hotel Finlandia, que comprende las habitaciones de los huéspedes, el área de lobby, restaurante, subsuelos y salones de eventos. Se pretenden obtener como resultado que los huéspedes así como a los propios empleados del Hotel Finlandia puedan contar con un servicio de cobertura Wi-Fi fiable, seguro y de calidad mediante la administración de políticas y perfiles de usuario.

1. FUNDAMENTOS TEÓRICOS DE WLAN

1.1 Definición

Una red inalámbrica de área local (WLAN o Wireless LAN) puede definirse como una red de alcance local que permite la transmisión y recepción de información mediante ondas electromagnéticas que se propagan a través del aire.

Wireless LAN es un sistema de comunicación de datos inalámbrico flexible muy utilizado como alternativa a las redes de área local cableadas o como extensión de éstas, esta tecnología está normada bajo el estándar IEEE802.11 y se encuentra situada entre las tecnologías inalámbricas de mediano alcance, como se puede verificar en la figura 1:

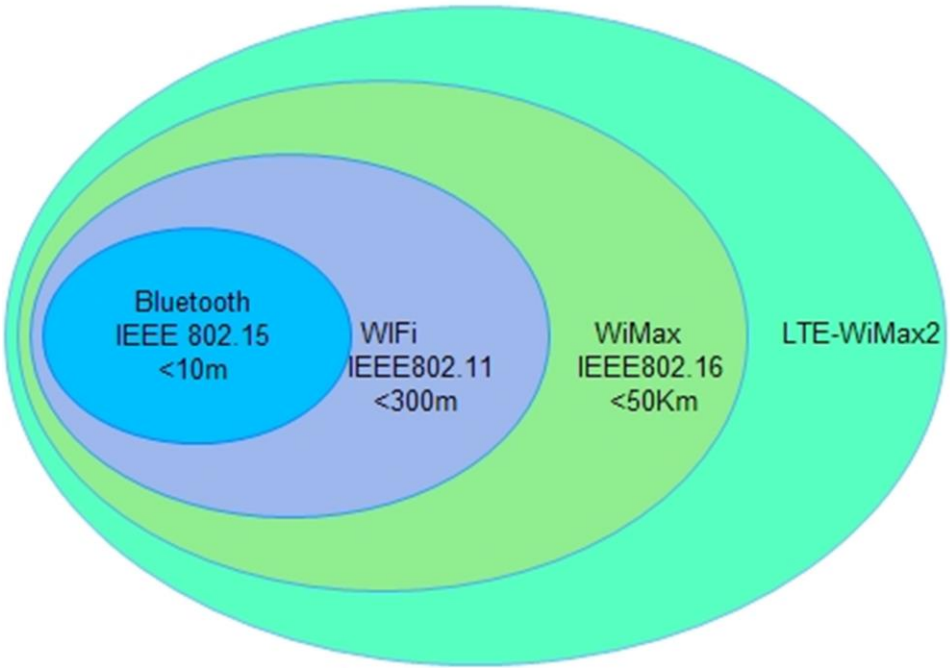


Figura 1. Tipos de Redes Inalámbricas

En la actualidad las redes inalámbricas de área local (WLANs) son comúnmente utilizadas en lugares como: aeropuertos, universidades, oficinas,

empresas, hoteles, hogares, etc. para proveer conectividad a los usuarios que generalmente poseen dispositivos móviles tales como: asistentes personales digitales (PDAs), computadoras portátiles (laptops), teléfonos inteligentes (Smartphones), tabletas, videoconsolas portátiles, etc., permitiendo la interacción entre ellos y el acceso a los servicios de la red sin la necesidad de utilizar medios cableados.

1.2 Importancia de las WLAN.

Las redes de área local (LANs) cableadas operan a velocidades de 100 Mbps en la capa de acceso, 1 Gbps en la capa de distribución, y hasta 10 Gbps a nivel de la capa principal (core). La mayoría de las WLANs operan a una velocidad de 11 Mbps a 54 Mbps en la capa de acceso y no opera en la capa de distribución ni en la principal.

Sin embargo, las WLANs a pesar de ser un sistema con baja capacidad de ancho de banda son una buena opción para entornos LAN pequeños en los que las velocidades lentas son adecuadas para soportar las necesidades de las aplicaciones y de los usuarios. Además, las WLANs pueden manejar las demandas de ancho de banda.

1.3 Características de las WLAN

Entre las características de las redes LAN inalámbricas más importantes tenemos:

Movilidad.- Permiten a los usuarios de dispositivos móviles el acceso a la información desde cualquier lugar de la organización o empresa. Mejorando de esta manera la productividad y las posibilidades de oferta de servicios.

Facilidad de instalación. Las Wireless LAN al no necesitar ser cableadas reduce significativamente el tiempo de instalación además permite el acceso instantáneo de usuarios temporales a la red.

Flexibilidad.- Permite el acceso al internet en lugares donde el cableado no lo permite o es muy costoso.

Costo reducido.- La inversión total de la instalación de una Wireless LAN es significativamente inferior que la red LAN tradicional. Los beneficios en cuanto a costos son superiores en ambientes dinámicos que requieren ampliación, movimiento y cambios de ubicaciones dentro de la red frecuentemente.

Velocidad Simétrica.- A diferencia de las redes físicas cableadas ADSL (Asymmetric Digital Subscriber Line), Wi-Fi es bidireccional, puede recibir y enviar datos a la misma velocidad, es por tanto útil para prestar servicios que requieren el mismo ancho de banda tanto de subida como de bajada.

Escalabilidad.- El cambio de topología de red es muy sencillo, lo que permite la ampliación y mejora de la red existente con gran facilidad. Además las configuraciones son fáciles de modificar permitiendo la incorporación de nuevos usuarios a la red.

1.4 Wi-Fi Alliance

Conocida anteriormente como WECA (Wireless Ethernet Compatibility Alliance) es una asociación global creada en 1999 encargada de promover la tecnología Wi-Fi y certifica los productos Wi-Fi si estos cumplen con el estándar 802.11.

WI-FI Alliance es un sello de calidad, el equipo que esté certificado, funcionará correctamente con el estándar 802.11. Las funciones principales que deben cumplir los dispositivos para obtener la certificación son los siguientes:

Interoperabilidad.- Los equipos de diferentes proveedores puedan coexistir y operar entre ellos sin ningún inconveniente.

Compatibilidad.- Los dispositivos antiguos tanto como los nuevos pueden trabajar a pesar de tener diferentes versiones.

Innovación.- La introducción de nuevos programas de certificación con la tecnología actual y las especificaciones para entrar en el mercado.

Wi-Fi se utiliza como denominación genérica para los dispositivos que incorporan cualquier variante de la tecnología inalámbrica IEEE 802.11. (UNAD)

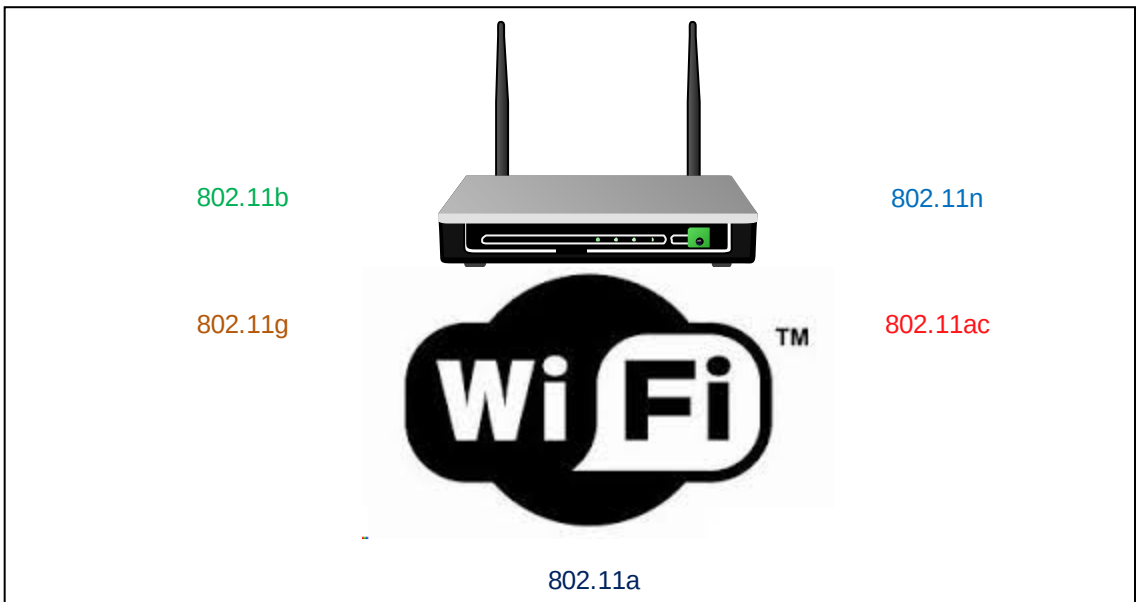


Figura 2. Wi-Fi
Adaptado de (Wifi, s.f.)

1.5 Estándar IEEE802.11

El estándar IEEE802.11 fue ratificado en 1997 por el Instituto de Ingeniería Eléctrica y Electrónica (IEEE) para el uso de redes inalámbricas que opera con velocidades de transmisión de 1 a 2 Mbps y desde esta versión inicial el IEEE ha llevado a cabo varias revisiones para lograr nuevos estándares que brinden velocidades de trasmisión más altas, entre los cuales se tiene 802.11a, 802.11b, 802.11g, 802.11n.

1.5.1 Estándar IEEE 802.11b

Este estándar fue ratificado en el año 1999, guarda compatibilidad con el estándar IEEE 802.11, razón por la cual la migración del estándar IEEE 802.11 a IEEE 802.11b podría ser realizada de manera rápida por las empresas.

El estándar IEEE 802.11b opera en la banda de 2.4 GHz y posee una velocidad de transmisión máxima de 11 Mbps, utiliza modulación DSSS (Direct Sequence Spread Spectrum) a nivel de capa de enlace e implementa a nivel de capa de física CCK (Complementary Code Keying). Utiliza el método de acceso CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). (Mantilla, 2007)

1.5.2 Estándar IEEE 802.11a

Fue ratificado en el año 1999 pero los primeros equipos aparecen en el año 2001, este estándar opera en la banda de frecuencia de 5 GHz y llega a alcanzar velocidades de transmisión de 54 Mbps, utiliza modulación OFDM (Orthogonal Frequency Division Multiplexing)

1.5.3 Estándar IEEE 802.11g

Este estándar fue ratificado en el año 2003 y es compatible con los dispositivos del estándar IEEE802.11b, facilitando así la migración de las redes a este nuevo estándar. El estándar IEEE802.11g opera en la banda de frecuencia 2.4 GHz con una velocidad de transmisión máxima de 54 Mbps y utiliza la modulación OFDM y DSSS. (Peeters, 2004). El esquema de modulación es CCK.

Multiplexado por división de frecuencia ortogonal (OFDM).- Es una técnica que divide un canal de comunicaciones en una cierta cantidad de bandas de frecuencia que se encuentran separadas igualmente unas de otras. OFDM utiliza múltiples subportadoras, en total 52, separadas por 312,5 KHz. Los datos son enviados por 48 portadoras simultáneamente, donde cada

subportadora transporta una parte de los datos del usuario. Cuatro subportadoras se utilizan como pilotos y cada subportadora es ortogonal e independiente del resto de subportadoras, de esta manera aumenta la eficiencia del uso del espectro debido a que no utiliza bandas de separación entre subportadoras.

El tiempo para transmitir cada bit se incrementa en proporción a la cantidad de portadoras. Esto hace al sistema menos sensible a la interferencia multitrayectoria que es una fuente importante de distorsión. (PEZO, 2010)

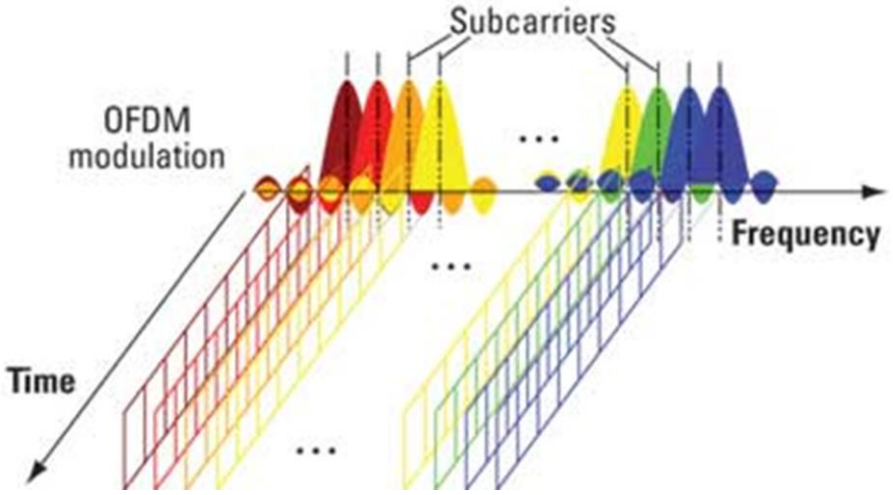


Figura 3. Multiplexado por división de frecuencia ortogonal

Tomado de (El androide libre, s.f.)

Espectro Disperso por Secuencia Directa (DSSS).- Esta técnica consiste en la generación de un patrón de bits redundante para cada uno de los bits que componen la señal de información y la posterior modulación de la señal resultante. Cuanto mayor sea esta señal, mayor será la resistencia de la señal a las interferencias, haciendo más difícil su intercepción, reduciendo perdidas, fortaleciendo la señal a los efectos de las multitrayectorias y proporcionando una capacidad de acceso múltiple. El estándar IEEE 802.11 recomienda un tamaño de 11 bits, pero el óptimo es de 100. En la parte de recepción se requiere realizar el proceso inverso para obtener la señal de información original. (Ramirez H, Colorado A, & Quintero Salazar, 2011)

La secuencia de bits utilizada para modular cada uno de los bits de información es la llamada secuencia pseudo-aleatoria o código de dispersión.

Se podrá pensar que la característica de aumentar el ancho de banda de la señal es contraproducente ya que el filtro en el receptor requerirá un ancho de banda aumentado causando más ruido al demodulador. Sin embargo, cuando a cualquier señal con ruido blanco gaussiano se le aplica a un filtro acoplado a la señal, el rendimiento del filtro tiene una proporción de señal-a-ruido (SNR) inversamente proporcional a la densidad espectral de la potencia del ruido.

El aspecto notable de este resultado es que el ancho de banda del filtro y la potencia de ruido con respecto al rendimiento son irrelevantes. (OCW, s.f.)

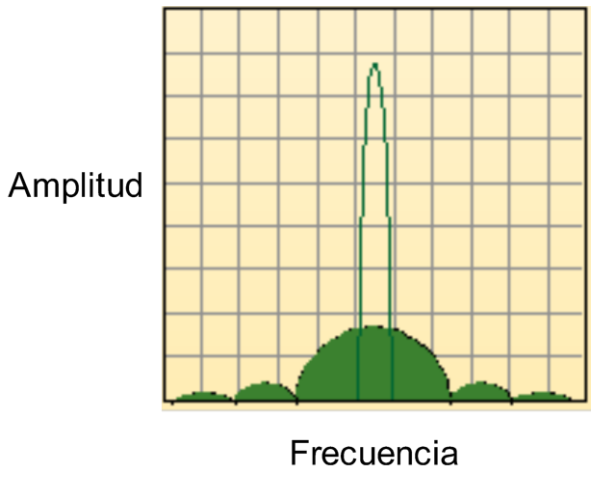


Figura 4. Espectro disperso por Secuencia Directa (DSSS)
Adaptado de (Monografías, s.f.)

1.5.4 Estándar IEEE 802.11n

Este estándar opera en las bandas de frecuencia de 2.4 GHz y 5 GHz con una velocidad de transmisión máxima de 600 Mbps. Utiliza un esquema de modulación basado en OFDM y la tecnología MIMO (Multiple- input Multiple - output) que permite aumentar la eficiencia espectral del sistema de comunicación inalámbrica.

Tecnología MIMO.- La tecnología de múltiples entradas y múltiples salidas se refiere al uso de múltiples antenas que junto al transistor y receptor mejoran el desempeño de los sistemas de radio comunicación. MIMO ofrece incrementos significativos en la transmisión de datos y un enlace de alcance sin ancho de banda adicional o un mayor poder de transmisión. Esto se alcanza con una eficiencia más alta del espectro (más bits por segundo por cada Hertz de ancho de banda) y un enlace más confiable o diverso (efecto de desvanecimiento reducido). (R.F., 2008)

Los sistemas MIMO envían y reciben la señal por varias antenas (normalmente tres), y mediante un sistema inteligente, vuelven a amplificar y a retransmitir las señales, incluso las reflejadas, consiguiendo:

Un menor margen de error.- Son comparadas con la original y si son correctas se vuelve a amplificar, y anuladas si son una interferencia real.

Un mayor alcance.- Los objetos que se encuentran entre dos puntos de comunicación, ya no merman la potencia de la señal, que es enviada por otras antenas.

Una mayor velocidad.- No porque la ganen, sino porque no la pierden a la hora de la comparación de datos recibidos. Si comparamos un sistema inalámbrico convencional (802.11b/g) con un MIMO en 802.11n, se puede hasta sextuplicar el alcance y llegar a velocidades de 300 Mbps, siempre en la banda de 2.4 GHz.

1.6 Topologías de Redes Inalámbricas Locales

Existen dos tipos de topologías: la configuración Ad-Hoc y la configuración Infraestructura.

1.6.1 Topología inalámbrica Ad-Hoc

La Red Ad-Hoc se basa en un grupo de dispositivos que se comunican cada uno directamente con los otros dispositivos a través de las señales de radio sin la necesidad de utilizar un nodo central. (Barata, 2008)

Figura 5. Topología Ad-Hoc
Adaptado de (Softigal, s.f.)

1.6.2 Topología inalámbrica de Infraestructura

En una red de infraestructura los clientes se conectan a la red a través de un punto de acceso (AP).

Si el punto de acceso se conecta a una red cableada los clientes inalámbricos pueden acceder a la red fija. Para interconectar los puntos de acceso y clientes inalámbricos, todos deben configurarse con el mismo Service Set Identifie (SSID). (Sebastian Buettrich, 2007)

El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el

número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del equipo. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño. (Liliana, 2011)

Figura 6. Topología de Infraestructura
Adaptado de (Softigal, s.f.)

1.7 Espectro de Radio para las Redes Inalámbricas

Las bandas de frecuencia que operan las WLAN son de 2.4 y 5 GHz, específicamente las tecnologías IEEE802.11b y IEEE 802.11g en la banda de frecuencia de 2400 MHZ - 2483.5 MHz y la tecnología IEEE802.11a en las bandas de frecuencia de 5150 MHz - 5250MHz y 5725 MHz - 5850 MHz. Según, el Art.23 del Reglamento de Radiotelecomunicaciones expedido por el Consejo Nacional de Telecomunicaciones (EXCONATEL) señala que *"Los usuarios del espectro radioeléctrico que operen equipos de radiocomunicaciones con potencias menores de 100 mW sin antenas directivas y que no corresponden a sistemas de última milla y los que operen al interior de locales, edificios y, en general, áreas privadas con potencias menores a 300 mW sin antenas exteriores, en cualquier tecnología, no requieren autorización del EXCONATEL".* (Arcotel, 2013)

Entonces, debido a que las redes inalámbricas IEEE802.11a/b/g operan con potencias menores a las establecidas en el Art. 23 no necesitan de un título habilitante para su operación debido a que trabaja en la banda ISM del espectro de radio. (Afonso, 2011)

Bandas ISM

Las Bandas ISM (Industrial Scientific and Medical) corresponden a parte del espectro de radio asignado para aplicaciones industriales, científicas y médicas de acuerdo al Reglamento de Radiocomunicaciones de la UIT. Las bandas ISM operan en las frecuencias de 902 MHz - 928 MHz, 2400 MHz - 24835 GHz y 5.725 GHz - 5.850 GHz. y se caracterizan porque dichas bandas permiten un funcionamiento sin licencias, siempre que los dispositivos cumplan determinadas restricciones de potencia.

El estándar 802.11 funciona en las bandas ISM junto con muchos otros dispositivos como por ejemplo un horno microondas, equipos Bluetooth, teléfonos inalámbricos, entre otros.

Canal	Frecuencia central (MHz)	Región o país			
		América/China	EMEA	Japón	Israel
1	2412	X	X	X	-
2	2417	X	X	X	-
3	2422	X	X	X	X
4	2427	X	X	X	X
5	2432	X	X	X	X
6	2437	X	X	X	X
7	2442	X	X	X	X
8	2447	X	X	X	X
9	2452	X	X	X	X
10	2457	X	X	X	-
11	2462	X	X	X	-
12	2467	-	X	X	-
13	2472	-	X	X	-
14	2484	-	-	X	-

Figura 7. Canales a 2,4GHz (802.11b/g)
Tomado de (Slideshare, s.f.)

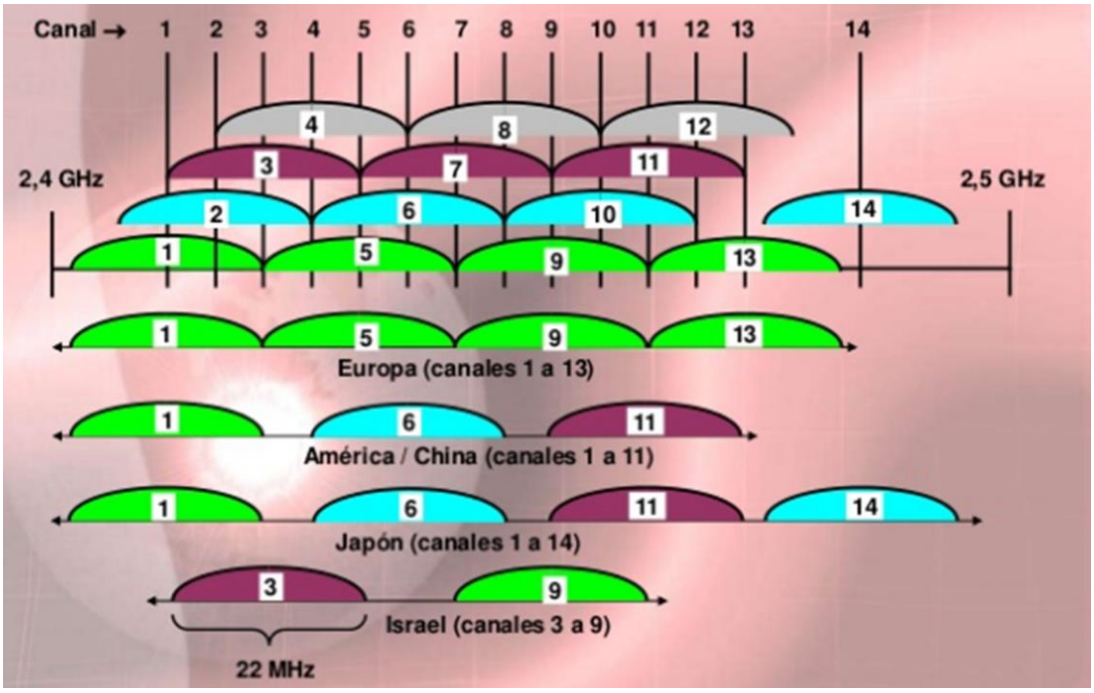


Figura 8. Distribución de canales 802.11b/g

Tomado de (Slideshare, s.f.)

Canal	Frecuencia central (MHz)	Región ITU-R o país					
		Europa	América	Japón	Singapur	Taiwan	Asia
36	5180	X	X	X	X	-	-
40	5200	X	X	X	X	-	-
44	5220	X	X	X	X	-	-
48	5240	X	X	X	-	-	-
52	5260	X	X	X	-	-	-
56	5280	X	X	X	-	-	-
60	5300	X	X	X	-	-	-
64	5320	X	X	X	-	-	-
100	5500	X	-	X	-	-	-
104	5520	X	-	X	-	-	-
108	5540	X	-	X	-	-	-
112	5560	X	-	X	-	-	-
116	5580	X	-	X	-	-	-
120	5600	X	-	X	-	-	-
124	5620	X	-	X	-	-	-
128	5640	X	-	X	-	-	-
132	5660	X	-	X	-	-	-
136	5680	X	-	X	-	-	-
140	5700	X	-	X	-	-	-
149	5745	-	X		X	X	X
153	5765	-	X		X	X	X
157	5785	-	X		X	X	X
161	5805	-	X		X	X	X
165	5825	-	X		X	X	-

Figura 9. Canales a 5GHz (802.11a/h)

Tomado de (Slideshare, s.f.)

1.8 Seguridad en Redes Inalámbricas

La red inalámbrica local brinda servicios de autenticación, confidencialidad, integridad, disponibilidad, autorización y control de acceso para tener una óptima seguridad de la misma.

Autenticación.- Es el proceso que debe seguir un usuario para identificarse y demostrar que es quien dice ser.

Confidencialidad.- Los datos son protegidos frente a la intercepción de personas no autorizadas para evitar que nadie pueda capturar las comunicaciones y acceder a la información.

Integridad.- Garantizar que los datos no sean modificados.
Disponibilidad.- La información debe encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones en el momento que así lo requieran.

Autorización y control de acceso.- Se implementa en la autenticación. Antes de garantizar el acceso a los recursos de la red se debe encontrar: el usuario (autenticación) y la operación que tiene acceso (autorización)

1.8.1 Protocolo de Seguridad WEP (Wired Equivalent Privacy)

Fue el primer mecanismo de seguridad que se introdujo en seguridad inalámbrica. El algoritmo utilizado es RC4 que utiliza claves de 64 bits o de 128 bits. Este protocolo es muy fácil de configurar pero su protección es demasiado débil.

1.8.2 Protocolo de Seguridad WPA (Wi-Fi Protected Access)

Surgió para corregir las limitaciones de WEP. Es un mecanismo de control de acceso a una red inalámbrica que permite la gestión de claves dinámicas, utiliza el algoritmo de seguridad TKIP (Temporal Key Integrity Protocol).

Una variante es WPA-Personal. Usa el sistema PSK (clave pre-compartida), todos los usuarios de la red inalámbrica tienen una misma contraseña Wi-Fi, que el propio usuario define.

Además existe una versión WPA empresarial (WPA-Enterprise). Ofrece seguridad adicional al obligar al usuario a identificarse con un nombre y contraseña en sistemas de autentificación especiales, como RADIUS (Remote Authentication Dial-In User Server) o 802.1X.

1.8.3 Protocolo de Seguridad WPA-2

Es una mejora del WPA, utiliza un algoritmo de encriptación más robusto denominado AES (Advanced Encryption Standard) lo que permite tener claves grandes que son difíciles de romper. Utiliza un protocolo de encriptación CMP (Internet Control Message Protocol) que se considera mucho más seguro y actualmente es el más utilizado.

1.8.4 FIREWALL

Un firewall es software o hardware que comprueba la información procedente de Internet o de una red y bloquea o permite el paso de ésta al equipo, en función de la configuración que tenga.

Un firewall puede impedir que hackers o software malintencionado (como gusanos) obtengan acceso al equipo a través de una red o de Internet. También puede ayudar a impedir que el equipo envíe software malintencionado a otros equipos. (Microsoft, s.f.)

1.9 Componentes de las Redes Inalámbricas

1.9.1 Tarjetas de Red Inalámbricas

Una tarjeta de red o adaptador de red inalámbrica permite la comunicación con dispositivos conectados entre sí y también permite compartir recursos entre dos o más computadoras. (LinkedIN Corporation, s.f.). Usualmente son 802.11 a,

802.11 b y 802.11 g. Cada dispositivo en la red, ya sea una PC, impresora, router, etc, que necesita comunicarse con otros dispositivos deben tener una tarjeta NIC (Network Interface Card), para poder comunicarse a través de la red.

Figura 10. NIC Inalámbrico
Adaptado de (Componentes de red inalámbricos, s.f.)

1.9.2 Ruteador Inalámbrico

El ruteador permite la interconexión de redes inalámbricas y su función es la de guiar los paquetes de datos para que fluyan hacia la red correcta e ir determinando que caminos debe seguir para llegar a su destino, básicamente se utiliza para servicios de Internet, los cuáles recibe de otro dispositivo como un módem inalámbrico del proveedor.

Figura 11. Ruteador Inalámbrico

1.9.3 Punto de Acceso (AP - Access Point)

El AP se encuentra conectado en una red local inalámbrica (WLAN). Los dispositivos inalámbricos externos le envían la petición de acceso a los recursos de la red (Internet, E-mail, impresión, Chat, etc.).

El AP se encarga de determinar en base a su configuración, que dispositivos están autorizados a acceder a la red y cuáles no. Un solo punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos 30m y hasta varios cientos. (Wordpress, s.f.). Sus funciones más importantes son:

Ampliar la distancia inalámbrica entre los PC (Computadores Personales) Clientes inalámbricos y el receptor de señal o punto de Acceso.

Si nuestro ruteador no tiene WLAN, el Punto de Acceso suple dicha función.

Es un buen gestor de tráfico de la red inalámbrica entre los terminales inalámbricos más próximos al Punto de Acceso.

Pueden gestionar y controlar simultáneamente muchos ordenadores Cliente a la vez, pudiendo llegar hasta 50 dispositivos simultáneos.

El alcance es de unos 150 metros en zonas abiertas, en zonas amplias (más de 150 metros) se necesiten más Puntos de Acceso o Puntos de Extensión para cubrir a todos los Ordenadores inalámbricos de la Red LAN.

Figura 12. Access Point

1.9.4 Antenas

Una antena es un dispositivo generalmente metálico capaz de radiar y recibir ondas de radio; que adapta la entrada/salida del receptor/transmisor al medio.

La antena convierte las ondas eléctricas entregadas por el emisor, en ondas electromagnéticas que se pueden transmitir por el espacio libre; y en el otro extremo, convierte las ondas electromagnéticas que recibe, en ondas eléctricas que entrega al receptor.

Básicamente su estructura consiste en un trozo de material conductor, al cual se le aplica una señal, y ésta es radiada por el espacio libre. Opera igualmente en sentido inverso, capturando la señal de radiofrecuencia del aire y entregándola posteriormente al receptor. a todos los Ordenadores inalámbricos de la Red LAN.

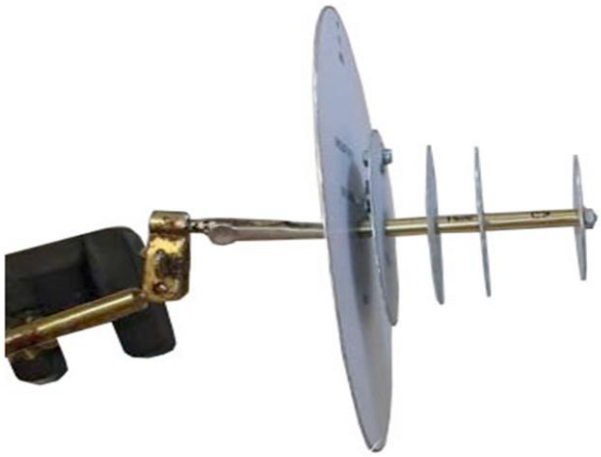


Figura 13. Antena para WiFi
Tomado de (Norfipc, s.f.)

Antenas Direccionales: Las antenas direccionales orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance, actúa de forma parecida a un foco de luz que emite un haz concreto y estrecho pero de forma intensa (más alcance). (Lacuevawifi.com, s.f.)

El alcance de una antena direccional viene dado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor.

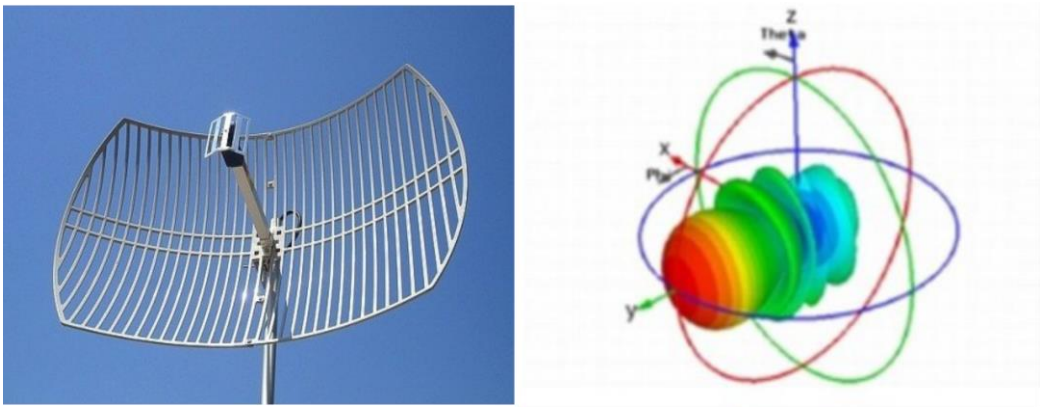


Figura 14. Antena Direccional
Adaptado de (Sensewifi, s.f.)

Antenas Omnidireccionales: Orientan la señal en todas direcciones con un haz amplio pero de corto alcance. Si una antena direccional sería como un foco, una antena omnidireccional sería como una bombilla emitiendo luz en todas direcciones con menor alcance. Las antenas Omnidireccionales “envían” la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

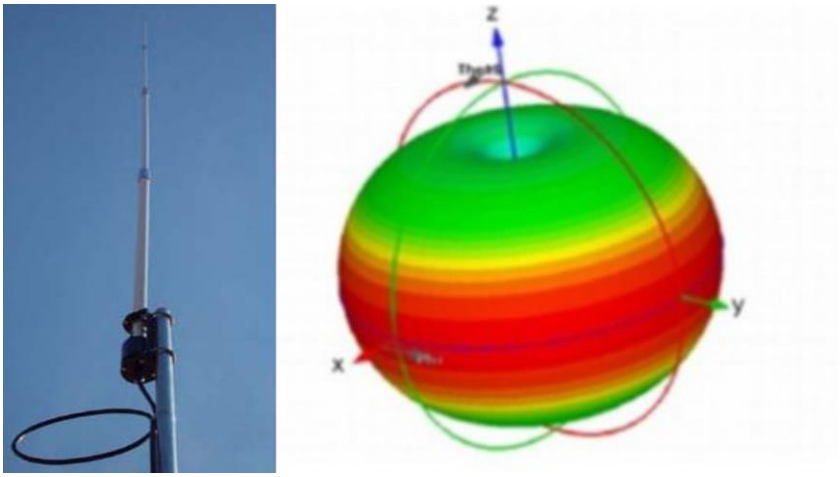


Figura 15. Antena Omnidireccional
Adaptado de (Taringa, s.f.)

Antenas Sectoriales: Son la mezcla de las antenas direccionales y las omnidireccionales. Las antenas sectoriales emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional. Para tener una cobertura de 360º (como una antena omnidireccional) y un largo alcance (como una antena direccional) deberemos instalar o tres antenas sectoriales de 120º ó 4 antenas sectoriales de 90º. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.

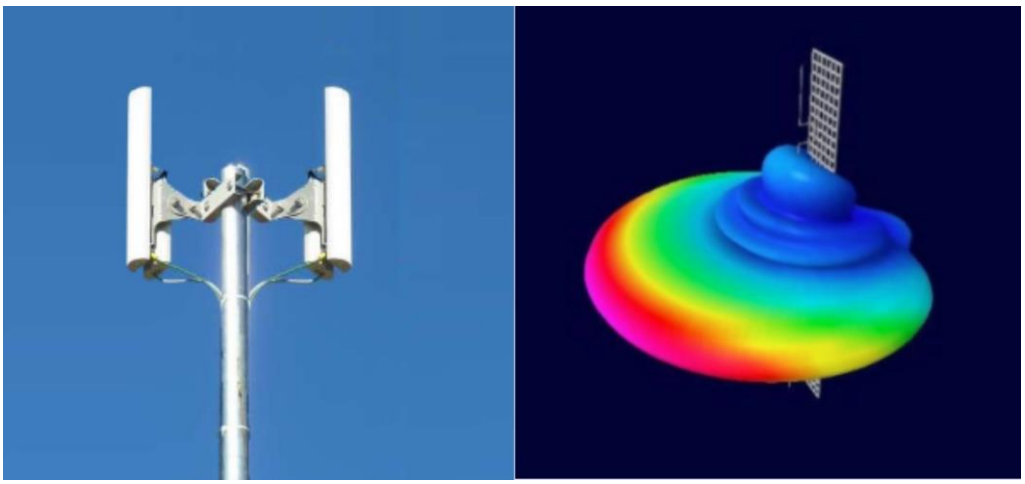


Figura 16. Antena Sectorial
Adaptado de (Slideshare, s.f.)

1.9.5 Punto de Extensión Inalámbrico

El Punto de Extensión (EPs) extiende el alcance de la red inalámbrica retransmitiendo las señales de un ordenador, Punto de Acceso o a otro punto de extensión. La finalidad de los puntos de Extensión es encadenarse para pasar los datos entre un AP, Punto de Extensión y Ordenadores lejanos de modo que se construye un puente entre ambos.

Los metros que cubren dichos aparatos van en función de los obstáculos (Edificios, Paredes, Puertas) a sortear, pero lo normal son 100 metros en interior y 300 metros en exterior.

Los puntos de Extensión tienen incorporado una tarjeta Ethernet para poder ser configurados vía Navegador, pero no es necesario ser conectados a la red inalámbrica cuando ya están configurados y funcionando.

En redes domésticas la solución para cubrir áreas que baja señal son los puntos de Extensión para ampliar toda la cobertura de la red inalámbrica entre nuestros ordenadores y el ruteador inalámbrico.

Figura 17. Punto de extensión inalámbrico
Tomado de (Dlinkla, s.f.)

1.9.6 Puente inalámbrico (bridge)

Un puente o bridge inalámbrico es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Se encarga de interconectar dos segmentos de red inalámbrica (o divide una red WLAN en segmentos) haciendo el pase de datos de una red hacia otra, con base en la dirección física de destino de cada paquete. (Peraltha, 2015). Un bridge conecta dos segmentos de red como una sola red usando el mismo protocolo de establecimiento de red.

Figura 18. Puente inalámbrico
Tomado de (Mesajilhnos, s.f.)

1.9.7 Cliente Inalámbrico

Todo aquel dispositivo susceptible de integrarse en una red wireless como PC, laptop, celulares, cámaras inalámbricas, impresoras, Tablet, etc.

Es todo aquel dispositivo que contenga una NIC. Generalmente unidos a un punto de acceso, son las comúnmente llamadas tarjetas wireless, Estos clientes pueden también conectarse entre sí sin necesidad de unirse mediante un punto de acceso.

Figura 19. Cliente inalámbrico
Adaptado de (Componentes dered inalámbricos, s.f.)

2. ANÁLISIS DE LA RED INALÁMBRICA ACTUAL

2.1 Antecedentes

El Hotel Finlandia se ha visto en la necesidad de ampliar y mejorar la infraestructura de red existente debido a que ha construido una nueva torre para ampliar sus instalaciones. La red inalámbrica actual se torna insuficiente ya que no tiene cobertura hacia la nueva construcción y presenta frecuentemente problemas de conexión a internet debido a la gran demanda de usuarios que se conectan simultáneamente y todos comparten el mismo ancho de banda provocando una saturación del canal. Además no permite una administración de políticas y perfiles de usuario para manejar el ancho de banda con la finalidad de restringir o dar prioridad tanto a los huéspedes como a los empleados propios del hotel.

2.2 Ubicación Hotel Finlandia

El Hotel Finlandia está ubicado en la ciudad de Quito, provincia de Pichincha en la República del Ecuador. Entre las calles Finlandia 35-129 y Suecia (esquina).

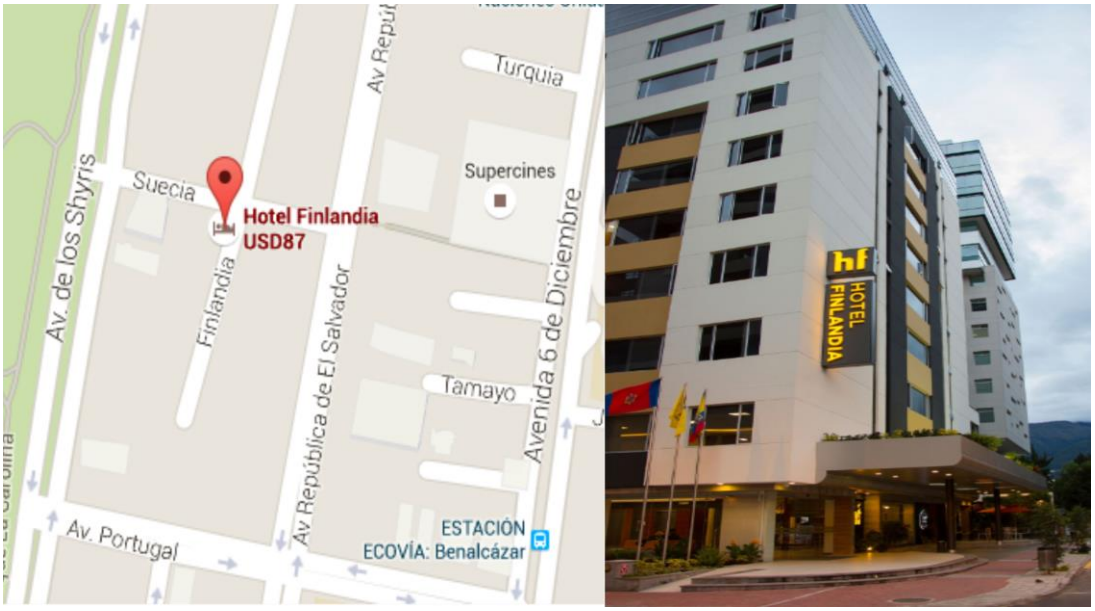


Figura 20. Ubicación Hotel Finlandia.

Tomado de (Hotel Finlandia Quito, s.f.)

2.3 Infraestructura de la Red Inalámbrica Actual

Actualmente la red inalámbrica del Hotel Finlandia es de poco alcance que no abastece a cubrir el nuevo edificio construido. El equipo que se encarga de la administración de la red inalámbrica es el software UniFi Controller, mediante el cual se enganchan los puntos de acceso UniFi AP con la información de configuración establecida dentro del WLC (Wireless LAN Controller). La red cuenta con un backbone de fibra óptica y cableado horizontal con cable UTP cat. 6A. La red es totalmente plana (192.168.1.0). Los APs se encuentran configurados para utilizar los canales manualmente en la banda de 2.4 GHz. La conexión a internet se realiza a través de un enlace simétrico con CNT con un ancho de banda de 10MHz. En la tabla 1 se muestra los SSID configurados en el WLC y el protocolo de seguridad utilizado.

Tabla 1. SSIDs actuales del HOTEL FINLANDIA

WLAN	WLAN SSID	TIPO DE ADMINISTRACION	PROTOCOLO DE SEGURIDAD
1	Huéspedes_Finlandia	Ninguno	WPA_PSK
3	Staff	Ninguno	WPA_PSK

2.4 Ubicación de los APs

El Hotel Finlandia cuenta con 19 APs modelo UAP (UniFi Access Point) distribuidos en todo el edificio, en la tabla 2 se detalla la distribución de los APs por piso. El gerente de sistemas del hotel da a conocer que actualmente cuenta con 56 habitaciones, llegando a un promedio de ocupabilidad de 40 habitaciones, el tiempo de alta ocupabilidad de martes a viernes y de baja ocupabilidad de sábados a lunes. Haciendo uso de la red inalámbrica un promedio de 50 pasajeros al mismo tiempo. En lo que respecta al restaurante y lobby un aproximado de 15 personas se conectan simultáneamente, dando un promedio aproximado 65 conexiones simultáneas. Generalmente las aplicaciones que utilizan los pasajeros son de acceso al correo, navegación en internet, videos. Se verifica los dispositivos conectados a cada uno de los puntos de acceso en el horario de las 9 a 10 de la mañana donde se considera que se tiene mayor número de huéspedes conectados a la red inalámbrica del Hotel y se lo realiza a través del software UniFi Controller.

