Implementación red Wi-Fi geo distribuida

Salvador Rubio Coderch
Grado de Ingeniería informática

José Manuel Castillo Pedrosa

01 de Junio de 2019

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Implementación red Wi-Fi geo distribuida*
Nombre del autor:	*Salvador Rubio Coderch*
Nombre del consultor:	*José Manuel Castillo Pedrosa*
Fecha de entrega:	*01/06/2019*
Área del Trabajo Final:	*Administración de redes i sistemas operativos*
Titulación:	*Grado de Ingeniería Informática*

Resumen del Trabajo (máximo 250 palabras):

El proyecto consistente en el despliegue de una red Wi-Fi geográficamente distribuida entre las diferentes sedes de una corporación. Para el correcto desarrollo e implantación del proyecto se han evaluado diferentes propuestas en base a las necesidades de la organización, primando el aprovechamiento de la red actual lo máximo posible y considerando una estimación de crecimiento de la organización en los próximos años.

En esta memoria se detallan los diferentes aspectos que se han tenido en cuenta para el diseño de la red, así como las diferentes configuraciones que han permitido poner en funcionamiento la red dadas las necesidades requeridas por la organización, destacando la segmentación de redes según propósito de uso, y parametrización de los distintos elementos de red para lograr una red altamente disponible.

Además, también se plantean problemas surgidos durante la fase de implementación, así como las correcciones adoptadas para mitigarlos y solucionarlos.

Finalmente detallaremos las posibilidades y ventajas que ofrece y aporta una red Wi-Fi implementada en base a una topología en malla explorando las posibilidades y capacidades relacionada con la integración con otros sistemas, lo que aportará valor añadido para la gestión de la red gracias al uso de distintas herramientas que facilitaran la configuración, monitorización, securización y optimización de la misma.

Abstract (in English, 250 words or less):

This project is about a deployment of a Wi-Fi network geographically distributed between different headquarters of a corporation. For the correct development and implementation of this project, we have evaluated different proposals based on the needs of the final organization, prioritizing the use of the current network infrastructure as much as possible and considering the capacity for growth of the Organization in the coming years.

In this memory, are detailed a different particularities to design the desired network, and also the different configurations that are allowed to put operative the Wi-Fi network needed for the organization, highlighting the segmentation of networks according to the purpose of use, and the parameterization of the different network elements to achieve a highly available network.

In addition, the problems that arise during the implementation phase, as well as the corrections adopted to mitigate and solve the problems identified are also detailed and explained.

Finally, the possibilities and advantages offered by a Wi-Fi network implemented based on a mesh topology are exposed, exploring the possibilities and capabilities with other integration systems. These systems will provide added value for the network management, thanks to use of different tools that will facilitate the configuration, monitoring, securization and optimization of it.

Paraules clave (entre 4 y 8):

Wi-Fi, Network, Vlan, Cisco, Wireless, Flexconnect, Access point

Índice

Lista de ilustraciones

Lista de tablas

1. Introducción

1.1 Contexto y justificación del trabajo

Este proyecto es llevado a cabo debido a la necesidad de una organización para renovar y mejorar su infraestructura actual relativa a la red Wi-Fi que ofrece tanto a empleados de su organización como a invitados que acuden a las distintas sedes de la organización.

Se espera principalmente obtener una mejora en la gestión de los puntos de acceso pasando de una red con puntos de acceso independientes a una red Wi-Fi en malla con gestión centralizada. Además, se busca adquirir una mejora en la cobertura y calidad del servicio, especialmente en las zonas donde se requiera el acceso por Wi-Fi para los procesos críticos de producción.

Dado los cambios a adoptar, al final de la implementación del proyecto, se prevé simplificar y minimizar los recursos necesarios para administrar la red Wi-Fi, y adquirir una fortaleza en la seguridad y calidad del servicio.

1.2 Objetivos del trabajo

- Diseñar una solución geo distribuida compatible con dispositivos Cisco.
- Mejorar la cobertura y calidad de la red Wi-Fi de la organización de las diferentes sedes y ubicaciones.
- Aprovechar en la medida de lo posible los dispositivos actuales de la organización.
- Segmentar las distintas redes Wi-Fi de la empresa según propósito de uso.
- Contar con un sistema altamente disponible para garantizar la continuidad de negocio.
- Interconectar los puntos de acceso con la red L2 y L3 de la organización.
- Interconectar los puntos de acceso con Firewall L4 - L7 de la organización.

1.3 Enfoque i método empleado

Dado que el alcance del proyecto está bien definido y acotado desde el inicio y el entorno de la organización está correctamente documentado, hecho que minimiza los riesgos o incertidumbres que pudieran presentarse al inicio del proyecto, la gestión del mismo se realizará siguiendo la Metodología Tradicional, basada en PMI Guía PMBOK 6.0, consistente en las siguientes fases:

- Inicio
- Planificación y Diseño
- Ejecución
- Monitorización & Control
- Cierre

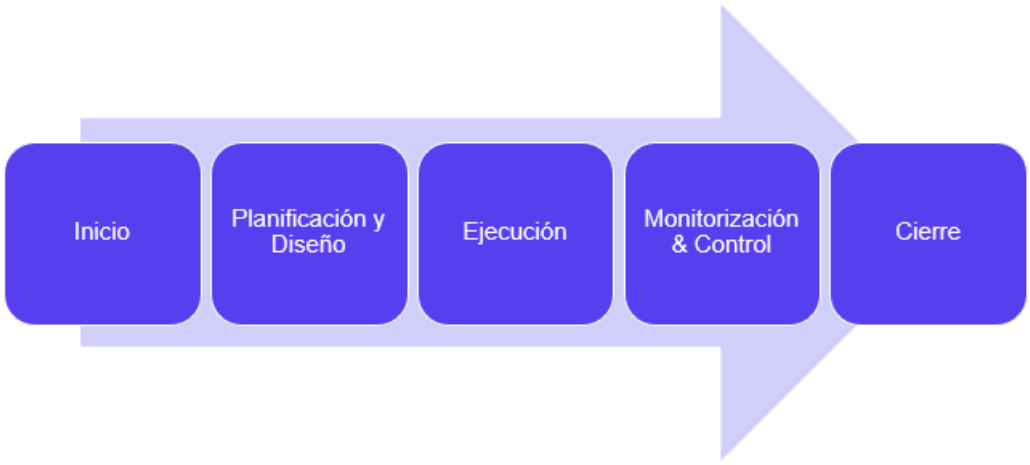


Ilustración 1 - Metodología

1.4 Planificación del Trabajo

Se detalla la estimación de jornadas para el estudio y implementación del proyecto a ejecutar. Para la planificación del proyecto se ha dividido el mismo según las fases detalladas según la metodología comentada anteriormente.

Task Name	Duration	Start	Finish
Presentación e iniciación del proyecto	**14 days**	**Wed 20/02/19**	**Sun 10/03/19**
Presentación Idea	1 day	Wed 20/02/19	Wed 20/02/19
Desarrollo Plan de trabajo	12 days	Thu 21/02/19	Fri 08/03/19
Diseño de la solución	**18 days**	**Mon 11/03/19**	**Thu 04/04/19**
Análisis situación actual y requisitos solución	**13 days**	**Mon 11/03/19**	**Thu 28/03/19**
Estudio de cobertura	5 days	Mon 11/03/19	Fri 15/03/19
Requisitos de la nueva solución	2 days	Mon 18/03/19	Wed 20/03/19