Tabla 2. Puntos de acceso inalámbrico HOTEL FINLANDIA

Piso	Cantidad APs	Nombre AP	Nº Dispositivos conectados
Piso 1	2	AP_P1_1	3
		AP_P1_2	2
Piso 2	2	AP_P2_1	5
		AP_P2_2	3
Piso 3	2	AP_P3_1	4
		AP_P3_2	2
Piso 4	2	AP_P4_1	3
		AP_P4_2	2
Piso 5	2	AP_P5_1	1
		AP_P5_2	3
Piso 6	2	AP_P6_1	4
		AP_P6_2	3
Piso 7	2	AP_P1_1	1
		AP_P1_2	2
Piso 8	2	AP_P2_1	4
		AP_P2_2	3
Piso 9	2	AP_P3_1	5
		AP_P3_2	2
TOTAL DE DISPOSITIVOS CONECTADOS			62

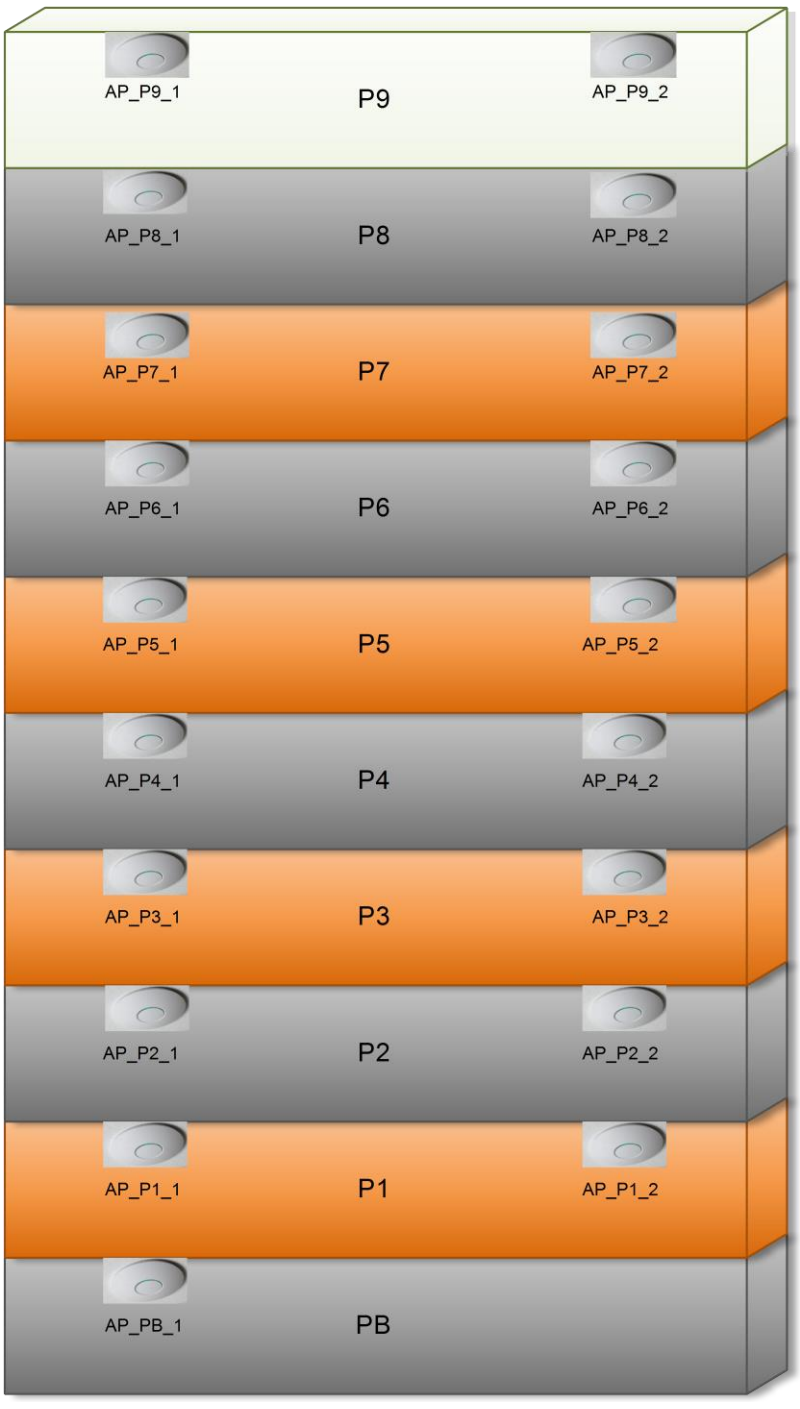


Figura 21. Ubicación APs en el Hotel Finlandia

2.5 Cobertura de la Red Inalámbrica Actual

En el estudio realizado de la situación actual de la red inalámbrica, se verifica que la cobertura de los APs que al momento se encuentran instalados no logra cubrir la nueva torre construida, dejando sin el acceso a internet a esta parte del edificio.

Se realiza un análisis de cobertura de cada uno de los pisos (en los pisos 8 y 9 no se realizará el análisis debido a que se encuentran en remodelación). Se detalla a continuación:

Primer Piso

En el primer piso se encuentran instalados 2 access points ubiquiti modelo UAP (Unifi AP) con puertos ethernet de 10/100 Mbps, cada uno de los APs cuentan con 2 antenas MIMO integradas, trabajan en la banda de frecuencia de 2.4 GHz en los estándares Wi-Fi 802.11 b / g / n (2.4 GHz), la velocidad máxima de transmisión es 54 Mbps, la potencia máxima de transmisión es de 20 dBm (100mW) y el tipo de seguridad configurada es WPA-PSK.

Tabla 3. Configuración APs primer piso.

Nombre AP	SSID	Velocidad de Tx	Banda de Frecuencia	Canal utilizado
AP_P1_1	Huespedes_Finlandia/Staff	54Mbps	2.4 GHz	11
AP_P1_2	Huespedes_Finlandia/Staff	54Mbps	2.4 GHz	11

Configuración básica de Access Point Ubiquiti:

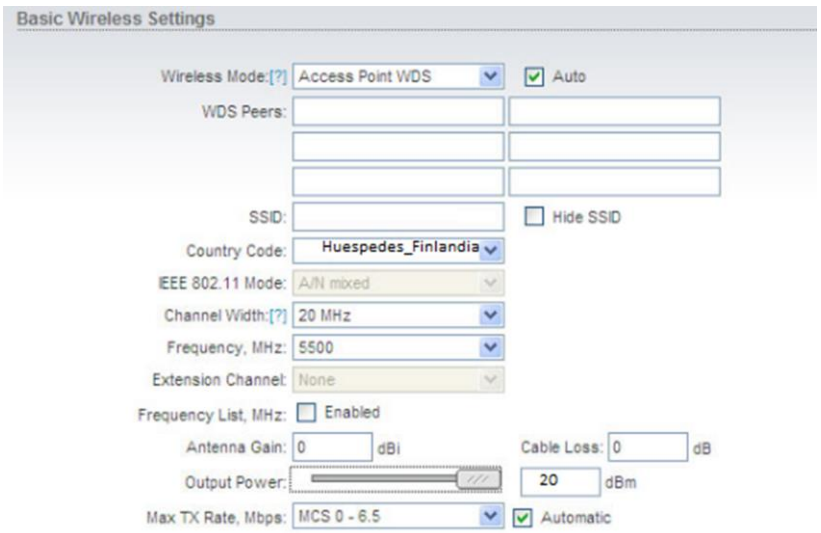


Figura 22. Configuración básica UAP

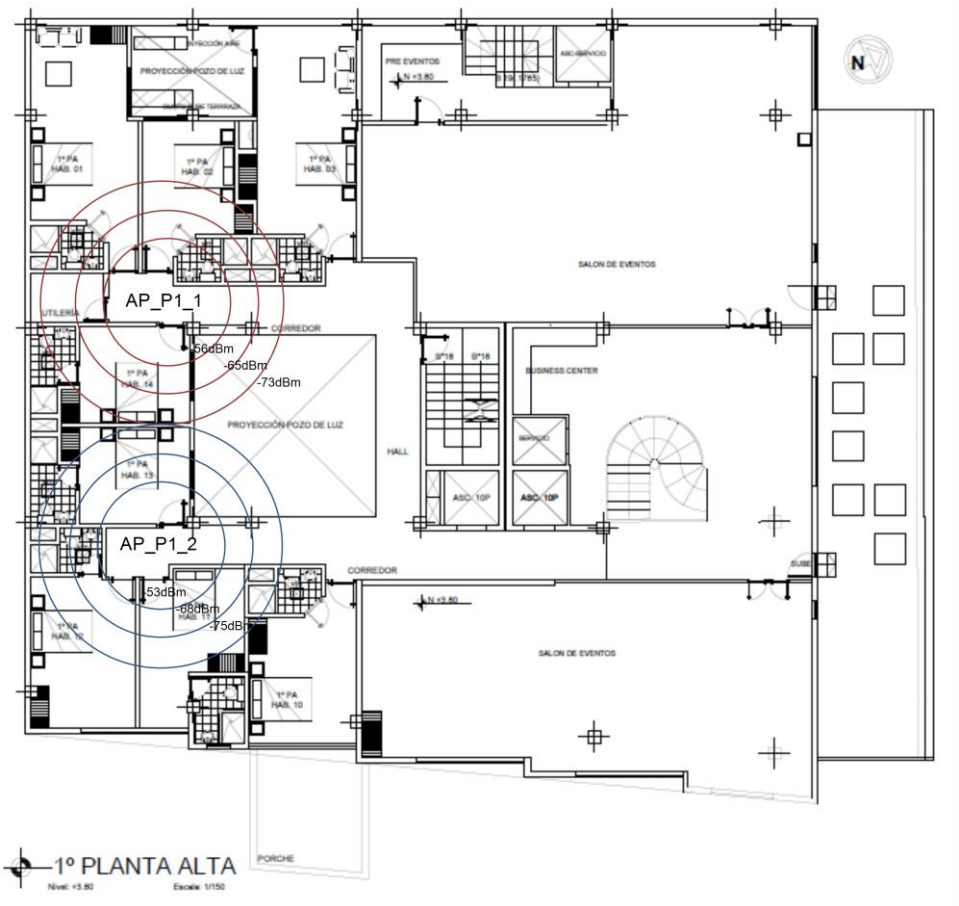


Figura 23. Cobertura APs del primer piso

Segundo Piso

En el segundo piso se encuentran instalados 2 access points ubiquiti modelo UAP (Unifi AP) con puertos ethernet de 10/100 Mbps, cada uno de los APs cuentan con 2 antenas MIMO integradas, trabajan en la banda de frecuencia de 2.4 GHz en los estándares Wi-Fi 802.11 b / g / n (2.4 GHz), la velocidad máxima de transmisión es 54 Mbps, la potencia máxima de transmisión es de 20 dBm (100mW) y el tipo de seguridad configurada es WPA-PSK.

Tabla 4. Configuración APs segundo piso.

Nombre AP	SSID	Velocidad de Tx	Banda de Frecuencia	Canal utilizado
AP_P2_1	Huespedes_Finlandia	54Mbps	2.4 GHz	9
AP_P2_2	Huespedes_Finlandia	54Mbps	2.4 GHz	9

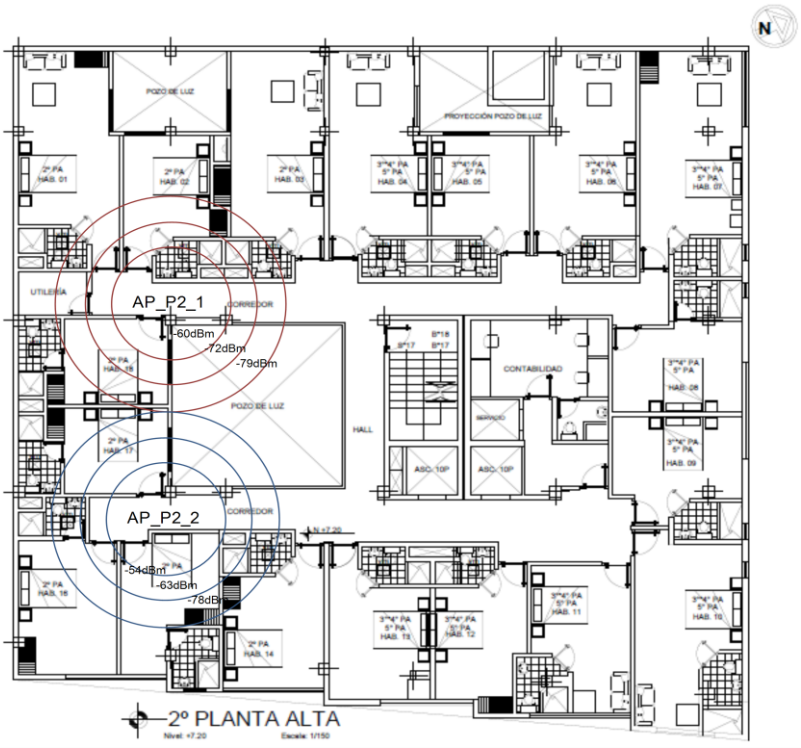


Figura 24. Cobertura APs del segundo piso

Tercer Piso

En el tercer piso se encuentran instalados 2 access points ubiquiti modelo UAP (Unifi AP) con puertos ethernet de 10/100 Mbps, cada uno de los APs cuentan con 2 antenas MIMO integradas, trabajan en la banda de frecuencia de 2.4 GHz en los estándares Wi-Fi 802.11 b / g / n (2.4 GHz), la velocidad máxima de transmisión es 54 Mbps, la potencia máxima de transmisión es de 20 dBm (100mW) y el tipo de seguridad configurada es WPA-PSK.

Tabla 5. Configuración APs tercer piso.

Nombre AP	SSID	Velocidad de Tx	Banda de Frecuencia	Canal utilizado
AP_P3_1	Huespedes_Finlandia	54Mbps	2.4 GHz	11
AP_P3_2	Huespedes_Finlandia	54Mbps	2.4 GHz	11

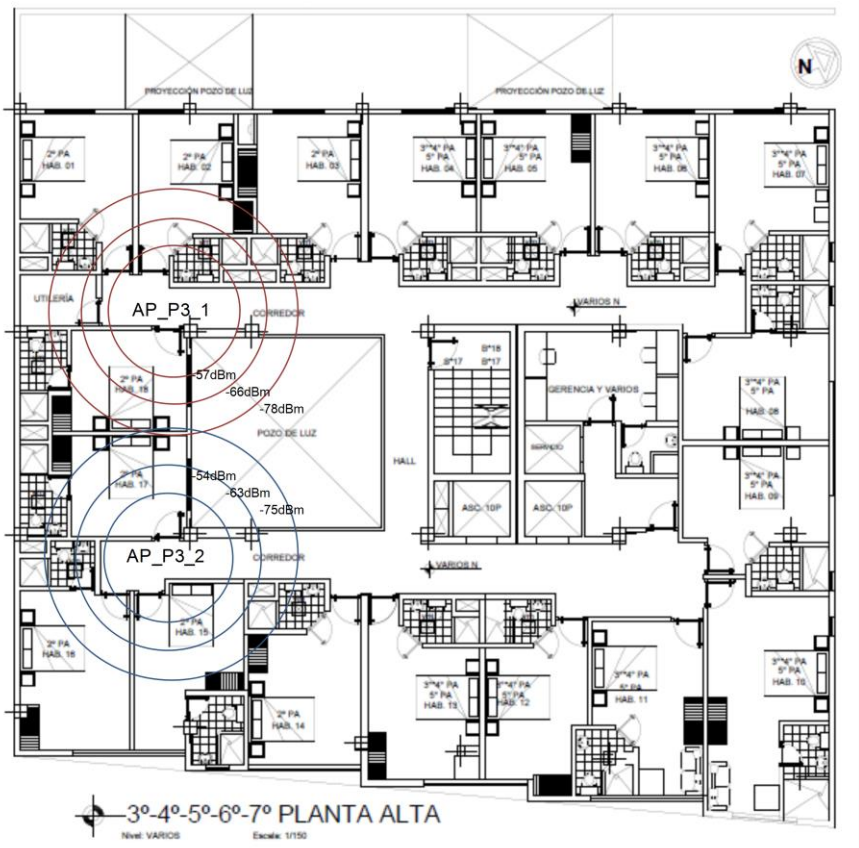


Figura 25. Cobertura APs del tercer piso

Cuarto Piso

En el cuarto piso se encuentran instalados 2 access points ubiquiti modelo UAP (Unifi AP) con puertos ethernet de 10/100 Mbps, cada uno de los APs cuentan con 2 antenas MIMO integradas, trabajan en la banda de frecuencia de 2.4 GHz en los estándares Wi-Fi 802.11 b / g / n (2.4 GHz), la velocidad máxima de transmisión es 54 Mbps, la potencia máxima de transmisión es de 20 dBm (100mW) y el tipo de seguridad configurada es WPA-PSK.

Tabla 6. Configuración APs cuarto piso.

Nombre AP	SSID	Velocidad de Tx	Banda de Frecuencia	Canal utilizado
AP_P4_1	Huespedes_Finlandia	54Mbps	2.4 GHz	9
AP_P4_2	Huespedes_Finlandia	54Mbps	2.4 GHz	9

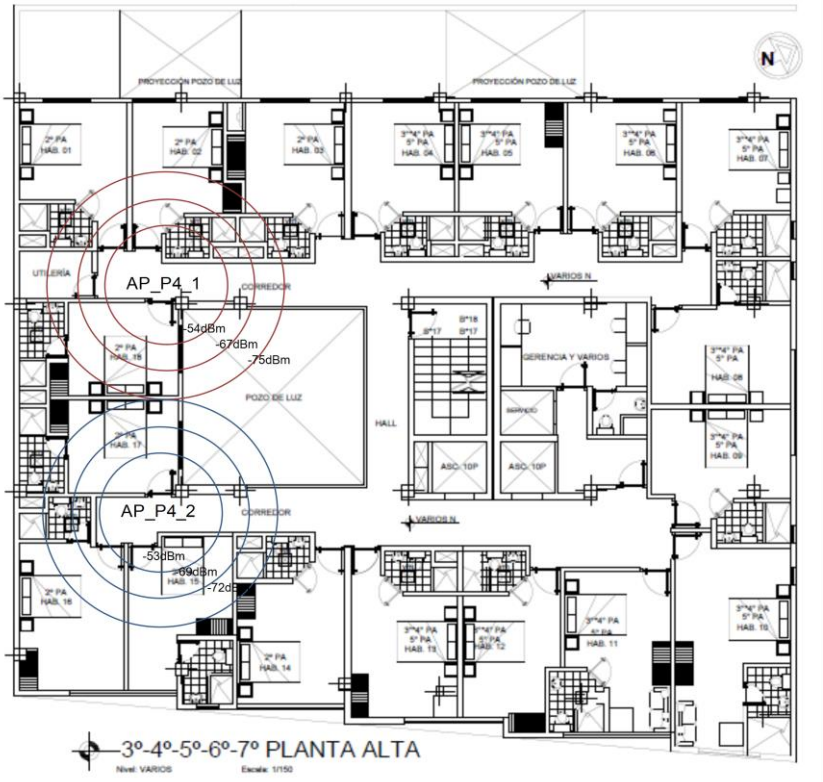


Figura 26. Cobertura APs del cuarto piso

Quinto Piso

En el quinto piso se encuentran instalados 2 access points ubiquiti modelo UAP (Unifi AP) con puertos ethernet de 10/100 Mbps, cada uno de los APs cuentan con 2 antenas MIMO integradas, trabajan en la banda de frecuencia de 2.4 GHz en los estándares Wi-Fi 802.11 b / g / n (2.4 GHz), la velocidad máxima de transmisión es 54 Mbps, la potencia máxima de transmisión es de 20 dBm (100mW) y el tipo de seguridad configurada es WPA-PSK.

Tabla 7. Configuración APs quinto piso.

Nombre AP	SSID	Velocidad de Tx	Banda de Frecuencia	Canal utilizado
AP_P5_1	Huespedes_Finlandia	54Mbps	2.4 GHz	11
AP_P5_2	Huespedes_Finlandia	54Mbps	2.4 GHz	11

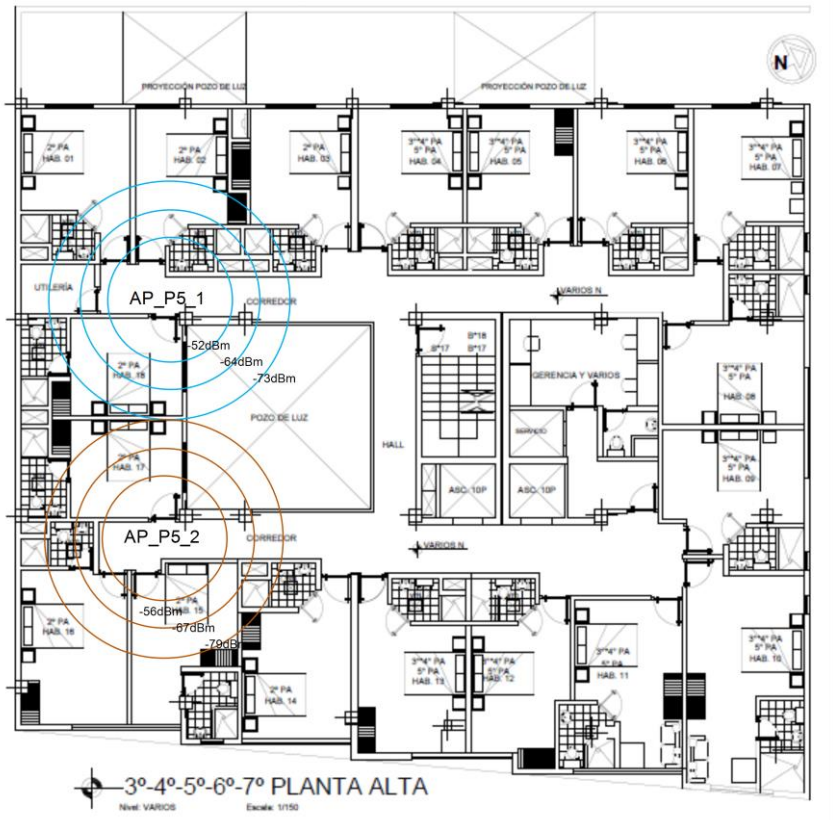


Figura 27. Cobertura APs del quinto piso

Sexto Piso

En el sexto piso se encuentran instalados 2 access points ubiquiti modelo UAP (Unifi AP) con puertos ethernet de 10/100 Mbps, cada uno de los APs cuentan con 2 antenas MIMO integradas, trabajan en la banda de frecuencia de 2.4 GHz en los estándares Wi-Fi 802.11 b / g / n (2.4 GHz), la velocidad máxima de transmisión es 54 Mbps, la potencia máxima de transmisión es de 20 dBm (100mW) y el tipo de seguridad configurada es WPA-PSK.

Tabla 8. Configuración APs sexto piso.

Nombre AP	SSID	Velocidad de Tx	Banda de Frecuencia	Canal utilizado
AP_P6_1	Huespedes_Finlandia	54Mbps	2.4 GHz	9
AP_P6_2	Huespedes_Finlandia	54Mbps	2.4 GHz	9

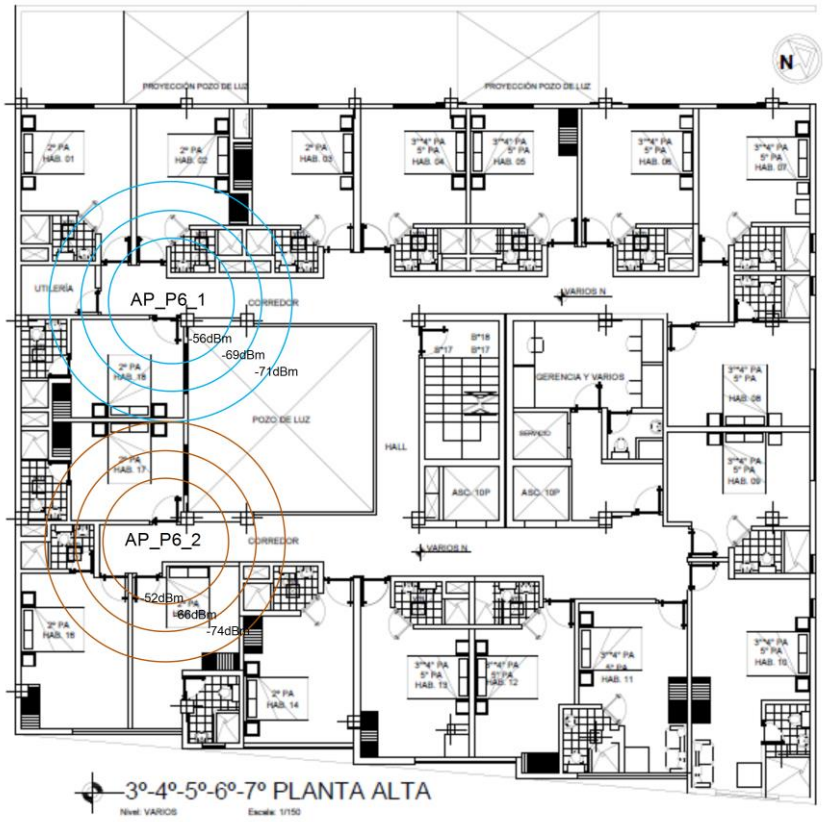


Figura 28. Cobertura APs del sexto piso

Séptimo Piso

En el séptimo piso se encuentran instalados 2 access points ubiquiti modelo UAP (Unifi AP) con puertos ethernet de 10/100 Mbps, cada uno de los APs cuentan con 2 antenas MIMO integradas, trabajan en la banda de frecuencia de 2.4 GHz en los estándares Wi-Fi 802.11 b / g / n (2.4 GHz), la velocidad máxima de transmisión es 54 Mbps, la potencia máxima de transmisión es de 20 dBm (100mW) y el tipo de seguridad configurada es WPA-PSK.

Tabla 9. Configuración APs séptimo piso.

Nombre AP	SSID	Velocidad de Tx	Banda de Frecuencia	Canal utilizado
AP_P7_1	Huespedes_Finlandia	54Mbps	2.4 GHz	11
AP_P7_2	Huespedes_Finlandia	54Mbps	2.4 GHz	11

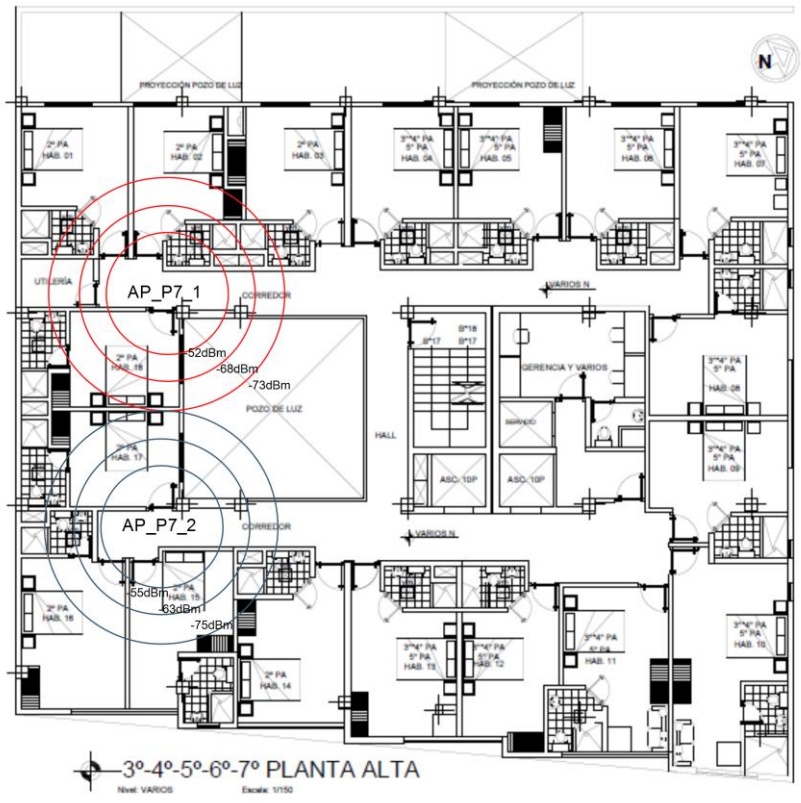


Figura 29. Cobertura APs del séptimo piso

3. DISEÑO DE LA SOLUCIÓN DE RED INALÁMBRICA PARA EL HOTEL FINLANDIA

3.1 Análisis de requerimientos

En base al estudio de la situación actual de la red inalámbrica del Hotel Finlandia surgieron algunos requerimientos que serán muy importantes para el diseño, los cuales se indican a continuación:

- Cobertura: Se requiere que la red inalámbrica cubra toda el área del edificio actual del Hotel Finlandia, que comprende las habitaciones de los huéspedes, el área de lobby, restaurante, subsuelos y salones de eventos

- Capacidad: Se requiere garantizar el ancho de banda para la conexión a internet de los usuarios.

- Seguridad: Se requiere brindar seguridad con alta velocidad en el tráfico de datos.

- Roaming: Transparente, para que los huéspedes no experimenten ninguna interrupción en sus conexiones inalámbricas.

- Administración: integrada y personalizable a través de políticas y perfiles de usuario.

- Gestión: Control del ancho de banda de la red.

- Permitir que los equipos terminales de los huéspedes tanto los que trabajan en las banda de frecuencia a 2.4 GHz y 5.8 GHz operen sin ningún inconveniente.

3.2 Diseño de la Red inalámbrica

En el presente diseño se busca cumplir con las necesidades encontradas en el análisis del estado actual de la red inalámbrica y prever una capacidad y rendimiento futuro. El diseño debe garantizar parámetros como: disponibilidad, escalabilidad, confiabilidad, seguridad, interoperabilidad, autenticación de usuarios, disponibilidad de ancho de banda, gestión y administración centralizada y movilidad.

El diseño de la solución de la red inalámbrica para el hotel Finlandia en el core se realizará con un switch 6850 Alcatel-Lucent (48 puertos Ethernet 100/100 Mbps) encargado de gestionar el tráfico de datos. Para la administración de políticas, anchos de banda y proveer el acceso al internet de calidad para los huéspedes y personal administrativo del hotel se instalará un controlador inalámbrico WHG325 “4ipnet” (Gestión de APs, autenticación de usuarios, asignación de políticas, limitación de tráfico, cortafuegos, etc.). Para proveer la cobertura de la red inalámbrica en el hotel, se ha distribuido access points (APs) en todo el edificio. Para los huéspedes se ha distribuido 4 APs modelo EAP727 por piso que van conectados a switches PoE (Power over Ethernet) que gestionarán el tráfico de red mediante los switches de acceso Alcatel-Lucent conectados mediante el enlace de fibra óptica. Para la recepción, restaurante, subsuelos y salas de eventos está gestionada por APs de alta densidad modelo EAP767.

3.3 Tecnología de la red inalámbrica.

La tecnología a utilizar en el presente diseño lleva el nombre de Wi-Fi o IEEE 802.11, ofreciendo una velocidad máxima de 1300 Mbps y capaz de soportar los siguientes estándares IEEE 802.11a, b, g, n, ac.

3.4 Topología y diseño de la red inalámbrica propuesto.

En el gráfico siguiente se describe la topología y el diseño completo de la solución de red inalámbrica para el Hotel Finlandia.

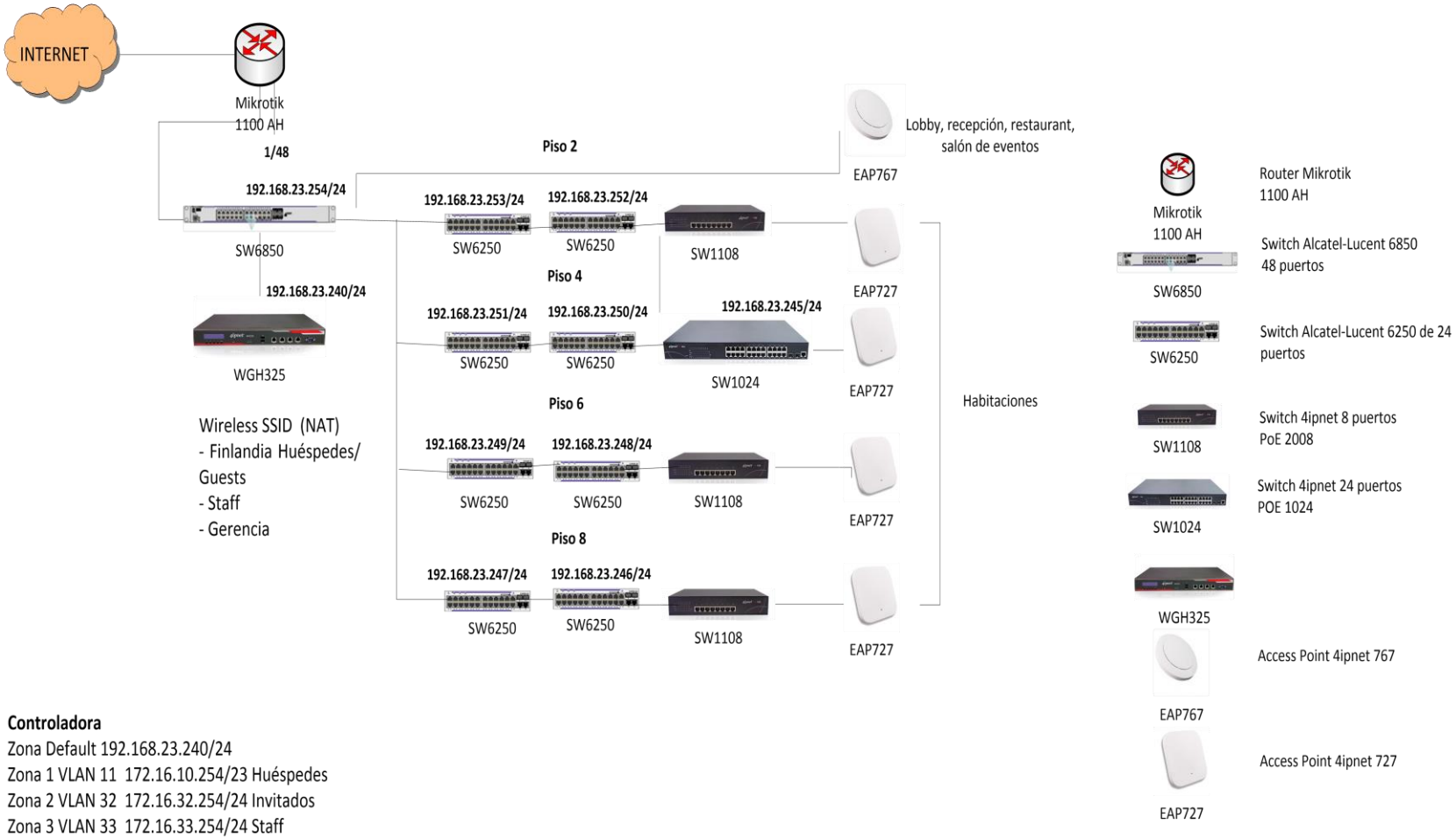


Figura 30. Topología de la Red Inalámbrica del Hotel Finlandia

3.5 Estimación de usuarios simultáneos y ancho de banda.

Las redes inalámbricas debido a la forma que acceden al medio comparten el mismo ancho de banda entre todos los usuarios conectados simultáneamente. Por tal motivo es necesario realizar un estimado de ancho de banda ya que mientras exista mayor cantidad de usuarios el rendimiento de la red inalámbrica será menor.

El Hotel Finlandia divide las zonas de servicios/clientes en base a los tipos de usuarios que harán uso de la red:

- *Huéspedes*
- *Invitados*
- *Staff*

Huéspedes: Dispondrá de una conexión con una velocidad limitada a 256Kps, y con la duración que dependerá de su estadía en el hotel, como base 7 días. Cuando realice el Check-In el personal de recepción le facilitará los datos de la red Wifi.

Invitados: Conexión con una velocidad limitada a 512Kbps individualmente y con un día de duración.

Staff: Conexión de 256Kps durante 24 horas.
Calculo de ancho de banda simultáneo:
70 huéspedes x 256Kps=17.9 Mbps
20 invitados x 512Kbps=10.2Mbps
10 staff x 256Kbps= 2.5Mbps

TOTAL: 100 Usuarios simultáneos y con un caudal total de =36.6Mbs

En una situación de consumo “máximo” podemos precisar de al menos 35Mbps, en otro caso sufriremos cuellos de botella en caso que se conecten más dispositivos de los estimados.

El control del ancho de banda es importante ya que permite manejar el total de ancho de banda disponible, para ofrecer diferentes niveles de servicios a diferentes usuarios o grupos de usuarios finales. También permite prestar servicios a más usuarios, ya que incluso un solo usuario puede utilizar todo el ancho de banda disponible para una sola aplicación. La regulación de ancho banda es una característica de calidad de servicio (QoS, Quality of Service).

3.6 Características principales de los equipos utilizados en el Diseño de la Red Inalámbrica.

3.6.1 Controlador inalámbrico WHG325

El WHG325 de “4ipnet” es un controlador LAN inalámbrico que permite la gestión de APs, la autenticación de usuarios, asignación de políticas, limitación de tráfico, y firewall, etc.

El WHG325 es capaz de gestionar hasta 80 APs (puntos de acceso inalámbricos) Los APs, así como los dispositivos Wi-Fi conectados, pueden ser monitoreados y gestionados desde un punto centralizado, con amplias funciones de registro y presentación de informes para ayudar en la solución de problemas y facilitar el mantenimiento óptimo de la red WI-FI.

Figura 31. Controlador inalámbrico WHG325
Tomado de (Storepcimagine, s.f.)

Características principales del controlador inalámbrico WHG325:

- Administración de hasta 80 APs
- Descubrimiento y carga automática de APs.
- Gestión de usuarios: asignación de políticas de usuario, limitación de ancho de banda.
- Seguridad de usuarios.
- Login automático por código QR.

En el Anexo A se encuentran las especificaciones del controlador inalámbrico “4ipnet” WHG325).

3.6.2 Access Point “4ipnet” 767

El punto de acceso inalámbrico EAP767 está diseñado para interiores, específicamente para entornos de alta densidad. Utiliza el estándar Wi-Fi 802.11ac que ofrece una mayor amplitud y más avanzadas técnicas de modulación; cuenta con dos radios MIMO 3x3 que puede soportar hasta 450 Mbps y 1300 Mbps velocidades de datos en las bandas de 2,4 GHz y 5 GHz respectivamente. Consta de 6 antenas internas para amplificar la cobertura inalámbrica y soporta PoE (Power over Ethernet) que elimina la necesidad de disponer de una toma de corriente cerca de la ubicación del dispositivo proporcionando máxima flexibilidad de despliegue. Al combinarlo con el controlador inalámbrico WHG325 de “4ipnet”, ofrece más características adicionales, tales como el control de ancho de banda, la autenticación de usuarios, gestión de red inalámbrica integrada y red personalizable.

Figura 32. Access Point 4ipnet 767
Tomado de (Wifisafe, s.f.)

Características principales del Access Point “4ipnet” 767:

- Estándar que utiliza: 802.11 a / b / g / n /ac.
- Bandas de frecuencia en que opera: 2,4 y 5 GHz a la vez.
- Potencia de salida: hasta 25 dBm en la banda de 2.4 GHz y hasta 25 dBm en la banda de 5 GHz.
- Velocidad de transmisión: hasta 450 Mbps (2.4 GHz) y hasta 1.3 Gbps (5 GHz)
- Canales de operación: 2.4 GHz: 1 – 11 (EE.UU.), 1 – 13 (Europa), 1 – 13 (Japón), 5 GHz: 36 – 165 (EE.UU.), 36 – 140 (Europa), 36 – 140 (Japón).
- Seguridad: WEP, WPA / WPA2, WPA2 - Personal, WPA2 - Enterprise (802.1X), TKIP y Cifrado AES. (4ipnet, 2016)
- Compatible con PoE (Power over Ethernet).

En el Anexo B se encuentran las especificaciones del Access Point “4ipnet” EAP767).

3.6.3 Access Point “4ipnet” EAP727

El EAP727 está diseñado para interiores, específicamente para entornos de alta densidad. Utiliza el estándar Wi-Fi 802.11ac que ofrece una mayor amplitud y más avanzadas técnicas de modulación; cuenta con dos radios MIMO 2x2 que puede soportar hasta 300 y 867 Mbps velocidades de transmisión de datos en las bandas de 2,4 GHz y 5 GHz respectivamente. Incluye 4 antenas internas para amplificar la cobertura inalámbrica y soporta PoE (Power over Ethernet) que elimina la necesidad de disponer de una toma de corriente cerca de la ubicación del dispositivo proporcionando máxima flexibilidad de despliegue. Al combinarlo con el controlador inalámbrico WHG325 de “4ipnet”, ofrece más características adicionales, tales como el control de ancho de banda, la autenticación de usuarios, gestión de red inalámbrica integrada y red personalizable.

Figura 33. Access Point 4ipnet 727
Tomado de (wifisafe, s.f.)

Características principales del AP “4ipnet” 727:

- Doble banda 2,4 y 5 GHz simultáneo.
- Estándar 802.11 a / b / g / n /ac. (4ipnet,s.f.)
- Potencia de salida: 2.4 GHz: hasta 27 dBm 5 GHz: hasta 26 dBm.

- Velocidad de transmisión: hasta 300 Mbps (2.4 GHz) y hasta 867 Mbps (5 GHz)
- Canales de operación: 2.4 GHz: 1 – 11 (EE.UU.), 1 – 13 (Europa), 1 – 13 (Japón), 5 GHz: 36 – 165 (EE.UU.), 36 – 140 (Europa), 36 – 140 (Japón).
- Seguridad: WEP, WPA/WPA2, WPA2-Personal, WPA2-Enterprise (802.1X), TKIP y cifrado AES. (4ipnet, s.f.)
- Compatible con PoE (Power over Ethernet).

(En el Anexo C se encuentran las especificaciones del Access Point “4ipnet” EAP727).

3.6.4 Switch Alcatel-Lucent 6850 48 puertos

El switch 6850-48 es apilable que cuenta con 44 puertos 10/100/1000Base-T, así como también de cuatro puertos individualmente configurables para ser 10/100/1000Base-T o 1000Base-X conexiones de alta velocidad. El panel frontal del chasis del switch 6850-48 contiene los siguientes componentes principales: estado del sistema y la ranura, LED indicador 44 compartir puertos 10/100/1000Base-T, combo compartida (4) puertos 10/100/1000Base-T, 4 ranuras SFP combinadas para 1000Base-X conexiones, puerto de consola (RJ-45) y un puerto USB (USB 2.0). (En el Anexo C se encuentran las especificaciones del Switch Alcatel-Lucent 6850).

Figura 34. Switch Alcatel-Lucent 6850
Tomado de (Tritel, s.f.)

Características principales Switch Alcatel-Lucent 6850:

- Alta disponibilidad.
- Gigabit en la periferia.
- Agregación y distribución de capa 3

(En el Anexo D se encuentran las especificaciones del Switch Alcatel-Lucent 6850).

3.6.5 Switch Alcatel-Lucent 6250

Figura 35. Switch Alcatel-Lucent 6250
Tomado de (Storemsifokom, s.f.)

Características principales Switch Alcatel-Lucent 6850:

- Alta disponibilidad.
- Gigabit en la periferia.
- Agregación y distribución de capa 3

(En el Anexo E se encuentran las especificaciones del Switch Alcatel-Lucent 6850).

3.6.6 Switch “4ipnet” 24 puertos PoE 1024

El SW1024 es totalmente administrable y se integra con el controlador LAN inalámbrico WHG325 y con los puntos de acceso EAP767 y EAP727. Es un switch de capa 2 de alto rendimiento, tiene 26 puertos PoE (Power over Ethernet) los cuales están conformados por 24 puertos Ethernet 10/100/1000 Mbps RJ-45 y 2 puertos gigabit SFP. Este equipo soporta la configuración de VLANs, Link Aggregation, Spanning Tree, Port trunking, Port Security, QoS, Rate Control, RADIUS, TACAS+, entre otros.

Figura 36. Switch 4ipnet 24 puertos PoE 1024
Tomado de (4ipnet, s.f.)