Estudio técnico y económico soluciones mercado	5 days	Thu 21/03/19	Wed 27/03/19
Selección solución y proveedor	1 day	Thu 28/03/19	Thu 28/03/19
Diseño conceptual	**5 days**	**Fri 29/03/19**	**Thu 04/04/19**
Definición, especificación de uso y definición SSID's	3 days	Fri 29/03/19	Tue 02/04/19
Arquitectura y dimensionamiento de la solución	2 days	Wed 03/04/19	Thu 04/04/19
Implementación de la solución	**37 days**	**Fri 05/04/19**	**Thu 30/05/19**
Implementación Solución Wireless	**18 days**	**Fri 05/04/19**	**Fri 03/05/19**
Cisco vWLC	**5 days**	**Fri 05/04/19**	**Thu 11/04/19**
Configuración base	1 day	Fri 05/04/19	Fri 05/04/19
Parametrización específica	2 days	Mon 08/04/19	Tue 09/04/19
Definición de políticas	2 days	Wed 10/04/19	Thu 11/04/19
Despliegue APs	**13 days**	**Fri 12/04/19**	**Fri 03/05/19**
Nuevos	6 days	Mon 15/04/19	Wed 24/04/19
Integración progresiva de los AP's reutilizados	6 days	Thu 25/04/19	Fri 03/05/19
Validación aprovisionamiento APs	1 day	Fri 12/04/19	Fri 12/04/19
Implementación e integración herramientas Cisco	**18 days**	**Mon 06/05/19**	**Wed 29/05/19**
Cisco Prime Infrastructure	**8 days**	**Mon 06/05/19**	**Wed 15/05/19**
Despliegue	1 day	Mon 06/05/19	Mon 06/05/19
Configuración base	1 day	Tue 07/05/19	Tue 07/05/19
Definición de políticas	3 days	Wed 08/05/19	Fri 10/05/19
Integración dispositivos	2 days	Mon 13/05/19	Tue 14/05/19
Configuración específica	1 day	Wed 15/05/19	Wed 15/05/19
Cisco CMX	**5 days**	**Thu 16/05/19**	**Wed 22/05/19**
Despliegue	1 day	Thu 16/05/19	Thu 16/05/19
Configuración base	1 day	Fri 17/05/19	Fri 17/05/19
Integración con Cisco Prime Infraestructure e vWLC	1 day	Mon 20/05/19	Mon 20/05/19
Configuración específica	2 days	Tue 21/05/19	Wed 22/05/19
Cisco ISE	**5 days**	**Thu 23/05/19**	**Wed 29/05/19**
Despliegue	1 day	Thu 23/05/19	Thu 23/05/19
Configuración base	1 day	Fri 24/05/19	Fri 24/05/19
Integración con vWLC (Radius)	1 day	Mon 27/05/19	Mon 27/05/19
Definición de políticas de seguridad en vWLC	1 day	Tue 28/05/19	Tue 28/05/19
Configuración específica	1 day	Wed 29/05/19	Wed 29/05/19
Cierre del proyecto	**8 days**	**Fri 31/05/19**	**Tue 11/06/19**
Resolución de problemas y Tunning de la solución.	4 days	Thu 30/05/19	Tue 04/06/19
Documentación	2 days	Wed 05/06/19	Thu 06/06/19
Traspaso conocimientos	2 days	Fri 07/06/19	Mon 10/06/19

Tabla 1 - Plan de proyecto

- **Recursos**

Se cuenta como recursos disponibles para la ejecución del proyecto, el personal técnico de Informática de la organización para soporte y colaboración en las fases de preparación y análisis del entorno, igualmente, trabajarán conjuntamente con el

implementador de la solución para obtener una mayor respuesta a las incidencias que puedan surgir y para el traspaso de conocimientos continuado durante la ejecución del proyecto.

Por otra parte, será necesaria la colaboración de personal de mantenimiento para la instalación de los puntos de acceso en los diferentes puntos estratégicos de la empresa.

- **Festivos**

Para la elaboración del plan de proyecto se ha tenido en consideración los festivos que tienen lugar en la Comunidad Valenciana en los meses comprendidos entre marzo y junio.

- 19/03/2019 → San José
- 19/04/2019 → Viernes Santo
- 22/04/2019 → Lunes de Pascua
- 01/05/2019 → Día del trabajo

- **Timeline**

Definimos el timeline de forma más gráfica, marcando los hitos más significativos del proyecto a ejecutar.

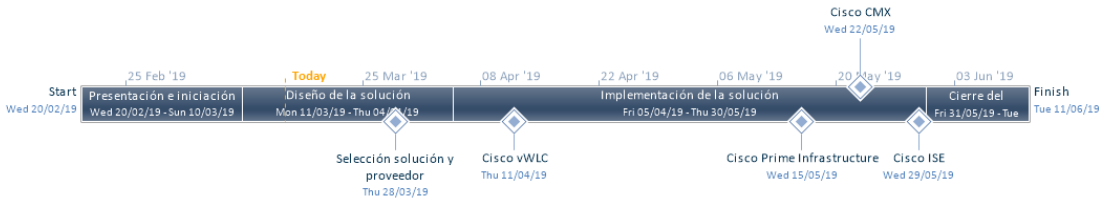


Ilustración 2 - Timeline

1.5 Breve sumario de los productos obtenidos

La organización recibirá durante el proyecto todos los elementos hardware y software para el desarrollo e implementación del mismo, así como la documentación correspondiente al proyecto:

- **Software:**
  - 2 x Cisco Virtual Wireless Controller (vWLC)
  - 1 x Cisco Prime Infraestructure
  - 1 x Cisco Connected Mobile Experiences
  - 1 x Cisco Identity services

- **Hardware:**
    - 28 x Cisco Access Point Aironet 1700
    - 28 x Soportes y kits de montaje
- **Licenciamiento**:
    - Licencias Cisco One para 38 Ap's y 17 switches.
- **Documentación**:
    - Estudio de cobertura
    - Análisis de las diferentes soluciones de mercado.
    - Diseño conceptual de la solución.
    - Detalles de implementación de la solución.

Adicionalmente, se hará entrega de una presentación del proyecto más enfocado a conocer el ámbito del mismo.

1.6 Breve descripción de los otros capítulos de la memoria

Esta memoria de distribuye en los siguientes capítulos:

- **Capítulo 2: Descripción del proyecto** → Pretende describir el proyecto con un nivel mayor de detalle.
- **Capítulo 3: Diseño de la solución** → Incluye los análisis de diferentes fabricantes tanto técnicos como económicos, para finalmente seleccionar el proveedor acorde a las necesidades del proyecto.
- **Capítulo 4: Arquitectura de la solución** → Se describe el diseño adoptado para la implementación del proyecto teniendo en cuenta el escenario de la organización.
- **Capítulo 5: Configuración de la solución** → Se especifican todos los detalles técnicos que se han tenido en cuenta para la configuración de los diferentes sistemas de la organización.
- **Capítulo 6: Incidencias** → Se documentan las incidencias detectadas durante y tras implementación del proyecto así como el análisis y resolución de las mismas.

- **Capítulo 7: Conclusiones** → Se exponen las conclusiones tras finalización de la implementación de los distintos sistemas.
- **Capítulo 8: Glosario** → Se presenta el glosario de terminología específica sobre el proyecto.
- **Capítulo 9: Bibliografía** → Se presentan las citas y la documentación consultada para la elaboración del proyecto.
- **Capítulo 10: Anexos** → Se adjunta la información relevante del proyecto no relacionada ni referenciada en los capítulos anteriores.

2. Descripción

El proyecto engloba una solución para una gestión centralizada de la red Wi-Fi de las diferentes sedes de una empresa, la cual cuenta con diferentes sedes geográficamente distribuidas. Para su implementación, se deberá adaptar y realizar cambios sobre la red interna de la empresa con el fin de implementar e integrar todos los puntos de acceso junto con las herramientas de administración y monitorización de Cisco: Cisco Prime Infraestructure; Cisco Connected Mobile Experiences (CMX); Cisco Identity services (ISE); Cisco virtual Wireless Controllers (vWLC); lo que facilitará un mayor control de la red y ventajas a nivel de seguridad y gestión. Dicho proyecto será desarrollado sobre un entorno real de producción.

Actualmente la empresa cuenta con un total de 600 usuarios, de los cuales, aproximadamente 150 se conectan de forma por Wi-Fi a la organización, la gran mayoría es personal interno el cual puede estar conectado indistintamente en cualquiera de las sedes, no obstante, también se ofrece acceso a personal externo (consultores y comerciales) eventualmente, considerando así que un 80% de las conexiones están identificadas y son efectuadas de forma regular, y el 20% restante es variable en función de las visitas. Dicho total se representa considerando el sumatorio de conexiones de las diferentes sedes las cuales se encuentran separadas 30Km entre sí. Dicho proyecto actualmente solo contempla la integración de dos sedes, no obstante, se debe prever un crecimiento de la organización en los próximos años, con lo que la solución debe ser escalable tanto para ser implementada en futuras ubicaciones como para soportar un crecimiento en el número de usuarios.

3. Diseño solución Wi-Fi

3.1 Análisis infraestructura actual

Con el fin de conocer y estudiar la implementación Wi-Fi actual de las diferentes sedes de la organización, se realiza un estudio de cobertura por sede y planta de cada una de las ubicaciones a tratar en el proyecto, para ello se ha empleado el software AirMagnet Survey, herramienta que permite generación de un informe basado en la importación de mapas de una infraestructura a analizar y basado en el autodescubrimiento de emisiones de señales Wi-Fi mientras desplazamos el equipo detector por las instalaciones de la organización. Todos los dispositivos analizados son de la marca Cisco, modelo 1130ag, 1600E y 1600I, y todos ellos funcionan de forma independiente, se detalla no obstante el resultado de los análisis de cobertura por planta y ubicación a continuación:

3.1.1. Cheste

Se trata de un edificio de planta baja, entresuelo y planta alta. Tiene distribuidas una serie de puntos de Acceso tanto en oficinas como en fábrica.

3.1.1.1. Planta Baja

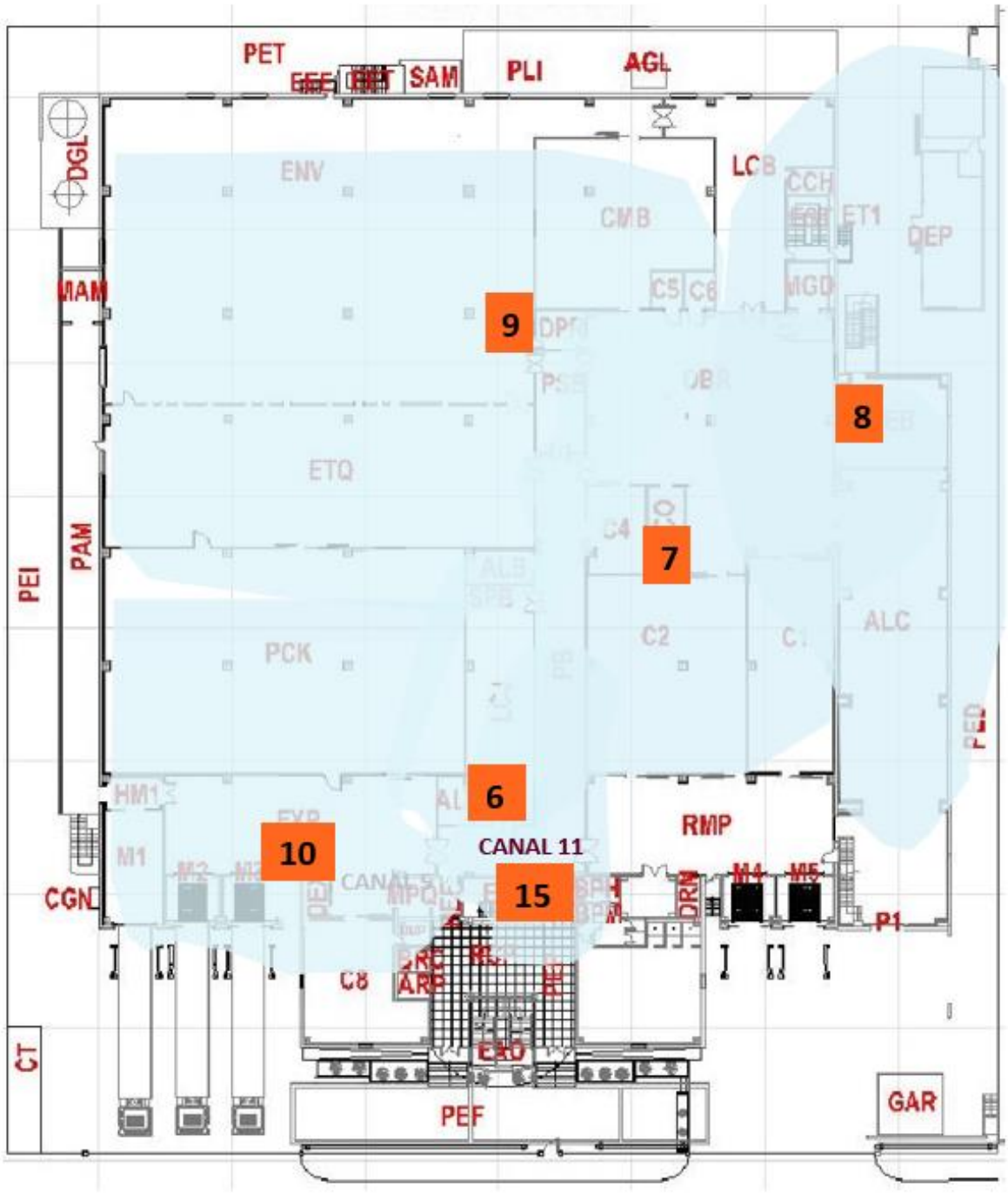


Ilustración 3 - Estudio Cobertura (Planta Baja Cheste)

3.1.1.2. Entreplanta

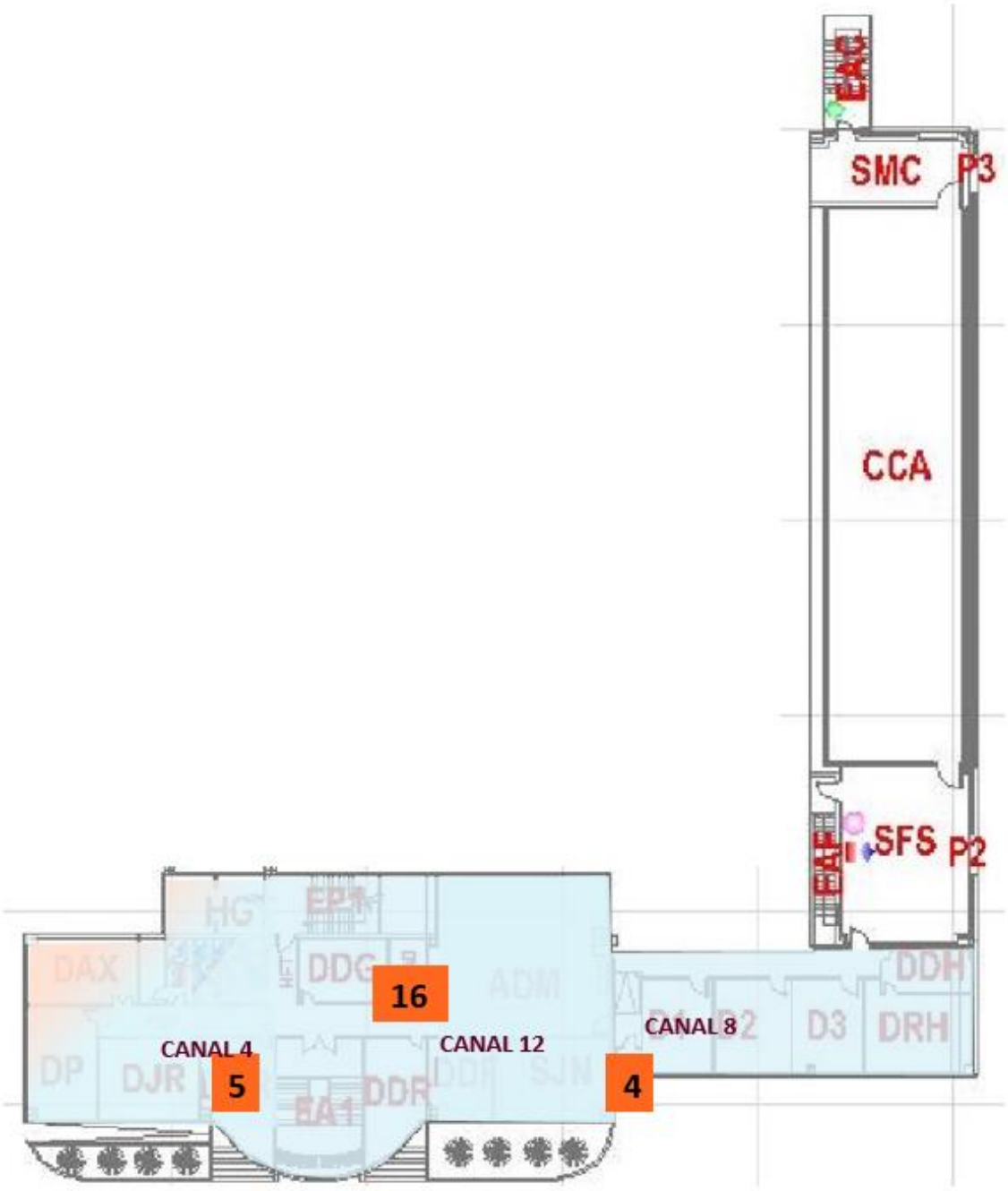


Ilustración 4 - Estudio Cobertura (Entreplanta Cheste)