Características principales del switch “4ipnet” 24 puertos PoE 1024:

- Fiable, robusto y seguro
- Alto rendimiento.
- Fácil instalación y mantenimiento.
- Compatible con PoE, también admite 802.3at PoE para alimentar nuevas 802.11n o puntos de acceso inalámbricos 802.11ac que tienen mayores consumos de energía.
- Múltiples métodos de autenticación de usuarios: 802.1X y Mac.

(En el Anexo F se encuentran las especificaciones del switch “4ipnet” 24 puertos PoE 1024).

3.6.7 Switch “4ipnet” 8 puertos PoE 2008

El switch de acceso SW1024 se integra con el controlador LAN inalámbrico WHG325 y con los puntos de acceso EAP767 y EAP727. Tiene 8 puertos PoE más 2 puertos gigabit SFP, soporta un total de 250W de salida para alimentar hasta 8 dispositivos PoE, con hasta 30W para cada uno de sus puertos IEEE 802.3af/at. Soporta una tasa de retransmisión de paquetes de 1.448.000 paquetes por segundo.

Figura 37. Switch 4ipnet 8 puertos PoE 2008
Tomado de (4ipnet, s.f.)

Características principales del switch “4ipnet” 8 puertos PoE 2008:

- Fácil configuración e implementación.
- Costos reducidos con la compatibilidad PoE.
- Potencia de salida 250W.
- Tasa de reenvío de 1.488 Mbps.

(En el Anexo G se encuentran las especificaciones del switch “4ipnet” 8 puertos PoE 2008).

3.6.8 Ticketera “4ipnet” WTG2

La ticketera WTG2 permite la creación e inicio de sesión de cuentas Wi-Fi utilizando el teclado SDS200W el cual activa las cuentas integradas en el plan de facturación on-demand(s) dentro del controlador inalámbrico y luego imprime tickets a través de la impresora PRT200. Además la ticketera WTG2 permite a los huéspedes logearse automáticamente mediante el uso de código QR2, los dispositivos móviles escanean el código QR impreso que pueden ser personalizados fácilmente en el controlador inalámbrico WHG325 según las necesidades.

Figura 38. Ticktera 4ipnet WTG2
Tomado de (Esoft, s.f.)

Características principales de la ticktera “4ipnet” WTG2:

- Interfaces del teclado inalámbrico SDS200W: Uplink:1 *10/100Base-T Ethernet, Auto MDIX.RJ45, Serial:1 * RS-232 DB9M.
- Incluye antena externa omnidireccional de 3dBi.
- Estándar que utiliza: 802.11 b / g / n, en la banda de 2.4 GHz. (4ipnet, s.f.)

(En el Anexo H se encuentran las especificaciones de la ticktera “4ipnet” WTG2).

3.7 Configuración de los puntos de acceso.

Se accede a la interfaz de administración web del controlador WHG325 a través del browser desde cualquier PC conectado a la interfaz LAN con la dirección IP por defecto 192.168.1.254.

Para la configuración de los puntos de acceso dentro del controlador inalámbrico se lo puede realizar a través de plantillas, se selecciona el modelo de AP y se configura la plantilla de defecto o a su vez se agrega una nueva.

Se selecciona la tarjeta de radiofrecuencia para el AP entre la tarjeta A de 2.4 GHz y la tarjeta B de 5 GHz. Dependiendo del modelo de AP podemos seleccionar la banda de frecuencia, el tipo de sincronización de 56 bits o 128 bits, el ancho del canal entre 20Mhz, 40Mhz o 20Mhz/40Mhz, (80 Mhz si es banda de 5Ghz) el canal, máxima velocidad de transmisión cuya valor predeterminado es automático, potencia donde el nivel 1 es el más alto y cada nivel representa un decremento de 1dB a la máxima potencia, umbral de retardo de paquetes y de frecuencia de transmisión, detección de interferencia, entre otros parámetros.

Las plantillas creadas para cargar a los puntos de acceso EAP727 son las siguientes: 727_SOC_NOC, 727_SOR_NOR, 727_Gerencia.

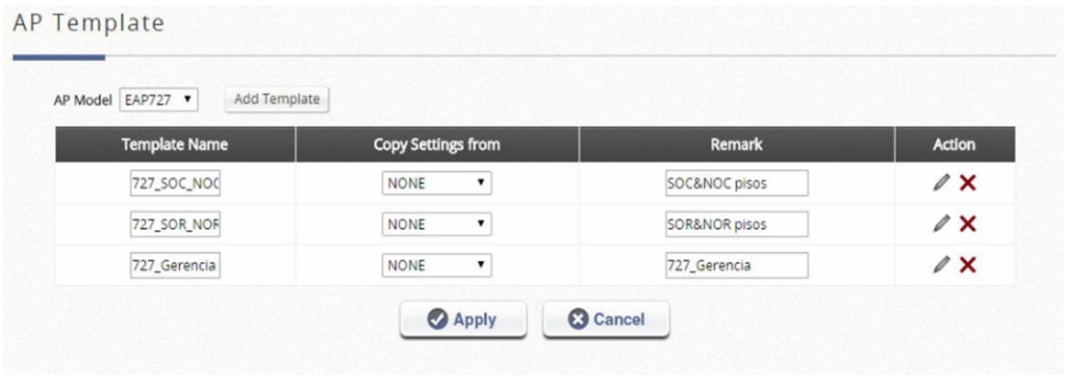


Figura 39. Plantillas creadas para configuración de APs EAP727

Las plantillas creadas para cargar a los puntos de acceso EAP767 son las siguientes: Config727 y Confi767face.

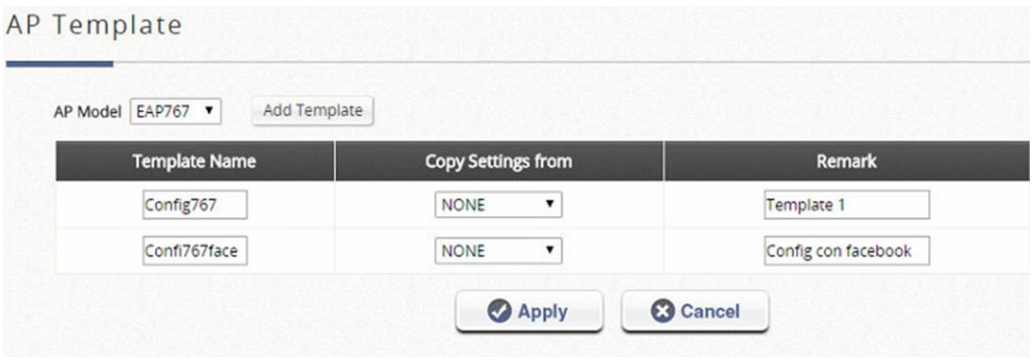


Figura 40. Plantillas creadas para configuración de los APs EAP767

Se agrega manualmente los APs a la lista de administración. Se requiere configurar los siguientes parámetros: el tipo de AP, nombre, IP y MAC.

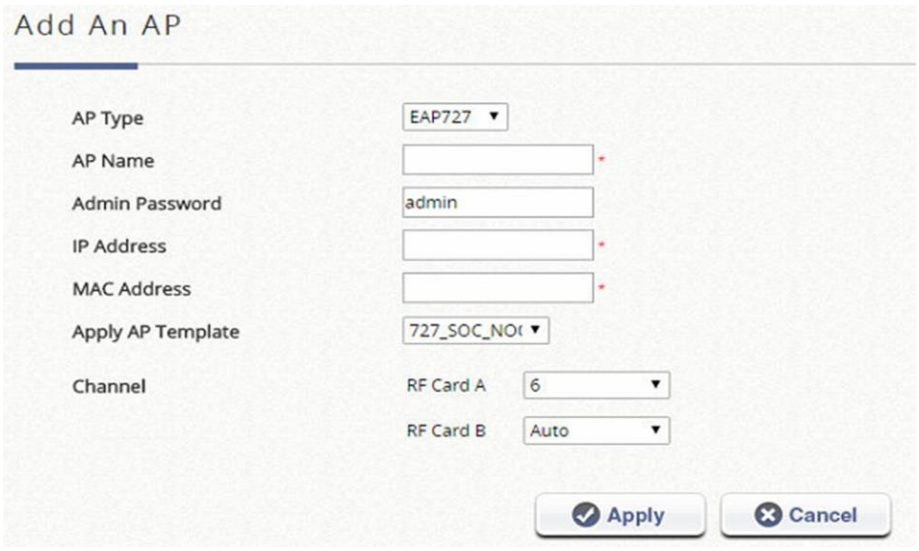


Figura 41. Parámetros a configurar al agregar los APs727

Configuración en la banda de 2.4Ghz, seleccionamos el ancho del canal, el nivel de potencia y el canal de operación en este caso es configurado manualmente.

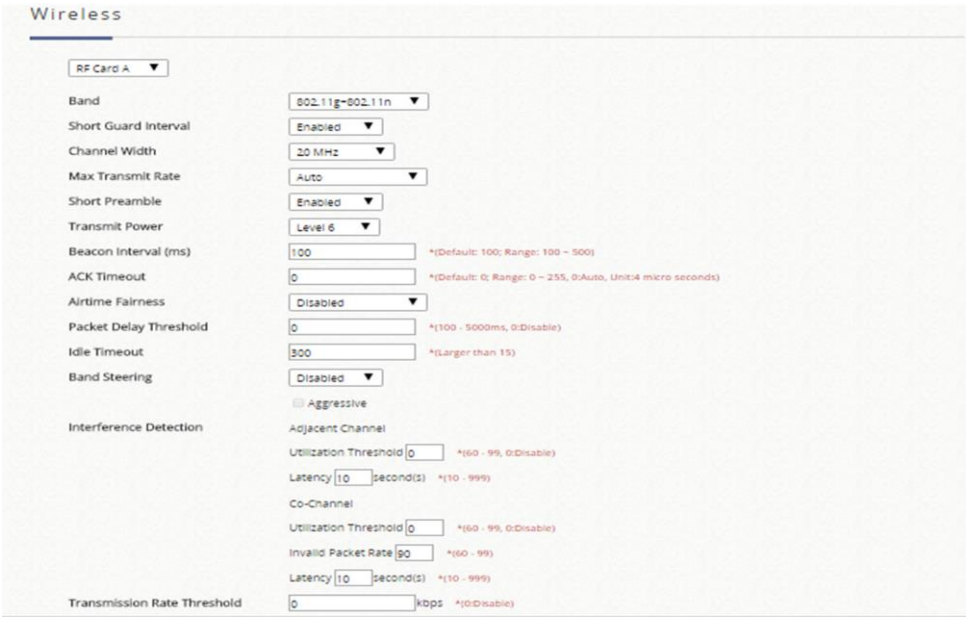


Figura 42. Parámetros a configurar en la banda de 2.4GHz

Configuración en la banda de 5Ghz, seleccionamos el ancho de banda, el nivel de potencia y el canal de operación en este caso es automático.

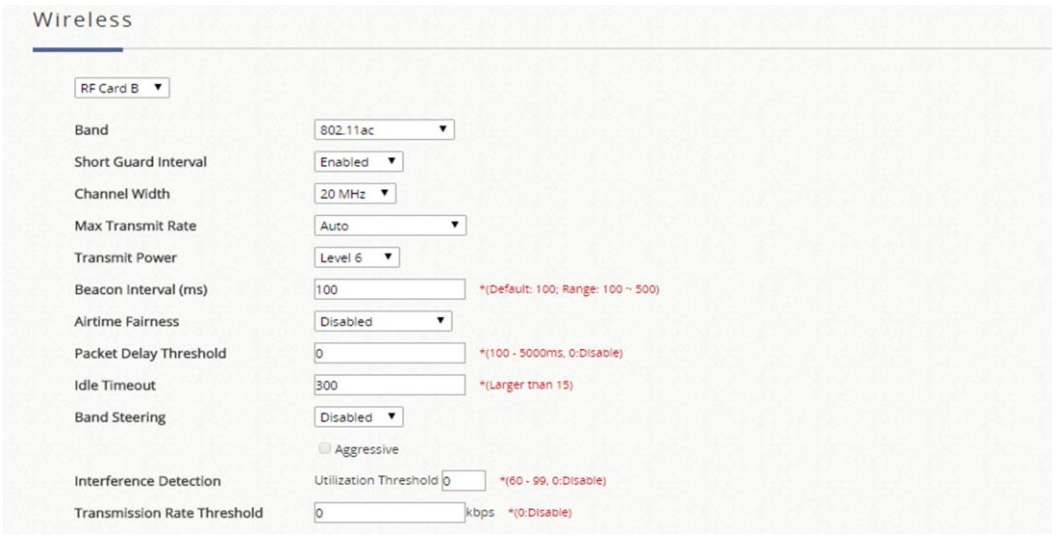


Figura 43. Parámetros a configurar en la banda de 5GHz

Una vez ingresados los APs, aplicamos la configuración de las plantillas creadas para cada tipo de Access point, en el cual se configura de forma manual los canales a utilizar en el caso de los APs EAP727 y el APs EAP767 de forma automática. La tabla 10 muestra el listado de los APs configurados:

Tabla 10. Listado de APs configurados

Ubicación	Nombre	Tipo de AP	IP	MAC
Subsuelo 1	AP_S1_SOCC	EAP767	192.168.23.48	00:1F:D4:04:6D:D9
Subsuelo 1	AP_S1_SOR	EAP767	192.168.23.49	00:1F:D4:04:6D:E8
Planta Baja	AP_PB_SOR	EAP767	192.168.23.24	00:1F:D4:04:6D:F7
Planta Baja	AP_PB_NOCC	EAP767	192.168.23.25	00:1F:D4:04:6D:F4
Piso 1	AP_P1_SOR	EAP727	192.168.23.10	00:1F:D4:04:45:3D
Piso 1	AP_P1_SOCC	EAP727	192.168.23.11	00:1F:D4:04:43:3F
Piso 1	AP_P1_NOR	EAP767	192.168.23.46	00:1F:D4:04:6D:EB
Piso 1	AP_P1_NOCC	EAP767	192.168.23.47	00:1F:D4:04:6D:C7
Piso 2	AP_P2_SOR	EAP727	192.168.23.12	00:1F:D4:04:45:43
Piso 2	AP_P2_SOCC	EAP727	192.168.23.13	00:1F:D4:04:43:48
Piso 2	AP_P2_NOR	EAP727	192.168.23.14	00:1F:D4:04:43:36
Piso 2	AP_P2_NOCC	EAP727	192.168.23.15	00:1F:D4:04:43:96

Piso 3	AP_P3_SOR	EAP727	192.168.23.16	00:1F:D4:04:45:40
Piso 3	AP_P3_SOCC	EAP727	192.168.23.17	00:1F:D4:04:45:28
Piso 3	AP_P3_NOR	EAP727	192.168.23.18	00:1F:D4:04:44:F8
Piso 3	AP_P3_NOCC	EAP727	192.168.23.19	00:1F:D4:04:44:6E
Piso 4	AP_P4_SOR	EAP727	192.168.23.20	00:1F:D4:04:45:4F
Piso 4	AP_P4_SOCC	EAP727	192.168.23.21	00:1F:D4:04:43:B1
Piso 4	AP_P4_NOR	EAP727	192.168.23.22	00:1F:D4:04:43:BD
Piso 4	AP_P4_NOCC	EAP727	192.168.23.23	00:1F:D4:04:43:B4
Piso 5	AP_P5_SOR	EAP727	192.168.23.26	00:1F:D4:04:42:D3
Piso 5	AP_P5_SOCC	EAP727	192.168.23.27	00:1F:D4:04:43:FC
Piso 5	AP_P5_NOR	EAP727	192.168.23.28	00:1F:D4:04:43:E1
Piso 5	AP_P5_NOCC	EAP727	192.168.23.29	00:1F:D4:04:43:FF
Piso 6	AP_P6_SOR	EAP727	192.168.23.30	00:1F:D4:04:42:E8
Piso 6	AP_P6_SOCC	EAP727	192.168.23.31	00:1F:D4:04:43:9C
Piso 6	AP_P6_NOR	EAP727	192.168.23.32	00:1F:D4:04:42:BB
Piso 6	AP_P6_NOCC	EAP727	192.168.23.33	00:1F:D4:04:44:F5
Piso 7	AP_P7_SOR	EAP727	192.168.23.34	00:1F:D4:04:44:74
Piso 7	AP_P7_SOCC	EAP727	192.168.23.35	00:1F:D4:04:43:F3
Piso 7	AP_P7_NOR	EAP727	192.168.23.36	00:1F:D4:04:43:7E
Piso 7	AP_P7_NOCC	EAP727	192.168.23.37	00:1F:D4:04:43:8D

3.8 Roaming

El roaming en los access points se da gracias a la presencia de la controladora inalámbrica y funcionara de la siguiente forma, pero cabe resaltar que la decisión la toma el dispositivo móvil:

- Un usuario inalámbrico está conectado al AP_P1_NOCC y de repente se desplaza y el nivel de RSSI baja y se desconecta, automáticamente la tarjeta de red Inalámbrica del usuario buscara la misma red en diferentes frecuencias y encontrara a AP_P1_SOR con el mismo: SSID, sistema de validación; y se conectara.
- Para ese momento el AP_P1_NOCC habrá notificado a la controladora inalámbrica que el usuario ya no se encuentra conectado y el AP_P1_SOR notificara la conexión de un nuevo usuario que tendrá la misma MAC que ha dejado el AP_P1_NOCC, entonces el controlador inalámbrico da la instrucción al AP_P1_NOCC de trasladar las sesiones del usuario al AP_P1_SOR, con esto se dará el Roaming.

3.9 Configuración de las zonas de servicio

Las zonas de servicio emulan la configuración de interfaces en un router, de tal modo que podemos realizar los ajustes acorde a los requerimientos de la red. Las zonas de servicio habilitadas son: Default, SZ1Huespedes, SZ2Invitados y SZ3Staff que se detallan en la tabla 11:

Tabla 11. Zonas configuradas.

ZONA	NOMBRE	IP	VLAN	RANGO DHCP		SSID
	Defecto	192.168.23.240	N/A	192.168.23.71	192.168.23.201	Gerencia
Zona 1	Huéspedes	172.16.10.254	10	172.16.10.10	172.16.13.250	Finlandia Huespedes/Guests
Zona 2	Invitados	172.16.32.254	32	172.16.32.10	172.16.32.250	Invitados
Zona 3	Staff	172.16.33.254	33	172.16.33.10	172.16.33.250	Staff

3.9.1 Zona Default

En esta zona se configura el direccionamiento IP de la red inalámbrica y se ingresa el controlador inalámbrico en este mismo segmento de red. El servicio de la zona default viene habilitado y se lo asigna a la configuración de los APs. Los parámetros a configurar son: nombre, modo de operación, dirección IP y la máscara.

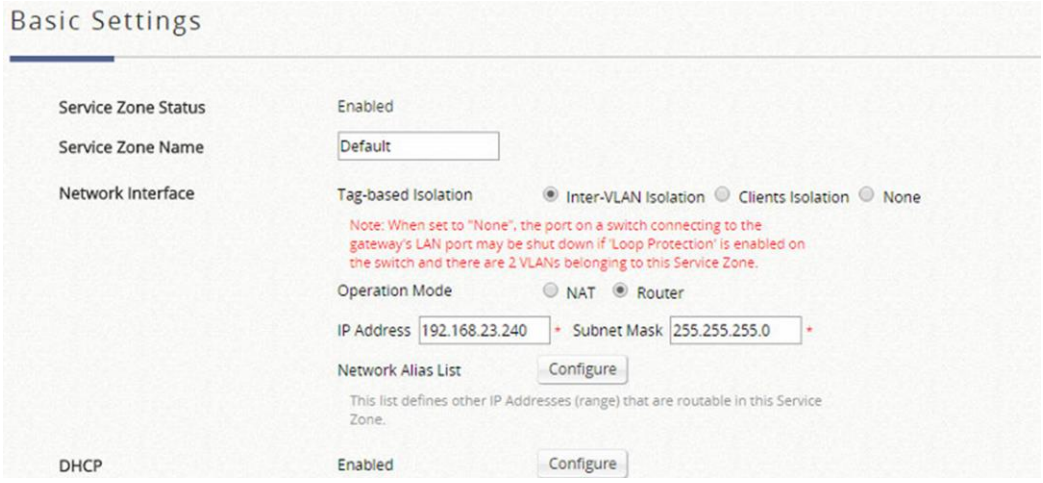


Figura 44. Configuración básica de la zona de servicio default

Se elige el rango de IP que serán asignados a los APs, se habilita la política 3 que posteriormente será configurada y se deshabilita la autenticación de la zona ya que no se necesitará del Hot-spot en dicha interfaz.

El Portal URL define el destino de enlace al cual el navegador web del usuario redireccionará al momento de realizar un login satisfactorio y en este caso se configura que sea http://www.google.com.

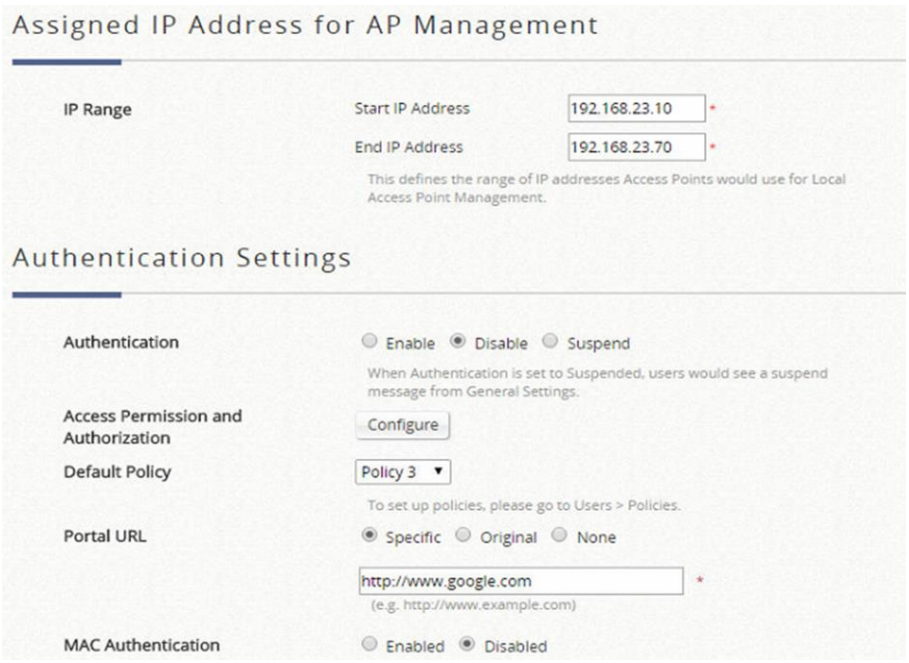


Figura 45. Configuración de la autenticación de la zona default

3.9.2 Zona SZ1Huespedes

A esta zona se le asignará el SSID “Finlandia Huespedes/Guests”, se configura la interfaz en modo de operación “router” para tener acceso a la red. Los parámetros configurados son: estado, nombre, vlan, asignamos una dirección IP y la máscara.

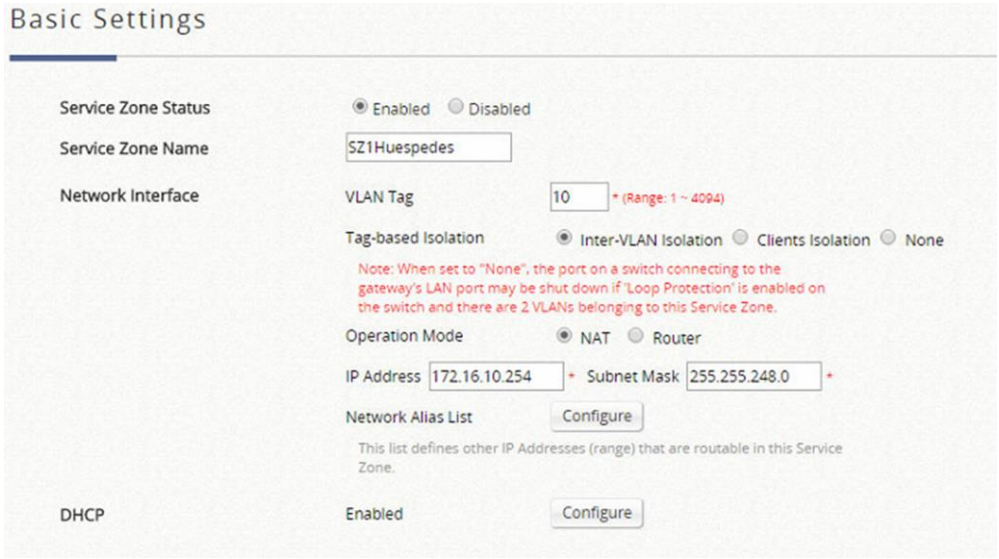


Figura 46. Configuración básica de la zona SZ1Huespedes

En esta zona no se configura el direccionamiento IP de este segmento de red ya que no se asignan APs, se deja asignada la política 1 que posteriormente se configura. Se habilita la autenticación de esta zona para que aparezca al portal de acceso en dicha interfaz.

El portal URL define el destino de enlace al cual el navegador web del usuario redireccionará al momento de realizar un login satisfactorio y en este caso se configura que sea http://www.google.com.

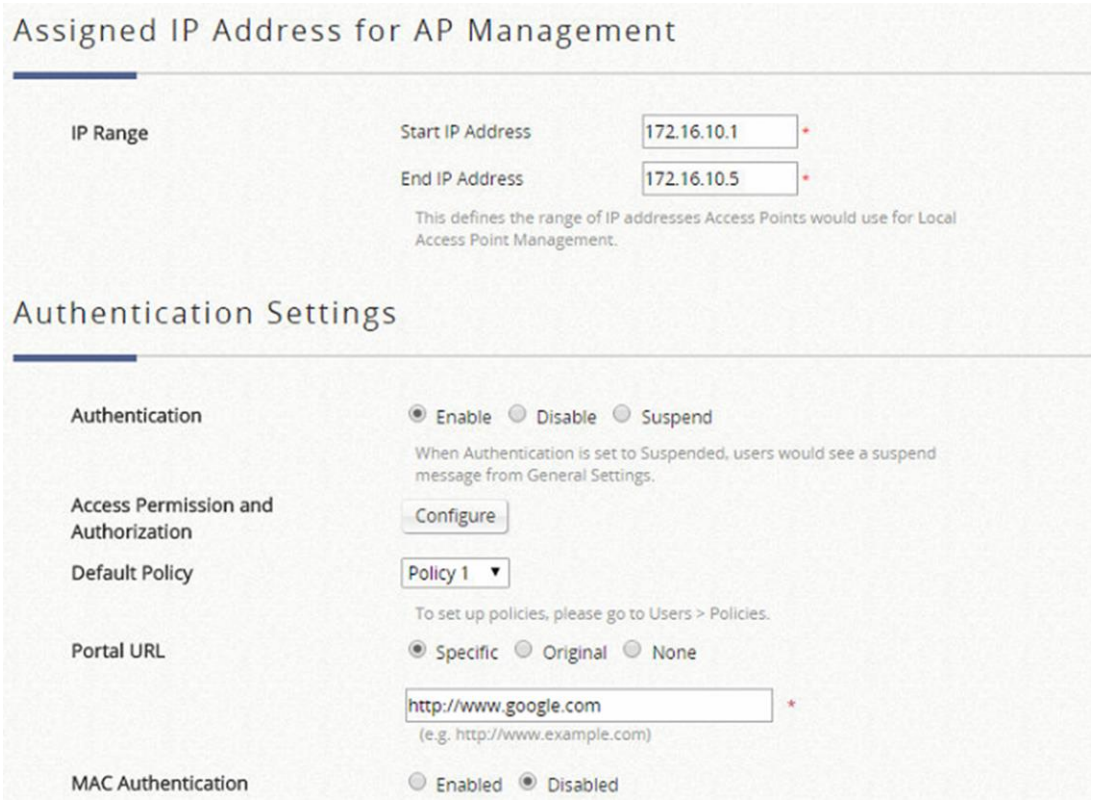


Figura 47. Configuración de autenticación de la zona SZ1Huespedes

Se habilita la configuración DHCP, el rango de direcciónes IP del DHCP y el servidor DNS.

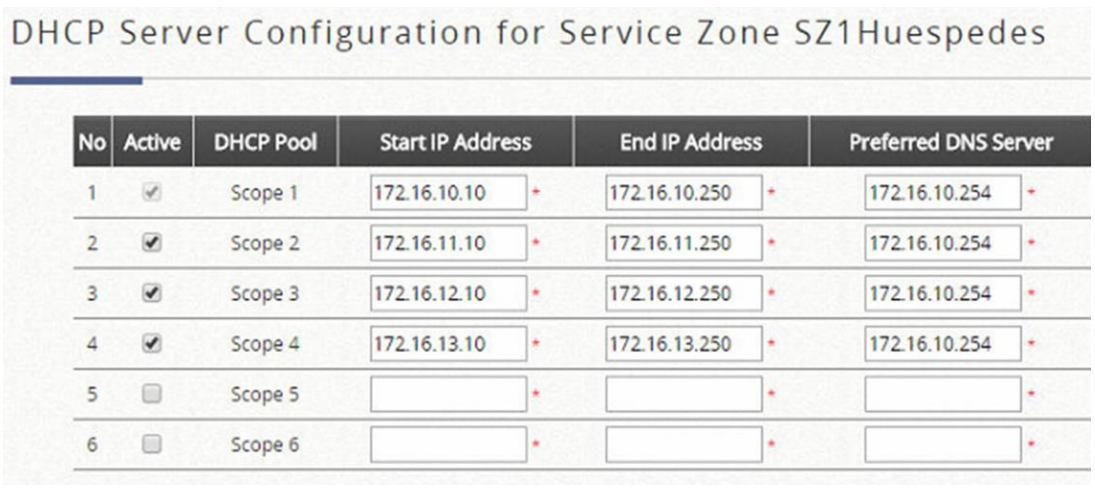


Figura 48. Configuración del DHCP para la zona SZ1Huespedes

3.9.3 Zona SZ2Invitados

A esta zona se le asigna el SSID “Invitados”, se configura la interfaz en modo “nat”, para que el controlador inalámbrico se encargue de administrar dichas interfaces y la conexión hacia redes externas lo realice a través de la WAN. Se configura los parámetros: estado, nombre, vlan, la dirección IP y la máscara.

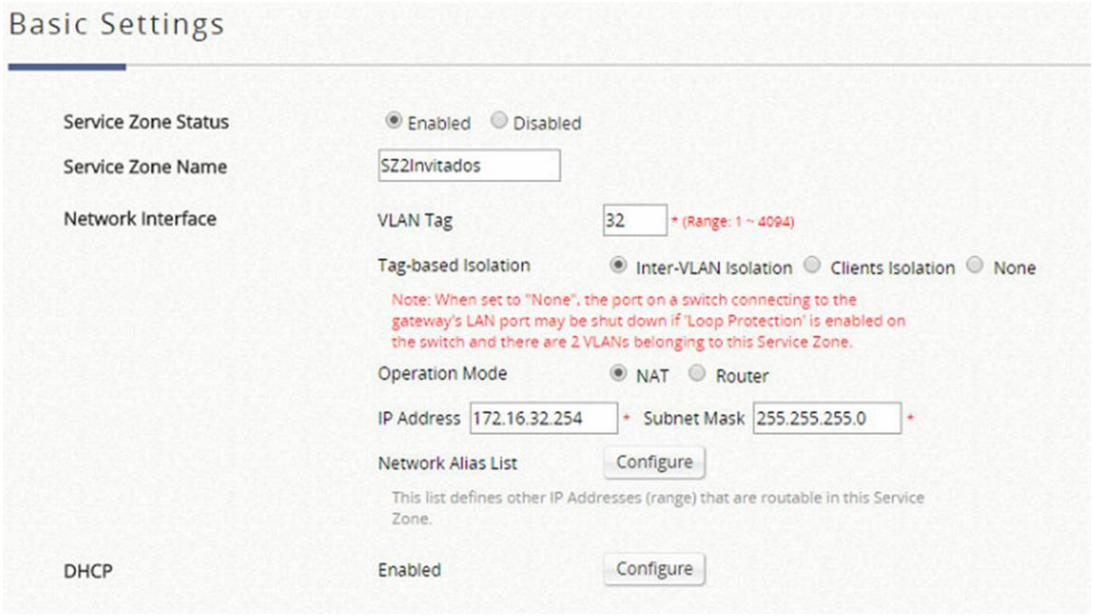


Figura 49. Configuración básica de la zona SZ2Invitados

En este caso los dispositivos AP están en el segmento de red de la interfaz de la zona default, es por ello que el direccionamiento IP de este segmento no dispone de rango para incluir APs, se deja asignada la política 2 que posteriormente se configura. Se habilita la autenticación de esta zona para que aparezca al portal de acceso en dicha interfaz. El portal URL define el destino de enlace al cual el navegador web del usuario redireccionará al momento de realizar un login satisfactorio y en este caso se configura que sea http://www.google.com.

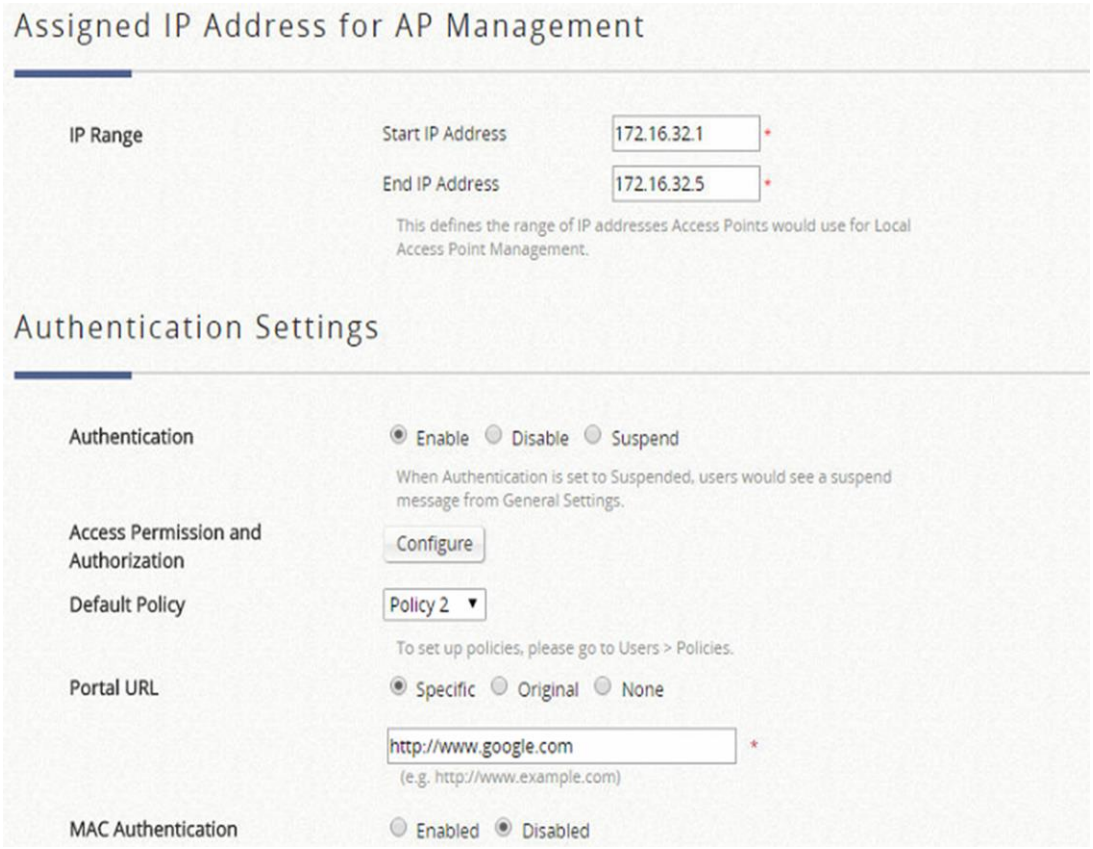


Figura 50. Configuración de autenticación de la zona SZ2Invitados

Se habilita la configuración DHCP, el rango de direcciónes IP del DHCP y el servidor DNS.

Figura 51. Configuración del DHCP para la zona SZ2Invitados

3.9.4 Zona SZ3_Staff

A esta zona se le asignará el SSID “Staff”. Se configura la interfaz en modo “nat”, para que el controlador inalámbrico se encargue de administrar dichas interfaces y la conexión hacia redes externas lo realice a través de la WAN. Se configura los parámetros: estado, nombre, vlan, la dirección IP y la máscara.

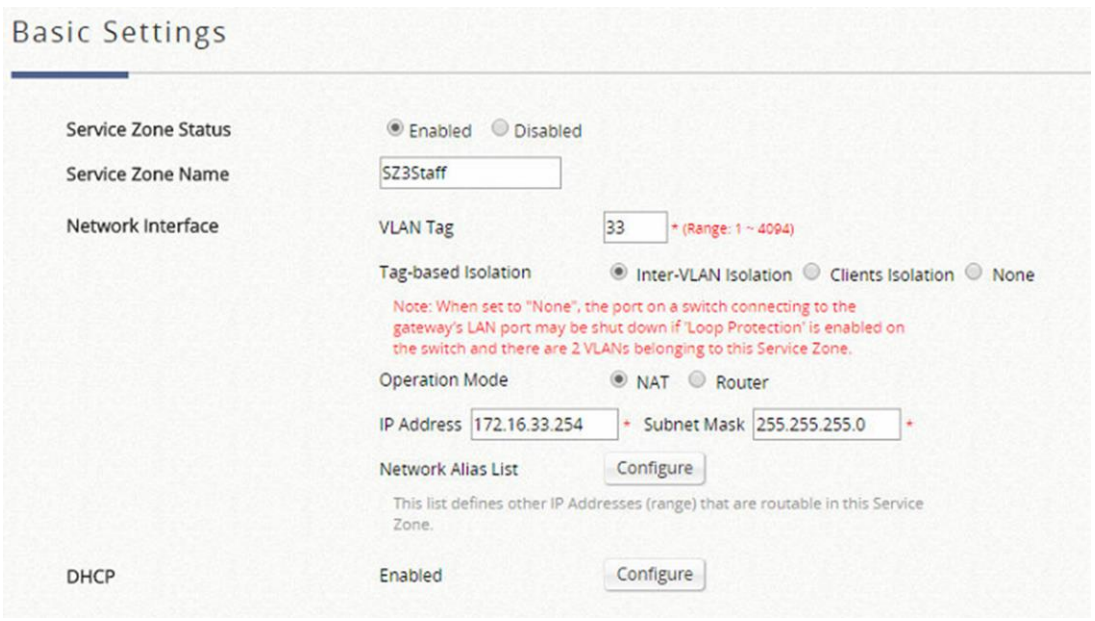


Figura 52. Configuración básica de la zona SZ3Staff

En esta zona no se configura el direccionamiento IP de este segmento de red ya que no se asignan APs, se deja asignada la política 3 que posteriormente se configura. Se deshabilita la autenticación de esta zona ya que no se requiere que aparezca al portal de acceso en dicha interfaz. El portal URL define el destino de enlace al cual el navegador web del usuario redireccionará al momento de realizar un login satisfactorio y en este caso se configura que sea http://www.google.com.

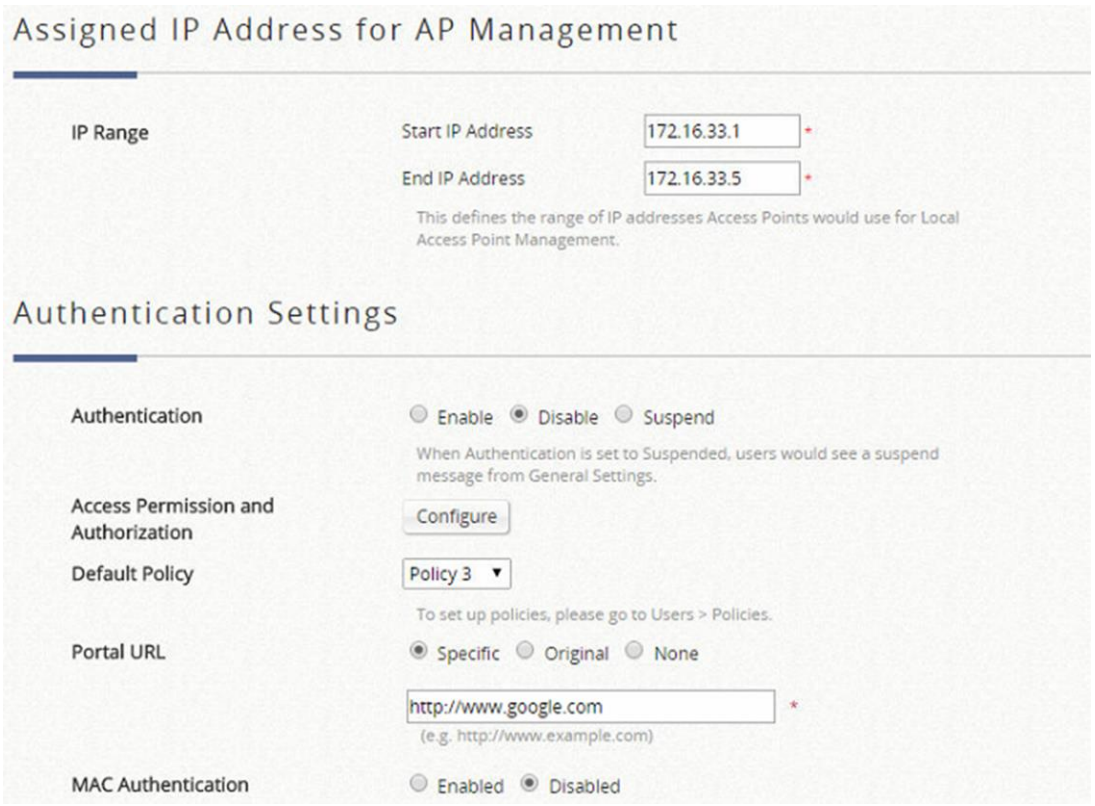


Figura 53. Configuración de autenticación de la zona SZ3Staff

Se habilita la configuración DHCP, el rango de direcciónes IP del servidor DHCP y el servidor DNS.

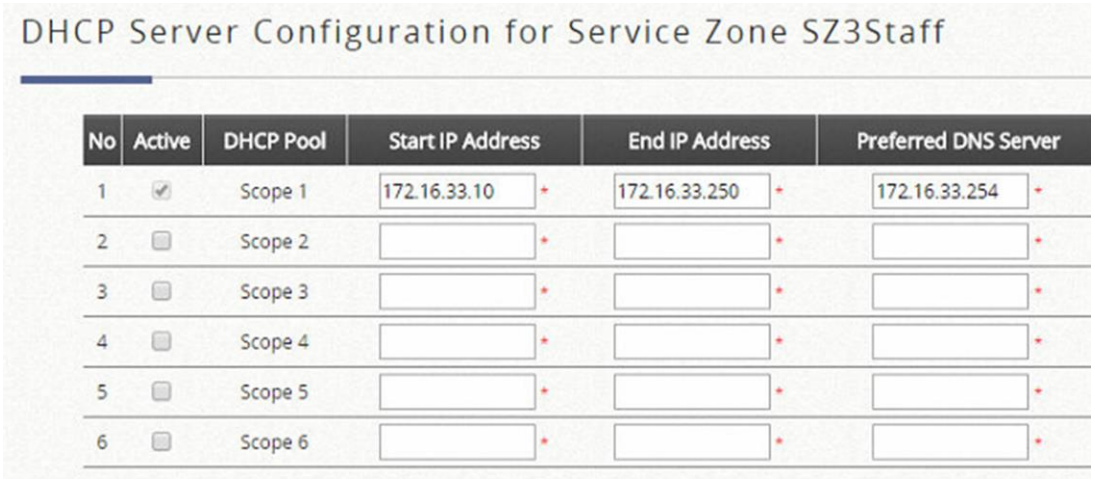


Figura 54. Configuración del DHCP para la zona de servicio SZ3Staff

3.10 Configuración de Grupos

Un grupo es un conjunto de usuarios con las mismas características que se rigen a las directrices establecidas en una política. Los grupos configurados son: Huéspedes, Invitados y Staff

El grupo y las políticas del sistema van a definir el tipo de acceso y privilegios que tendrán los usuarios en la red con el fin de establecer restricciones sobre el comportamiento de los mismos.