3.1.1.3. Planta Primera

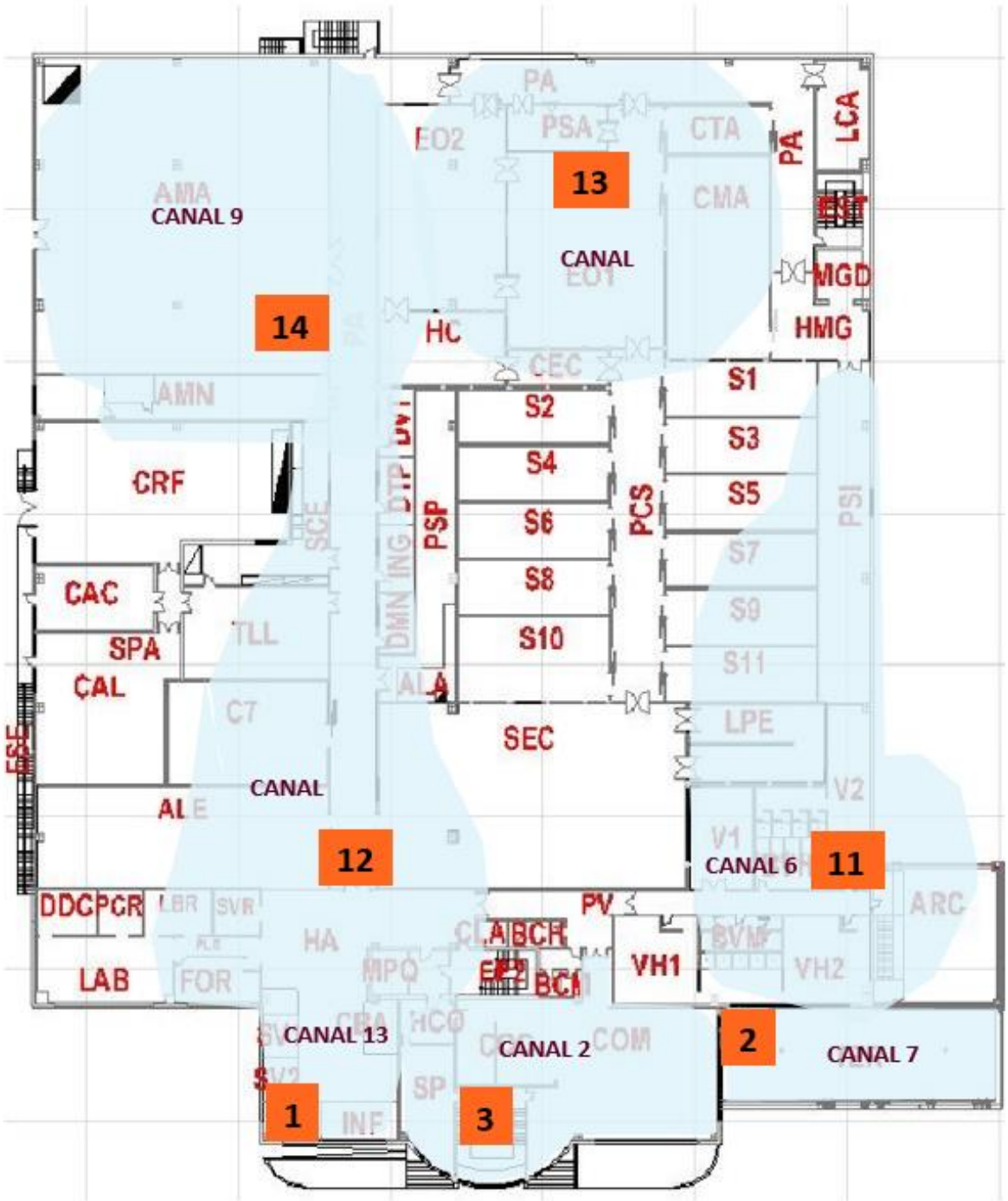


Ilustración 5 - Estudio Cobertura (Primera Planta Cheste)

3.1.1.4. Equipamiento

La relación del material descubierto en la toma de cobertura es el siguiente:

PUNTO	MAC Address	IP	CANAL	PLANTA	UBICACIÓN	DESCRIPCION
1	00:3A:9A:C9:4E:00	172.29.0.64	13	ALTA	SRA	Sala de visitas
2	20:4C:9E:EB:E3:C0	172.29.0.65	7	ALTA	TER	Thinking Area
3	00:3A:99:BE:32:B0	172.40.0.5	2	ALTA	EA2	Escalera de acceso a pta 1
4	00:3A:9A:DA:1C:80	172.29.0.52	8	ALTA	D1	Despachos de administracion e informatica
5	00:3A:9A:60:E7:40	172.29.0.56	4	ENTREPLANTA	DGR	Escalera de acceso a entreplanta
6	00:3A:9A:DA:2C:A0	172.29.0.60		BAJA	LCJ	Tripas
7	00:3A:99:D7:DA:B0	172.29.0.62		BAJA	SCO	Sala de Control
8	00:3A:9A:68:F1:30	172.29.0.57		BAJA	AEB	Especias
9	00:3A:99:77:9E:E0	172.29.0.58		BAJA	ENV	Envasado
10	00:3A:98:BC:4A:20	172.29.0.59	5	BAJA	EXP	Expediciones
11	00:26:99:E4:AD:B0	172.29.0.54	6	ALTA	PV	Pasillo
12	00:3A:9A:1C:68:60	172.29.0.50		ALTA	PA	Pasillo
13	00:3A:98:63:24:20	172.29.0.61		ALTA	EO1	Seco
14	00:27:0D:70:E9:70	172.29.0.53		ALTA	AMA	Almacen de Material Auxiliar
15	00:3A:9A:66:78:90	172.29.0.55	11	BAJA	REP	Vestuario Planta Baja
16	80:E8:6F:98:EF:80	172.29.0.66	12	ENTREPLANTA	ADM	Administracion
	00:3a:9a:21:0c:b0	172.29.0.63				¿Cámara caótica?
	00:16:01:2e:5e:0b	172.29.0.82		CHROMECAST		¿Sala de Juntas?

Tabla 2 - Equipamiento Cheste

Estas dos últimas se nos indican que existen, pero no llegamos a detectarlas durante el estudio de cobertura, probablemente por desconexión de los mismos.

3.1.1.5. Conclusiones

En general la cobertura de todo el edificio para las zonas de oficinas y producción es correcta salvo que existen salas en las que no llega la señal o llega débil, la distribución de canales está bien realizada, si bien alguna antena podría ser desplazada a ubicaciones (p.ej. Antenas 15 y 6) y quizá la 3 a comedor.

Cabe destacar que la posición de instalación de las antenas puede dar lugar a una menor cobertura. En general el modelo de Cisco 1130ag está diseñado para instalación en techo, una ubicación en pared puede ser efectiva en espacios pequeños, pero reduce en gran parte la amplitud de cobertura.

Citamos la recomendación del fabricante **[1]** :

Basic Installation Guidelines

Because the access point is a radio device, it is susceptible to interference that can reduce throughput and range. Follow these basic guidelines to ensure the best possible performance:

- Ensure a site survey has been performed to determine the optimum placement of access points.
- For lightweight access points, check the latest release notes to ensure that your controller software version supports the access points to be installed. You can find the controller release notes by selecting your controller under Wireless LAN Controllers at this URL: http://www.cisco.com/cisco/web/psa/default.html
- Ensure that access points are not mounted closer than 20 cm (7.9 in) from the body of all persons.
- Do not mount the access point within 3 feet of metal obstructions.

- Install the access point away from microwave ovens. Microwave ovens operate on the same frequency as the access point and can cause signal interference.
- Do not mount the access point outside of buildings.
- The integrated antenna design of the 1130AG series access point is designed for horizontal surfaces, (table top and ceiling installations). When mounted to such surfaces, the integrated antennas produce the best antenna radiation pattern. For advanced features such as voice, location, and rogue access point detection, ceiling mounting is strongly recommended. However, for smaller areas such as conference rooms, kiosks, transportation, and hot-spot usage where the customer is concerned primarily with data coverage and not advanced features, this unit may be wall mounted using the supplied plastic wall anchors and #8 screws.

Así pues, es recomendable revisar la instalación en fábrica para la reorientación de un equipo en horizontal y también el aprovisionamiento de nuevos puntos de acceso para cubrir los puntos ciegos.

Se recomienda la instalación de un total de 25 AP's para esta ubicación en caso de instalación nueva para la mejora de la señal a las diferentes zonas de la sede.

3.1.2. Torrente

Se trata de un edificio de planta baja y planta primera. Tiene distribuidas una serie de puntos de acceso tanto en oficinas como en fábrica.

3.1.2.1. Planta Baja

Ilustración 6 - Estudio Cobertura (Planta Baja Torrente)

3.1.2.2. Planta primera

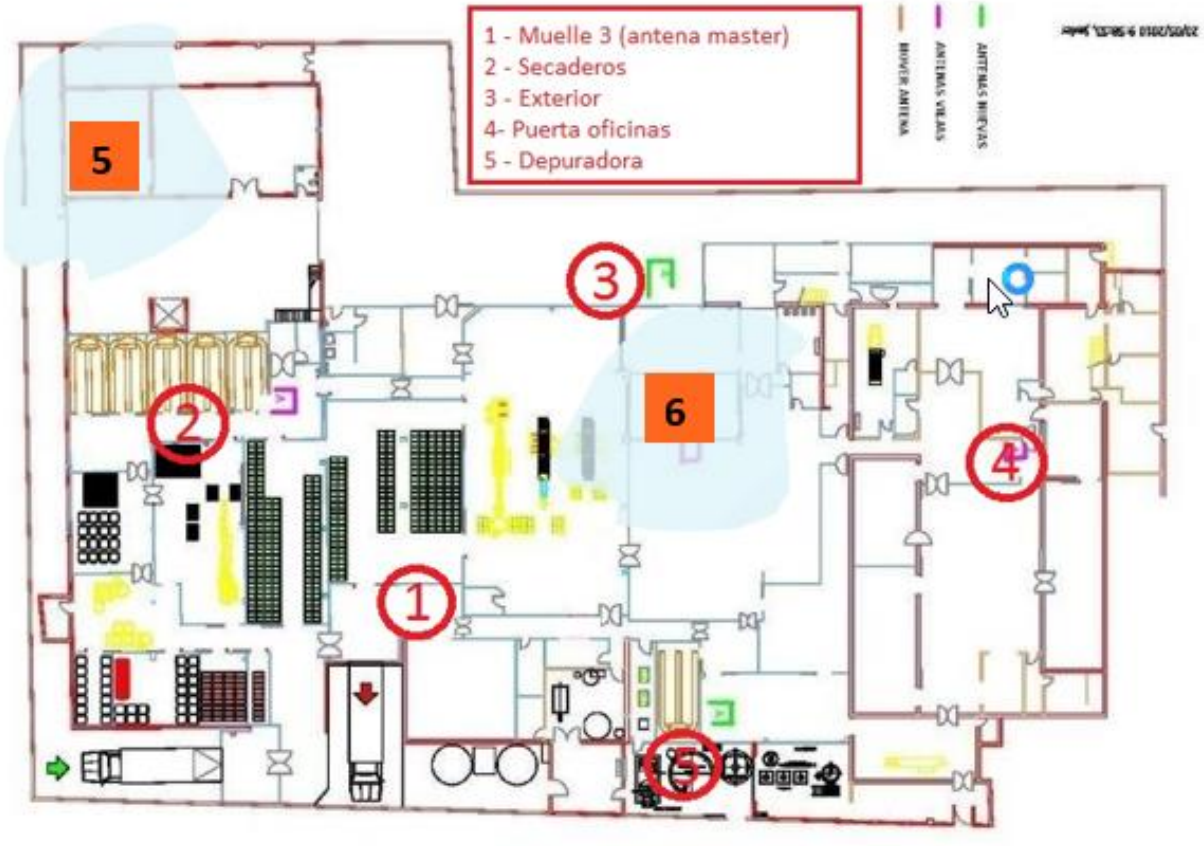


Ilustración 7 - Estudio Cobertura (Primera Planta Torrente)

3.1.2.3. Equipamiento

La relación del material descubierto en la toma de cobertura es el siguiente:

PUNTO	MAC Address	IP	CANAL	PLANTA	UBICACIÓN	DESCRIPCION
1	XX:XX:XX:XX:2F:60			BAJA		Puerta oficinas
2	XX:XX:XX:XX:DB:C1			BAJA		Oficinas muelle
3	XX:XX:XX:XX:37:30			BAJA		Almacén
4	XX:XX:XX:XX:D9:30			BAJA		
5	XX:XX:XX:XX:D8:D0			ALTA		
6	XX:XX:XX:XX:CC:20			ALTA	EM Libre	Comedor

Tabla 3 - Equipamiento Torrente

3.1.2.4. Conclusiones

En general la cobertura de todo el edificio es correcta en las zonas en las que se requiere, no obstante, perfiles móviles pueden experimentar problemas al desplazarse por el edificio, la distribución de canales no se ha estudiado en este caso debido a la poca densidad de puntos de acceso.

Igualmente que en la sede anterior, la posición de instalación de las antenas puede dar lugar a una menor cobertura. En general el modelo de Cisco 1130ag está diseñado para instalación en techo, una ubicación en pared puede ser efectiva en espacios pequeños, pero reduce en gran parte la amplitud de cobertura.

Se recomienda la instalación de un total de 12 AP's para esta ubicación en caso de instalación nueva para la mejora de la señal a las diferentes zonas de la sede.

3.2 Requisitos nueva infraestructura

- Mejora cobertura en las diferentes zonas de la fábrica y oficinas.
- Roaming según sede
- Gestión centralizada del entorno.
- Simplificar la gestión, administración, monitorización y configuración del entorno.
- Entorno altamente disponible.
- Aprovechamiento de los diferentes elementos de red actuales.
    - Puntos de acceso Cisco compatibles en modo lightweight (Cisco 1600E y 1600I).
    - Electrónica de red Cisco
- Conexión de hasta 50 AP's
- Capacidad para conexión entre 600 hasta 1000 Usuarios y 3000 dispositivos.
- Alimentación Power Over Ethernet (POE) de los puntos de acceso.
- Todos los Access Points deben ir instalados en el interior de las instalaciones.
- Tendencia a entorno virtualizado.

3.3 Análisis técnico

Para la evaluación de los requisitos en base a las diferentes alternativas se ha requerido el estudio y comparación de las diferentes opciones y soluciones disponibles actualmente en el mercado orientadas a la implementación de redes Wi-Fi en malla.

- **Aruba (HPE)**

  Aruba Networks es considerada una empresa especializada en proveer soluciones de networking para grandes empresas, desde su adquisición por HPE ha logrado mejorar su posición en el mercado siendo una compañía muy bien considerada en el sector.

  Analizamos los componentes que ofrece y revisamos en detalle los que encajan con la solución que se pretende adoptar:

  - **Controlador**: Se opta por la selección del controlador más básico de la gama de Aruba al cumplir con los requisitos de conexión anteriormente comentados. En este caso es posible la implementación tanto de un controlador físico como virtual, no obstante, la característica para High Availability (HA) solo es posible mediante la implementación de un clúster gestionado con la solución **Mobility Master** (MM-VA-50). Para la monitorización del entorno en tiempo real y servicios de localización, es necesario la implementación de **AirWave**.
    - Los diferentes controladores de Aruba ofrecen las siguientes características en sus distintas modalidades:
      - Soporte para 802.11ax (Wi-Fi 6)
      - Soporte para WPA3 y EAP
      - Firewall integrado
      - Inspección de paquetes para análisis de tráfico y filtrado por QoS.
      - Filtrado Web.
      - Soporte software incluido 90 días.
      - Soporte hardware incluido 1 año.
    - Físico: MOBILITY CONTROLLER 7030 **[2]**
      - Permite segmentación dinámica
      - Soporte servicio VPN integrado.
      - Hasta 64 Ap’s
      - Hasta 4096 usuarios / dispositivos concurrentes.
    - Virtual: VIRTUAL MOBILITY CONTROLLER **[3]**

- Permite la implementación como máquina virtual
- Hasta 50 Ap's
- Hasta 800 clientes.

- Access Point
  - Se selecciona la serie Aruba 207 **[4]** debido a que las características que ofrecen cumplen con las necesidades para el proyecto a implementar.
    - Banda dual 802.11ac
      - Hasta 867 Mbps → Banda 5 GHz
      - Hasta 400 Mbps → Banda 2.4 GHz
    - Detección radio BLE
    - Gestión avanzada coexistencia redes móviles 3G y 4G
    - QoS para apps.
    - Autoconfiguración de radiofrecuencia.
    - Inspección de paquetes.

- **Huawei**

  Huawei es una gran empresa cada vez más presente en el entorno empresarial, con un amplio portfolio, teniendo como principal ventaja un coste muy competitivo con respecto a la competencia.

  Analizamos los componentes que ofrece y revisamos en detalle los que encajan con la solución que se pretende adoptar:

  - **Controlador**: Se opta por la selección del controlador más básico de la gama de Huawei, siendo únicamente posible la implementación del mismo en físico. Alternativamente, Huawei ofrece la **solución Cloud Managed Network** (CMN) para la gestión centralizada de los AP's. también existe la posibilidad de adquirir un switch de la serie S5720-HI, los cuales incorporan funciones de WLAN para administrar hasta 1000 AP's.
    - Físico: HUAWEI AC6003-8 **[5]**
      - Permite la Autenticación 802.1X

- Soporte alta disponibilidad AC 1+1 HSB y N+1 Backup.
- Hasta 48 Ap's
- Hasta 1024 usuarios / dispositivos concurrentes.
- Monitorización integrada e identificación de apps.