Nota: El grupo, la política y las zonas de servicio están ligados unos con otros.

3.10.1 Grupo Huéspedes

La variable “0” en el campo de número de dispositivos permitidos, define un número ilimitado de usuarios que pueden inicializar sesión. La zona de configuración de permisos permite determinar el acceso entre el grupo, la política y la zona de servicio.

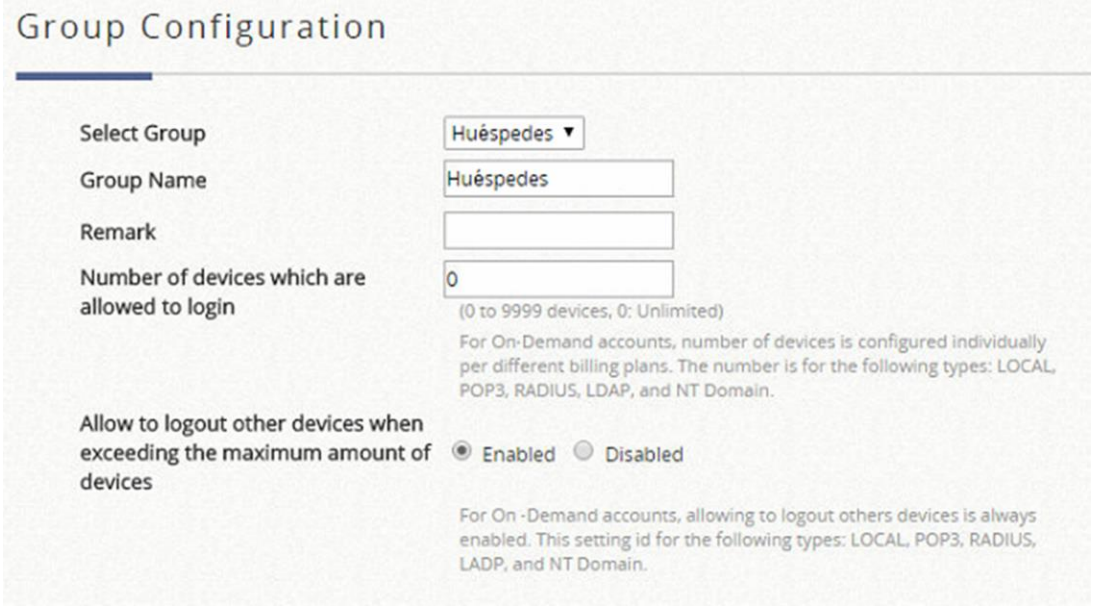


Figura 55. Configuración del grupo Huéspedes

En este caso los usuarios del grupo Huéspedes puedan acceder todas las zonas de servicio ya que se habilita el “check” en las zonas y de esta manera estamos dando la autorización del caso.

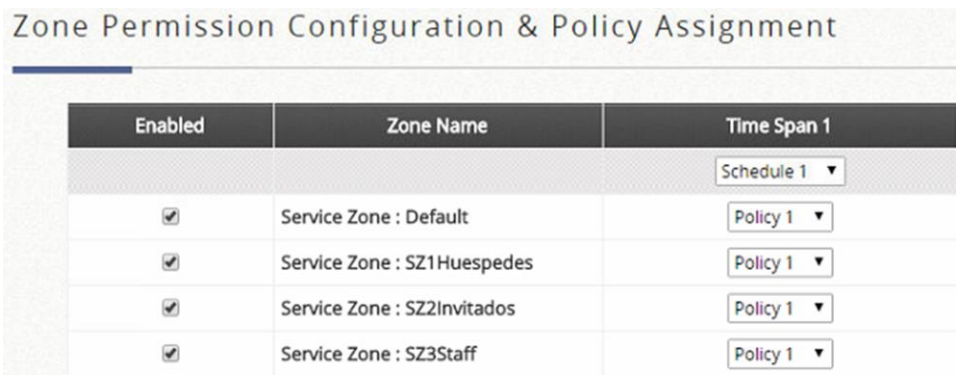


Figura 56. Configuración de permisos de acceso a las zonas y políticas asignadas al grupo Huéspedes.

Adicional se debe permitir el acceso a los grupos en la zona de servicio SZ1Huespedes. Los grupos autorizados para la zona SZ1Huespedes son Huéspedes y Staff.

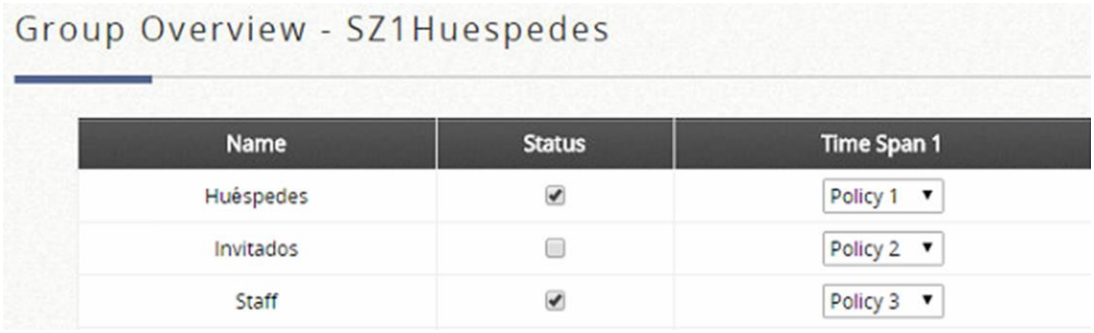


Figura 57. Configuración de permisos de acceso a los grupos en la zona SZ1Huespedes

3.10.2 Grupo Invitados

El número de dispositivos para este grupo se configura de forma individual por el plan de facturación 2. El número de dispositivos es para la autenticación de tipo local.

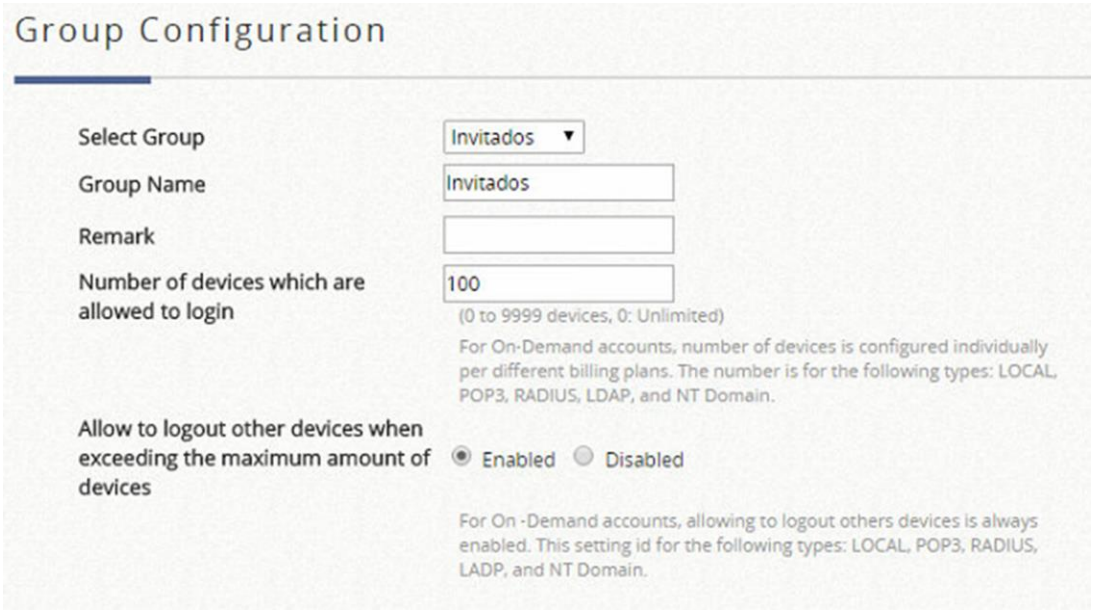


Figura 58. Configuración del grupo Invitados

Para permitir que los usuarios del grupo Invitados puedan acceder a las zonas de servicio habilitamos el “check”, de esta manera estamos dando la autorización. En este caso se puede acceder a las zonas:default, SZ2Invitados y SZ3Staff.

Figura 59. Configuración de permisos de acceso a las zonas de servicio y políticas asignadas para el grupo Invitados.

Adicional se configura los permisos de acceso a los grupos en la zona de servicio SZ2Invitados, en este caso todos los grupos están autorizados.

Figura 60. Configuración de permisos de acceso a los grupos en la zona de servicio SZ2Invitados.

3.10.3 Grupo Staff

Como la cuenta Staff es bajo demanda el número de dispositivos está configurado de forma individual por el plan de facturación 3.

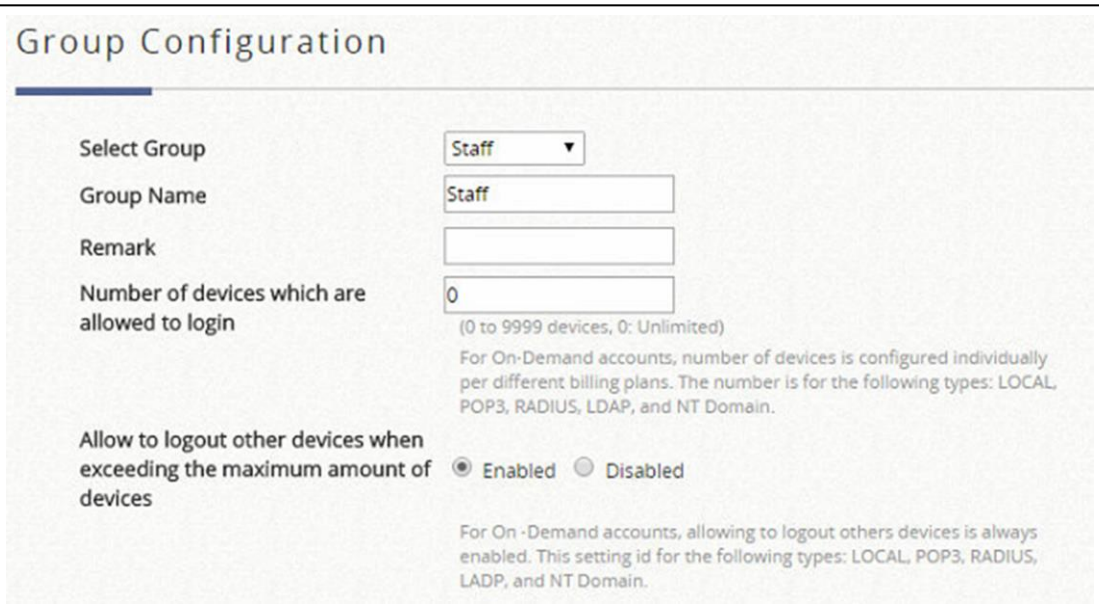


Figura 61. Configuración del grupo Staff

En este caso los usuarios del grupo Staff puedan acceder todas las zonas de servicio ya que se habilita el “check” en las zonas y de esta manera se da la autorización del caso.

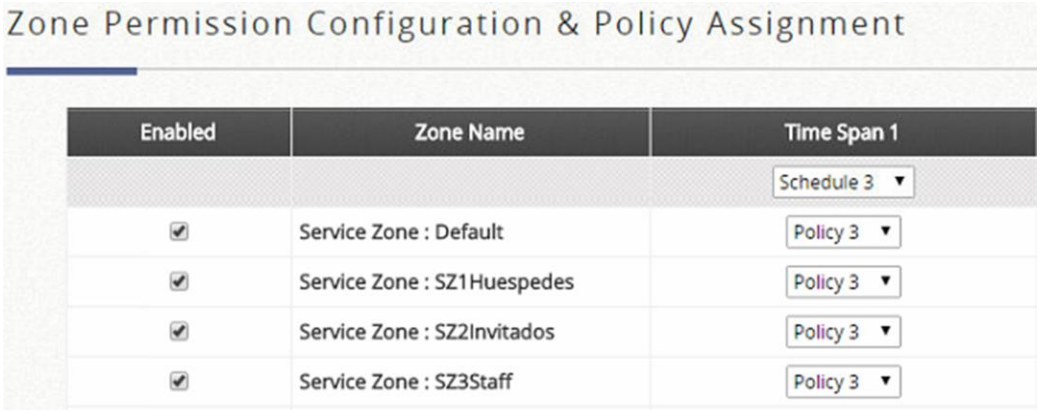


Figura 62. Configuración de los permisos de acceso a las zonas de servicio y políticas asignadas del grupo Staff.

Adicional para permitir que los usuarios del grupo Staff puedan acceder a las zonas de servicio habilitamos el “check” en la zona SZ3_Staff, de esta manera estamos dando autorización. En este caso todos los grupos tienen autorización.

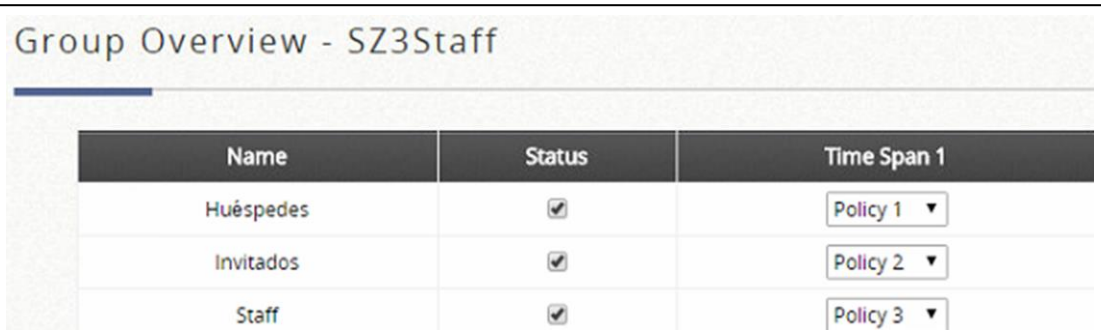


Figura 63. Configuración de permisos de acceso a los grupos en la zona de servicio SZ3Staff.

3.11 Configuración de Políticas

Las políticas consiste en una serie de campos configurables que definen perfiles de red que estarán atados al grupo de usuarios, por ende los usuarios que ingresan a través del host-spot van a heredar dichas políticas de acuerdo

al grupo donde haya sido colocado por el sistema. El grupo definirá las políticas y la zona dará el acceso a la interfaz de red establecida en la zona de servicio. Algunas de las políticas configurables son: reglas de firewall, horario de navegación y login, reglas de enrutamientos, privilegios y sesiones concurrentes, rutas de destino, etc. Existen 12 perfiles de políticas para configurar más una política global que viene por defecto. Se puede tener un grupo con políticas diferentes en diferentes zonas de servicio o una zona de servicio puede tener muchos grupos con diferentes políticas.

Se selecciona una de las políticas en la lista desplegable y empezamos a configurar cada atributo, luego de editar damos click en aplicar para guardar los cambios realizados.

Tabla 12. Políticas configuradas.

POLÍTICAS	NOMBRE	FIREWALL	QoS	RUTAS
Política 1	Huespedes	Block ssh, telnet, icmp	5MB indvidual - 35MB grupo	WAN2
Política 2	Invitados	Block ssh, telnet, icmp	512KB indvidual - 4MB grupo	WAN2
Política 3	Staff	N/A	6MB indvidual - 35MB grupo	WAN1

3.12 Planes de Facturación

Los planes de facturación definen los términos y las condiciones de acceso a internet de los usuarios bajo demanda y se pueden configurar hasta 10.
Los tipos de plan de facturación bajo demanda son: tiempo de uso, volumen, tiempo de corte y duración de tiempo.

Tiempo de uso.- En este tipo de plan de facturación los usuarios pueden acceder a Internet siempre y cuando la cuenta este activa. Esto es ideal para uso a corto plazo como en cafeterías, en aeropuertos, etc. Se facturará de acuerdo al tiempo de uso.

Volumen.- Los usuarios pueden acceder a Internet siempre y cuando la cuenta este en vigencia. El consumo de megabytes que dispone un usuario a

raíz de la creación del ticket (1 a 1000000 Mbytes). Es ideal para la pequeña cantidad de aplicaciones como correo electrónico, transferencia de archivos, etc.

Tiempo de corte.- Es la hora del reloj del sistema en la que la cuenta se caduca. Si se crea una cuenta después de la hora de cierre, automáticamente la cuenta expirará, siendo este tipo de facturación es ideal para centros comerciales.

Duración de tiempo.- La cuenta se activa tras la creación de la misma, la cuenta caduca una vez que el período de tiempo se termina. Es ideal para ofrecer servicio de internet inmediatamente después de la creación de una cuenta durante un período específico de tiempo.

3.12.1 Planes de facturación por duración de tiempo

El perfil del plan de facturación por duración de tiempo configurado consta de los siguientes parámetros: número del plan, tipo, tiempo de duración, hora de duración, cuota (días, horas, minutos en tendrá validez la cuenta), número de dispositivos que pueden conectarse por cuenta (laptops, smartphones, tablets, etc.), precio, grupo de acceso al sistema y referencia adicional. Los planes de facturación que se encuentran configurados son los siguientes:

Tabla 13. Planes configurados.

PLANES		
PLAN	DESCRIPCIÓN	GRUPO
1	válido por 7 días, 3 equipos por usuario	Huéspedes
2	válido por 2 horas, 1 equipo por usuario	Invitados
3	válido por 24 horas, 1 equipo por usuario	Staff

3.13 Configuración del servidor de Impresión (Impresora despachadora de tickets)

Se configura el generador de tickets para que se comunique con el sistema y no necesite ir a través de la autenticación. Se pueden configurar hasta 10

servidores de impresión, solo se necesita ingresar los campos requeridos como se muestra en la siguiente figura:

Figura 64. Configuración del terminal de impresión.

Figura 65. Formato de ticket para impresión

3.14 Simulación, pruebas y resultados.

Teniendo como base el diseño planteado y los equipos a utilizar es necesario confirmar el buen funcionamiento del diseño para lo cual utilizamos la herramienta software gratuita de simulación “VisualRF Plan 7.7_473” que permite visualizar el estado de cobertura de la señal de red inalámbrica sobre un área determinada. Además, se utiliza en el site survey presencial la herramienta “inSSIDer 3.1.2.1” que permite visualizar redes inalámbricas que están al alcance, los canales utilizados, el nivel de señal y potencia de las redes Wi-Fi de forma gráfica.

VisualRF Plan.- Es un software desarrollado por Aruba que ofrecen una parametrización de los equipos a utilizarse y permite importar los planos disponibles de las instalaciones del cliente para obtener un informe con el

detalle de la ubicación de los puntos de acceso inalámbricos contemplados en el diseño o con características análogas. Los datos capturados serán procesados mediante el uso de distintos algoritmos matemáticos de interpolación para realizar una representación, lo más exacta posible, de cómo se comportan las señales en el medio analizado. Las funciones de generación de mapas de señal Wi-Fi pueden ser aplicadas sobre redes de 2.4GHz y/o 5GHz y visualizadas sobre los planos. Se pueden definir los niveles de señal de barrera, estableciendo aquellos umbrales a partir de los cuales descartar la representación de las mediciones de señal obtenidas, en este caso se toma -75dBm que representa un nivel de señal excesivamente débil. Esta información puede ser visualizada en tiempo real en forma de mapas de cobertura Wi-Fi y facilita la ubicación de zonas muertas, la realización de ajustes y la optimización de la cobertura.

Las mediciones realizadas en campo fueron cotejadas con las que se obtienen mediante software, la coincidencia de las mismas reflejan el desempeño que tendrá en el futuro la red WLAN.

Los resultados obtenidos sirven perfectamente como punto de partida para llevar a cabo la instalación y puesta en marcha de la red inalámbrica planteada y se puede ser utilizado como entregable al cliente para que pueda evaluar que la red inalámbrica se ajustará en dichas condiciones a las necesidades propias del hotel. A continuación el detalle de los resultados obtenidos:

Planta Subsuelo 1

En la planta del subsuelo 1 se instalan 2 access points “4ipnet” modelo UAP (EAP767) que trabajan en la banda de frecuencia de 2.4 GHz y 5GHz, en los estándares Wi-Fi 802.11 b / g / n /ac, la potencia máxima de transmisión es de 25 dBm (2.4GHz y 5GHz) y el tipo de seguridad configurada es WPA2-Personal.

Tabla 14. Configuración APs subsuelo 1.

Nombre AP	SSID	Banda de Frecuencia	Canal utilizado
AP_S1_NOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	6/automático
AP_S2_NOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	1/automático

Con los 2 APs instalados se cubre con una intensidad de potencia de -45 dBm a un 80% del área útil (color rojo), con una intensidad de potencia de -55 dBm a un 15 % (color naranja), con un intensidad de potencia a -65 dBm al 5% (color verde) y con una intensidad de potencia de -75dBm al resto del piso (color celeste).

Anteriormente en la planta del subsuelo 1 no se tenía cobertura de red inalámbrica Wi-Fi.

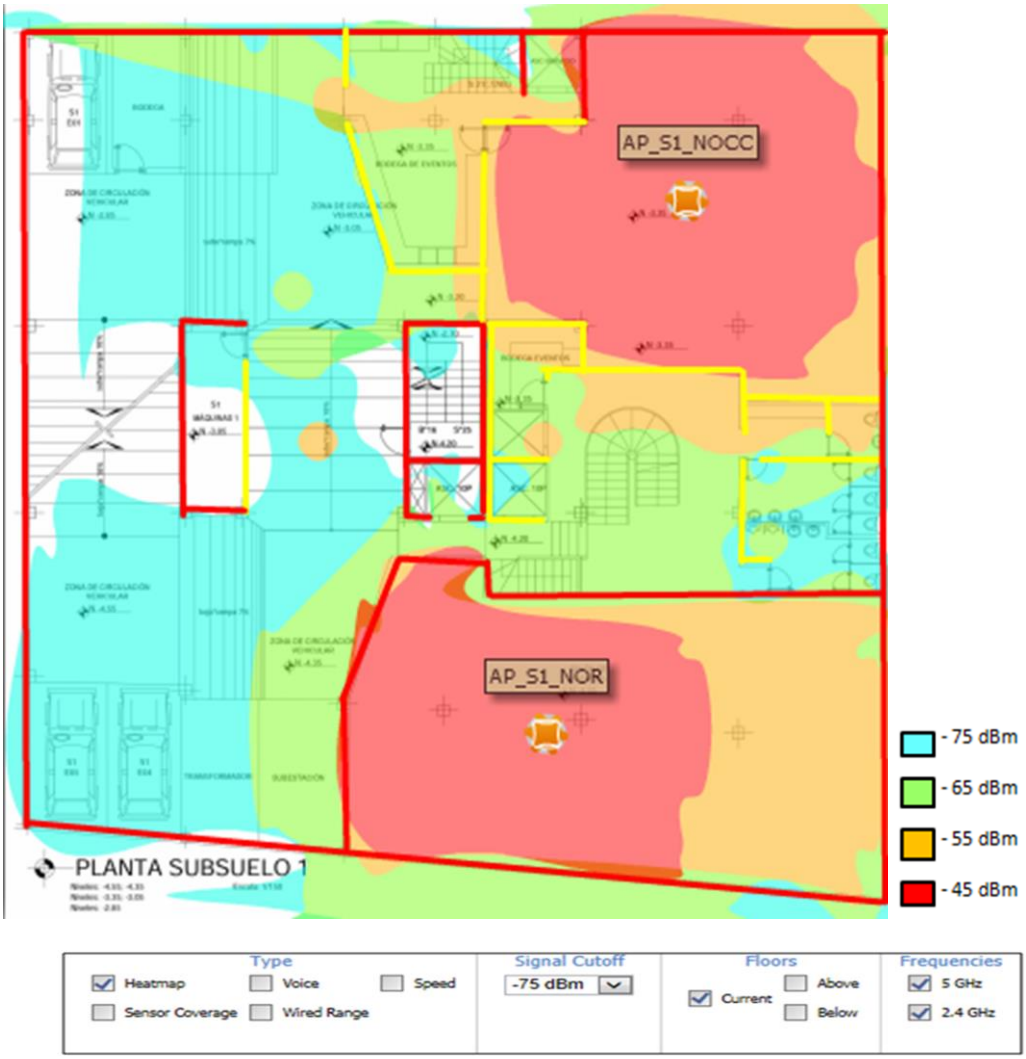


Figura 66. Propuesta de cobertura de la Planta del Subsuelo 1

El punto de acceso inalámbrico AP_S1_NOR (00:1F:D4:04:6D:E8) como se puede apreciar en la Figura 67, ocupa el canal 6 y el equipo AP_S1_NOCC (00:1F:D4:04:6D:D9) ocupa el canal 1. La seguridad que utiliza es WPA2-personal. El piso de ruido en el Subsuelo 1 tiene un nivel de -90 dBm y los demás APs que se visualizan llegan a tener una intensidad de señal de -80 dBm. Se puede verificar con la gráfica que el canal no está interferido.

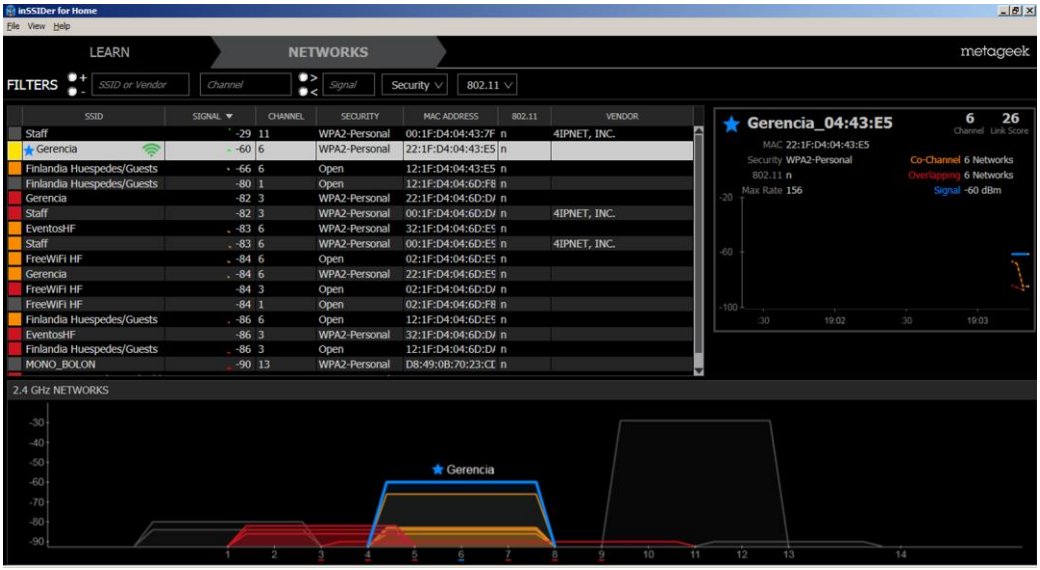


Figura 67. Análisis de señales Wi-FI en Subsuelo 1

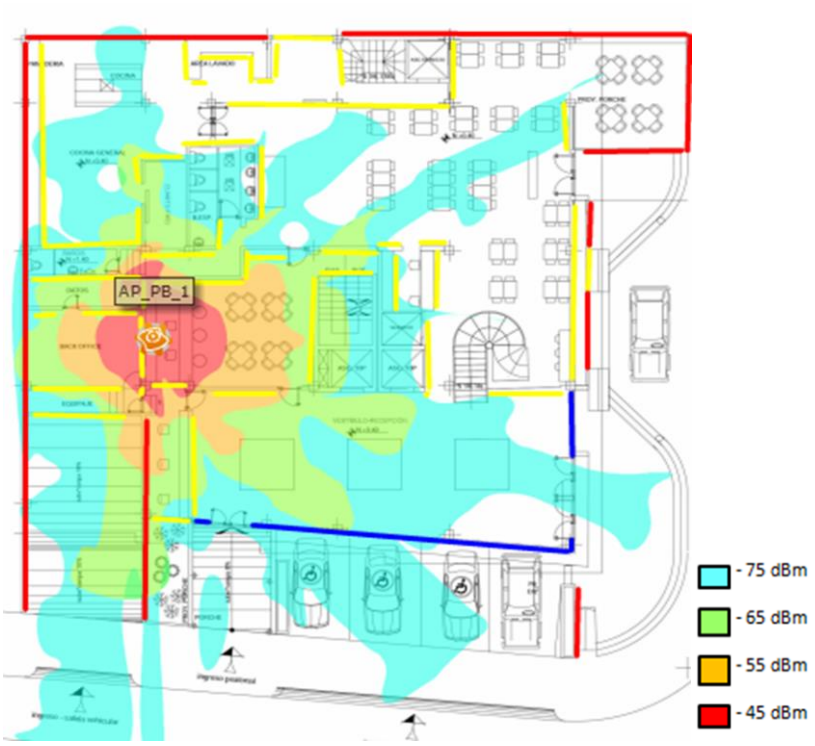
Planta Baja

En la planta baja se instalan 2 access points “4ipnet” modelo UAP (EAP767), trabajan en la banda de frecuencia de 2.4 GHz y la de 5GHz, en los estándares Wi-Fi 802.11 b / g / n /ac, la tasa de transmisión de datos es 450 Mbps (2.4GHz) y 1.3 Gbps(5GHz), la potencia máxima de transmisión es de 25 dBm (2.4GHz y 5GHz) el tipo de seguridad configurada es WPA2-Personal.

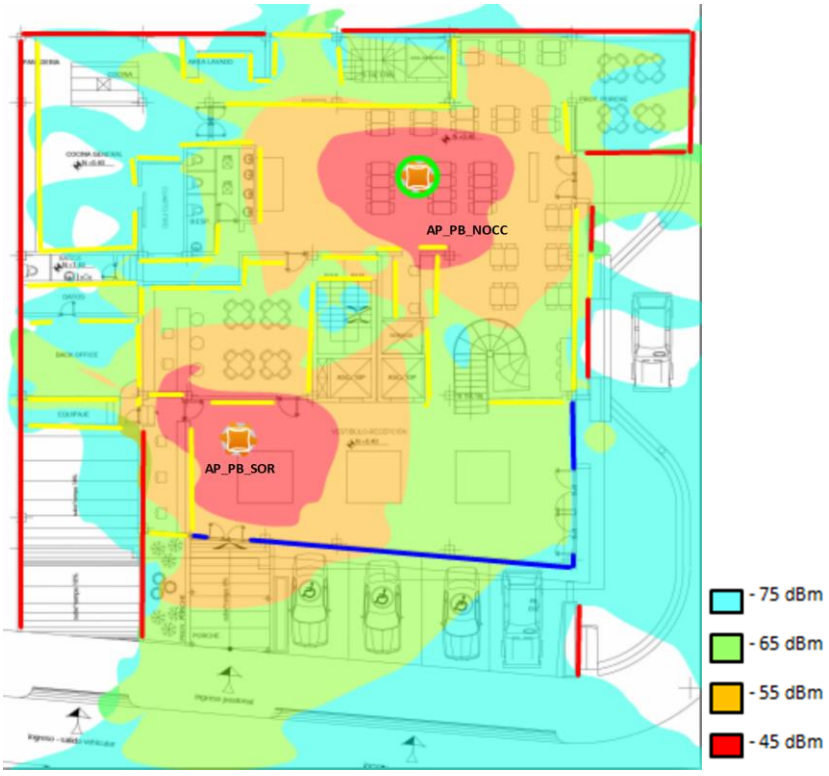
Tabla 15. Configuración APs planta baja.

Nombre AP	SSID	Banda de Frecuencia	Canal utilizado
AP_PB_SOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	1/automático
AP_PB_NOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	6/automático

Con los 2 APs instalados se cubre con una intensidad de potencia de -45 dBm a un 50% del área de lobby y restaurant (color rojo), con una intensidad de potencia de -55 dBm a un 20 % (color naranja), con un intensidad de potencia a -65 dBm a un 20 % (color verde) y con una intensidad de potencia de -75dBm al resto del piso (color celeste).



a)



b)

Figura 68. Cobertura APs en Planta Baja

a) Cobertura actual
b) Propuesta de cobertura

Al realizar la prueba de conexión a la red inalámbrica con una laptop que tiene la antena inalámbrica de 2.4 GHz en el área de recepción se conecta al punto de acceso inalámbrico AP_PB_NOCC (00:1F:D4:04:6D:F4) como se puede apreciar en la Figura 69, ocupa el canal 6 y el equipo AP_PB_SOR (00:1F:D4:04:6D:F7) ocupa el canal 1. La seguridad que utiliza es WPA-2 Personal.

El piso de ruido en la planta baja tiene un nivel de -90 dBm y los demás APs que se visualizan llegan a tener una intensidad de señal de -65dBm. Se puede verificar con la gráfica que el canal no está interferido.

Figura 69. Análisis de señales Wi-Fi en Planta Baja

Primer piso

En el primer piso se instalan 4 access points “4ipnet” que trabajan en la banda de frecuencia de 2.4 GHz y la de 5GHz en los estándares Wi-Fi 802.11 b / g / n /ac.

Dos APs modelo UAP (EAP767) cuya tasa de transmisión de datos es 450 Mbps (2.4GHz) y 1.3 Gbps(5GHz), la potencia máxima de transmisión es de

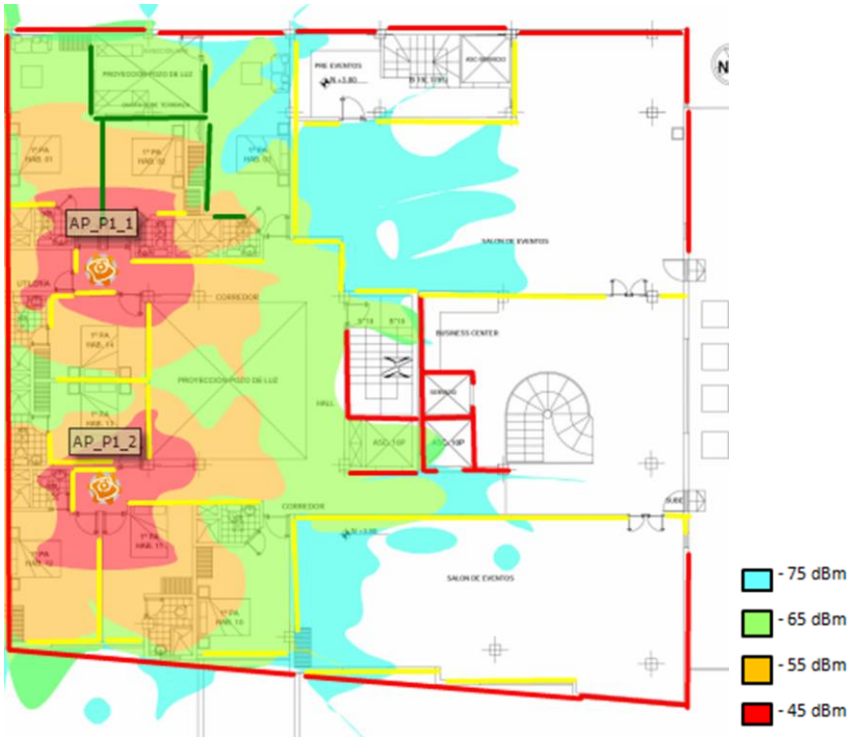
25 dBm (2.4GHz y 5GHz). Dos APs modelo (EAP727) cuya tasa de transmisión de datos es 300 Mbps (2.4GHz) y 867 Mbps(5 GHz), la potencia máxima de transmisión es de 27 dBm (2.4GHz) y 26 dBm(5 GHz), el tipo de seguridad configurada en los 4 access points es WPA2-Personal.

Tabla 16. Configuración APs piso 1.

Nombre AP	SSID	Banda de Frecuencia	Canal utilizado
AP_P1_SOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	11/automático
AP_P1_SOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	11/automático
AP_P1_NOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	1/automático
AP_P1_NOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	6/automático

Con los 2 APs (EAP767) instalados en los salones de eventos se cubre con una intensidad de potencia de -45 dBm a un 80% del área de salones de eventos (color rojo), con una intensidad de potencia de -55 dBm a un 15 % (color naranja), con un intensidad de potencia a -65 dBm a un 5 % (color verde) del área .

Al igual que con los otros 2 APs (EAP727) instalados en los corredores del primer piso se cubre con una intensidad de potencia de -45 dBm a un 50% del área habitaciones (color rojo), con una intensidad de potencia de -55 dBm a un 30 % (color naranja), con un intensidad de potencia a -65 dBm a un 20 % (color verde) y con una intensidad de potencia de -75dBm al resto del piso (color celeste).



a)

b)

Figura 70. Cobertura APs en el primer piso

a) Cobertura actual
b) Propuesta de cobertura

Al realizar la prueba de conexión a la red inalámbrica con una laptop que tiene la antena inalámbrica de 2.4 GHz en el área de hall se conecta al punto de acceso inalámbrico MAC (00:1F:D4:04:45:28) como se puede apreciar en la Figura 71, ocupa el canal 1 y el tipo de seguridad configurada que utiliza es WPA-2 Personal. El piso de ruido en el primer piso tiene un nivel de -90 dBm y los demás APs que se visualizan llegan a tener una intensidad de señal de -67dBm.

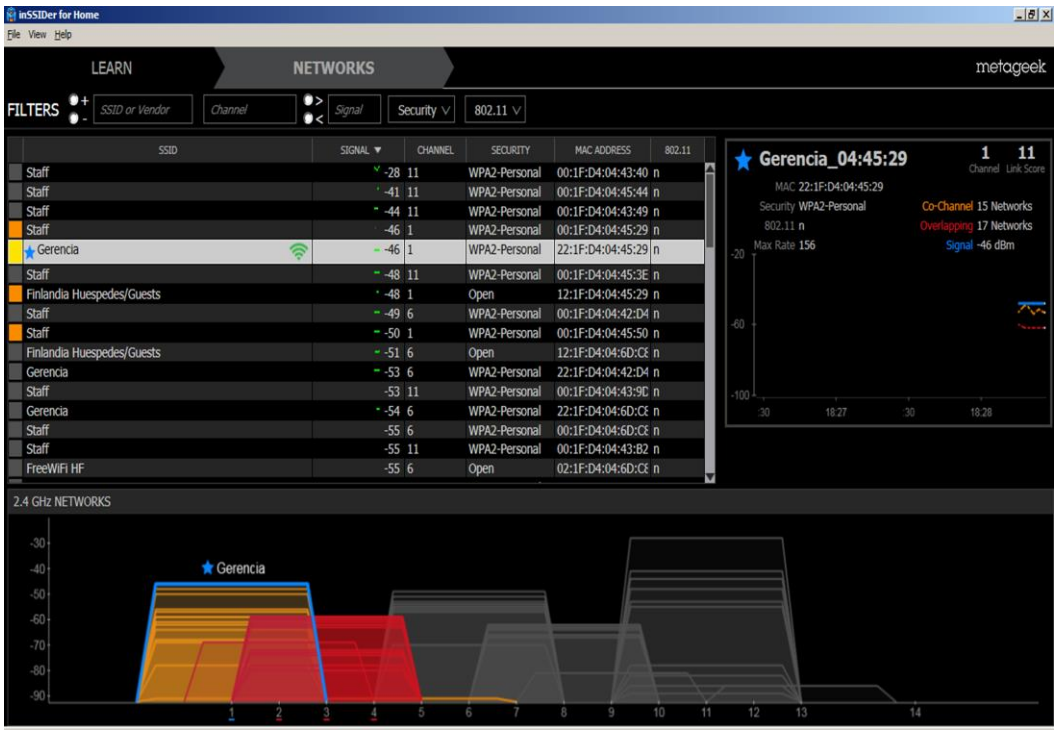


Figura 71. Análisis de señales Wi-Fi en Piso 1

Segundo piso

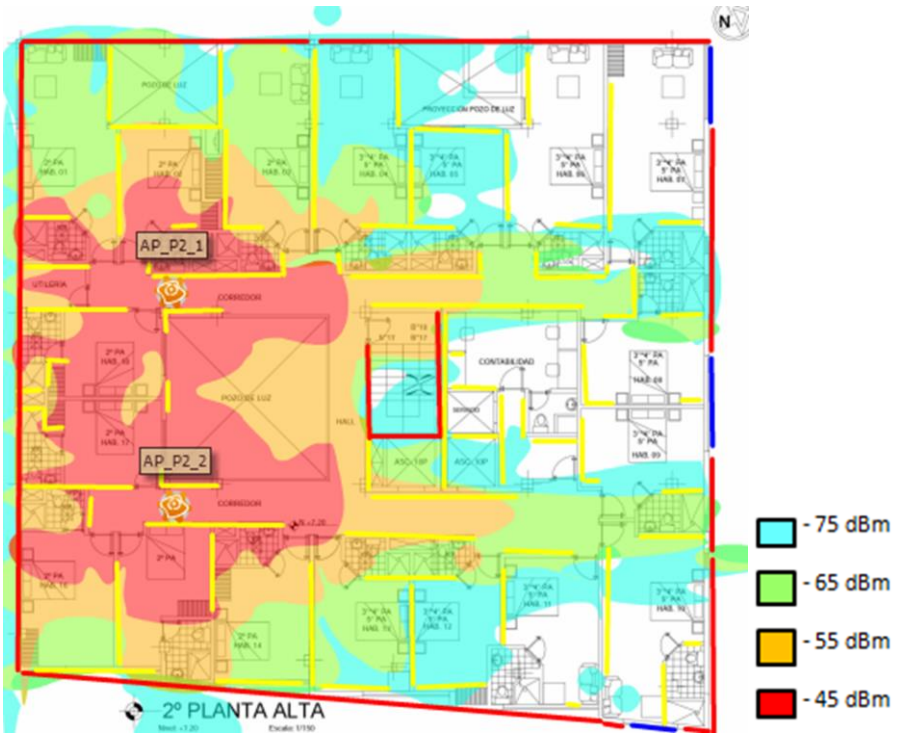
En el segundo piso se encuentran instalados 4 access points “4ipnet” modelo UAP (EAP727), trabajan en la banda de frecuencia de 2.4 GHz y la de 5GHz, en los estándares Wi-Fi 802.11 b / g / n /ac, la tasa de transmisión de datos es 300 Mbps (2.4GHz) y 867 Mbps (5 GHz), la potencia máxima de transmisión es de 27 dBm (2.4GHz) y 26 dBm(5 GHz) y el tipo de seguridad configurada es WPA2-Personal.

Tabla 17. Configuración APs piso 2.

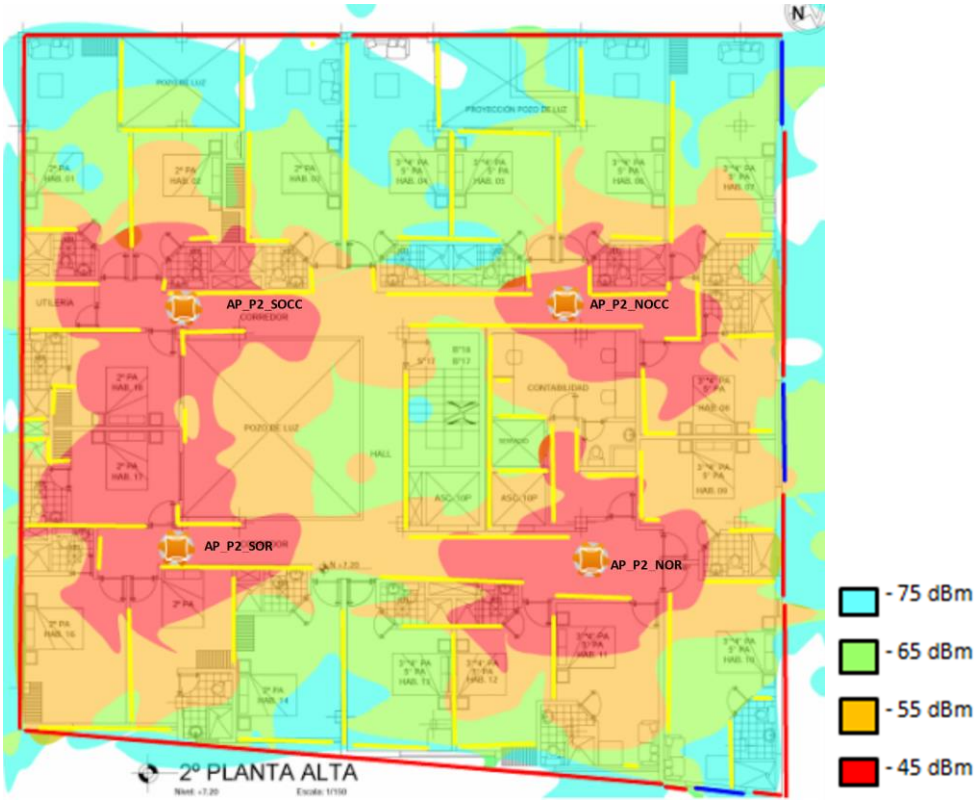
Nombre AP	SSID	Banda de Frecuencia	Canal utilizado
AP_P2_SOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	1/automático
AP_P2_SOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	11/automático
AP_P2_NOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	8/automático
AP_P2_NOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	3/automático

Se utiliza un corte de señal en -75dBm que en la práctica es el mínimo necesario para una conectividad aceptable hacia la navegación en internet. Sin embargo, como puede notarse en el mapa de calor, la señal mínima en la mayoría de las áreas a cubrir es -65dBm.