- **Access Point**
  - Se selecciona el HUAWEI AP1050DN-S **[6]** siendo el punto de acceso más básico de Huawei pero suficiente en requisitos técnicos:
    - Banda dual 802.11ac
      - Hasta 433 Mbps → Banda 5 GHz
      - Hasta 200 Mbps → Banda 2.4 GHz
    - Supresión de interferencias.
    - Priorización banda 5Ghz.
    - Balanceo de carga entre AP's.
    - Implementación de protocolos de roaming: 802.11k, 802.11v, y 802.11r.
    - Autoconfiguración de radiofrecuencia.
    - Inspección de paquetes.

- **AeroHive**

  Aerohive es una un gran competidor en el campo de las redes Wi-Fi, destacando por su simplicidad de administración y la robustez y resistencia de los puntos de acceso que diseñan. Así mismo también ofrecen una gran variedad de modalidades para el despliegue de su consola central más conocido como **HiveManager**.

  Analizamos los componentes que ofrece y revisamos en detalle los que encajan con la solución que se pretende adoptar:

  - **Controlador**: Así como hemos comentado, en el caso de AeroHive, no existe un controlador físico como tal, sino que los puntos de acceso son gestionados desde una consola llamada HiveManager. Dicha utilidad puede ser implementada como appliance en un entorno privado on-

premises o cloud. Adicionalmente, AeroHive ofrece también otras herramientas para la gestión centralizada de más dispositivos de red con la solución **Connect**, y permite añadir monitorización avanzada y otros servicios de gestión especializada mediante la solución **Select**.

- Virtual on-premises: HiveManager Classic **[7]**
  - Uso de templates para la configuración.
  - Soporte alta disponibilidad mediante replicación automática de la bbdd.
  - Herramientas de diseño y monitorización de la red.
  - Hasta 15000 Ap's
  - Monitorización integrada e identificación de apps.

- **Access Point**
  - Se selecciona el AP130 **[8]** siendo el punto de acceso más básico de AeroHive pero suficiente en requisitos técnicos:
    - Banda dual 802.11ac
      - Hasta 867 Mbps → Banda 5 GHz
      - Hasta 300 Mbps → Banda 2.4 GHz
    - Supresión de interferencias.
    - QoS
    - Balanceo de carga entre AP's.
    - Firewall capas L2 – L7
    - Autoconfiguración de radiofrecuencia.
    - Inspección de paquetes.

- **Cisco**

  Cisco es una compañía considerada líder en el sector de las telecomunicaciones, ofreciendo un gran abanico de posibilidades y una alta calidad en todos los dispositivos que ofrece. Así mismo ofrece sistemas que se pueden integrar los con los dispositivos de cisco para la monitorización y adición de mejoras sobre los mismos.

Analizamos los componentes que ofrece y revisamos en detalle los que encajan con la solución que se pretende adoptar:

- **Controlador**: Cisco ofrece una alta variedad de modalidades para la implementación de sus diferentes controladores, desde controladores físicos, a controladores cloud, embebidos en switches, o incluso embebidos en el propio AP permitiendo un entorno sin controlador. Para este caso, se va a evaluar la solución virtual de Cisco.
  - Virtual: vWLC **[9]**
    - Uso de templates para la configuración.
    - Soporte alta disponibilidad mediante N+1
    - Herramientas de diseño y monitorización de la red.
    - Hasta 3000 AP's
    - Hasta 32000 Usuarios
    - Integración Flexconnect.
- **Access Point**
  - Se selecciona el Cisco Aironet 1700 **[10]** el cual cumple con los requisitos técnicos requeridos:
    - Banda dual 802.11ac
      - Hasta 867 Mbps → Banda 5 GHz
      - Hasta 300 Mbps → Banda 2.4 GHz
    - Detección de Interferencias con Clean Air.
    - Implementación de protocolos de roaming optimizado.
    - Equalización MIMO
    - Autoconfiguración de radiofrecuencia.

Una vez analizadas las diferentes opciones del mercado que encajan en los requisitos de la organización para la renovación tecnológica de la red Wi-Fi, a modo comparativo, incluimos un resumen de las características más destacables de cada uno de los fabricantes, tanto para los controladores como para los puntos de acceso:

- **Controladores:**

CONTROLADOR	MÁXIMOS AP'S	MÁXIMOS CLIENTES	APPLIANCE	ALTA DISPONIBILIDAD
ARUBA MC-VA-50	50	800	Virtual	HA Cluster
ARUBA MC 7030	64	4096	Físico	HA Cluster
HUAWEI AC6003-8	48	1024	Físico	AC 1+1 HSB/N+1
AEROHIVE CLASSIC WITH AVC	6000	N/A	Virtual	DB Sync
CISCO VWLC (SMALL SCALE)	200	6000	Virtual	N+1 HA

Tabla 4 - Comparativa Controladores

De la comparativa referente a los controladores se concluye que todos son aptos en cuestiones de alta disponibilidad y todos toleran la cantidad de usuarios y puntos de accesos estimados para la instalación. No obstante, por distribuirse en modo appliance virtual y por la capacidad de escalado, se consideran como mejores opciones las ofrecidas por AeroHive y Cisco.

- **Puntos de acceso:**

PUNTOS DE ACCESO	BANDA 2.4 GHZ	BANDA 5 GHZ	POWER	ANTENAS INTEGRADAS	INTERFACES	RESISTENCIA	POE
ARUBA 207	<= 400 Mbps	<= 867 Mbps	12.3W	2 x dual band/omni-directional / Ganancia: 3.9dBi en 2.4GHz y 6.8dBi en 5GHz / omnidireccional	1x GE uplink port + 1x Console	Operating: 0 to 50 °C Humidity: 5% - 93%	Si
HUAWEI AP1050DN-S	<= 200 Mbps	<= 433 Mbps	8.1W	1 x dual band / Ganancia: 5dBi / omnidirectional	1x GE uplink port + 1x Console	Operating: -10 to 50 °C Humidity: 5% - 95%	Si
AEROHIVE AP130	<= 300 Mbps	<= 867 Mbps	11W	2x single band, 2.4-2.5 GHz & 2x single band, 5.1-5.8 Ghz / omnidirectional	1x GE uplink port	Operating: 0 to 40 °C Humidity: 95%	Si
CISCO AIRONET 1700	<= 300 Mbps	<= 867 Mbps	15W	1x single band 2.4 GHz y 1x single band 5Ghz / Ganancia 4 dBi / omnidirectional	2x GE uplink port + 1x Console	Operating: 0 to 40 °C Humidity: 10 - 90%	Si

Tabla 5 - Comparativa Puntos de acceso

De la comparativa referente a los puntos de acceso, observamos que a excepción de Huawei todos los AP's ofrecen unas altas capacidades de transferencia en ambas bandas, especialmente el Aruba 207 el cual destaca adicionalmente por su nivel de ganacia en las antenas. Para entornos con requisitos de bajo consumo sería recomendable el AP de Huawei, sin embargo, para entornos más exigentes con respecto a la temperatura y humedad ambiente destaca el ensamblaje del Aerohive. Finalmente, el AP de Cisco es el único que ofrece más de una interfaz ethernet, muy interesante si se desea configurar una red exclusiva para gestión o se desea segmentar tráficos distintos en la capa física y no lógica.

3.4 Análisis económico

Tras la evaluación técnica de las diferentes soluciones, se procede con el análisis económico del mismo, evaluando así el coste de todas las soluciones para la adquisición de un controlador virtual y 39 antenas.

Para ello se considera para los controladores, el coste de licencia anual para los virtuales (Aruba, AeroHive y Cisco), y un pago único para el caso de controlador físico (Huawei). Todos los precios indicados fueron consultados el 31 de marzo de 2019 y se ha realizado una conversión de divisas a Euros debido a que algunos precios consultados están bajo la divisa del Dólar Estadounidense.

FABRICANTE	CONTROLADOR	COSTE CONTROLADOR	ACCESS POINT	COSTE ACCESS POINT
ARUBA	MC-VA-50 **[11]**	928,55€	AP-207 **[12]**	357,86€
HUAWEI	AC6003-8-8AP **[13]**	791,45€	AP1050DN-S **[14]**	151,75€
AEROHIVE	AH-HM-VA **[15]**	1773.09€	AP130 **[16]**	266,19€
CISCO	vWLC **[17]**	667,70€	AIRCAP1702I **[18]**	143,48€

Tabla 6 - Comparativa costes Hardware

Adicionalmente, se realiza una estimación de licenciamiento y soporte por año para cada una de las soluciones. Dado que cada fabricante ofrece un modelo de suscripción/licenciamiento diferente, detallamos según cada caso el coste oportuno:

- **Aruba**

El coste de la licencia para el controlador ya incluye licenciamiento para un total de 50 AP's. Lo que simplifica la compra del licenciamiento necesario para dicha solución, teniendo un coste de 4255,63€ **[19]**.

- **Huawei**

Para licenciar la infraestructura Wi-Fi de Huawei es necesario adquirir las licencias para el número de AP's necesarios. Dado que para el controlador AC6003 solo se incluyen paquetes para 8 AP's, será necesario adquirir 5 de ellos ya que dicho controlador soporta hasta 48 AP's.

- AC6003-L-AC6003-8AP-AC6003 Wireless Access Controller AP Resource License(8 AP) – 203,87€ **[20]**

- **AeroHive**

En el caso de AeroHive, deberemos contar que la licencia del apliance ya es adquirida junto al controlador, y adicionalmente se requiere adquirir una licencia por AP a registrar en el controlador.

- Aerohive HiveAP License for HiveManager → 70.96€ **[21]**

No obstante, existe la posibilidad de adquirir los AP's con dicho licenciamiento ya incluido de tal forma que en el cómputo global sale más económico, a pesar que fuerza el uso del HiveManager en versión cloud.

- Aerohive AP130 w FCC Domain, HiveManager 6 Online, Select Support (1 Year) → 330,29€ **[22]**

Dado que se prefiere optar por la versión on-premise del controlador se considera el coste en base a AP y licenciamiento clásico por separado, resultado un coste de 2696,48€ para licenciamiento de los puntos de acceso.

- **Cisco**

El controlador de cisco ya incluye con el licenciamiento del controlador un total de licencias para 5 AP's, se deberán adquirir 8 paquetes iguales para licenciar un total de 40 antenas. Además, por AP se deberá licenciar cada dispositivo que se quiera añadir a los sistemas de Cisco Prime, CMX e ISE de forma conjunta con Cisco One.

- Virtual Wireless Controller (vWLC) L-AIR-CTVM-5-K9 → 667,70€ **[23]**
- Cisco ONE Foundation Wireless - license - 1 license → 202,98€ **[24]**

Todos los precios son orientativos y a término unitario, pudiendo disminuir el precio de los puntos de acceso al realizar la compra por lotes.

Por tanto, considerando el cómputo para cada una de las soluciones incluyendo el coste hardware y software para un total de 38 AP's según recomendaciones del análisis de cobertura (25 AP's para Cheste, 12 AP's para Torrente y 1 AP como Spare).

Así pues, daría lugar a la siguiente estimación (recordar que para el caso de Cisco se considera la adquisición únicamente 28 antenas, ya que 10 son reaprovechables para la implementación planteada):

FABRICANTE	COSTE HARDWARE	COSTE LICENCIAMIENTO	TOTAL
ARUBA	14525,96€	4255,63€	18781,58€
HUAWEI	6542,60€	1019,36€	7561,96€
AEROHIVE	11888,31€	2696,48€	14584,79€
CISCO	4017,33€	13054,93€	17072,26€

Tabla 7 - Comparativa Costes Licenciamiento

Adicionalmente, conviene considerar el coste de jornadas de consultoría para los servicios de implementación del proyecto. Para ello nos basamos en la planificación del proyecto para estimar las jornadas requeridas para la implementación del proyecto considerando la necesidad especialmente de valorar el coste del diseño por parte de un consultor especializado, y la implementación y documentación por parte de un técnico senior.

Por tanto, considerando el precio por hora de un Técnico/Consultor de sistemas/telecomunicaciones está valorado aproximadamente en 50€[1] [25], y se requieren 63 Jornadas de 4 horas, el coste de servicios asciende a 12.600€, coste que repercute para cualquiera de las soluciones valoradas.

Por último, como un aspecto opcional, se debe considerar la adquisición de un servicio de soporte de la plataforma implementada para el mantenimiento de los servicios y la

[1] Precios orientativos en base a los precios públicos de la Consultoría TIC Ocellum. Estos pueden ser muy variables en función de la ubicación de la empresa de servicios, de los desplazamientos y de la experiencia y reputación del proveedor seleccionado.

infraestructura implementada. Se considera un coste adicional de 3.000€ anuales para atención y soporte de incidencias relacionadas con la infraestructura a desplegar.

3.5 Conclusión y selección solución final

Finalmente, se ha recomendado la elección de Cisco como proveedor de la solución, ya que, a pesar de ser la segunda opción con más coste, es la solución que más confianza confiere por su gran experiencia en el ámbito de las redes informáticas.

Entre los diferentes aspectos a valorar, cabe destacar las posibilidades de escalabilidad de la solución, las cuales permiten el crecimiento de hasta 200 dispositivos para la versión small scale del appliance virtual y 6000 usuarios concurrentes, especialmente a tener en cuenta considerando la posible implementación de la solución en otras sedes de cara al futuro. Además, para el proyecto actual, permite la posibilidad de reutilizar parte de la infraestructura Wi-Fi para su reacondicionamiento y reutilización en el nuevo proyecto de renovación tecnológica. Se considera también que la organización actualmente ya cuenta con una infraestructura de red Cisco en la capa de red de acceso, distribución y core que puede facilitar la configuración y despliegue de la solución, además de facilitar la administración de la infraestructura a los técnicos de la organización gracias a la familiarización con las interfaces gráficas y de comando de los productos de Cisco.

Dada la tendencia de la organización hacia un entorno virtual y on-premise, contando ya varios entornos virtualizados con VMware en las distintas ubicaciones, se ha valorado muy positivamente la posibilidad de Cisco de desplegar los controladores como appliance virtual.

Así como el resto de las soluciones incorporan sistemas propios de monitorización, el ofrecido por Cisco es el único que posibilita un mayor nivel de monitorización de la red en comparación al resto de soluciones gracias a la implementación de sistemas como Cisco Prime Infraestructure, CMX y ISE, herramientas que veremos en próximos apartados del presente documento, que además permiten también la integración del controlador mediante el despliegue de un appliance on-premise. Especialmente Cisco Prime Infraestructure permite además de monitorizar la red Wi-Fi la red cableada

gracias a la posibilidad de inventariar otros dispositivos como routers y switches de la organización.

El modelo de licenciamiento de Cisco también ha sido considerado como más simple con respecto a otras soluciones, gracias a la simplicidad del modelo de licenciamiento de Cisco One, que permite unificar el licenciamiento de diferentes dispositivos para múltiples utilidades en una única licencia y facilita la escalabilidad de la solución en caso de requerir nuevos dispositivos en la infraestructura.

En último lugar, por parte de la organización se ha destacado la gran calidad del soporte de Cisco la buena atención recibida por parte de Cisco para la resolución de los incidentes que han podido surgir históricamente en su infraestructura.

4. Arquitectura

4.1 Arquitectura tecnológica

4.1.1 Diseño Conceptual

El diseño de la solución para la infraestructura Wi-Fi, se ha basado en el uso de la tecnología Flexconnect que permite que los puntos de acceso obtengan su configuración directamente de los vWLC, pudiendo funcionar de forma autónoma en caso de que no exista conectividad con los mismos ya que el tráfico de datos nunca será tratado por los vWLC, sino que será directamente enrutado según el direccionamiento de cada una de las sedes o grupos de flexconnect configurados en los vWLC.

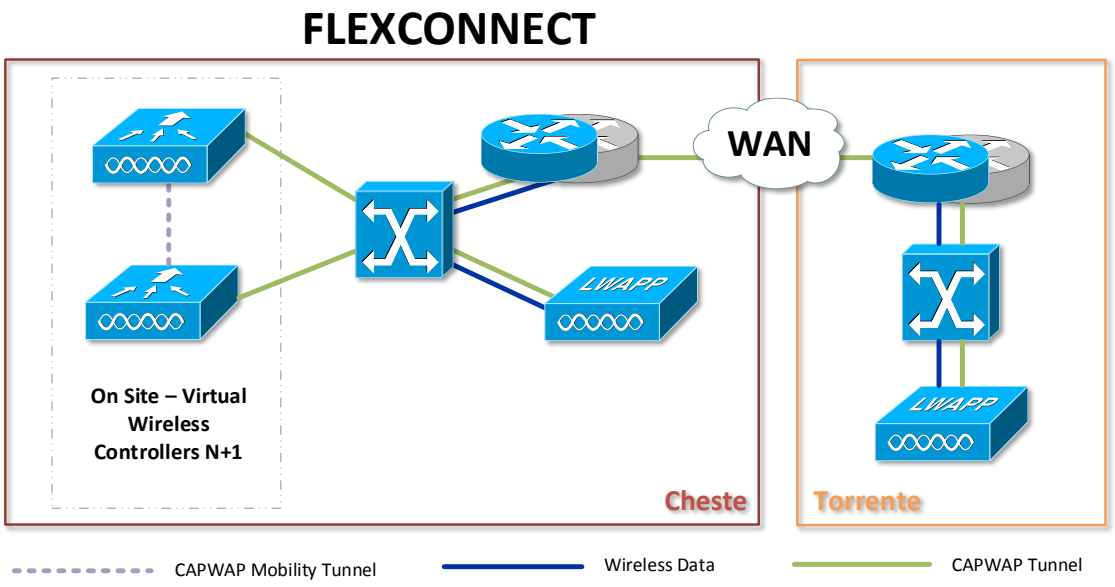


Ilustración 8 - Diseño Conceptual

4.1.2 Diseño Lógico

En el presente diseño, se refleja a nivel global los distintos elementos que forman parte de la solución, así como las particularidades a nivel de red de cada uno de los diferentes SSID's según su propósito y configuración final.