Con los 4 APs instalados se cubre con una intensidad de potencia de -45 dBm a un 40% del piso (color rojo), con una intensidad de potencia de -55 dBm a un 40 % (color naranja), con un intensidad de potencia a -65 dBm a un 15 % (color verde) y con una intensidad de potencia de -75dBm al resto del piso (color celeste).



a)



b)

Figura 72. Cobertura APs en el segundo piso

a) Cobertura actual

b) Propuesta de cobertura

Al realizar la prueba de conexión a la red inalámbrica con una laptop que tiene la antena inalámbrica de 2.4 GHz en el área de hall se conecta al punto de acceso inalámbrico MAC (00:1F:D4:04:45:29) como se puede apreciar en la Figura 73, ocupa el canal 1 y el tipo de seguridad que utiliza es WPA-2 Personal. El piso de ruido en el segundo piso tiene un nivel de -90 dBm y los demás APs que se visualizan llegan a tener una intensidad de señal de -65dBm.

Figura 73. Análisis de señales Wi-Fi en Piso 2

Tercer piso

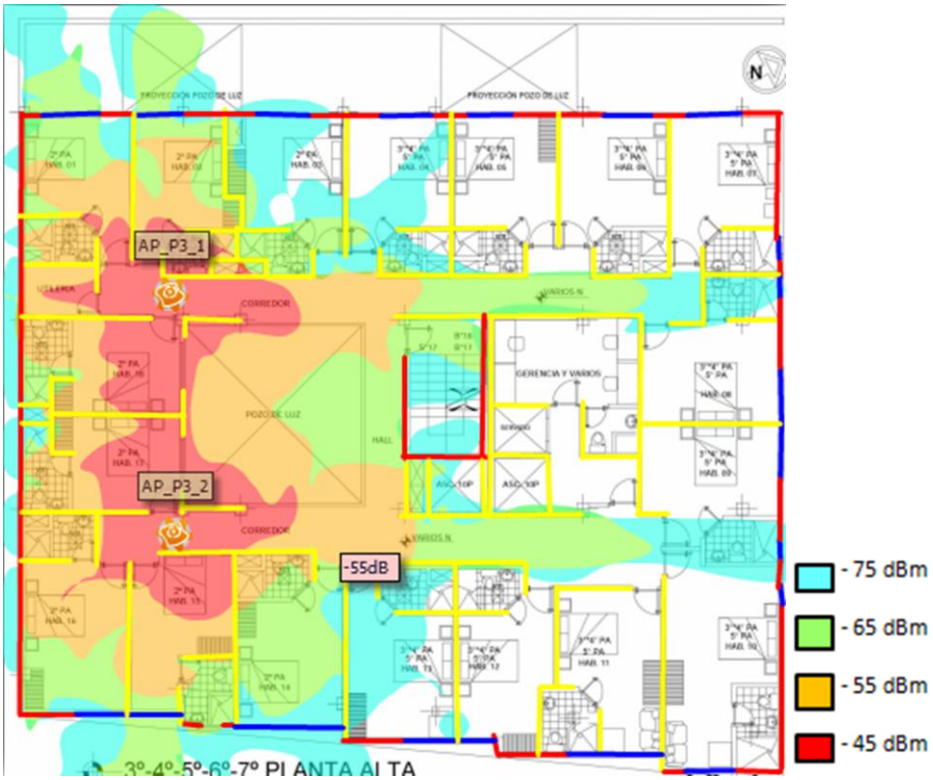
En el tercer piso se encuentran instalados 4 access points “4ipnet” modelo UAP (EAP727), trabajan en la banda de frecuencia de 2.4 GHz y la de 5GHz, en los estándares Wi-Fi 802.11 b / g / n /ac, la tasa de transmisión de datos es 300 Mbps (2.4GHz) y 867 Mbps (5 GHz), la potencia máxima de transmisión es de 27 dBm (2.4GHz) y 26 dBm(5 GHz) el tipo de seguridad configurada es WPA2-Personal.

Tabla 18. Configuración APs piso 3.

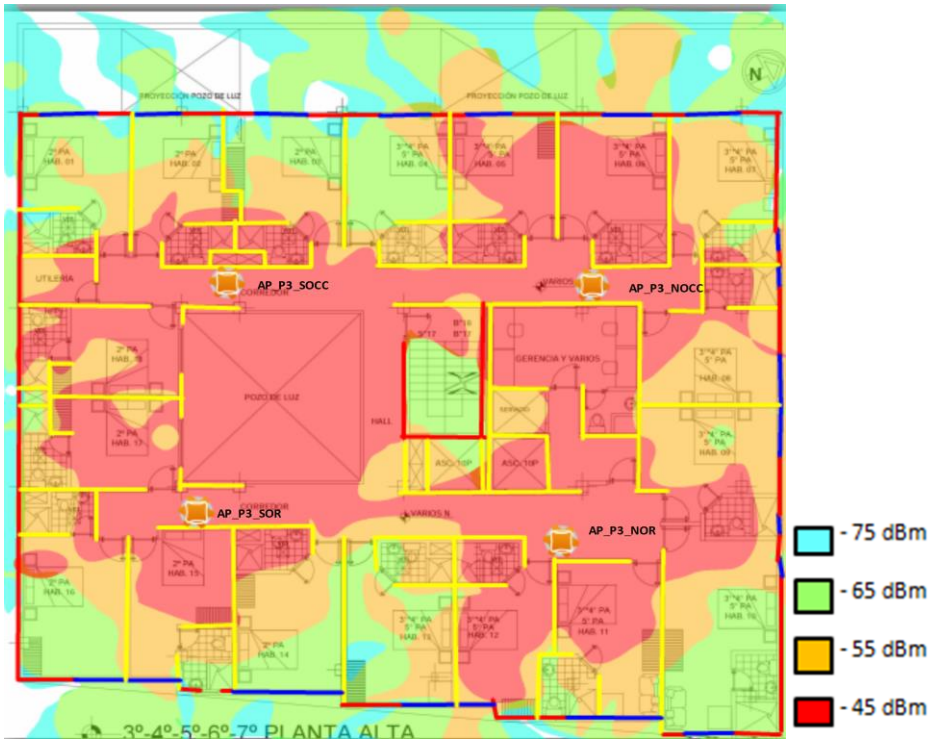
Nombre AP	SSID	Banda de Frecuencia	Canal utilizado
AP_P3_SOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	11/automático
AP_P3_SOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	11/automático
AP_P3_NOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	1/automático
AP_P3_NOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	6/automático

Se utiliza un corte de señal en -75dBm que en la práctica es el mínimo necesario para una conectividad aceptable hacia la navegación en internet. Sin embargo, como puede notarse en el mapa de calor, la señal mínima en la mayoría de las áreas a cubrir es -65 dBm.

Con los 4 APs instalados se cubre con una intensidad de potencia de -45 dBm a un 70% del piso (color rojo), con una intensidad de potencia de -55 dBm a un 15 % (color naranja), con un intensidad de potencia a -65 dBm a un 10 % (color verde) y con una intensidad de potencia de -75dBm al resto del piso (color celeste).



a)



b)

Figura 74. Cobertura APs en el tercer piso

a) Cobertura actual
b) Propuesta de cobertura

Al realizar la prueba de conexión a la red inalámbrica con una laptop que tiene la antena inalámbrica de 2.4 GHz en el área de hall se conecta al punto de acceso inalámbrico MAC (00:1F:D4:04:44:75) como se puede apreciar en la Figura 75, ocupa el canal 6. La seguridad que utiliza es WPA-2 Personal. El piso de ruido en el tercer piso tiene un nivel de -90 dBm y los demás APs que se visualizan llegan a tener una intensidad de señal de -60dBm.

Figura 75. Análisis de señales Wi-Fi en Piso 3

Cuarto Piso

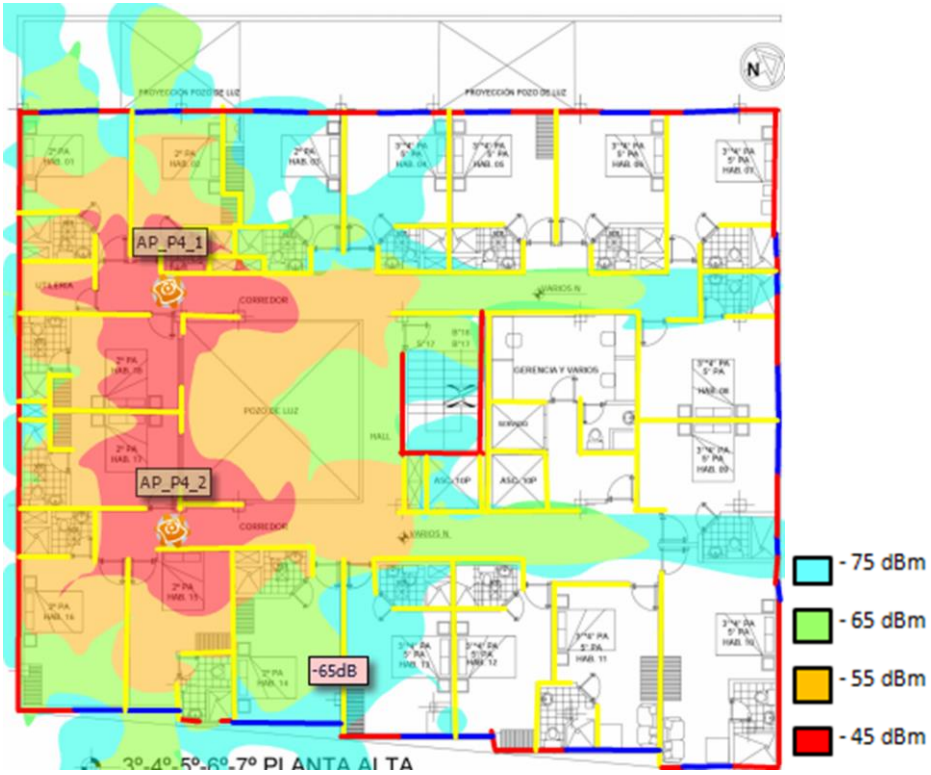
En el cuarto piso se encuentran instalados 4 access points “4ipnet” modelo UAP (EAP727), trabajan en la banda de frecuencia de 2.4 GHz y la de 5GHz, en los estándares Wi-Fi 802.11 b / g / n /ac la tasa de transmisión de datos es 300 Mbps (2.4GHz) y 867 Mbps(5 GHz), la potencia máxima de transmisión es de 27 dBm (2.4GHz) y 26 dBm(5 GHz) el tipo de seguridad configurada es WPA2-Personal.

Tabla 19. Configuración APs piso 4.

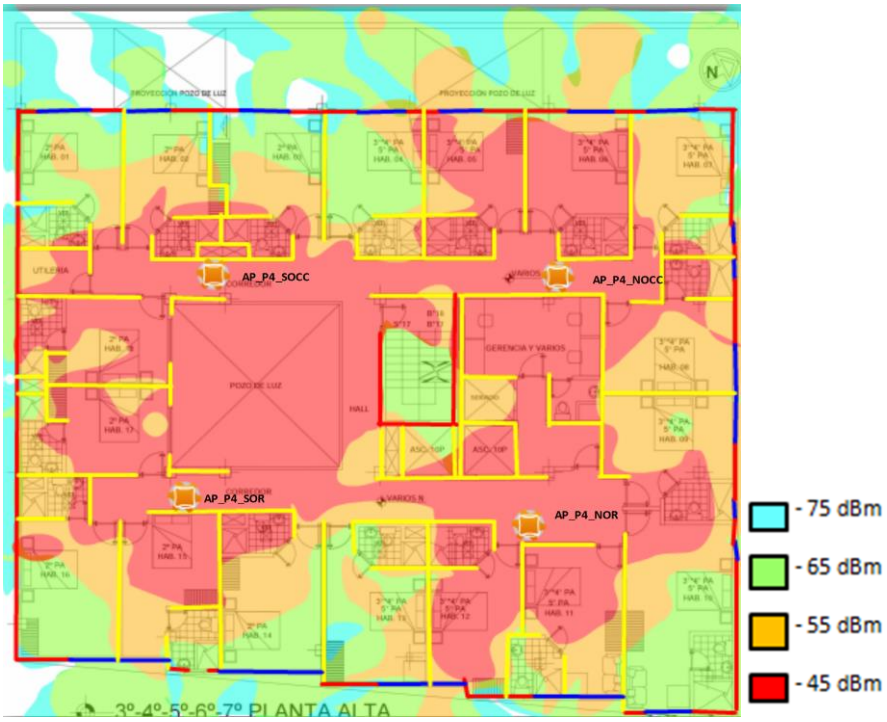
Nombre AP	SSID	Banda de Frecuencia	Canal utilizado
AP_P4_SOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	1/automático
AP_P4 _SOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	11/automático
AP_P4_NOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	8/automático
AP_P4_NOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	3/automático

Se utiliza un corte de señal en -75dBm que en la práctica es el mínimo necesario para una conectividad aceptable hacia la navegación en internet. Sin embargo, como puede notarse en el mapa de calor, la señal mínima en la mayoría de las áreas a cubrir es -65 dBm.

Con los 4 APs instalados se cubre con una intensidad de potencia de -45 dBm a un 70% del piso (color rojo), con una intensidad de potencia de -55 dBm a un 15 % (color naranja), con un intensidad de potencia a -65 dBm a un 10 % (color verde) y con una intensidad de potencia de -75dBm al resto del piso (color celeste).



a)



b)

Figura 76. Cobertura APs del cuarto piso

a) Cobertura actual

b) Propuesta de cobertura

Al realizar la prueba de conexión a la red inalámbrica con una laptop que tiene la antena inalámbrica de 2.4 GHz en el área de hall se conecta al punto de acceso inalámbrico MAC (00:1F:D4:04:42:D4) como se puede apreciar en la Figura 77, ocupa el canal 6. La seguridad que utiliza es WPA-2 Personal con una intensidad de señal de -42dBm. El piso de ruido en el cuarto piso tiene un nivel de -90 dBm y los demás APs que se visualizan llegan a tener una intensidad de señal de -60dBm.

Figura 77. Análisis de señales Wi-FI en Piso 4

Quinto Piso

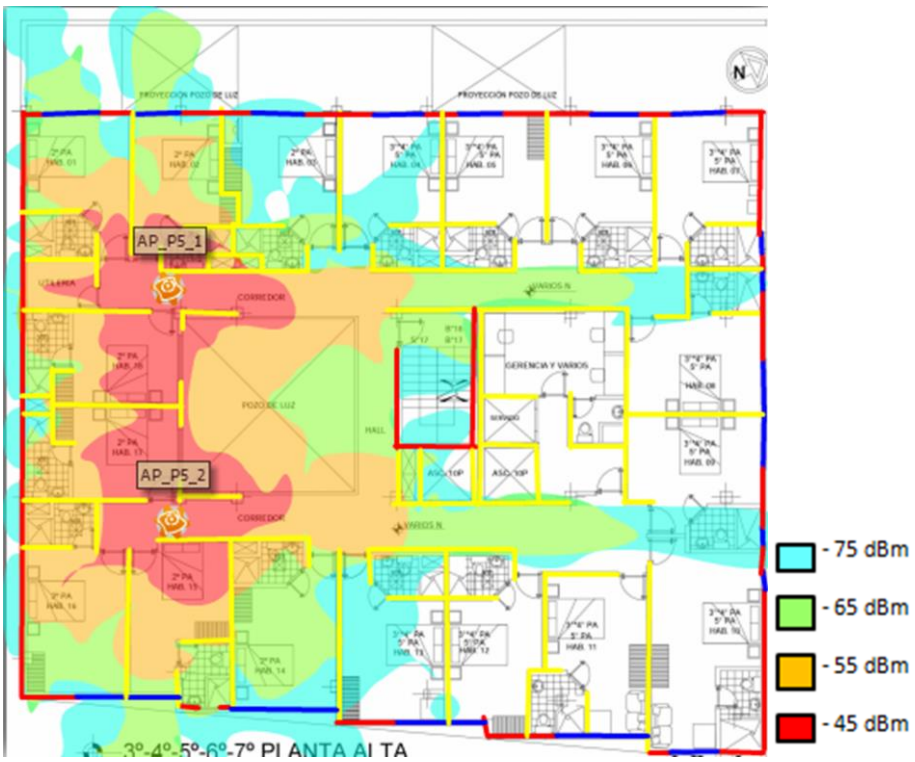
En el quinto piso se encuentran instalados 4 access points “4ipnet” modelo UAP (EAP727), trabajan en la banda de frecuencia de 2.4 GHz y la de 5GHz, en los estándares Wi-Fi 802.11 b / g / n /ac la tasa de transmisión de datos es 300 Mbps (2.4GHz) y 867 Mbps (5 GHz), la potencia máxima de transmisión es de 27 dBm (2.4GHz) y 26 dBm(5 GHz) el tipo de seguridad configurada es WPA2-Personal.

Tabla 20. Configuración APs piso 5.

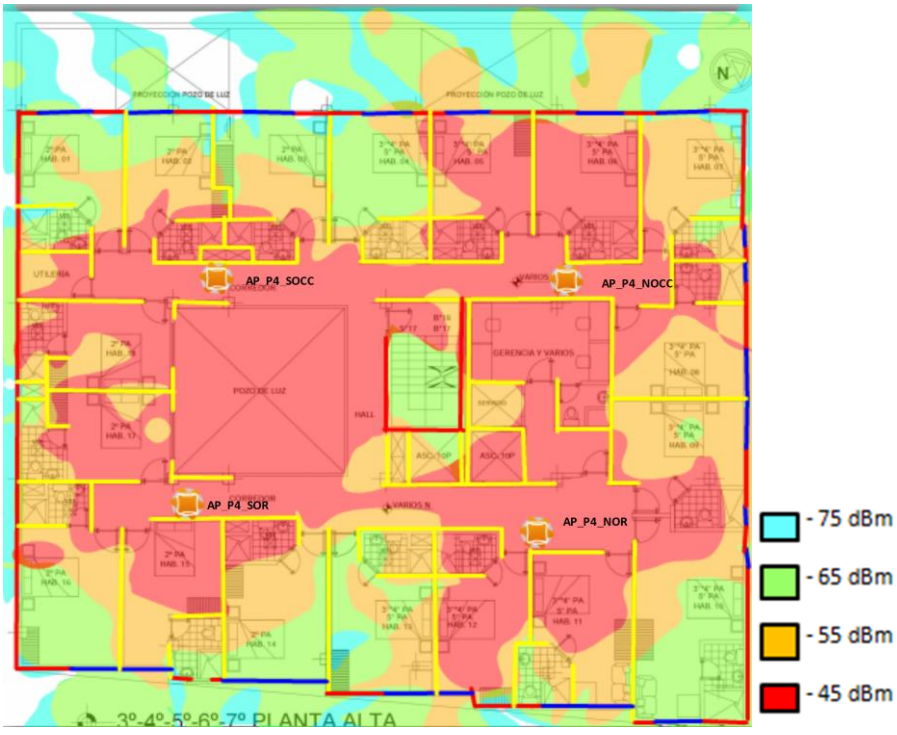
Nombre AP	SSID	Banda de Frecuencia	Canal utilizado
AP_P5_SOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	11/automático
AP_P5_SOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	11/automático
AP_P5_NOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	1/automático
AP_P5_NOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	6/automático

Se utiliza un corte de señal en -75dBm que en la práctica es el mínimo necesario para una conectividad aceptable hacia la navegación en internet. Sin embargo, como puede notarse en el mapa de calor, la señal mínima en la mayoría de las áreas a cubrir es -65 dBm.

Con los 4 APs instalados se cubre con una intensidad de potencia de -45 dBm a un 70% del piso (color rojo), con una intensidad de potencia de -55 dBm a un 15 % (color naranja), con un intensidad de potencia a -65 dBm a un 10 % (color verde) y con una intensidad de potencia de -75dBm al resto del piso (color celeste).



a)



b)

Figura 78. Cobertura APs del quinto piso

a) Cobertura actual

b) Propuesta de cobertura

Al realizar la prueba de conexión a la red inalámbrica con una laptop que tiene la antena inalámbrica de 2.4 GHz en el área de hall se conecta al punto de acceso inalámbrico MAC (00:1F:D4:04:44:75) como se puede apreciar en la Figura 79, ocupa el canal 6. La seguridad que utiliza es WPA-2 Personal con una intensidad de señal de -43dBm. El piso de ruido en el quinto piso tiene un nivel de -90 dBm y los demás APs que se visualizan llegan a tener una intensidad de señal de -60dBm.

Figura 79. Análisis de señales Wi-FI en Piso 5

Sexto Piso

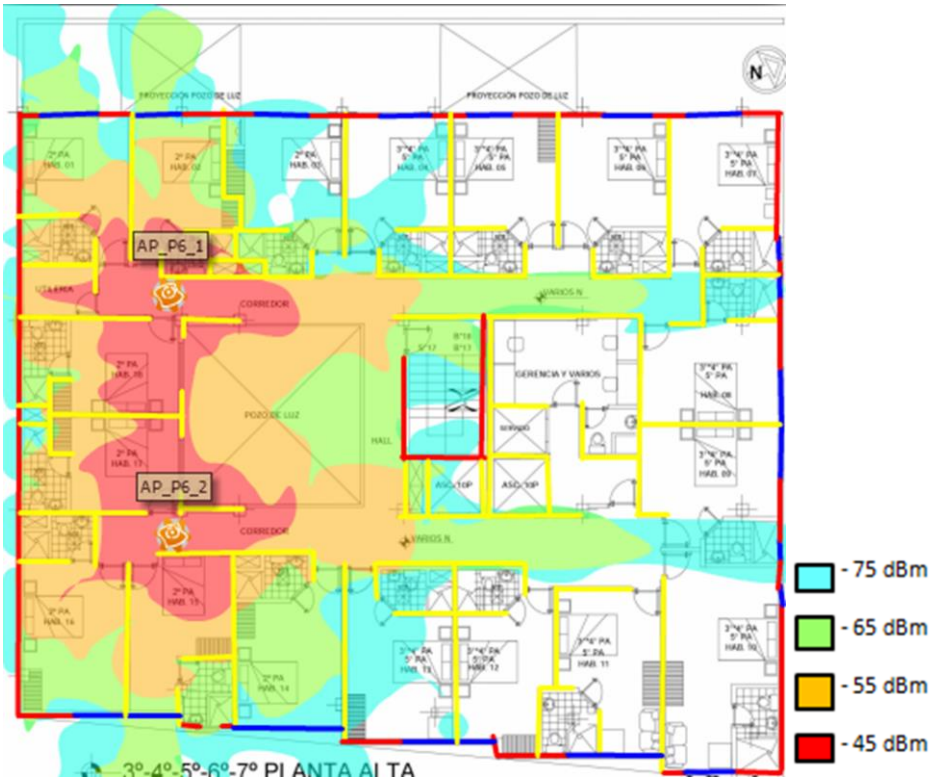
En el sexto piso se encuentran instalados 4 access points “4ipnet” modelo UAP (EAP727), trabajan en la banda de frecuencia de 2.4 GHz y la de 5GHz, en los estándares Wi-Fi 802.11 b / g / n /ac la tasa de transmisión de datos es 300 Mbps (2.4GHz) y 867 Mbps (5 GHz), la potencia máxima de transmisión es de 27 dBm (2.4GHz) y 26 dBm(5 GHz) el tipo de seguridad configurada es WPA2-Personal.

Tabla 21. Configuración APs séptimo piso.

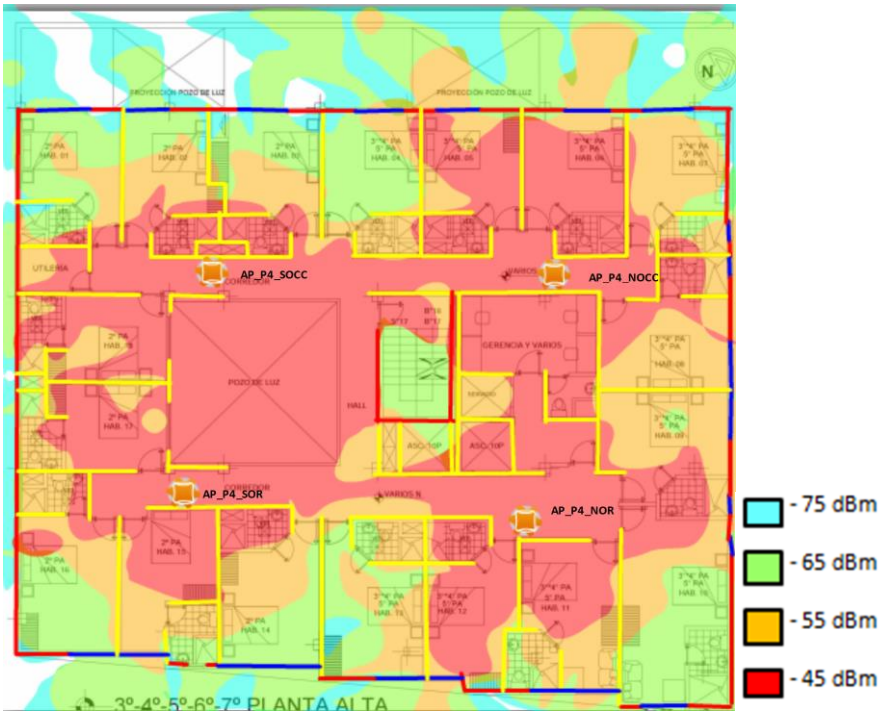
Nombre AP	SSID	Banda de Frecuencia	Canal utilizado
AP_P6_SOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	1/automático
AP_P6 _SOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	11/automático
AP_P6_NOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	8/automático
AP_P6_NOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	3/automático

Se utiliza un corte de señal en -75dBm que en la práctica es el mínimo necesario para una conectividad aceptable hacia la navegación en internet. Sin embargo, como puede notarse en el mapa de calor, la señal mínima en la mayoría de las áreas a cubrir es -65 dBm.

Con los 4 APs instalados se cubre con una intensidad de potencia de -45 dBm a un 70% del piso (color rojo), con una intensidad de potencia de -55 dBm a un 15 % (color naranja), con un intensidad de potencia a -65 dBm a un 10 % (color verde) y con una intensidad de potencia de -75dBm al resto del piso (color celeste).



a)



b)

Figura 80. Cobertura APs del sexto piso

a) Cobertura actua

b) Propuesta de cobertura

Al realizar la prueba de conexión a la red inalámbrica con una laptop que tiene la antena inalámbrica de 2.4 GHz en el área de hall se conecta al punto de acceso inalámbrico MAC (00:1F:D4:04:44:75) como se puede apreciar en la Figura 77, ocupa el canal 6. La seguridad que utiliza es WPA-2 Personal con una intensidad de señal de -42dBm. El piso de ruido en el sexto piso tiene un nivel de -90 dBm y los demás APs que se visualizan llegan a tener una intensidad de señal de -60dBm.

Figura 80. Análisis de señales Wi-Fi en Piso 6

Séptimo Piso

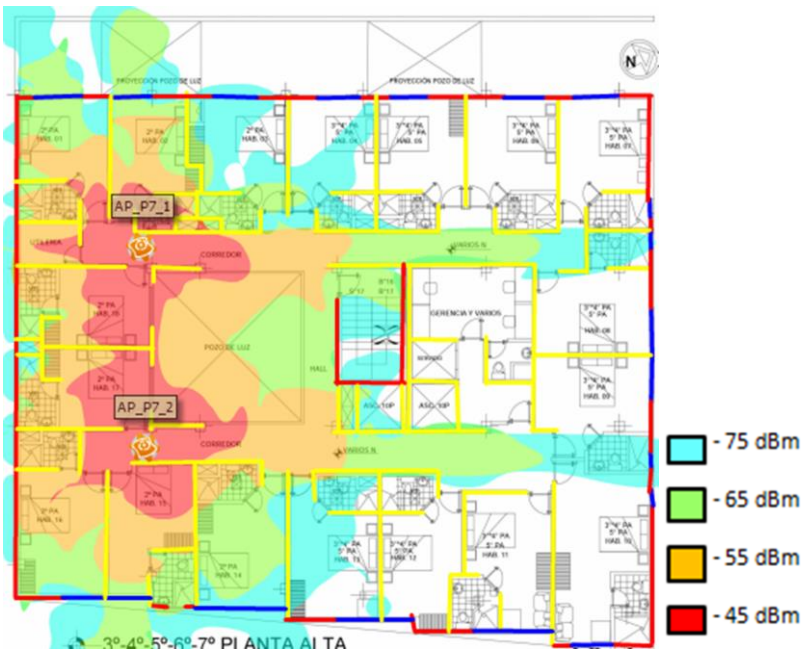
En el séptimo piso se encuentran instalados 4 access points “4ipnet” modelo UAP (EAP727), trabajan en la banda de frecuencia de 2.4 GHz y la de 5GHz, en los estándares Wi-Fi 802.11 b / g / n /ac la tasa de transmisión de datos es 300 Mbps (2.4GHz) y 867 Mbps (5 GHz), la potencia máxima de transmisión es de 27 dBm (2.4GHz) y 26 dBm(5 GHz) el tipo de seguridad configurada es WPA2-Personal.

Tabla 22. Configuración APs séptimo piso.

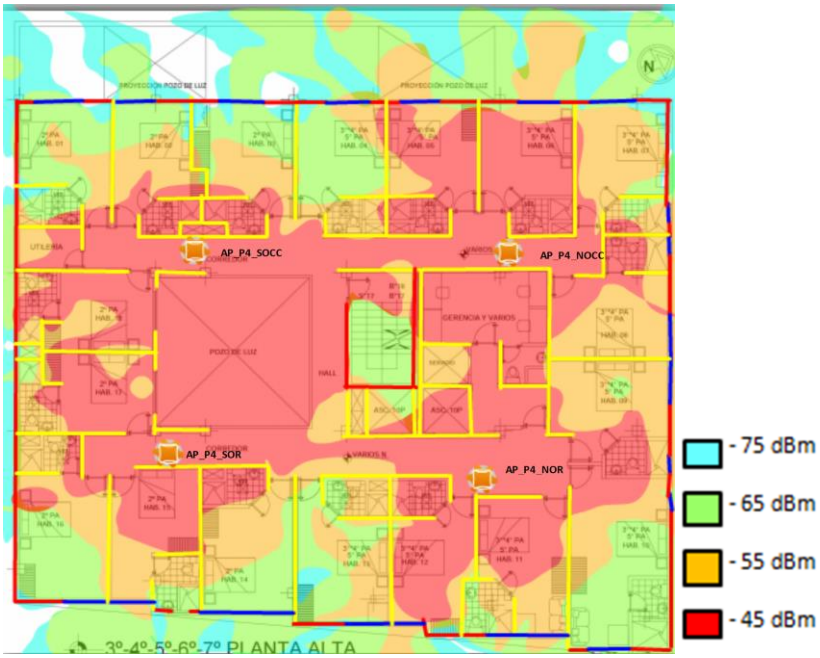
Nombre AP	SSID	Banda de Frecuencia	Canal utilizado
AP_P7_SOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	11/automático
AP_P7_SOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	11/automático
AP_P7_NOR	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	1/automático
AP_P7_NOCC	Huespedes_Finlandia/ Gerencia/Staff	2.4 GHz/5Ghz	6/automático

Se utiliza un corte de señal en -75dBm que en la práctica es el mínimo necesario para una conectividad aceptable hacia la navegación en internet. Sin embargo, como puede notarse en el mapa de calor, la señal mínima en la mayoría de las áreas a cubrir es -65 dBm.

Con los 4 APs instalados se cubre con una intensidad de potencia de -45 dBm a un 70% del piso (color rojo), con una intensidad de potencia de -55 dBm a un 15 % (color naranja), con un intensidad de potencia a -65 dBm a un 10 % (color verde) y con una intensidad de potencia de -75dBm al resto del piso (color celeste).



a)



b)

Figura 81. Cobertura APs del séptimo piso

a) Cobertura actual

b) Propuesta de cobertura

Al realizar la prueba de conexión a la red inalámbrica con una laptop que tiene la antena inalámbrica de 2.4 GHz en el área de hall se conecta al punto de

acceso inalámbrico MAC (00:1F:D4:04:44:75) como se puede apreciar en la Figura 82, ocupa el canal 6. La seguridad que utiliza es WPA-2 Personal. La intensidad de señal es de -36dBm. El piso de ruido en la planta baja tiene un nivel de -90 dBm y los demás APs que se visualizan llegan a tener una intensidad de señal de -67dBm.

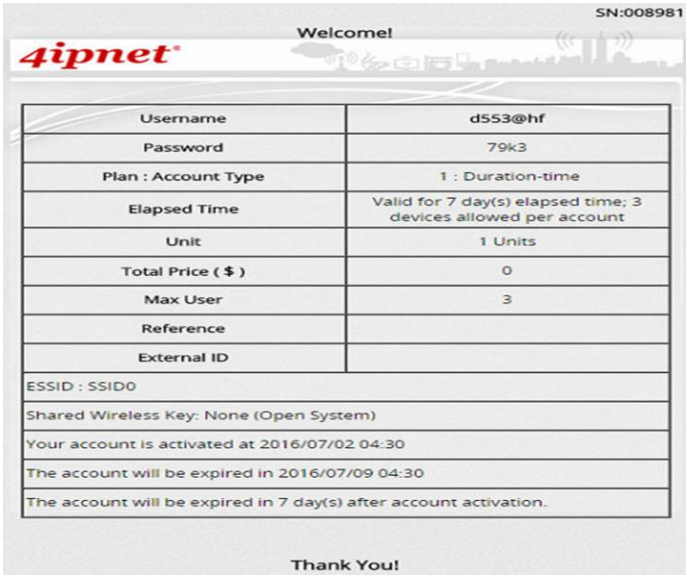
Figura 82. Análisis de señales Wi-FI en Piso 7

3.15 Pruebas de creación de cuentas:

Se puede crear cuentas a través de la controladora o mediante la impresora utilizando las teclas de acceso directo:

Opción 1: Huéspedes

Mediante la impresora utilizando las teclas de acceso directo: ‘1’ + ENTER


SN:008981

Welcome!

4ipnet

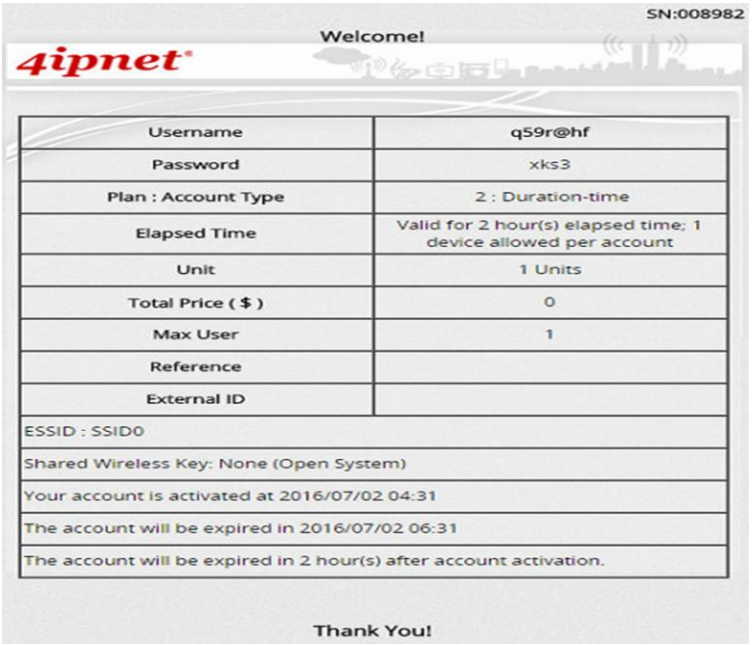
Username	d553@hf
Password	79k3
Plan : Account Type	1 : Duration-time
Elapsed Time	Valid for 7 day(s) elapsed time; 3 devices allowed per account
Unit	1 Units
Total Price ($)	0
Max User	3
Reference	
External ID	
ESSID : SSID0	
Shared Wireless Key: None (Open System)	
Your account is activated at 2016/07/02 04:30	
The account will be expired in 2016/07/09 04:30	
The account will be expired in 7 day(s) after account activation.	

Thank You!

Figura 83. Ticket válido para 7 días, 3 equipos por usuario

Opción 2: Invitados

Mediante la impresora utilizando las teclas de acceso directo: ‘2’ + ENTER


SN:008982

Welcome!

4ipnet

Username	q59r@hf
Password	xks3
Plan : Account Type	2 : Duration-time
Elapsed Time	Valid for 2 hour(s) elapsed time; 1 device allowed per account
Unit	1 Units
Total Price ($)	0
Max User	1
Reference	
External ID	
ESSID : SSID0	
Shared Wireless Key: None (Open System)	
Your account is activated at 2016/07/02 04:31	
The account will be expired in 2016/07/02 06:31	
The account will be expired in 2 hour(s) after account activation.	

Thank You!

Figura 84. Ticket válido para 2 horas, 1 equipos por usuario

Opción 3: Staff

Mediante la impresora utilizando las teclas de acceso directo: ‘3’ + ENTER


SN:008983

Welcome!

4ipnet

Username	z8t7@hf
Password	3h88
Plan : Account Type	3 : Duration-time
Elapsed Time	Valid for 1 day(s) elapsed time; 1 device allowed per account
Unit	1 Units
Total Price ($)	0
Max User	1
Reference	Empleados
External ID	
ESSID : SSID0	
Shared Wireless Key: None (Open System)	
Your account is activated at 2016/07/02 04:32	
The account will be expired in 2016/07/03 04:32	
The account will be expired in 1 day(s) after account activation.	

Thank You!

Figura 85. Ticket válido para 1 día, 1 equipos por usuario

3.16 Pruebas de ingreso a la red

Página de inicio de sesión con el SSDI Finlandia Huespedes/Guests

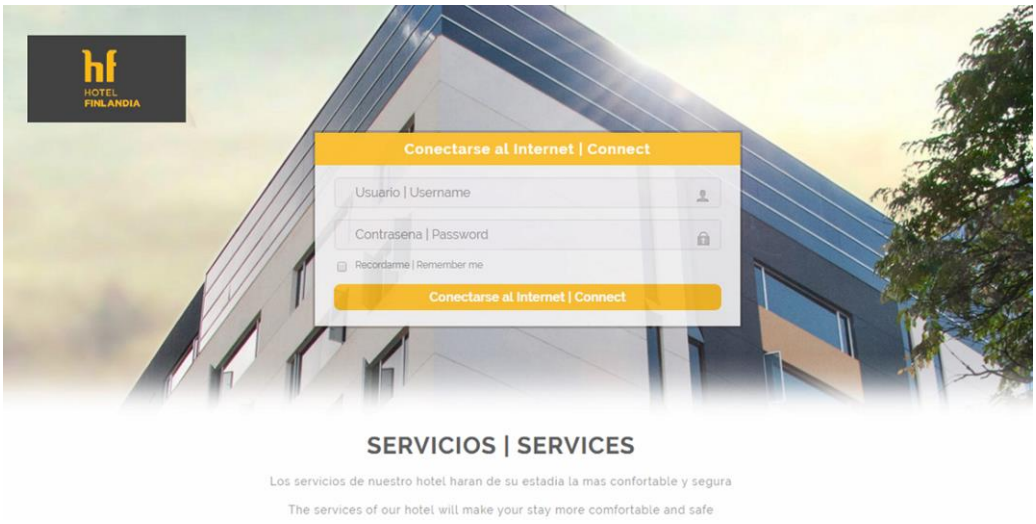


Figura 86. Hotspot Huespedes

Página de inicio de sesión con el SSDI Invitados:

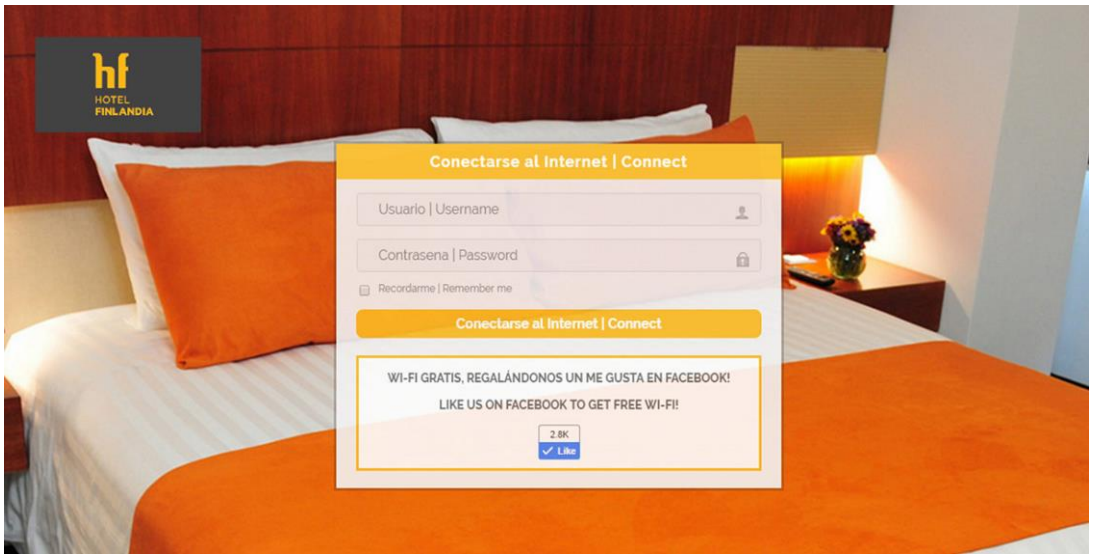


Figura 87. Hotspot Invitados

3.17 Análisis de tráfico de la red

Mediante la interfaz de administración que incluye el controlador inalámbrico se puede monitorear, configurar, controlar, administrar la red inalámbrica de forma fácil y sencilla.

3.17.1 Interfaz WAN1

El controlador inalámbrico permite monitorear el tráfico entrante y saliente de la red, al seleccionar la interfaz de red WAN1 podemos obtener los datos estadísticos del tráfico de la red a manera de resumen, tráfico del día, del mes y de los 10 primeros días.

En la siguiente figura 42 se puede verificar gráficamente que la tasa de transmisión es mucho menor que la tasa de recepción.

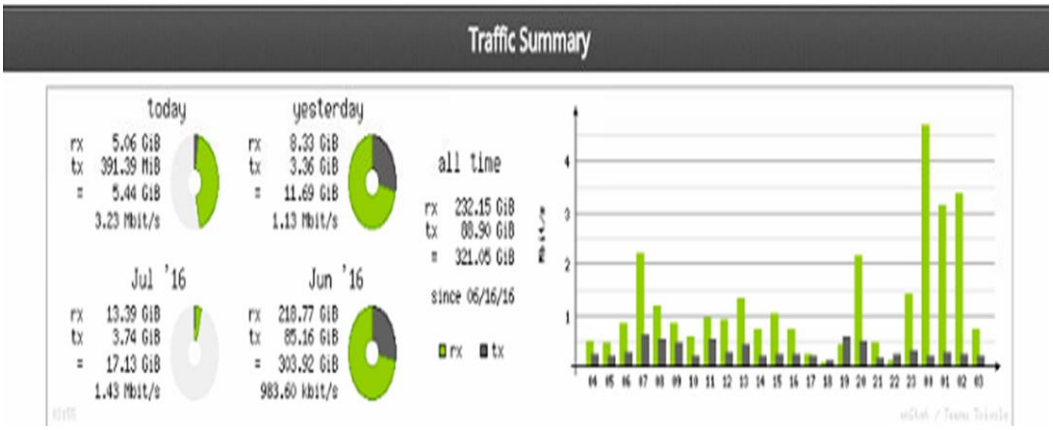
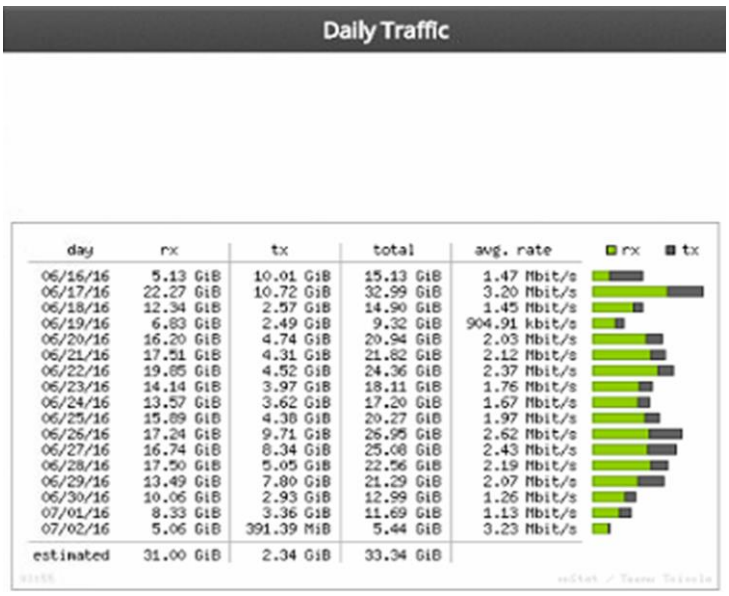


Figura 88. Resumen del tráfico de la interfaz WAN1

La siguiente figura muestra las estadísticas del tráfico tanto de recepción como de transmisión por día, teniendo un estimado de de 31 GB de trafico entrante y de 2 GB de tráfico saliente de transmisión.



day	rx	tx	total	avg. rate
06/16/16	5.13 GiB	10.01 GiB	15.13 GiB	1.47 Mbit/s
06/17/16	22.27 GiB	10.72 GiB	32.99 GiB	3.20 Mbit/s
06/18/16	12.34 GiB	2.57 GiB	14.90 GiB	1.45 Mbit/s
06/19/16	6.83 GiB	2.49 GiB	9.32 GiB	904.91 kbit/s
06/20/16	16.20 GiB	4.74 GiB	20.94 GiB	2.03 Mbit/s
06/21/16	17.51 GiB	4.31 GiB	21.82 GiB	2.12 Mbit/s
06/22/16	19.85 GiB	4.52 GiB	24.36 GiB	2.37 Mbit/s
06/23/16	14.14 GiB	3.97 GiB	18.11 GiB	1.76 Mbit/s
06/24/16	13.57 GiB	3.62 GiB	17.20 GiB	1.67 Mbit/s
06/25/16	15.89 GiB	4.38 GiB	20.27 GiB	1.97 Mbit/s
06/26/16	17.24 GiB	9.71 GiB	26.95 GiB	2.62 Mbit/s
06/27/16	16.74 GiB	8.34 GiB	25.08 GiB	2.43 Mbit/s
06/28/16	17.50 GiB	5.05 GiB	22.56 GiB	2.19 Mbit/s
06/29/16	13.49 GiB	7.80 GiB	21.29 GiB	2.07 Mbit/s
06/30/16	10.06 GiB	2.93 GiB	12.99 GiB	1.26 Mbit/s
07/01/16	8.33 GiB	3.36 GiB	11.69 GiB	1.13 Mbit/s
07/02/16	5.06 GiB	391.39 MiB	5.44 GiB	3.23 Mbit/s
estimated	31.00 GiB	2.34 GiB	33.34 GiB	

Figura 89. Estadísticas del tráfico por dìa de la interfaz WAN1

La siguiente figura muestra las estadísticas del tráfico tanto de recepción como de transmisión mensual.

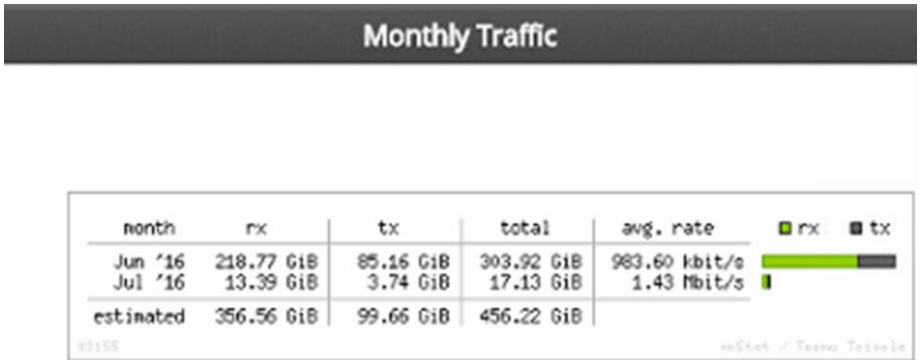


Figura 90. Estadísticas del tráfico del mes de la interfaz WAN1

3.17.2 Interfaz WAN2

Al seleccionar la interfaz de red WAN2 podemos obtener las estadísticas del tráfico en forma de resumen, el tráfico del día, del mes y de los 10 primeros días.

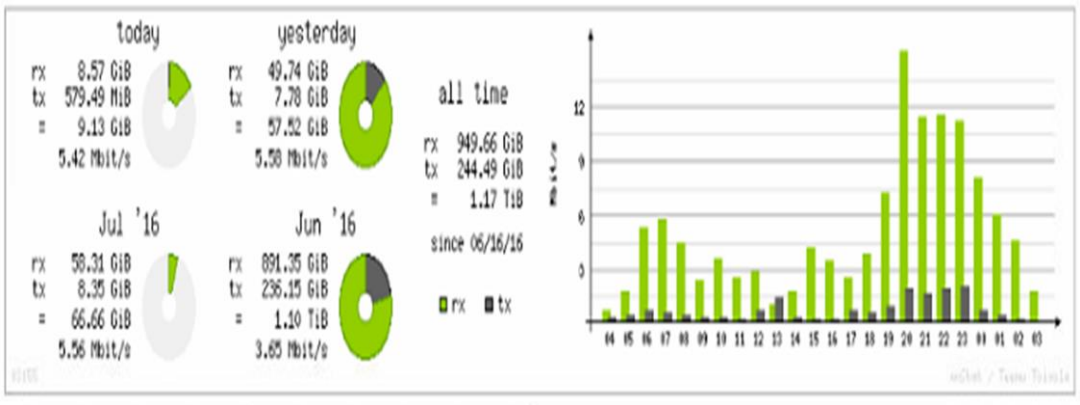


Figura 91. Resumen del tráfico de la interfaz WAN2

La siguiente figura muestra las estadísticas del tráfico tanto de recepción como de transmisión por día, teniendo un estimado de de 52 GB de trafico entrante y de 3 GB de tráfico saliente de transmisión.

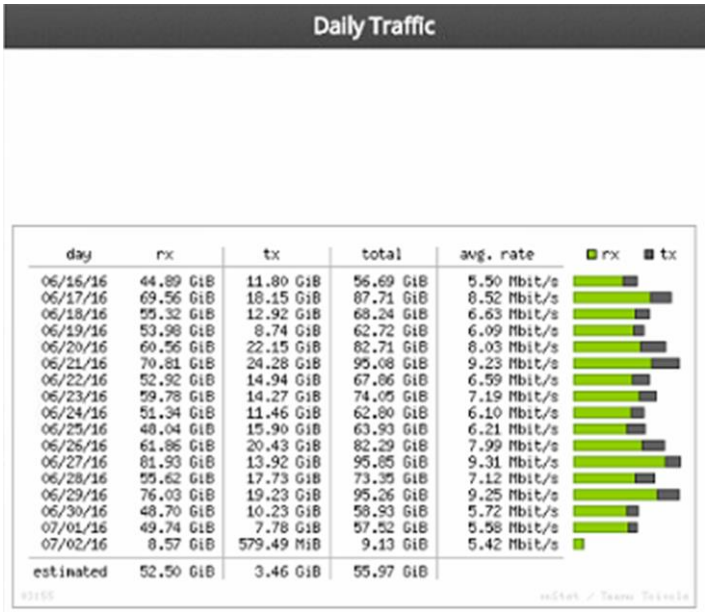


Figura 92. Estadísticas del tráfico por día de la interfaz WAN2

La siguiente figura muestra las estadísticas del tráfico tanto de recepción como de transmisión mensual.

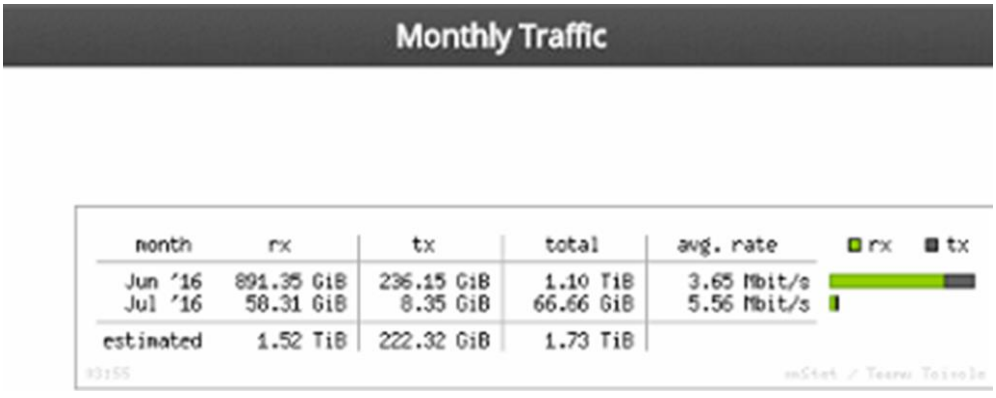


Figura 93. Estadísticas del tráfico del mes de la interfaz WAN2

4. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Se eligió el equipamiento necesario acorde a las necesidades del mercado y crecimiento tecnológico del medio.

Se realizó la distribución de 4 APs 727 por piso para dar cobertura al área de habitaciones, teniendo una intensidad de señal de -45 dBm en un promedio de 50% del área útil de las habitaciones.

Se utilizó los APs 767 de alta densidad para cubrir con el área de lobby, restaurant y salones de eventos, ya que estas áreas tienen mayor número de usuarios. Teniendo una intensidad de potencia de -45dBm en el 40% del área total.

Se realizó un diseño de red inalámbrica personalizable, mediante configuraciones y administración de políticas y perfiles de usuario para el Hotel.

Se configura planes de facturación para los SSIDs: Finlandia huéspedes/guests, invitados y staff que ayudan a tener un control del acceso al internet de los usuarios.

Se configura QoS de acuerdo a la política: para la política 1-Huespedes se tiene un ancho de banda de 5MB por usuario y para la política 2- Invitados 4MB de ancho de banda por grupo.

Se configura el bloqueo de los servicios: ssh, telnet, icmp para las políticas 1-Huespedes y 2-Invitados, para mayor seguridad de la red.

Se brindó movilidad y transparencia de cobertura para los usuarios del Hotel, tanto personal administrativo como huéspedes.

Se establecieron archivos de configuración de coberturas y selección de canales mediante el estudio de cada piso para brindar un mejor acceso y fiabilidad a la red al momento de navegar hacia el internet.

Se establecieron rutas de salida alternas para la navegación por internet, en donde los usuarios administrativos del hotel permanecen en la intranet y los usuarios tanto huéspedes como invitados son enrutados directamente al proveedor ISP.

4.2 Recomendaciones

Se recomienda, escanear la interferencia de canales inalámbricos debidamente al momento de ingresar equipos en la red, ya que de acuerdo a la ubicación geográfica del hotel, existen muchas redes inalámbricas aledañas que pueden provocar interferencias provocando malestar en el servicio al usuario del hotel.

Al momento de identificar saturaciones de tráfico en la red inalámbrica de los huéspedes, se recomienda verificar logs del sistema en el controlador inalámbrico y no correr servicios de analizador de paquetes, estos programas consumen tráfico y puertos en la red.

Se recomienda eliminar de forma periódica los usuarios con cuentas bajo demanda expiradas ya que esto puede colapsar el buffer del controlador inalámbrico.

Proporcionar un ambiente adecuado de temperatura estándar de 20ºC en el datacenter, ahí se aloja toda la infraestructura del hotel.

Se recomienda crear plantillas de configuraciones diferentes al momento de proporcionar cuentas temporales, debido a que son datos provisionales y no se desea afectaciones al resto de dispositivos.

REFERENCIAS

4ipnet. (s.f.). *EAP767 Indor access point*. Recuperado el 28 de marzo de 2016 de: http://documents.”4ipnet”.com/datasheet/en/EAP767_Datasheet.pdf.

4ipnet. (s.f.). *EAP727 Indor access point*. Recuperado el 28 de marzo de 2016 de: http://documents.4ipnet.com/datasheet/en/EAP727_Datasheet.pdf

4ipnet. (s.f.). *EAP767.* Recuperado el 28 de marzo de 2016 de http://www.4ipnet.com/products/wireless-access-point/EAP767

4ipnet. (s.f.). *Controladora Wireless*. Recuperado el 05 de abril de 2016 de http://documents.4ipnet.com/datasheet/en/HSG260_Datasheet.pdf

4ipnet. (s.f.). *Productos 4ipnet*. Recuperado el 05 de abril de 2016 de http://www.4ipnet.com/products/wireless-access-point/EAP767

Andreu. J. (2011). *Redes inalámbricas (Servicios en red)*. Recuperado el 15 de marzo de 2016 de https://books.google.com.ec/books?id=98_TAwAAQBAJ&pg=PA212&dq=redes+inal%C3%A1mbricas&hl=es&sa=X&redir_esc=y#v=onepage&q=redes%20inal%C3%A1mbricas&f=false7/.

4ipnet (s.f.). *Unified access switch*. Recuperado el 05 de abril de 2016 de: http://www.4ipnet.com/products/unified-access-switch/SW1024

Afonso, C. (2011). *Uso del espectro en América Latina.* Recuperado el 05 de abril de 2016 de http://www.apc.org/en/system/files/ca_sintesis_final-AF.pdf

Arcotel. (s.f.). *Plan nacional de Frecuencias*. Recuperado el 05 de abril de 2016 de http://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/07/plan_nacional_frecuencias_2012.pdf

Barata, M. (2008). *Universidad Politécnica de Catalunya*. Recuperado el 05 de abril de 2016 de http://upcommons.upc.edu/bitstream/handle/2099.1/7202/memoria.pdf?sequence=1

Cruz. D. (2011). *Diseño e implementación de un portal cautivo que permita la venta de tickets de internet para un hotspot, empleando herramientas de software libre*. Recuperado el 12 de marzo de 2016 de http://bibdigital.epn.edu.ec/bitstream/15000/3953/1/CD-3714.pdf.

Cybercursos (s.f.). *Redes inalámbricas*. Recuperado el18 de marzo de 2016http://www3.uah.es/vivatacademia/ficheros/n54/redesinalam.PDF.

Es.scribd (s.f.). *Fundamentals of wireless LAN*. Recuperado el 15 de marzo de 2016 de https://es.scribd.com/doc/19370287/Fundamentos-de-WLAN-Redes-Inalambricas-en-Espanol.

Hotels (s.f.). *Encuesta de hotels.com revela que la disponibilidad de conexión Wi-Fi gratuita es el factor decisivo al elegir alojamiento*. Recuperado 03 marzo de 2016 de http://press.hotels.com/es-us/news-releases/encuesta-de-hotels-com-revela-que-la-disponibilidad-de-conexion-wi-fi-gratuita-es-el-factor-decisivo-al-elegir-alojamiento/.

Lacuevawifi. (s.f.). *Tipos Antena WiFi*. Recuperado el 05 de abril de 2016 de http://www.lacuevawifi.com/equipos-de-red/tipos-de-antena-wifi/

Liliana, P. (2011). *Topologias de las redes inalambricas*. Recuperado el 05 de abril de 2016 de http://plgarcia.blogspot.com/2011/06/definicion.html

LinkedIN Corporation. (s.f.). *Tarjeta de Red*. Recuperado el 05 de abril de 2016 de http://es.slideshare.net/jorgelpa94/una-tarjeta-de-red-o-adaptador-de-red-permite-la-comunicacin-con-aparatos-conectados-entre-si-y-tambin-permite-compartir-recursos-entre-dos-o-ms-computadoras

Mantilla, C. (2007). *Repositorio ESPE*. Recuperado el 05 de abril de 2016 de http://repositorio.espe.edu.ec/bitstream/21000/607/1/T-ESPE-014615.pdf

Microsoft. (s.f.). *Soporte Microsoft*. Recuperado el 05 de abril de 2016 de https://support.microsoft.com/es-es/products/windows?os=windows-7

OCW. (s.f.). *Sistema de Espectro Disperso de Secuencia Directa DSSS*. Recuperado el 05 de abril de 2016 de http://ocw.uis.edu.co/ingenieria-electronica/comunicaciones/espectrod/dsss.html

Peeters, E. (2004). *Wireless security beyond WEP and WPA*. Recuperado el 05 de abril de 2016 de https://www.sans.org/reading-room/whitepapers/wireless/wireless-security-beyond-wep-and-wpa-1425?show=1425.php&cat=wireless

Peraltha, D. (s.f.). *Administracion de los recursos de una red*. Recuperado el 05 de abril de 2016 de http://miblogdvdykrn.blogspot.com/2015/07/administracion-de-los-recursos-de-una_7.html

PEZO, A. (2010). *Universidad Ricardo Palma*. Recuperado el 05 de abril de 2016 de http://cybertesis.urp.edu.pe/bitstream/urp/60/1/reategui_a.pdf

R.F., J. (2008). *MIMO: Tecnología inalámbrica*. Recuperado el 05 de abril de 2016 de http://www.malavida.com/post/mimo-tecnologia-inalambrica

Ramirez H., Colorado A. y Quintero, E. (2011). *Sistema de transmisión de información sobre FPGA`s mediante la modulación spread spectrum*. Recuperado el 05 de abril de 2016 de http://www.redalyc.org/html/849/84922625045/

Sebastian Buettrich, A. E. (s.f.). *Topología e Infraestructura Básica de Redes Inalámbricas*. Recuperado el 05 de abril de 2016 de http://www.it46.se/courses/wireless/materials/es/04_Topologia-Infraestructura/04_es_topologia-e-infraestructura_guia_v01.pdf

UNAD. (s.f.). *Universidad Nacional Abierta y Distancia*. Recuperado el 05 de abril de 2016 de http://datateca.unad.edu.co/contenidos/201493/CONTENIDO%20DIDACTICO%20EXE1/leccin_46_wifi.html

Wndw (2013). *Redes inalámbricas en los paises en desarrollo*. Recuperado el 10 de marzo de 2016 de http://wndw.net/pdf/wndw3-es/wndw3-es-ebook.pdf.

Wifisafe (s.f.). *Manual de configuración 4ipnet sds200w botonera + impresora + controlador*. Recuperado el 28 de marzo de 2016 de https://www.wifisafe.com/blog/manual-de-configuracion-4ipnet-sds200w-botonera-impresora-controlador/

Web 2.0. (s.f.). *Redes Sociales, Movilidad y Sostenibilidad: áreas de mejora para los hoteleros*. Recuperado el 03 de marzo de 2016 de

https://socialmediacomunicacion.wordpress.com/tag/noticias-2/page/7/.

Wordpress. (s.f.). *Punto de Acceso*. Recuperado el 05 de abril de 2016 de https://manejoderedes6203.wordpress.com/1-1-configura-el-acceso-a-los-recursos-de-la-red-inalambrica-a-traves-de-las-herramientas-que-provee-los-dispositivos-de-red/punto-de-acceso-access-point/

ANEXOS

ANEXO 1

Especificaciones Switch Alcatel-Lucent 6850

Product Specifications

Features

SIMPLIFIED MANAGEABILITY

- Dual image and dual configuration file storage provides backup
- Intuitive Alcatel-Lucent CLI with familiar interface reducing training costs
- Extensive user manuals with examples
- Easy to use, point-and-click web based element manager (WebView) with built-in help for easy configuration of new technology features
- Remote telnet management or secure shell access using SSH
- Secured file upload using SFTP, or SCP
- Human readable ASCII based config files for offline editing and bulk configuration
- IGMPv1/v2/v3 snooping to optimize multicast traffic
- BootP/DHCP client allows auto-config of switch IP information to simplify deployment
- Auto-negotiating 10/100/1000 ports automatically configure port speed and duplex setting
- Auto MDI/MDIX automatically configures transmit and receive signals to support straight through and crossover cabling
- DHCP relay to forward client requests to a DHCP server
- SNMPv1/v2/v3
- Integration with SNMP manager Alcatel-Lucent OmniVista for network wide management
- Supports RFC 2819 RMON group (1-Statistics, 2-History, 3-Alarm & 9-Events)
- Network Time Protocol (NTP) for network wide time synchronization
- Alcatel-Lucent Mapping Adjacency Protocol (AMAP) for building topology maps within OmniVista
- Port based, port mirroring for troubleshooting and lawful interception, supports four sessions with multiple sources-to-one destination configuration
- Port monitoring feature that allows capture of Ethernet packets to a file, or for on-screen display to assist in troubleshooting
- sFlow v5 support to monitor and effectively control and manage the network usage
- Local (on the flash) and remote logging (Syslog)
- GVRP for 802.1Q-compliant VLAN pruning and dynamic VLAN creation

HIGH AVAILABILITY

- Ring Rapid Spanning Tree optimized for ring topology to provide less than 100ms convergence time
- 802.1w rapid recovery spanning tree allows subsecond failover to redundant link
- Alcatel-Lucent per-VLAN spanning tree (1x1)
- 802.1D spanning tree for loop free topology and link redundancy
- 802.1s multiple spanning tree
- Fast forwarding mode on user ports to bypass 30-second delay for spanning tree
- Static and 802.3ad dynamic link aggregation that supports automatic configuration of link
- Broadcast storm control
- Redundant 1:1 power provided by the OS6850-BPS
- BPDU blocking – automatically shuts down switch ports being used as user ports if a spanning tree BPDU packet is seen. Prevents unauthorized spanning-tree enabled attached bridges from operating.
- Priority queues: eight hardware-based queues per port

CONVERGENCE/ TRIPLE PLAY

- Traffic prioritization: Flow-based QoS with internal and external (a.k.a., remarking) prioritization
- Bandwidth management: flow based bandwidth management, ingress policing/egress shaping and port based egress shaping
- Queue management: Random Early Detect/Discard (RED), configurable de-queuing algorithm; Strict Priority, Weighted and Deficit Round Robin.
- Power-over-Ethernet: IEEE 802.3af – maximum total power of 380W for PoE

ADVANCED SECURITY

- 802.1X multi-client, multi-VLAN support for perclient authentication and VLAN assignment
- IEEE 802.1X with group mobility
- IEEE 802.1X with MAC based authentication, group mobility or "guest" VLAN support
- MAC-based authentication for non-802.1X host
- Authenticated VLAN that challenges users with username and password and supports dynamic VLAN access based on user
- PKI authentication for SSH access
- Support for host integrity check and remediation VLAN
- Support for Alcatel-Lucent Quarantine Manager and quarantine VLAN
- Learned Port Security (LPS) or MAC address lockdown allows only known devices to have network access preventing unauthorized network device access
- RADIUS and LDAP admin authentication prevents unauthorized switch management
- TACACS+ client allows for authentication authorization and accounting with a remote TACACS+ server
- Secure Shell (SSH), Secure Socket Layer (SSL) for HTTPS access and SNMPv3 for encrypted remote management communication
- Access control lists to filter out unwanted traffic including denial of service attacks; Flow based filtering in hardware (L1-L4)
- Support of Microsoft Network Access Protection (NAP)*
- Switch protocol security
  - MD5 for RIPv2, OSPFv2 and SNMPv3
  - SSH for secure CLI session with PKI support
  - SSL for secure HTTP session
- DHCP Snooping, DHCP IP Spoof protection

RESIDENTIAL METRO TRIPLE-PLAY ETHERNET ACCESS

- DHCP Option 82 – relay agent information
- QinQ (Vlan stacking)
- Ethernet OAM compliant with 802.1ag version 5.2

L3 ROUTING

IP Routing

- Static routing
- RIP v1 & v2
- OSPF v2
- BGP v4
- ISIS

Multicast

- IGMP v1, v2 & v3 snooping
- PIM-SM
- PIM-DM
- DVMRP

Protocols (IPv4) Network Protocol

- TCP/IP stack
- ARP
- DHCP relay
- Generic UDP relay per VLA

Resilience

- VRRP v2

LAYER-3 ROUTING (IPX)

IP Routing

- Static routing
- RIP/SAP

POWER OVER ETHERNET

- IEEE 802.3af (supported on all POE chassis)

STACKING

- Two built-in stacking ports to provide fault tolerant looped stacking configuration
- 10 Gbps full-duplex bandwidth per stacking port

COMBO PORTS

- OS6850-24, -24X, -P24, -P24X, - 48, -P48 Four Gigabit Ethernet SFP combo ports
- OS6850-24L, -P24L, - 48L, -P48L Four Gigabit Ethernet SFP combo ports
- OS6850-U24X Two Gigabit Ethernet SFP combo ports

10GIGE UPLINKS

OS6850-24X, -P24X, -48X, -P48X and -U24X

- Two built-in XFP ports that support industry standard XFP-based 10GIgE optical transceivers

POWER SUPPLIES AND POWER CONSUMPTION

- Main and backup power supplies are external either directly connected to the rear of the unit or remotely
- Supports redundant dual hot swappable power supplies
- Power shelf that holds one 510W AC or two 360W AC, 126W AC or120W DC power supplies
- 126W (AC) and 120W (DC) power supplies only used with non-PoE models.
- 360W (AC) and 510W (DC) power supplies only used with PoE models.

Specifications

Indicators

PER PORT LEDS

- 10/100/1000: PoE, link/activity
- SFP: link/activity
- XFP: link/activity

SYSTEM LEDS

- Switch ID (indicates the stack ID of the unit in the stack: 1 to 7)
- System (OK) (chassis HW/SW status)
- PWR (primary power supply status)
- PRI (virtual chassis primary)
- BPS (backup power status)

Physical Dimensions (WxDxH)

CHASSIS SIZE (WITHOUT POWER SUPPLY OR PS SHELF)

- 17.32 x 10.63 x 1.73 in (44.0 x 27.0 x 4.4 cm)

TOTAL SIZE INCLUDING POWER SUPPLY'S SHELF AND MOUNTING EARS

- 19.00 x 17.56 x 1.73 in (48.2 x 44.6 x 4.4 cm)

CHASSIS SIZE (WITH MOUNTING EARS,WITHOUT POWER SUPPLY OR PS SHELF)

- 19 x 10.63 x 1.73 in (48.2 x 27.0 x 4.4 cm)

Weight

CHASSIS WITHOUT THE POWER SUPPLY

- OS6850-P24 and -P24L 8.62 lb (3.91kg)
- OS6850-P24X 8.86 lb (4.02 kg)
- OS6850-P48and -P48L 9.39 lb (4.26kg)
- OS6850-P48X 9.59 lb (4.35kg)
- OS6850-24 and 24L 8.36 lb (3.79kg)

POWER SUPPLIES

- 510W AC 5.71 lb (2.59kg)
- 360W AC 3.22 lb (1.46kg)
- 126W AC 2.45 lb (1.11kg)
- 120W DC 2.09 lb (0.95kg)
- Power supply tray 1.26 lb (0.57kg)

EMC

- FCC CRF Title 47 Subpart B (Class A limits. Note: Class A with UTP cables)
- VCCI (Class A limits. Note: Class A with UTP cables)
- AS/NZS 3548 (Class A limits. Note: Class A with UTP cables)
- CE marking for European countries (Class A. Note: Class A with UTP cables)
- EN 55022: 1995 (Emission Standard)
- EN 61000-3-3: 1995
- EN 61000-3-2: 2000
- EN 55024: 1998 (Immunity Standards)
- EN 61000-4-2: 1995+A1: 1998
- EN 61000-4-3: 1996+A1: 1998
- EN 61000-4-4: 1995
- EN 61000-4-5: 1995
- EN 61000-4-6: 1996
- EN 61000-4-8: 1994
- EN 61000-4-11: 1994
- IEEE802.3: Hi-Pot Test (2250 VDC on all Ethernet ports)

Safety Agency Certifications

- US UL 60950
- IEC 60950-1:2001; all national deviations
- EN 60950-1: 2001; all deviations
- CAN/CSA-C22.2 No. 60950-1-03
- NOM-019 SCFI, Mexico
- AS/NZ TS-001 and 60950:2000, Australia
- UL-AR, Argentina
- UL-GS Mark, Germany
- EN 60825-1 Laser, EN60825-2 Laser
- CDRH Laser
- China CCC

IEEE Standards

- IEEE 802.1D (STP)
- IEEE 802.1p (CoS)
- IEEE 802.1Q (VLANs)
- IEEE 802.1QinQ(VLAN stacking)
- IEEE 802.1ag (Connectivity Fault Management)
- IEEE 802.1s (MSTP)
- IEEE 802.1w (RSTP)
- IEEE 802.1X (Port Based Network Access Protocol)
- IEEE 802.3i (10BaseT)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (Gigabit Ethernet)
- IEEE 802.3ab (1000BaseT)
- IEEE 802.3ac (VLAN Tagging)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3af (Power-over-Ethernet)
- IEEE 802.3ae (10G Ethernet)

ANEXO 2

Especificaciones Switch Alcatel-Lucent 6250

DETAILED PRODUCT FEATURES

Simplified management

Configuration management interfaces

- Intuitive command line interface (CLI) with familiar interface, reducing training costs
- Easy-to-use, point-and-click web-based element manager (WebView) with built-in help for easy configuration
- Integration with Alcatel-Lucent OmniVista® 2500 for network management
- Full configuration and reporting using SNMPv1/2/3 across all OmniSwitch families to facilitate third-party network management system (NMS) integration
- Remote Telnet management or Secure Shell access using SSHv2
- File upload using USB, TFTP, FTP, SFTP, or SCP for faster configuration
- Human-readable ASCII-based configuration files for off-line editing and bulk configuration
- Managed by Alcatel-Lucent 5620 Service Aware Manager

Monitoring and troubleshooting

- Local (on the flash) and remote server logging: Syslog and command log
- Port-based mirroring for troubleshooting and lawful interception supports four sessions with multiple sources-to-one destinations
- Policy-based mirroring that allows selecting the type of traffic to mirror by using QoS policies
- Remote port mirroring that facilitates passing mirrored traffic through the network to a remotely connected device
- Port monitoring feature that allows capturing Ethernet packets to a file, or to an on-screen display to assist in troubleshooting
- sFlow v5 and RMON for advanced monitoring and reporting capabilities for statistics, history, alarms and events
- IP tools: Ping and trace route
- Digital Diagnostic Monitoring (DDM): Real-time diagnostics of fiber connections for early detection of optical signal deterioration
- Time Domain Reflectometry (TDR) for locating breaks or other discontinuity in copper cables

Network configuration

- Remote auto-configuration download
- Auto-negotiating 10/100/1000 ports automatically configure port speed and duplex setting
- Auto MDI/MDIX configureing transmit and receive signals to support straight-through and crossover cabling
- BOOTP/DHCP client that allows auto-configuring switch IP information for simplified deployment
- DHCP relay for forwarding client requests to a DHCP server
- Alcatel-Lucent Mapping Adjacency Protocol (AMAP) for building topology maps
- IEEE 802.1AB Link Layer Discovery Protocol (LLDP) with MED extensions for automated device discovery
- Multiple VLAN Registration Protocol (MVRP) for IEEE 802.1Q-compliant virtual LAN (VLAN) pruning and dynamic VLAN creation
- Auto QoS for switch management traffic and traffic from Alcatel-Lucent IP phones
- Network Time Protocol (NTP) for network-wide time synchronization
- Stackable to eight units

Resiliency and high availability

- Ring Rapid Spanning Tree (RRSTP) optimized for ring topology to provide less than 100 ms convergence time
- IEEE 802.1s Multiple Spanning Tree Protocol: Encompasses IEEE 802.1D STP and IEEE 802.1w Rapid Spanning Tree Protocol
- Per-VLAN spanning tree (PVST) and 1x1 STP mode
- Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP) and static LAG groups across modules
- Dual-home link (DHL) support for sub-second link protection without STP
- Virtual Router Redundancy Protocol (VRRP) providing highly available routed environments
- Broadcast and multicast storm control to avoid degradation in overall system performance
- Unidirectional Link Detection (UDLD) for detecting and disabling unidirectional links on fiber optic interfaces
- Layer-2 port loopback detection for preventing customer loops on Ethernet access ports
- Redundant and hot-swappable power supplies, transceiver modules offering uninterruptable service
- Dual-image and dual-configuration file storage provide backup

Advanced security

Access control

- AOS Access Guardian framework for comprehensive user-policy-based network access control (NAC)
- Auto-sensing IEEE 802.1X multi-client, multi-VLAN MAC-based authentication for non-802.1X hosts
- Web-based authentication (Captive Portal): A customizable web portal residing on the switch that can be used for authenticating supplicants as well as non-supplicants
- Group mobility rules and "guest" VLAN support
- Host Integrity check (HIC) agent on each switch makes it an HIC enforcer and facilitates endpoint device control for company policy compliance. Support for quarantine and remediation as required.
- Support for dynamic change of authentication (CoA) and enforcing traffic remediation or restriction for non-compliant devices
- User network profile (UNP): Simplify NAC management and control by dynamically providing predefined policy configuration to authenticated clients (VLAN, ACL, BW, HIC)
- SSH for secure CLI session with public key infrastructure (PKI) support
- Centralized Remote Access Dial-In User Service (RADIUS) and LDAP user authentication
- Private VLAN feature for user traffic segregation

Containment, monitoring and quarantine

- DHCP snooping, DHCP IP spoof protection
- Terminal Access Controller Access Control System Plus (TACACS+) client allowing authentication, authorization and accounting with a remote TACACS+ server
- Dynamic ARP protection and ARP poisoning detection

- ACLs filtering out unwanted traffic including DoS attacks; flow-based filtering in hardware (L1 to L4)
- BPDU blocking: Automatically shutting down user ports if an STP BPDU packet is seen to prevent topology loops
- STP Root Guard: Prevents edge devices from becoming Spanning Tree Protocol root nodes

Converged networks

PoE

- PoE models support Alcatel-Lucent IP phones and WLAN access points, as well as any IEEE 802.3af or IEEE 802.3at-compliant end devices
- Configurable per-port PoE priority and max power for power allocation
- Dynamic PoE allocation: Delivering only the power needed by the powered devices (PD) up to the total power budget for most efficient power consumption

QoS

- Priority queues: Eight hardware-based queues per port for flexible QoS management
- Traffic prioritization: Flow-based QoS with internal and external (remarking) prioritization
- Bandwidth management: Flow-based bandwidth management, ingress rate limiting; egress rate shaping per port
- Queue management: Configurable scheduling algorithms, including Strict Priority Queuing (SPQ), Weighted Round Robin (WRR) and Deficit Round Robin (DRR)
- Congestion avoidance: Support for End-to-End Head-Of-Line (E2E-HOL) Blocking Protection
- Auto QoS for switch management traffic as well as traffic from Alcatel-Lucent IP phones
- Three-color marker: Single/Dual Rate policing with commit BW, excess BW and burst size

Layer-2, Layer-3 Routing and Multicast

Layer-2 switching

- Up to 16,000 MACs
- Up to 4000 VLANs
- Up to 2000 ACLs
- Latency: < 4 µs
- Max Frame: 9216 bytes (jumbo)

IPv4 and IPv6

- Static routing for IPv4 and IPv6
- RIP v1 and v2 for IPv4; RIPng for IPv6
- Up to 256 IPv4 and 128 IPv6 static and RIP routes
- Up to 128 IPv4 and 16 IPv6 interfaces
- Up to 1k Arp entries

Multicast

- IGMPv1/v2/v3 snooping for optimized multicast traffic
- Multicast Listener Discovery (MLD) v1/v2 snooping
- Up to 1000 multicast groups per stack
- IP Multicast VLAN (IPMVLAN) for optimized multicast replication at the edge, saving network core resources

Network protocols

- DHCP relay including generic UDP relay
- ARP
- Dynamic Host Configuration Protocol (DHCP) relay
- DHCP relay for forwarding client requests to a DHCP server
- Generic User Datagram Protocol (UDP) relay per VLAN
- DHCP Option 82: Configurable relay agent information

Metro Ethernet access (features available through Metro license upgrade)

- Ethernet services support per IEEE 802.1ad Provider Bridge
  - Transparent LAN Services with Service VLAN (SVLAN) and Customer VLAN (CVLAN) concept
  - Ethernet network-to-network interface (NNI) and user network interface (UNI) services
  - Service Access Point (SAP) profile identification
  - CVLAN to SVLAN translation and mapping
- IEEE 802.1ag Ethernet OAM: Connectivity Fault Management (L2 ping and link trace)
- Ethernet OAM compliant with IEEE 802.3ah
- ITU-T G.8032 Ethernet Ring Protection designed for loop protection and fast convergence times (< 50 ms) in ring topologies
- Private VLAN feature for user traffic segregation
- Service Assurance Agent (SAA) for proactively measuring network health, reliability and performance. Four SAA tests including L2-MAC, IP, ETH-LB and ETH-DMM depending on network requirements
- Customer provider edge (CPE) test head traffic generator and analyzer tool used in the metro Ethernet network to validate customer Service Level Agreements (SLAs)
- IPMVLAN for optimized multicast replication at the edge, saving network core resources
- Layer-2 Multicast VLAN Replication (MVR) that allows users from different multicast VLANs to subscribe to a multicast group from an upstream trunk interface
- Three-color marker: Single/Dual Rate policing with commit BW, excess BW and burst size
- TR-101 PPPoE Intermediate Agent allowing the PPPoE network access method
- MAC-forced forwarding support according to RFC 4562
- Layer-2 Control Protocol (L2CP) for tunneling a customer's L2CP frames through a well-known address, on a given UNI for Ethernet Private Line (EPL) and Ethernet Virtual Private Line (EVPL) services
- Dying Gasp through SNMP and Ethernet OAM delivery
- Metro Ethernet Forum CE 2.0 Certified
- Managed by Alcatel-Lucent 5620 SAM

ANEXO 3

Especificaciones Switch “4ipnet” 8 puertos PoE 2008

PHYSICAL INTERFACES	
100/1000 SFP Ports	• 2
10/100/1000Base-T RJ-45 Ports	• 8
PoE Ports	• 8
802.3af/at Compliant	• Yes
Transmission Media	• 10Base-T Cat-3/4/5 UTP/STP • 100Base-TX Cat-5 UTP/STP • 1000Base-T Cat-5e UTP/STP
Max. Output Power per Port	• 30W
Max. Output Power per System	• 250W

PERFORMANCE	
Standards	• IEEE 802.3 10Base-T • IEEE 802.3u 100Base-TX • IEEE 802.3ab 1000Base-T • IEEE 802.3af/802.3at PoE • IEEE 802.3x Flow Control
Forwarding Rate	• 1,488,000 pps
MAC Address Table Size	• 8K
Packet Buffer	• 128K
Jumbo Frame Support	• 9K
Automatic PoE Detection	

MECHANICAL	
Dimensions (L x W x H)	• 280 mm x 215 mm x 44 mm
Weight	• 2.3 kg
Environmental Conditions	• Operating Temperature: 0°C (32°F) to 40°C (104°F) • Operating Humidity: 5% to 90% non-condensing
LED Indicators	• Power • Ethernet LNK/ACT • PoE
Power	• AC Input: 100 to 240V, 50/60 Hz

ANEXO 4

Especificaciones Switch “4ipnet” 24 puertos PoE 1024

INTERFACES	
10/100/1000Base-T Ethernet RJ-45 Ports with PoE+	• 24
100/1000Base-X SFP Ports	• 2
Auto MDI / MDIX	• Yes
POWER	
Maximum System Power Consumption (without PoE)	• 21.5W
Maximum PoE Power Per Port	• 30W
Total PoE Power Budget	• 500W
Per Port Power Prioritization	• Yes
PERFORMANCE	
Switching Capacity	• 52 Gbps
Throughput	• 38.7 Mpps
SECURITY	
MAC-based Port Security	• Yes
802.1X User Authentication	• Yes
MAC-based User Authentication	• Yes
Browser-based Authentication	• Yes
IP Source Guard	• Yes
DHCP Snooping	• Yes
Access Control List	• Yes
QUALITY OF SERVICE	
Hardware Queues Per Port	• 8
Scheduling Methods	• Strict Priority • Weighted Round Robin • Hybrid
802.1p Class of Service	• Yes
DSCP / IP Precedence Marking	• Yes
Ingress / Egress Rate Limiting	• Yes
MANAGEMENT	
Command Line Interface (CLI)	• Yes
Browser-based GUI	• Yes
Telnet	• Yes
SNMP	• v1, v2c, v3
Remote Monitoring (RMON)	• Groups 1, 2, 3, 9
DHCP	• Client • Relay
Event and Error Logging	• Yes
Configuration Backup	• Yes
Network Time Protocol (NTP)	• Yes
RADIUS Authentication	• Yes
TACACS+ Authentication	• Yes
HTTPS/SSLv2	• Yes
Port Mirroring	• 1:1 or N:1

LAYER 2	
Standards Supported	• IEEE 802.1AB: Link Layer Discovery Protocol • IEEE 802.1D: Spanning Tree Protocol • IEEE 802.3p: CoS Prioritization • IEEE 802.1Q: VLAN Tagging • IEEE 802.1Q-in-Q: VLAN Stacking • IEEE 802.1s: Multiple Spanning Tree Protocol • IEEE 802.1v: VLAN Classification by Protocol and Port • IEEE 802.1w: Rapid Spanning Tree Protocol • IEEE 802.1X: Port Access Control • IEEE 802.3: 10Base-T • IEEE 802.3u: 100Base-T • IEEE 802.3ab: 1000Base-T • IEEE 802.3z: 1000Base-X • IEEE 802.3af: PoE • IEEE 802.3at: PoE+ • IEEE 802.3ad: Link Aggregation Control Protocol • IEEE 802.3x: Flow Control
Jumbo Frames	• 9K
MAC Address Table Size	• 8K
Packet Buffer	• 4MB
Number of VLANs	• 4K
Port-based VLAN	• Yes
MAC-based VLAN	• Yes
Voice VLAN	• Yes
Private VLAN (PVLAN)	• Yes
Multicast VLAN Registration (MVR)	• Yes
Storm Control	• Yes
IGMP	• v1, v2, v3
IGMP Snooping	• Yes
802.3ad LACP	• Link Aggregation Groups: 13 • Maximum Ports Per Group: 16
MECHANICAL	
Dimensions (L x W x H)	• 440 mm x 330 mm x 45 mm
Weight	• 4.7 kg (10.4 lbs)
Environmental Conditions	• Operating Temperature: 0°C (32°F) to 40°C (104°F) • Operating Humidity: 5% to 90% non-condensing
Certifications	• CE • FCC Class A

ANEXO 5

Controlador inalámbrico "4ipnet" WHG325

SPECIFICATIONS

SYSTEM CAPACITY*1	
Managed APs	• Up to 80
Local Accounts	• Up to 10,000
On-Demand Accounts	• Up to 10,000
Managed Switches	• 10
HARDWARE SPECIFICATIONS	
Form Factor	• 19" (1U) Rack Mount (Mounting bracket included)
Dimensions (W x D x H)	• 43.0 cm x 28.0 cm x 4.4 cm
Weight	• 5.99 kg (13.20 lbs)
Power	• Input: 100-240 VAC, 50/60 Hz (Power cord included)
Interfaces	• WAN: 2 x 10/100/1000Base-T Ethernet, Auto-MDIX, RJ-45 • LAN: 2 x 10/100/1000Base-T Ethernet, Auto-MDIX, RJ-45 • Console: 1 x DB9 (DB9 to RS-232 console cable adapter included) • USB: 2 x USB 3.0
LED Indicators	• Power • Status
Buttons	• Reset
LCD Display	• Yes
Environmental Conditions	• Operating Temperature: 0°C (32°F) to 50°C (122°F) • Operating Humidity: 5% to 95% non-condensing

*1: Capacity limits may vary depending on configuration parameters

ANEXO 6

Access Point “4ipnet” EAP767

PHYSICAL	
Power	• DC Input: 12V / 2.5A (Power adapter optional) • PoE: 802.3at compliant (PoE injector optional)
Dimensions	• 18.0 cm (L) x 18.0 cm (W) x 4.4 cm (H)
Weight	• 0.61 kg (1.35 lbs)
Interfaces	• Uplink: 1 x 10/100/1000Base-T Ethernet, Auto MDIX, RJ-45 with 802.3at PoE
LED Indicator	• Uplink
Environmental Conditions	• Operating Temperature: -10°C (14°F) to 40°C (104°F) • Operating Humidity: 10% to 90% non-condensing • UL94-5VB Rating
Power Consumption	• 17W max.
Antenna	• Type: 6 x Built-in PIFA (3 x 2.4 GHz, 3 x 5 GHz) • Gain: 3 dBi (2.4 GHz), 5 dBi (5 GHz)
Mounting	• Wall mount (Mounting panel included) • Ceiling mount (Ceiling mount kit included)

WI-FI	
Standards	• 802.11 a/b/g/n/ac • Concurrent dual-band 2.4 & 5 GHz
Supported Data Rates	• 802.11b: 1, 2, 5.5, 11 Mbps • 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps • 802.11n: 6.5 – 216.7 Mbps (20 MHz) • 802.11n: 13.5 – 450 Mbps (40 MHz) • 802.11ac: 6.5 – 260.1 Mbps (20 MHz) • 802.11ac: 13.5 – 600 Mbps (40 MHz) • 802.11ac: 29.3 – 1300 Mbps (80 MHz)
Radio Chains	• 3 x 3
Spatial Streams	• 3
Output Power	• 2.4 GHz: Up to 25 dBm*1 • 5 GHz: Up to 25 dBm*1
Channelization	• 20 MHz • 40 MHz • 80 MHz
Frequency Band	• 2.412 – 2.472 GHz • 5.180 – 5.825 GHz
Operating Channels	• 2.4 GHz: 1 – 11 (US), 1 – 13 (Europe), 1 – 13 (Japan) • 5 GHz*2: 36 – 165 (US), 36 – 140 (Europe), 36 – 140 (Japan)
ESSIDs	• Up to 16 per radio (32 total)
Certifications	• FCC (United States), CE (Europe), NCC (Taiwan)

PERFORMANCE	
Physical Data Rate	• Up to 450 Mbps (2.4 GHz) • Up to 1.3 Gbps (5 GHz)
Concurrent Users	• Up to 384 (256 on 2.4 GHz, 128 on 5 GHz)

QUALITY OF SERVICE

Wireless QoS (802.11e/WMM)
DSCP (802.1p)
Airtime Fairness
Band Steering
Multicast to Unicast Conversion
Optimal Client Filtering

MANAGEMENT

Deployment	• Standalone • Tunneled management by 4ipnet WHG Controller • IPv4 & IPv6 compatible
Configuration	• Web User Interface (HTTP/HTTPS) • SNMP v1, v2c, v3

SECURITY

Wireless Security	• WEP • WPA/WPA2 Mixed • WPA2-Personal • WPA2-Enterprise (802.1X) • TKIP and AES Encryption
VLAN Tagging (802.1Q)	
Station Isolation	
DHCP Snooping	
Layer-2 Firewall	

MOBILITY/ROAMING

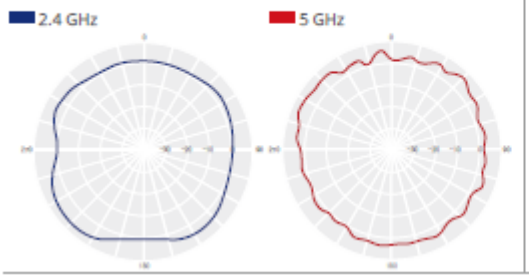
802.1X Preauthentication
Layer 2/Layer 3 Fast Roaming

RECEIVE SENSITIVITY

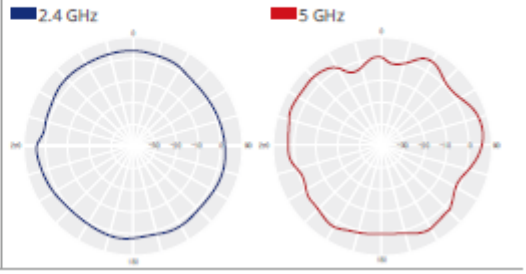
Operating Mode	Data Rate	Receive Sensitivity (dBm)
802.11b	1 Mbps	-93
	11 Mbps	-85
802.11a	6 Mbps	-89
	54 Mbps	-73
802.11g	6 Mbps	-89
	54 Mbps	-73
802.11n (HT20)	MCS0	-88
	MCS7	-68
	MCS8	-88
	MCS15	-68
802.11n (HT40)	MCS0	-85
	MCS7	-67
	MCS8	-85
	MCS15	-67
802.11ac (VHT20)	MCS0	-89
	MCS8	-65
802.11ac (VHT40)	MCS0	-86
	MCS9	-60
802.11ac (VHT80)	MCS0	-84
	MCS9	-57

SIGNAL COVERAGE PATTERN

H-plane (Horizontal)



E-plane (Vertical)



ANEXO 7

Access Point “4ipnet” 727

PHYSICAL	
Power	• DC Input: 12V / 1A (Power adapter optional) • PoE: 802.3af compliant (PoE injector optional)
Dimensions	• 16.0 cm (L) x 16.0 cm (W) x 2.8 cm (H)
Weight	• 0.275 kg (0.6 lbs)
Interfaces	• Uplink: 1 x 10/100/1000Base-T Ethernet, Auto MDIX, RJ-45 with 802.3af PoE
LED Indicator	• Power/Status
Buttons	• Reset / Restart
Environmental Conditions	• Operating Temperature: 0°C (32°F) to 40°C (104°F) • Operating Humidity: 10% to 90% non-condensing
Power Consumption	• 14.4W max.
Antenna	• Type: 4 x Built-in PIFA (2 x 2.4 GHz, 2 x 5 GHz) • Gain: 3 dBi (2.4 GHz), 5 dBi (5 GHz)
Mounting	• Wall/Ceiling mount (Mounting kit included)

WI-FI	
Standards	• 802.11 a/b/g/n/ac • Concurrent dual-band 2.4 & 5 GHz
Supported Data Rates	• 802.11b: 1, 2, 5.5, 11 Mbps • 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps • 802.11n: 6.5 – 144 Mbps (20 MHz) • 802.11n: 13.5 – 300 Mbps (40 MHz) • 802.11ac: 6.5 – 173.4 Mbps (20 MHz) • 802.11ac: 13.5 – 400 Mbps (40 MHz) • 802.11ac: 29.3 – 866.6 Mbps (80 MHz)
Radio Chains	• 2 x 2
Spatial Streams	• 2
Output Power	• 2.4 GHz: Up to 27 dBm*1 • 5 GHz: Up to 26 dBm*1
Channelization	• 20 MHz • 40 MHz • 80 MHz
Frequency Band	• 2.412 – 2.472 GHz • 5.180 – 5.825 GHz
Operating Channels	• 2.4 GHz: 1 – 11 (US), 1 – 13 (Europe), 1 – 13 (Japan) • 5 GHz*2: 36 – 165 (US), 36 – 140 (Europe), 36 – 140 (Japan)
ESSIDs	• Up to 16 per radio (32 total)
Certifications	• FCC (United States), CE (Europe)

PERFORMANCE	
Physical Data Rate	• Up to 300 Mbps (2.4 GHz) • Up to 867 Mbps (5 GHz)
Concurrent Users	• Up to 384 (256 on 2.4 GHz, 128 on 5 GHz)

QUALITY OF SERVICE

Wireless QoS (802.11e/WMM)
DSCP (802.1p)
Airtime Fairness
Band Steering
Multicast to Unicast Conversion
Optimal Client Filtering

MANAGEMENT

Deployment	• Standalone • Tunneled management by 4ipnet WHG Controller • IPv4 & IPv6 compatible
Configuration	• Web User Interface (HTTP/HTTPS) • SNMP v1, v2c, v3

SECURITY

Wireless Security	• WEP • WPA/WPA2 Mixed • WPA2-Personal • WPA2-Enterprise (802.1X) • TKIP and AES Encryption
VLAN Tagging (802.1Q)	
Station Isolation	
DHCP Snooping	
Layer-2 Firewall	

MOBILITY/ROAMING

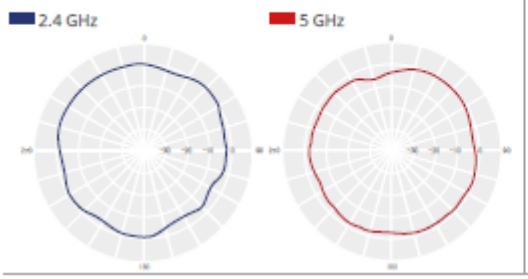
802.1X Preauthentication
Layer 2/Layer 3 Fast Roaming

RECEIVE SENSITIVITY

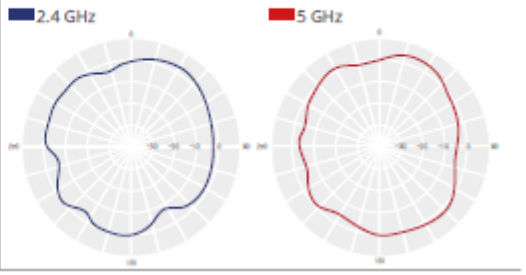
Operating Mode	Data Rate	Receive Sensitivity (dBm)
802.11b	1 Mbps	-98
	11 Mbps	-90
802.11a	6 Mbps	-93
	54 Mbps	-76
802.11g	6 Mbps	-90
	54 Mbps	-76
802.11n (HT20)	MCS0	-90
	MCS7	-72
	MCS8	-90
	MCS15	-72
802.11n (HT40)	MCS0	-87
	MCS7	-70
	MCS8	-87
	MCS15	-70
802.11ac (VHT20)	MCS0	-93
	MCS8	-69
802.11ac (VHT40)	MCS0	-90
	MCS9	-64
802.11ac (VHT80)	MCS0	-87
	MCS9	-61

SIGNAL COVERAGE PATTERN

H-plane (Horizontal)



E-plane (Vertical)



ANEXO 8

Ticketera “4ipnet” WTG2

SDS200W WIRELESS SMART DEVICE SERVER		
	Power	• Input: 100-240 VAC, 50/60 Hz (Power cord included) • DC Output: 5V / 1.5A
	Dimensions	• 16.5 cm (L) x 8.2 cm (W) x 2.5 cm (H)
	Weight	• 0.4 kg (0.83 lbs)
	Interfaces	• Uplink: 1 x 10/100Base-T Ethernet, Auto MDIX, RJ-45 • Serial: 1 x RS-232 DB9M
	Buttons	• TAS, Reset
	Antenna	• Type: 1 x External 2.4 GHz omnidirectional (included) • Gain: 3 dBi (2.4 GHz)
	Standard	• 802.11b/g/n • Single-band 2.4 GHz
	Configuration	• Administer the system from any standard web browser
PRT200 POS PRINTER*1		
	Power	• Input: 24 VDC / 2.5A (Power cord included)
	Dimensions	• 17.6 cm (L) x 14.6 cm (W) x 12.4 cm (H)
	Weight	• 1.22 kg (2.69 lbs)
	Interfaces	• Serial: 1 x RS-232
	Print Method	• Thermal line printing
	Print Speed	• 250 mm/sec
	Print Life	• 100 km
	Print Resolution	• 576 dots/line or 512 dots/line
	Effective Print Width	• 72mm
	Paper Width	• 79.5 ± 0.5mm
	Character	• ASCII: 12 x 24 dots • Graphic font: 24 x 24 dots
	Operating Temperature	• 0°C (32°F) to 45°C (113°F)
	Storage Temperature	• -10°C (14°F) to 60°C (140°F)
	Certifications	• FCC (United States), CE (Europe), RoHS

ANEXO 9

Listado de Aps configurados en el controlador inalámbrico WHG325

AP Name	Client	IP Address	Service Zone / VLAN ID / SSID	Status	MAC Address	Channel
AP_P1_SOR	2	192.168.23.10	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:45:3D	11 / 64
AP_P1_SOCC	3	192.168.23.11	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:43:3F	11 / 36
AP_P2_SOR	1	192.168.23.12	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:45:43	11 / 48
AP_P2_SOCC	2	192.168.23.13	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:43:48	11 / 157
AP_P2_NOR	6	192.168.23.14	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:43:36	8 / 108
AP_P2_NOCC	7	192.168.23.15	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:43:96	3 / 36
AP_P3_SOR	0	192.168.23.16	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:45:40	11 / 52
AP_P3_SOCC	3	192.168.23.17	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:45:28	1 / 52

☐	AP_P4_SOR	4	192.168.23.20	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:45:4F	1 / 52
☐	AP_P4_SOCC	0	192.168.23.21	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:43:B1	11 / 52
☐	AP_P4_NOR	1	192.168.23.22	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:43:BD	8 / 108
☐	AP_P4_NOCC	4	192.168.23.23	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:43:B4	3 / 100
☐	AP_PB_SOR	12	192.168.23.24	RF Card A SZ3Staff / 33 / Staff SZ2Invitados / 32 / FreeWIFI HF SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia SZ3Staff / 33 / EventosHF RF Card B SZ3Staff / 33 / Staff SZ2Invitados / 32 / FreeWIFI HF SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia SZ3Staff / 33 / EventosHF	Online (Enabled)	00:1F:D4:04:6D:F7	1 / 36
☐	AP_PB_NOCC	7	192.168.23.25	RF Card A SZ3Staff / 33 / Staff SZ2Invitados / 32 / FreeWIFI HF SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia SZ3Staff / 33 / EventosHF RF Card B SZ3Staff / 33 / Staff SZ2Invitados / 32 / FreeWIFI HF SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia SZ3Staff / 33 / EventosHF	Online (Enabled)	00:1F:D4:04:6D:F4	6 / 56
☐	AP_P5_SOR	4	192.168.23.26	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:42:D3	6 / 108
☐	AP_P5_SOCC	0	192.168.23.27	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:43:FC	6 / 40

☐	AP_P5_NOR	4	192.168.23.28	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:43:E1	6 / 100
☐	AP_P5_NOCC	4	192.168.23.29	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:43:FF	1 / 108
☐	AP_P6_SOR	0	192.168.23.30	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:42:E8	1 / 104
☐	AP_P6_SOCC	0	192.168.23.31	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:43:9C	11 / 153
☐	AP_P6_NOR	8	192.168.23.32	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:42:BB	8 / 161
☐	AP_P6_NOCC	2	192.168.23.33	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:44:F5	3 / 52
☐	AP_P7_SOR	4	192.168.23.34	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:44:74	6 / 56
☐	AP_P7_SOCC	0	192.168.23.35	RF Card A SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia RF Card B SZ3Staff / 33 / Staff SZ1Huespedes / 10 / Finlandia Huespedes/Guests	Online (Enabled)	00:1F:D4:04:43:F3	1 / 149

☐	AP_P1_NOR	6	192.168.23.46	RF Card A SZ3Staff / 33 / Staff SZ2Invitados / 32 / FreeWIFI HF SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia SZ3Staff / 33 / EventosHF RF Card B SZ3Staff / 33 / Staff SZ2Invitados / 32 / FreeWIFI HF SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia SZ3Staff / 33 / EventosHF	Online (Enabled)	00:1F:D4:04:6D:E8	3 / 100
☐	AP_P1_NOCC	2	192.168.23.47	RF Card A SZ3Staff / 33 / Staff SZ2Invitados / 32 / FreeWIFI HF SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia SZ3Staff / 33 / EventosHF RF Card B SZ3Staff / 33 / Staff SZ2Invitados / 32 / FreeWIFI HF SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia SZ3Staff / 33 / EventosHF	Offline	00:1F:D4:04:6D:C7	6 / 161
☐	AP_S1_SOCC	0	192.168.23.48	RF Card A SZ3Staff / 33 / Staff SZ2Invitados / 32 / FreeWIFI HF SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia SZ3Staff / 33 / EventosHF RF Card B SZ3Staff / 33 / Staff SZ2Invitados / 32 / FreeWIFI HF SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia SZ3Staff / 33 / EventosHF	Online (Enabled)	00:1F:D4:04:6D:D9	3 / 108
☐	AP_S1_SOR	0	192.168.23.49	RF Card A SZ3Staff / 33 / Staff SZ2Invitados / 32 / FreeWIFI HF SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia SZ3Staff / 33 / EventosHF RF Card B SZ3Staff / 33 / Staff SZ2Invitados / 32 / FreeWIFI HF SZ1Huespedes / 10 / Finlandia Huespedes/Guests Default / 0 / Gerencia	Online (Enabled)	00:1F:D4:04:6D:E8	6 / 161

ANEXO 10

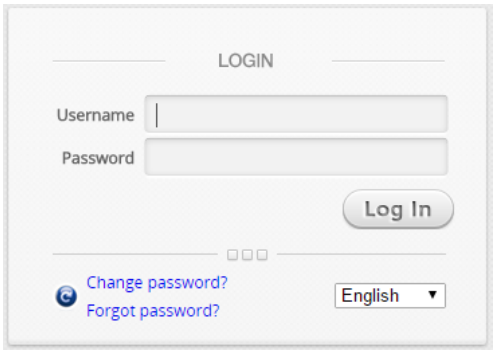
Configuración de políticas y perfiles de usuario en controlador inalámbrico WHG325

Configuración Inicial

Interfaz de Administración Web

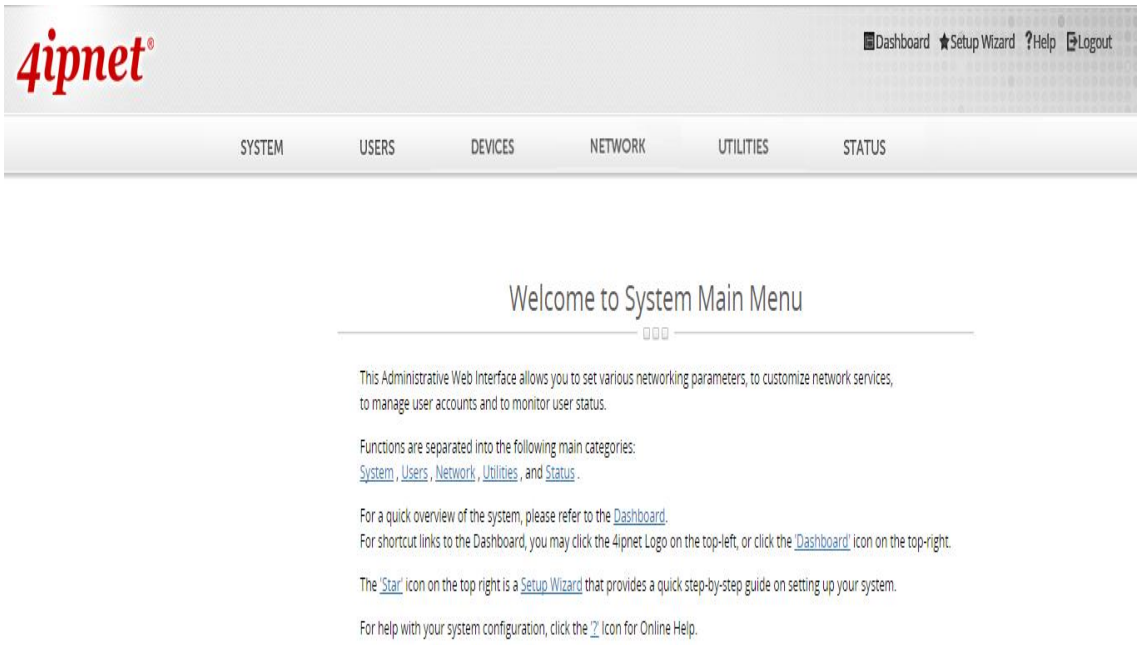
Se puede acceder a la interfaz de administración web del controlador WHG201 a través del browser desde cualquier PC conectado a la interfaz LAN con la dirección IP por defecto 192.168.1.254.
Las credenciales por defecto son:

Username: admin
Password: admin



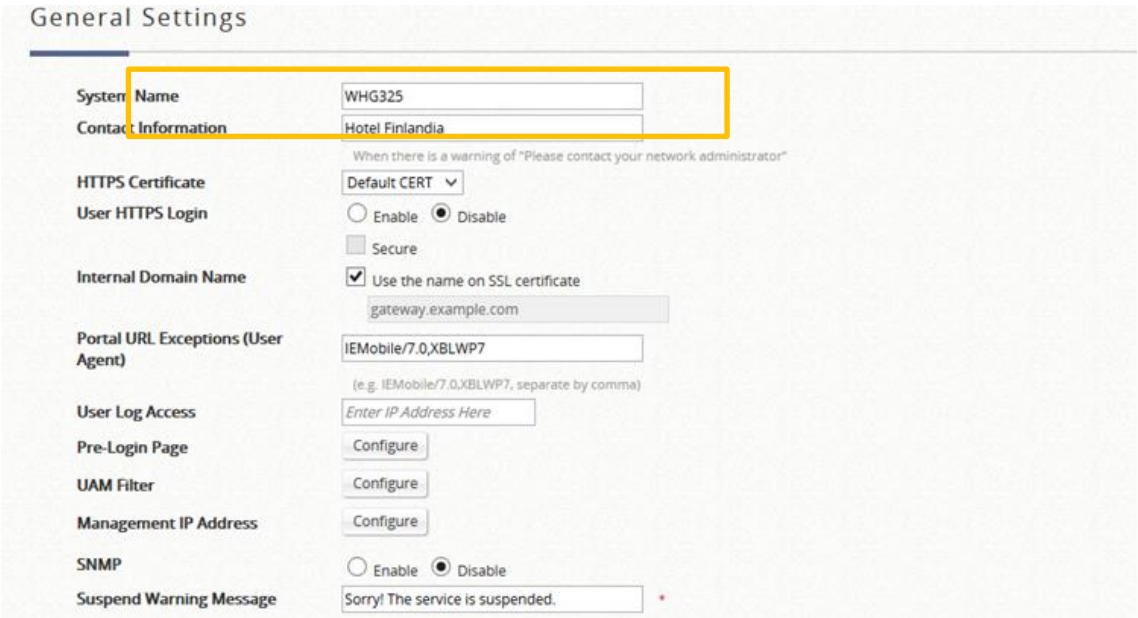
Al momento inicializar la sesión, el sistema solicita cambiar la contraseña por seguridad.

En la siguiente figura se ilustra la página de bienvenida de interfaz de administración web.



Configuración del sistema

Se selecciona System >> General y se edita el nombre y contacto.

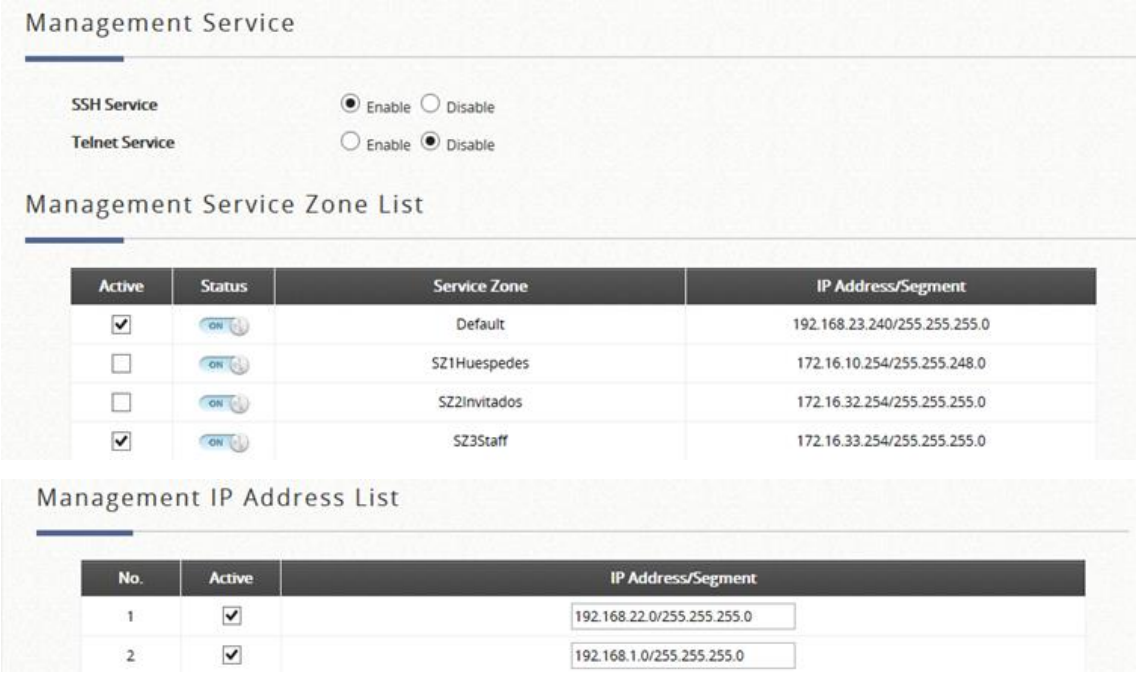


Configuración del servicio de administración

Se selecciona >> System >> Management IP Address List.

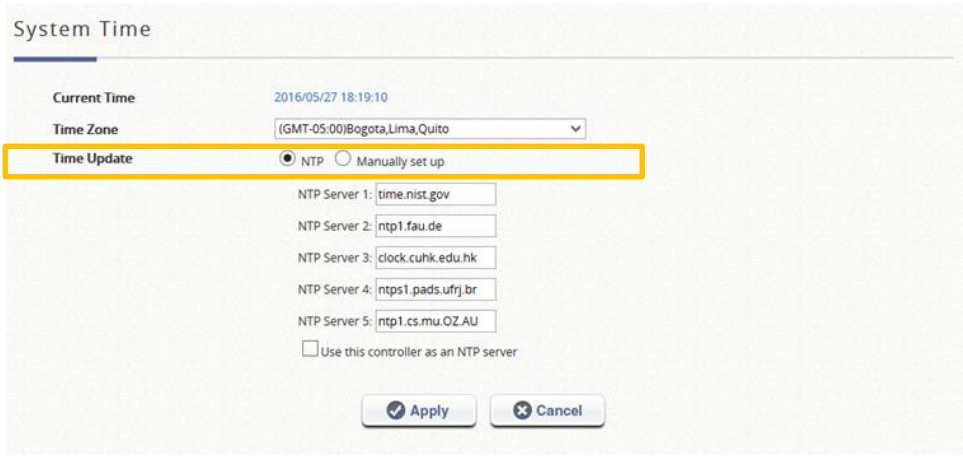
La interfaz de consola remota está deshabilitada de forma predeterminada podemos habilitar el acceso remoto desde esta sección. (SSH, Telnet). Se

edita la lista de zonas de servicio y las direcciones IP reservadas/rango que tendrán total acceso y autorización de ingreso a la interfaz de administración Web.



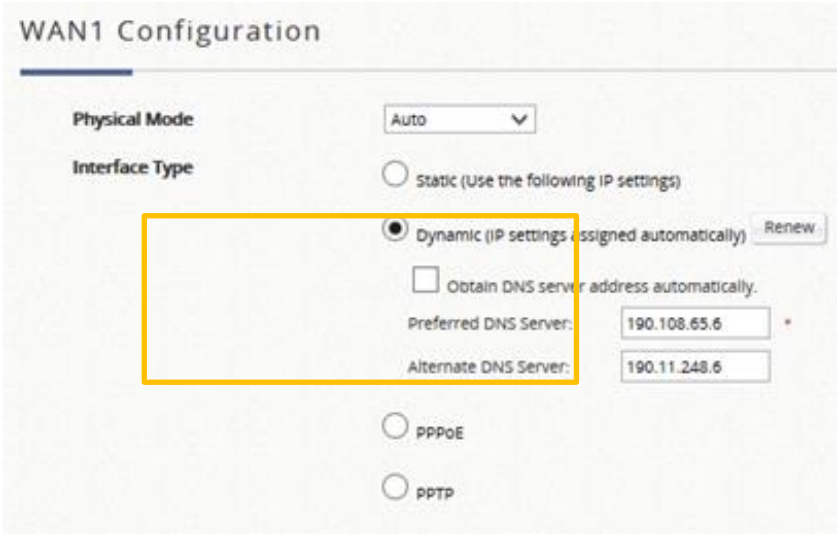
Configuración de la fecha/hora del sistema

Se elige la zona horaria de la lista desplegable >> System >> General >> System Time y click en aplicar para guardar los cambios.



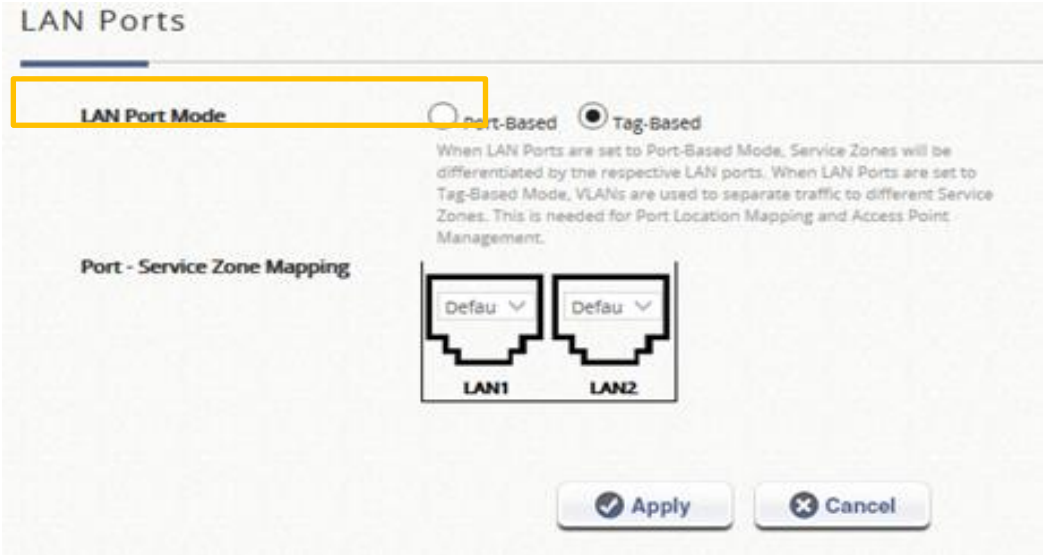
Configuración Puerto WAN1

Se selecciona >> System >> WAN. Se elige el tipo de conexión para el puerto WAN1 y editamos el servidor DNS principal. Existen 4 tipos de conexiones WAN: estática, dinámica, PPPoE y PPTP.



Configuración Puertos LAN

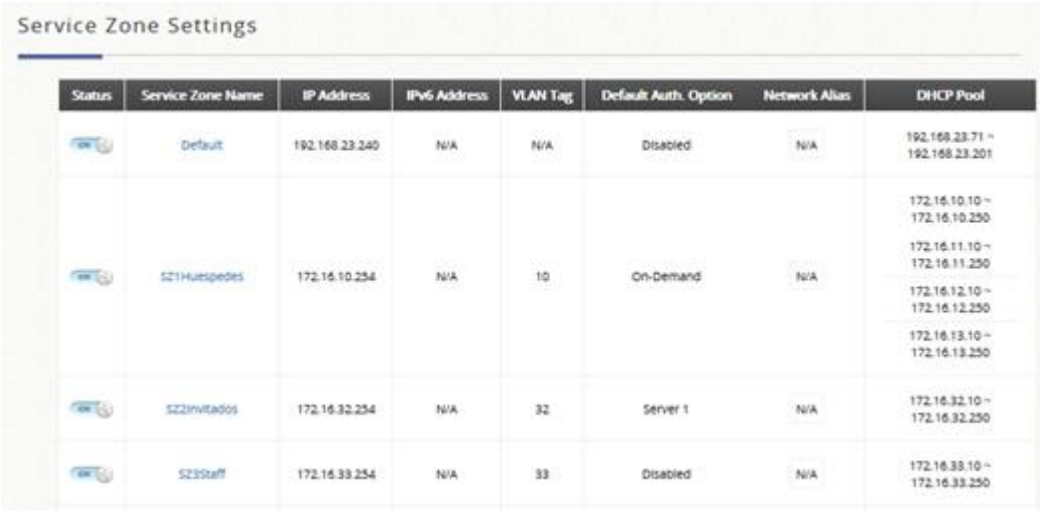
Se selecciona >> System >> LAN Ports. Se elige el tipo de puerto y el modo de funcionamiento. Tag-Based permite el paso de todas las zonas de servicios creadas a través de la VLAN ID. Port-Based se establece una zona de servicio predeterminada para cada puerto.



Configuración de las Zonas de Servicio

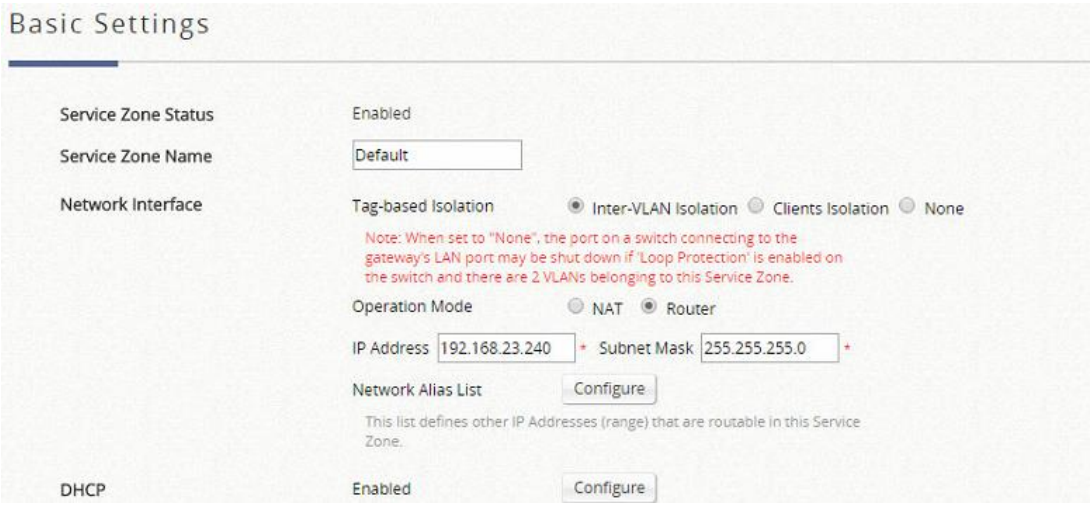
Las zonas de servicio emula la configuración de interfaces en un router, de tal modo que podemos realizar los ajustes acorde a los requerimientos de nuestra red.

Se selecciona >> System >> Services Zones. Se pueden habilitar hasta 8 zonas de servicio. Las zonas de servicio habilitadas son: default, SZ1, SZ2 y SZ3.



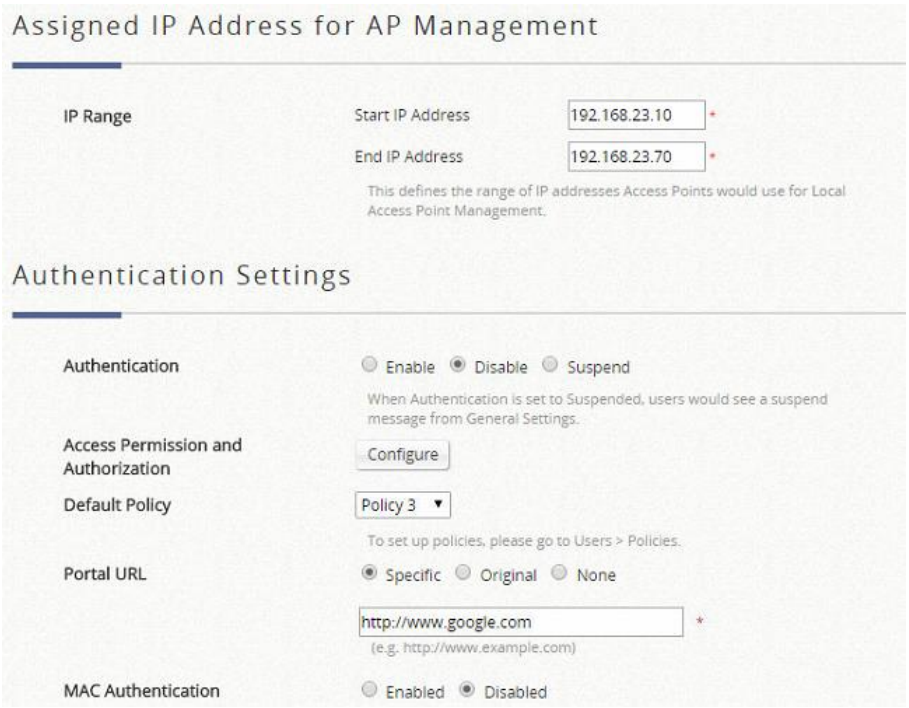
Zona Default

En esta zona se configura el direccionamiento IP de la red inalámbrica y se ingresa el controlador inalámbrico en este mismo segmento de red. El servicio de la zona default viene habilitado y se lo asigna a la configuración de los APs. Los parámetros a configurar son: nombre, modo de operación, dirección IP y la máscara.



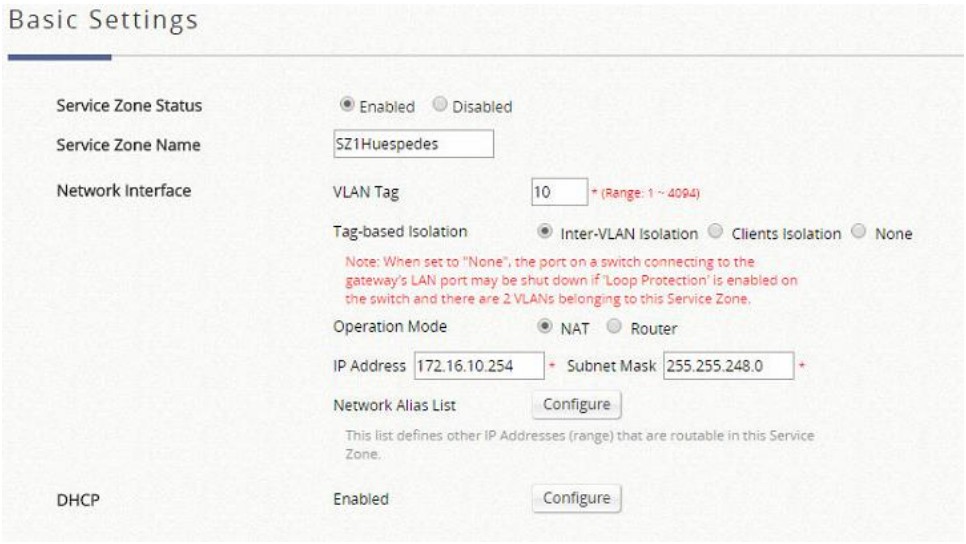
Se elige el rango de IP que serán asignados a los APs, y se deshabilita la autenticación de la zona ya que no se necesitará del Hot-spot en dicha interfaz.

El Portal URL define el destino de enlace al cual el navegador web del usuario redireccionará al momento de realizar un login satisfactorio y en este caso se configura que sea http://www.google.com.

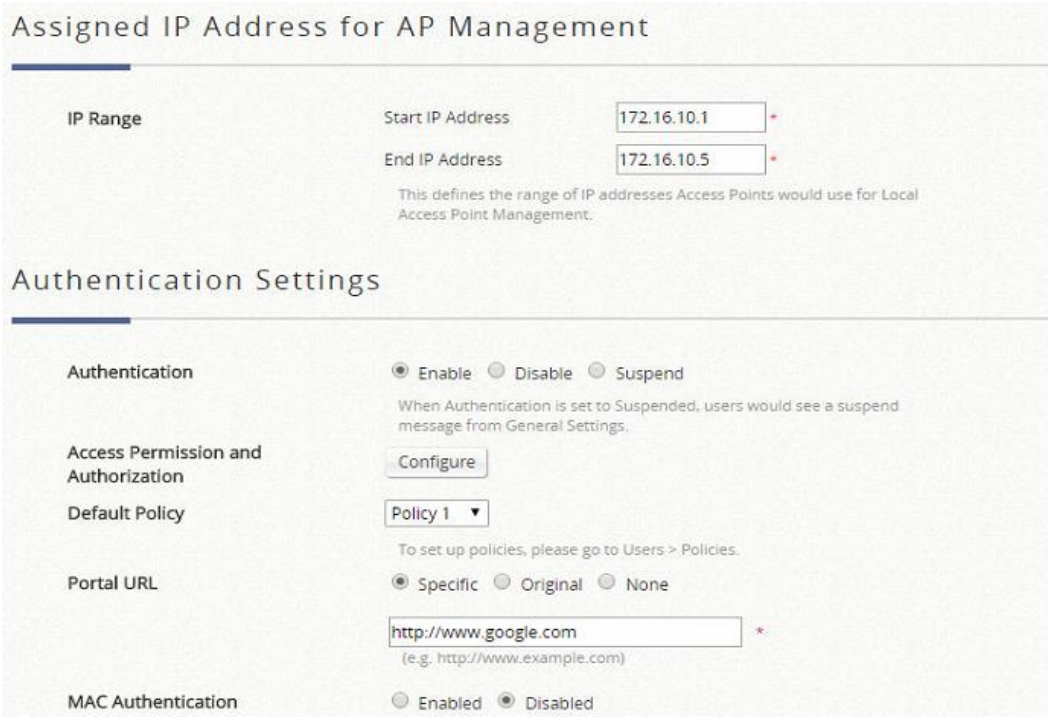


Zona SZ1Huespedes

A esta zona se le asignará el SSID “Finlandia Huespedes/Guests”, se configura la interfaz en modo de operación “router” para tener acceso a la red. Los parámetros configurados son: estado, nombre, vlan, asignamos una dirección IP y la máscara.



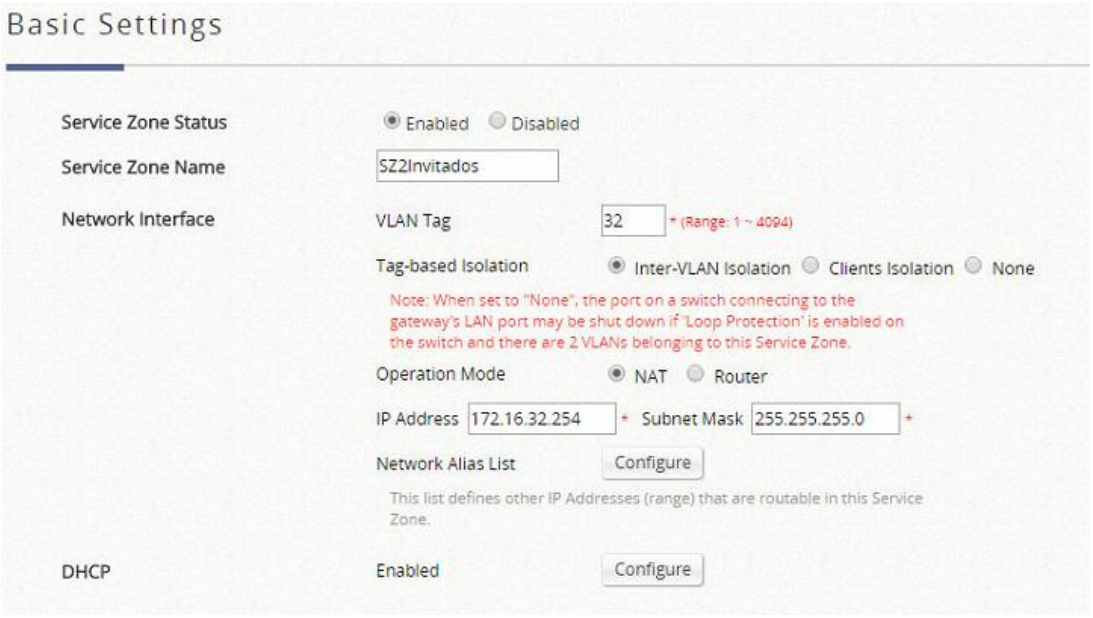
Se habilita la autenticación de esta zona para que aparezca al portal de acceso en dicha interfaz.



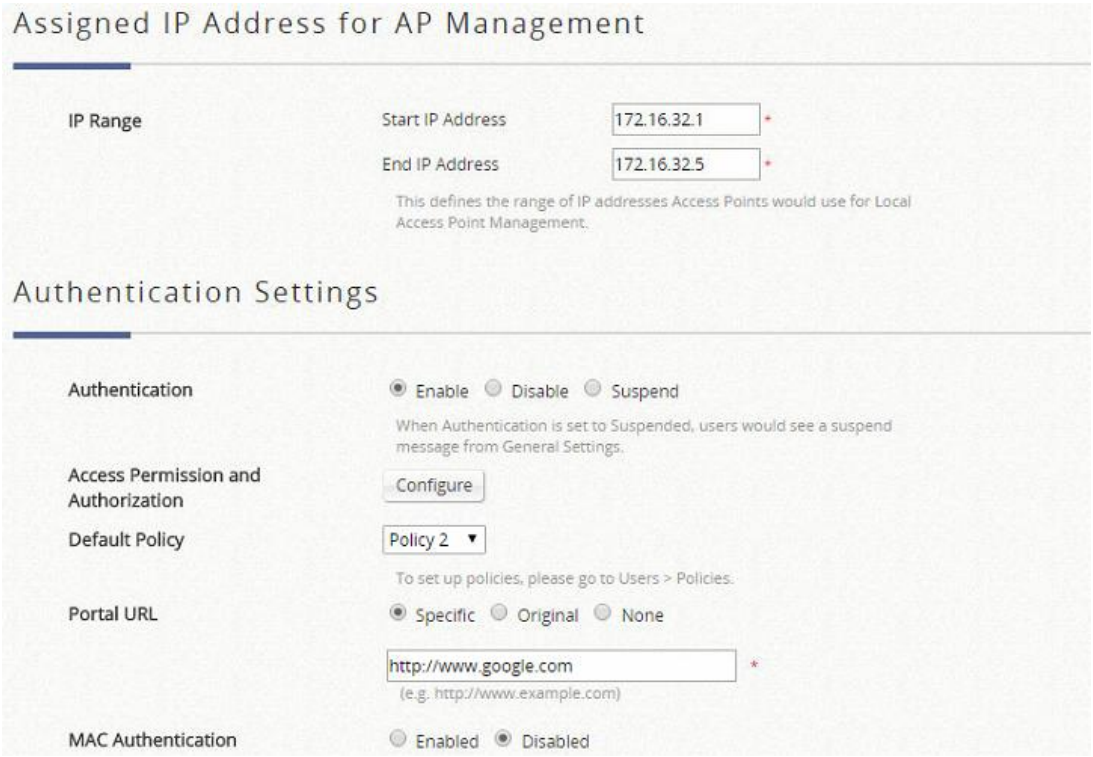
Se habilita la configuración DHCP, el rango de direcciónes IP del DHCP y el servidor DNS.

Zona SZ2Invitados

A esta zona se le asigna el SSID “Invitados”, se configura la interfaz en modo “nat”, para que el controlador inalámbrico se encargue de administrar dichas interfaces y la conexión hacia redes externas lo realice a través de la WAN. Se configura los parámetros: estado, nombre, vlan, la dirección IP y la máscara.



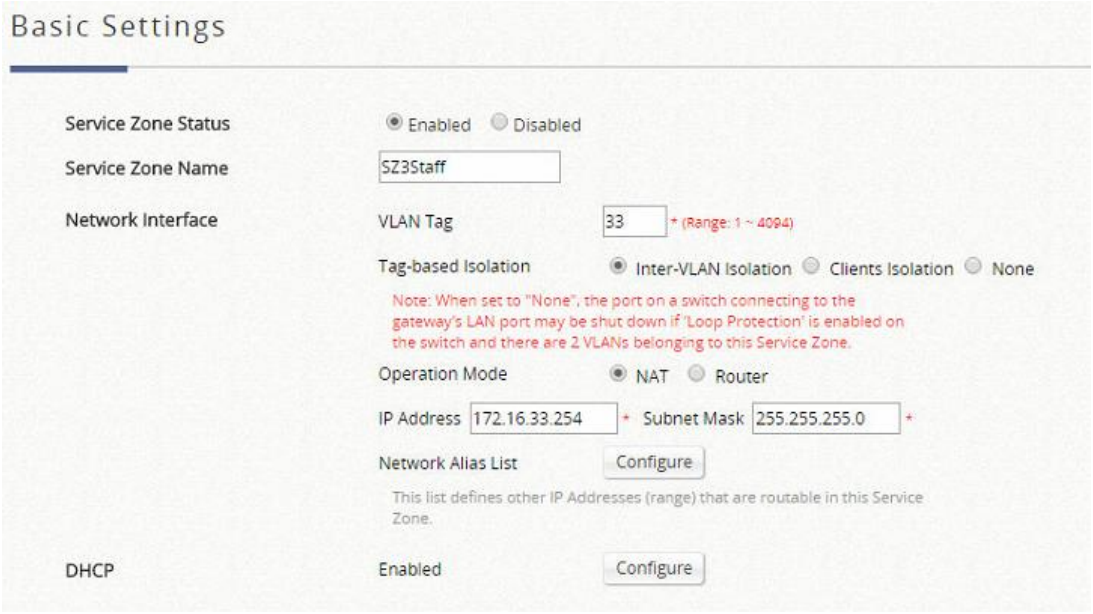
Se habilita la autenticación de esta zona para que aparezca al portal de acceso en dicha interfaz.



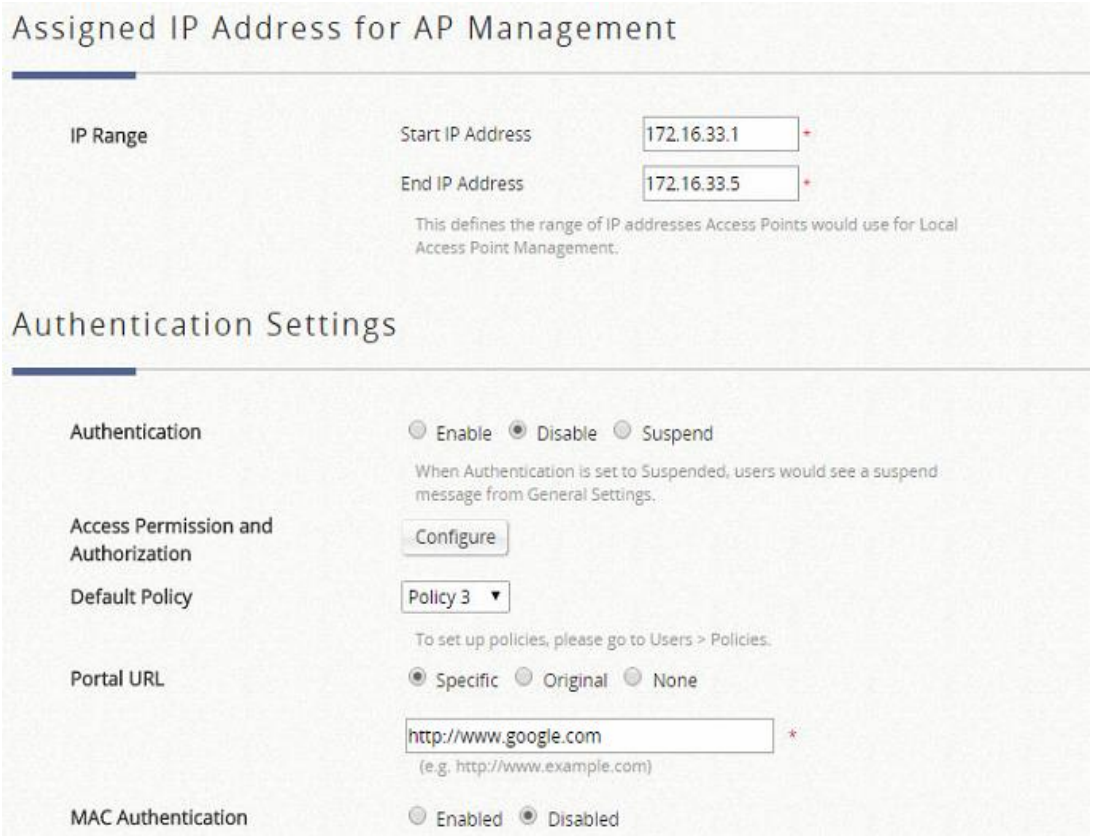
Se habilita la configuración DHCP, el rango de direcciónes IP del DHCP y el servidor DNS.

Zona SZ3_Staff

A esta zona se le asignará el SSID “Staff”. Se configura la interfaz en modo “nat”, para que el controlador inalámbrico se encargue de administrar dichas interfaces y la conexión hacia redes externas lo realice a través de la WAN. Se configura los parámetros: estado, nombre, vlan, la dirección IP y la máscara.



Se deshabilita la autenticación de esta zona ya que no se requiere que aparezca al portal de acceso en dicha interfaz.



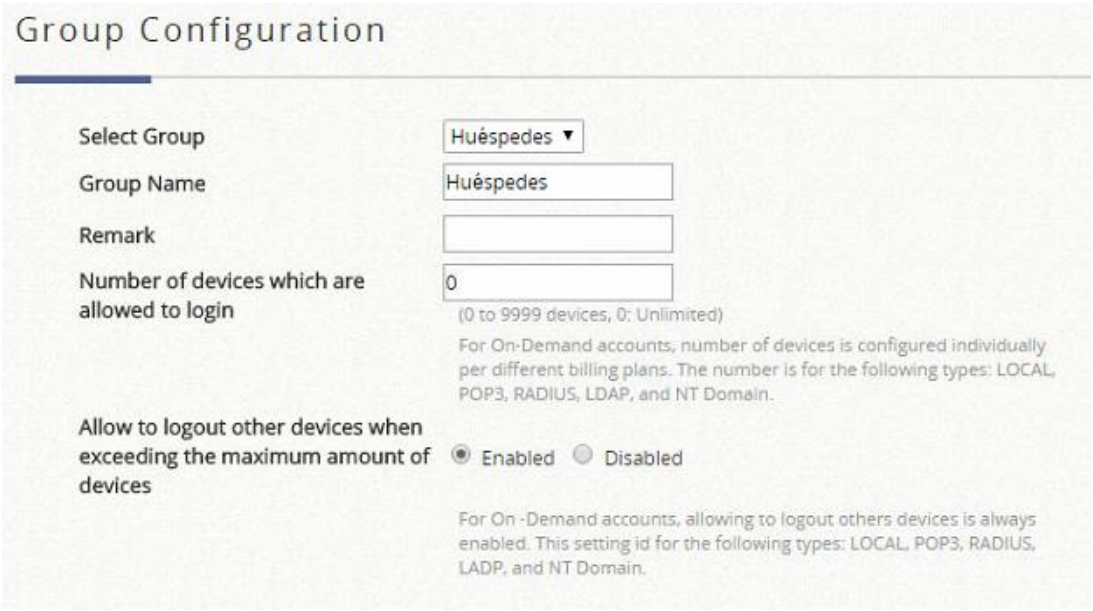
Se habilita la configuración DHCP, el rango de direcciónes IP del servidor DHCP y el servidor DNS.

Configuración de Grupos

Para configurar el grupo se selecciona >> Users >> Groups >> Configuration

Grupo Huéspedes

La variable “0” en el campo de número de dispositivos permitidos, define un número ilimitado de usuarios que pueden inicializar sesión. La zona de configuración de permisos permite determinar el acceso entre el grupo, la política y la zona de servicio.

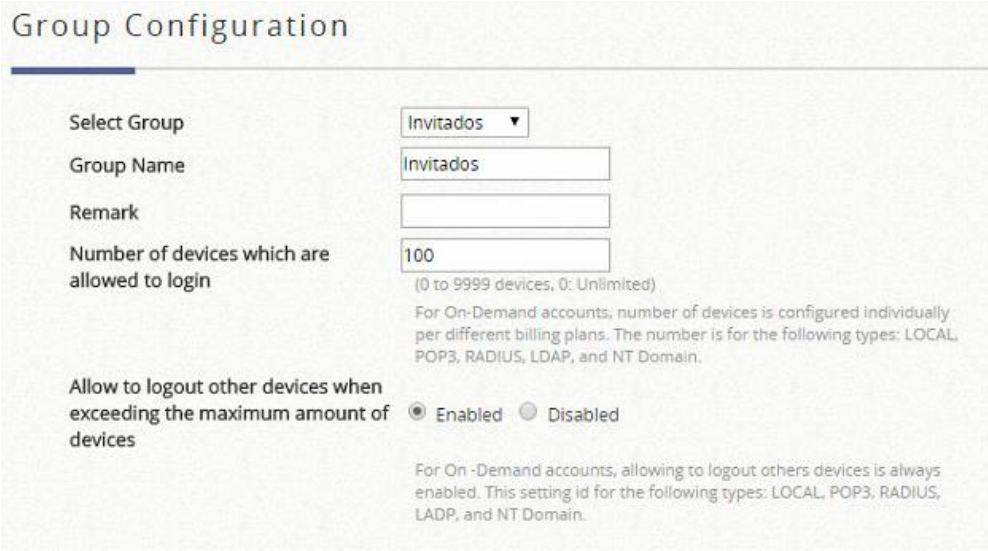


En este caso los usuarios del grupo Huéspedes puedan acceder todas las zonas de servicio ya que se habilita el “check” en las zonas y de esta manera estamos dando la autorización del caso.

Adicional se debe permitir el acceso a los grupos en la zona de servicio SZ1Huespedes. Los grupos autorizados para la zona SZ1Huespedes son Huéspedes y Staff.

Grupo Invitados

El número de dispositivos para este grupo se configura de forma individual por el plan de facturación 2. El número de dispositivos es para la autenticación de tipo local.

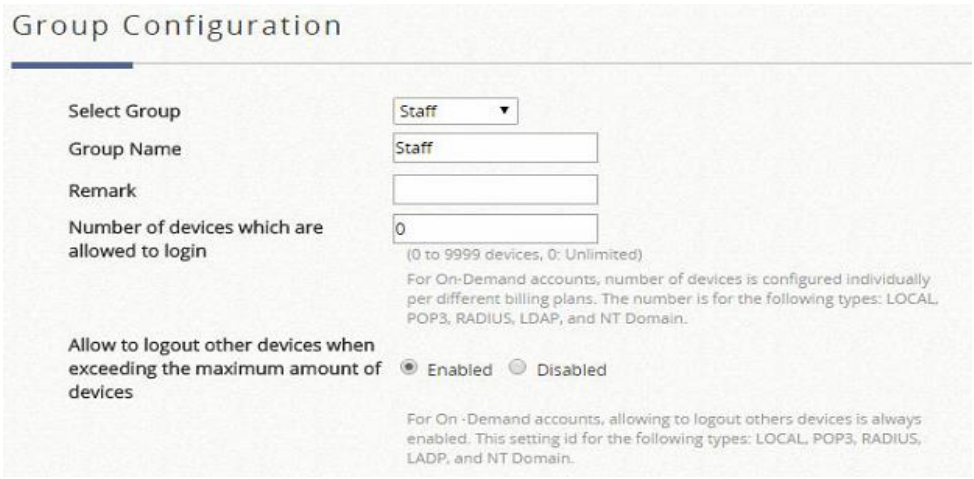


Para permitir que los usuarios del grupo Invitados puedan acceder a las zonas de servicio habilitamos el “check”, de esta manera estamos dando la autorización. En este caso se puede acceder a las zonas:default, SZ2Invitados y SZ3Staff.

Adicional se configura los permisos de acceso a los grupos en la zona de servicio SZ2Invitados, en este caso todos los grupos están autorizados.

Grupo Staff

Como la cuenta Staff es bajo demanda el número de dispositivos está configurado de forma individual por el plan de facturación 3.



En este caso los usuarios del grupo Staff puedan acceder todas las zonas de servicio ya que se habilita el “check” en las zonas y de esta manera se da la autorización del caso.

Adicional para permitir que los usuarios del grupo Staff puedan acceder a las zonas de servicio habilitamos el “check” en la zona SZ3_Staff, de esta manera estamos dando autorización. En este caso todos los grupos tienen autorización.

Configuración de Políticas

Se selecciona una de las políticas en la lista desplegable y empezamos a configurar cada atributo, luego de editar damos click en aplicar para guardar los cambios realizados.

Política 1

Se selecciona >> Users >> Policies >> Policy Configuration.

Política 2

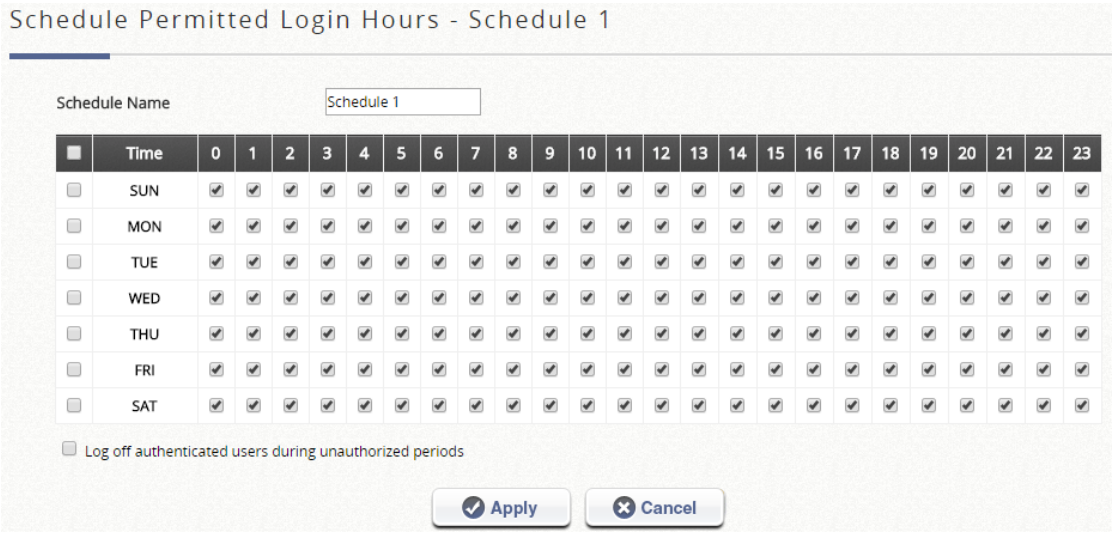
Se selecciona >> Users >> Policies >> Policy Configuration.

Política 3

Se selecciona >> Users >> Policies >> Policy Configuration.

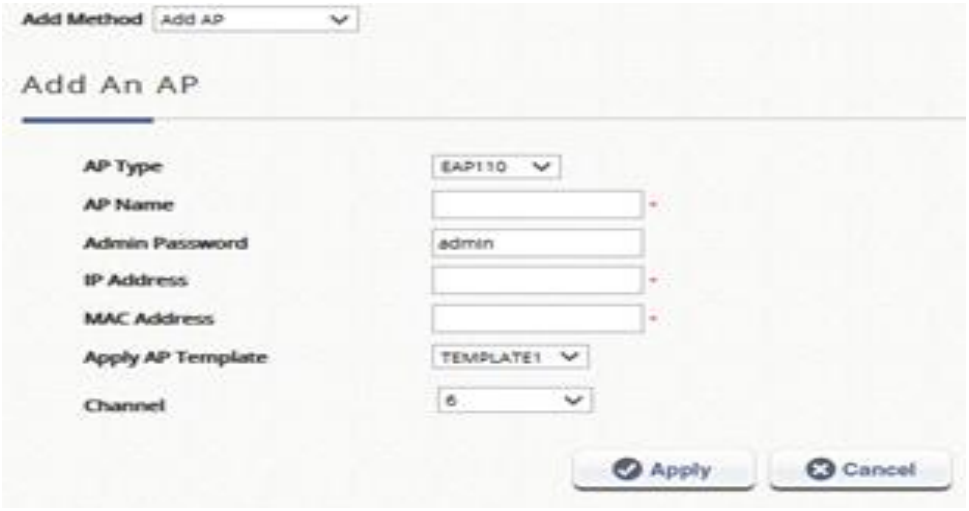
Configuración de Calendario

Esta función nos permite editar el horario permitido para la asignación de inicio de sesión de los usuarios en períodos de tiempo de 1 hora. Por defecto se encuentra seleccionado todo el día; se denota el día en 24h, hora militar.



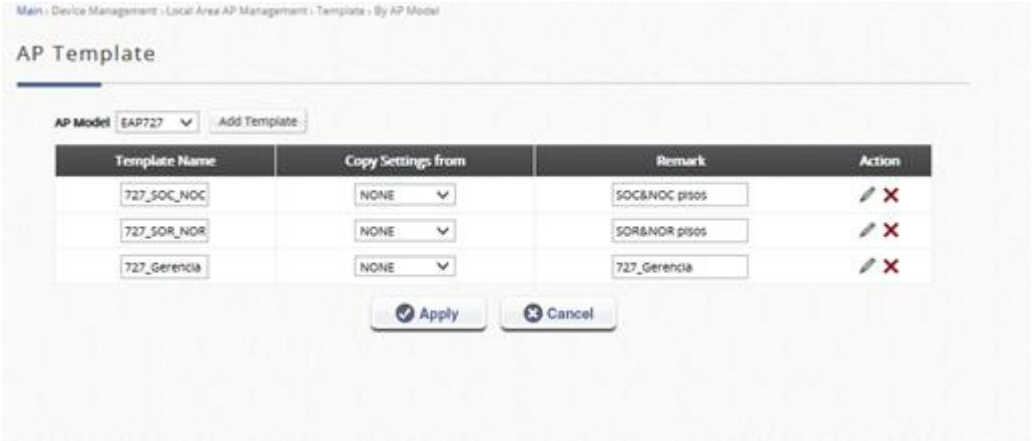
Ingreso de Access Points

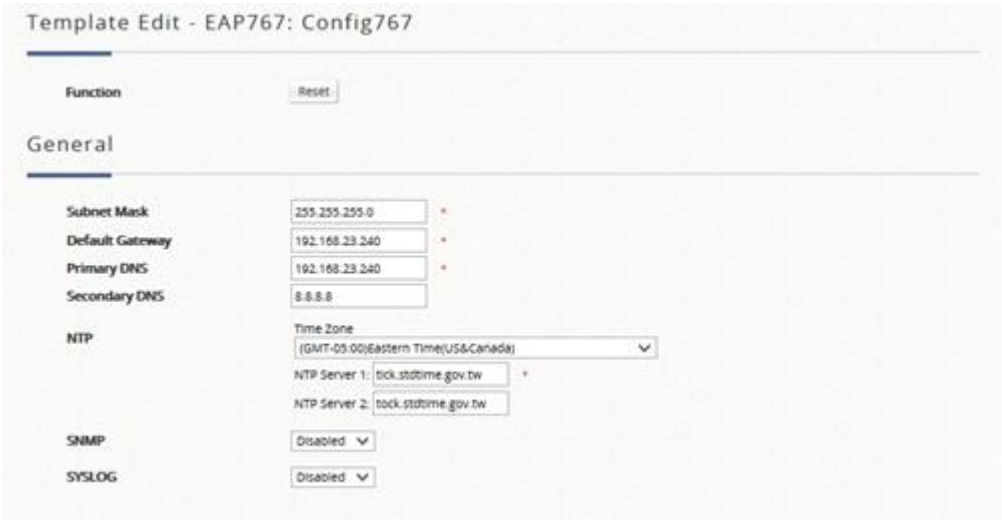
Agregar un AP.- Esta opción nos permite agregar manualmente los APs a la lista de administración. Se requiere configurar el tipo de AP, nombre, IP y MAC. Elegimos >> Devices >>Local Area AP Management>>AP list>>Add



Plantillas de configuración

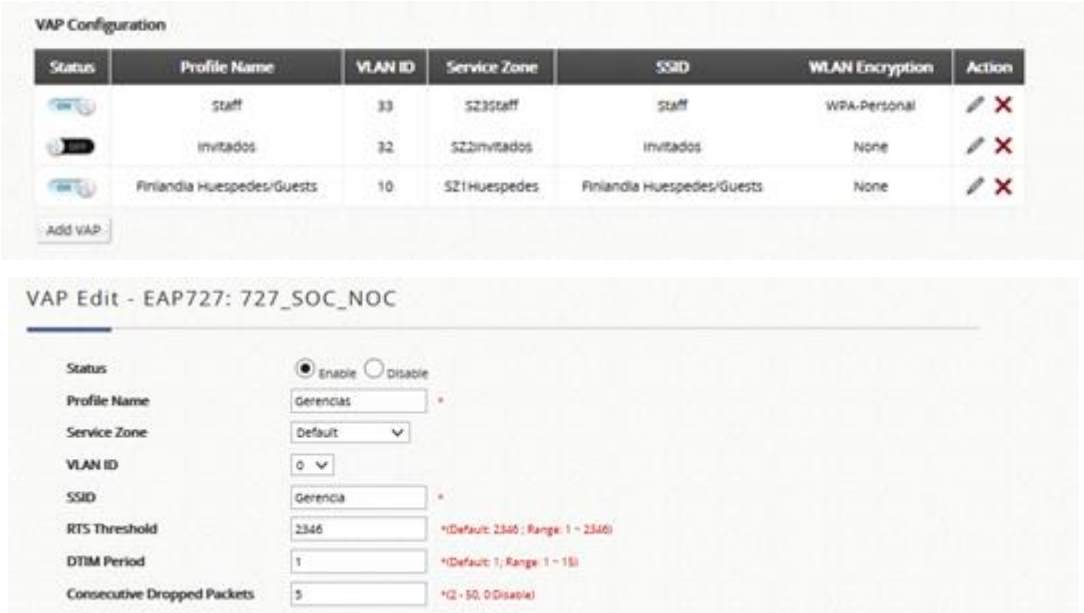
Se elige >> Devices >> Local Area AP Management >> Templates. Se selecciona el modelo de AP de la lista desplegable y se edita la plantilla de defecto o a su vez se agrega una nueva. Se puede agregar hasta 8 plantillas.





Configuración VAP (Virtual Access Point)

Podemos editar el estado, nombre, la zona de servicio, VLAN ID, SSID entre otros parámetros.

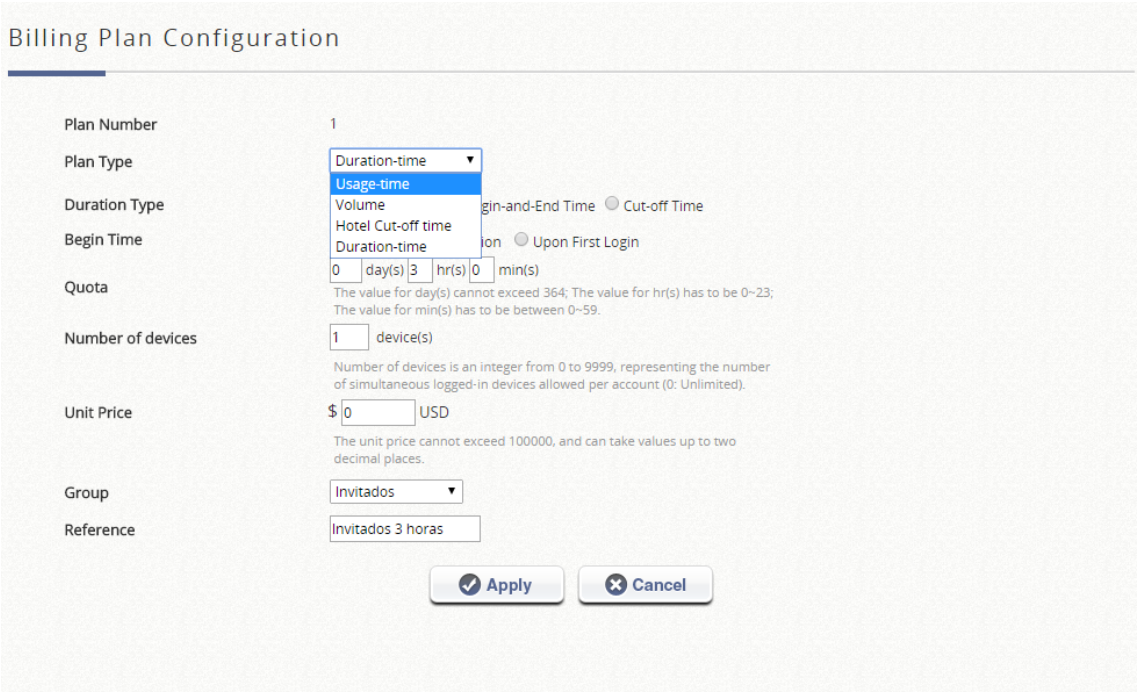


Configuración de Planes de Facturación bajo demanda

Los planes de facturación definen los términos y las condiciones de acceso a internet de los usuarios bajo demanda y se pueden configurar hasta 10.

Los tipos de plan de facturación bajo demanda son: tiempo de uso, volumen, tiempo de corte y duración de tiempo.

Se selecciona >> Users >> Internal Authentication >> On-Demand >> Billing Plans



Configuración del servidor de Impresión (Impresora despachadora de tickets)

Se configura el generador de tickets para que se comunique con el sistema y no necesite ir a través de la autenticación. Se selecciona >> Users >> Internal Authentication >> On-Demand Authentication >> Terminal Server.

Configuración POS tickets

Se selecciona >> Users >> Internal Authentication >> On Demand Authentication

```
                                SN: $remain
                    $date

                Welcome
--------------------------------
Username:
 $username
Password:
 $password
Quota: $quota
Price: $price
--------------------------------
ESSID:
--------------------------------
Activation:
Before $expire_time
Expiration:
$duration days after activation
--------------------------------
External ID: $extid
Remark: $remark
--------------------------------
                Thank You
```

Creación de página de inicio de sesión de las zonas de servicio

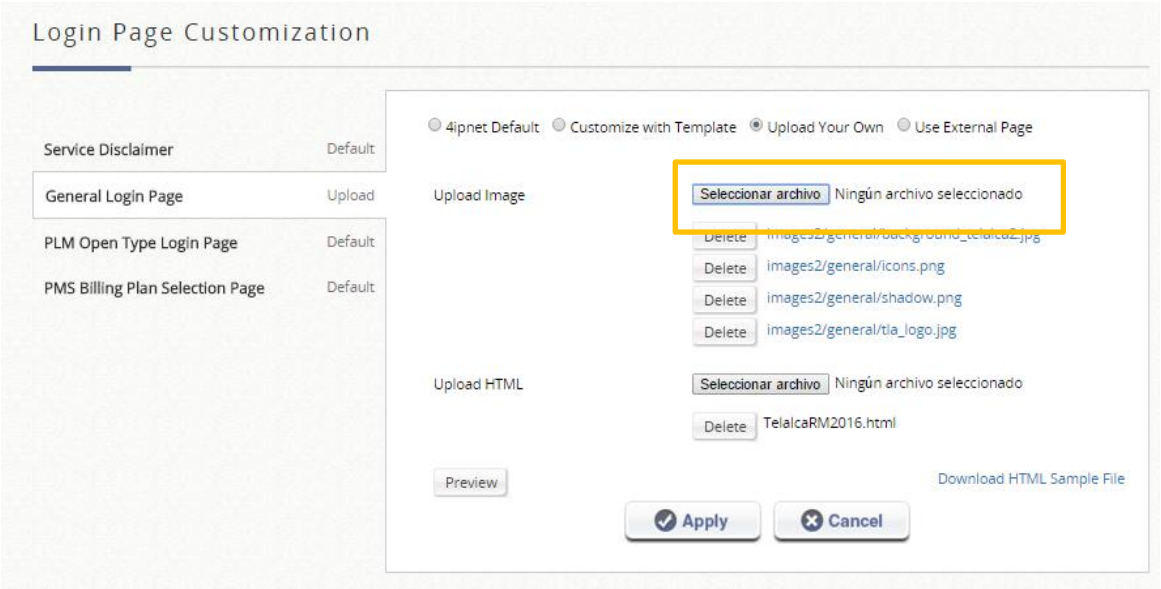
Para la zona de servicio default, SZ3Staff la autentificación se encuentra deshabilitada y no sería necesaria la configuración de la página de login.

Página de inicio de sesión de la zona de servicio SZ2_Huespedes

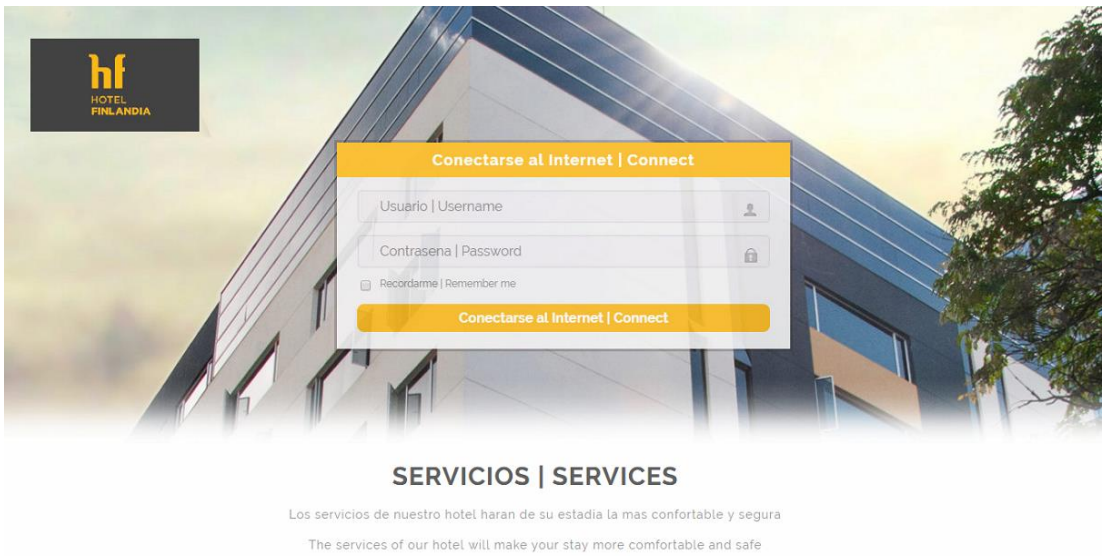
Se selecciona >> System >> Service Zones >> Services Zones Settings >> Page Customization.

Se selecciona el archivo HTML que deseamos cargar para la página Huéspedes, el sistema automáticamente agrega images2 al nombre del archivo a cargar. Es decir; images2 debido a que se está cargando la plantilla HTML en

la zona 2.Adicional se debe cargar las imágenes para que el HTML busque la ruta de las mismas.

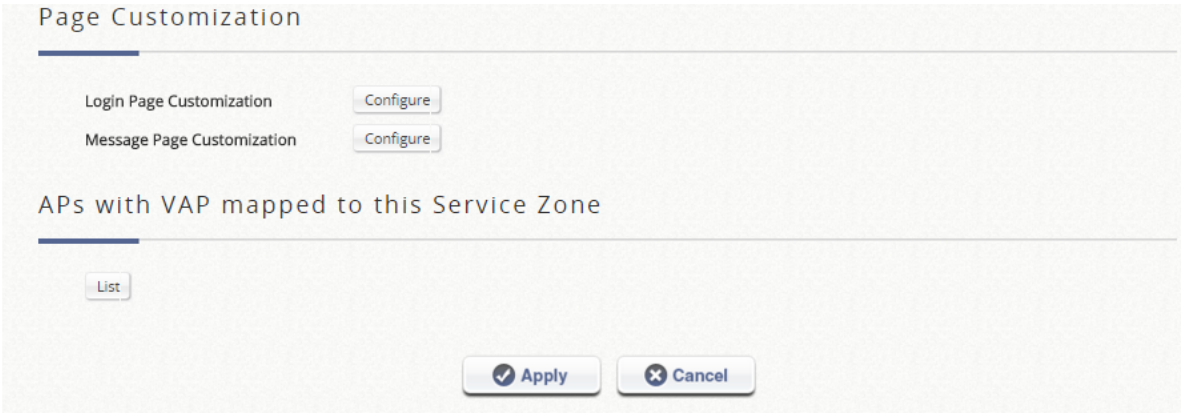


Página de inicio de sesión Huéspedes:

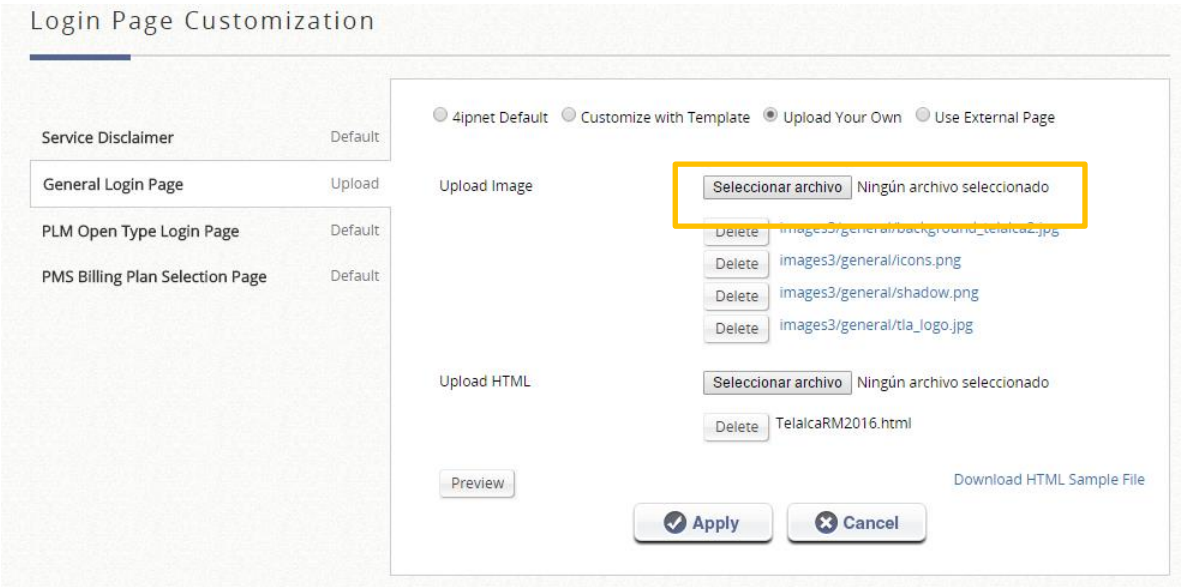


Página de inicio de sesión de la zona de servicio SZ2Invitados

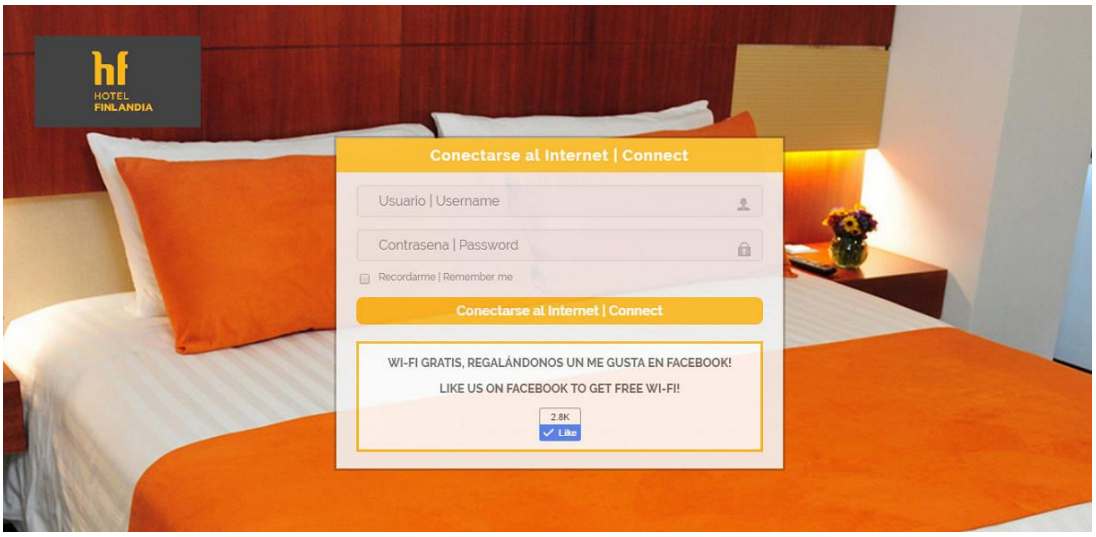
Se selecciona >> System >> Service Zones >> Services Zones Settings >> Page Customization.



Se selecciona el archivo HTML que deseamos cargar para la página Capacitaciones, el sistema automáticamente agrega images3 al nombre del archivo a cargar. Es decir; images3 debido a que se está cargando la plantilla HTML en la zona 3. Además se debe cargar las imágenes para que el HTML busque la ruta de las mismas.

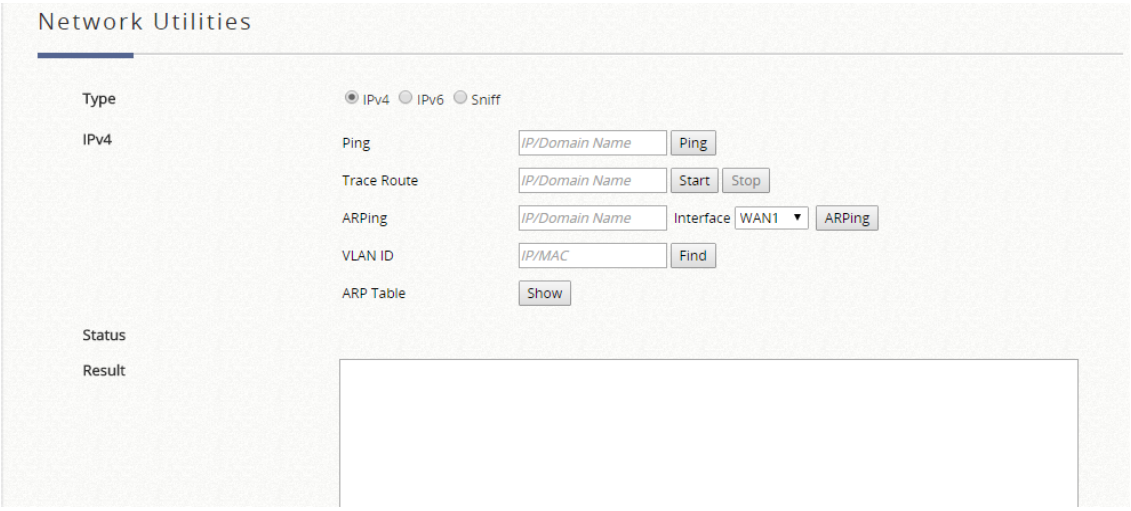


Página de inicio de sesión de Invitados



Herramientas de Red

Algunas utilidades de red basada en web como ping, trace route, y la tabla ARP son compatibles con el sistema.



Ping.- Es una de las herramientas de administración de redes más simple ya que permite al administrador detectar un dispositivo que utiliza la dirección IP o nombre de dominio host está activo o no.

Trace route.- Esta herramienta permite recuperar la ruta efectuada por los paquetes desde el Gateway a un destino utilizando la dirección IP o nombre de dominio host.

ARPing.- Permite enviar peticiones ARP a una dirección IP específica o nombre de dominio.

ARP Table.- Esta herramienta permite ver la tabla de asignaciones de direcciones IP y direcciones MAC utilizando ARP “protocolo de resolución de direcciones”.