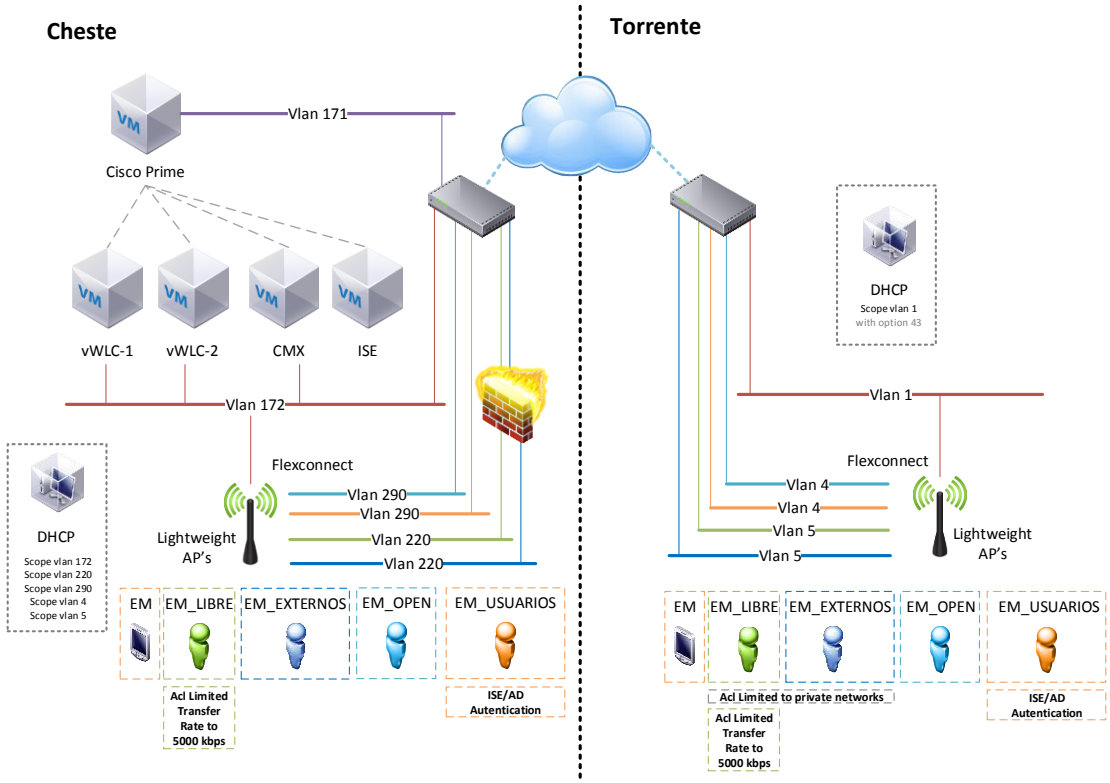


Ilustración 9 - Diseño Lógico

Tal y como se aprecia en el diagrama, ambas sedes comunican entre sí a través de una Macrolan de un proveedor de Servicios. Dado la estrategia de negocio, el core IT se encuentra en la sede de Cheste, por lo que será la sede que acogerá el despliegue de servicios necesarios para la implementación de la infraestructura. No obstante, los SSID desplegados en ambas sedes, a pesar de ser los mismos y compartir propósito, serán reencaminados por las diferentes VLAN de cada sede con el fin de permitir la navegación y controlar dicho tráfico según el direccionamiento de cada sede.

Cabe destacar que todo tráfico entre sedes no atraviesa el Firewall de la organización, sino se queda en los cores. No obstante, todo tráfico destinado a Internet si será reencaminado hacia el Firewall y por tanto será tráfico tratado por el mismo.

5. Configuración

5.1 Virtual Wirelless Controller (vWLC)

El Virtual Wireless Controller es un servidor encargado de centralizar la configuración y conexión a todos los Access Point Lightweight que requieran ser gestionados de forma centralizada publicando SSID's de forma global mediante la configuración y asociación de AP's por grupos de Flexconnect según la ubicación. En este caso la configuración detallada está basada en una implementación en HA N+1 para tolerar la caída de uno de los nodos, y además los vWLC también incluye una capa para la monitorización de uso de los clientes conectados a la infraestructura mediante los AP's conectados a los mismos.

Mostramos a continuación los diferentes paneles de gestión que presentan los vWLC:

- Portal de monitorización:

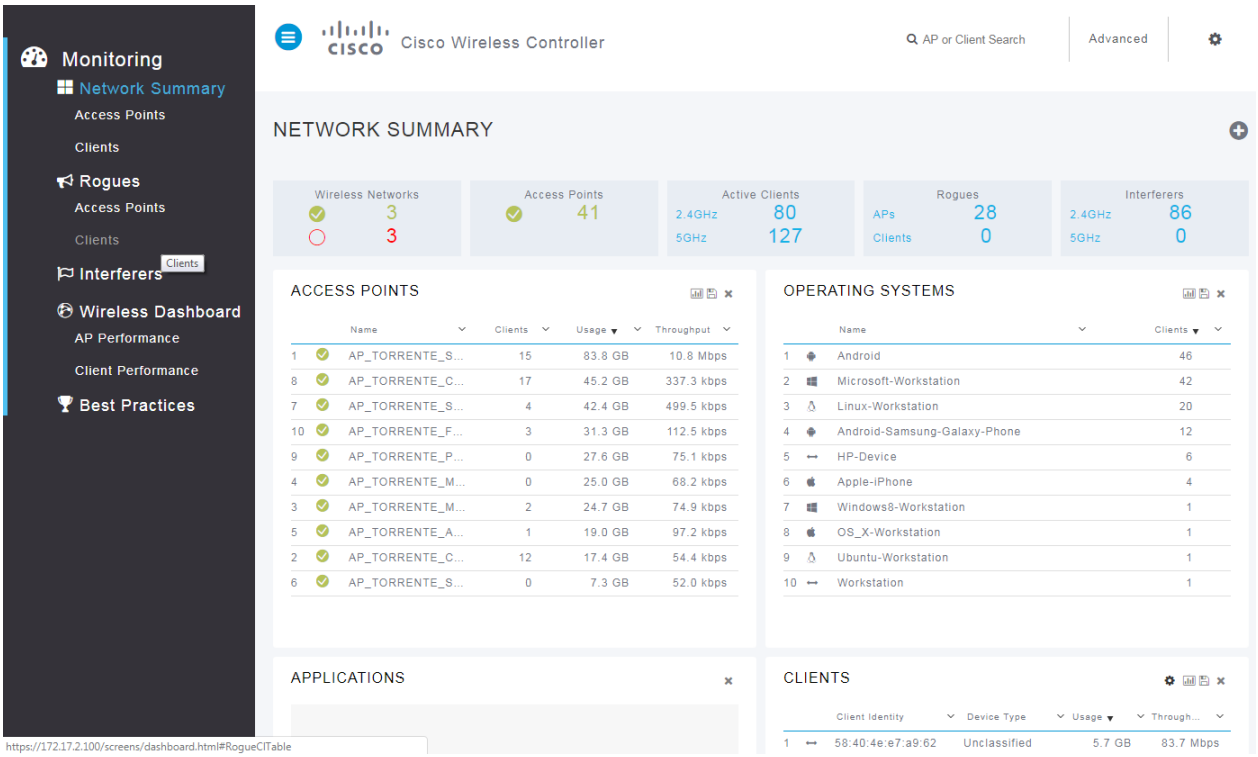


Ilustración 10 - Portal de monitorización de vWLC

- Portal de configuración:

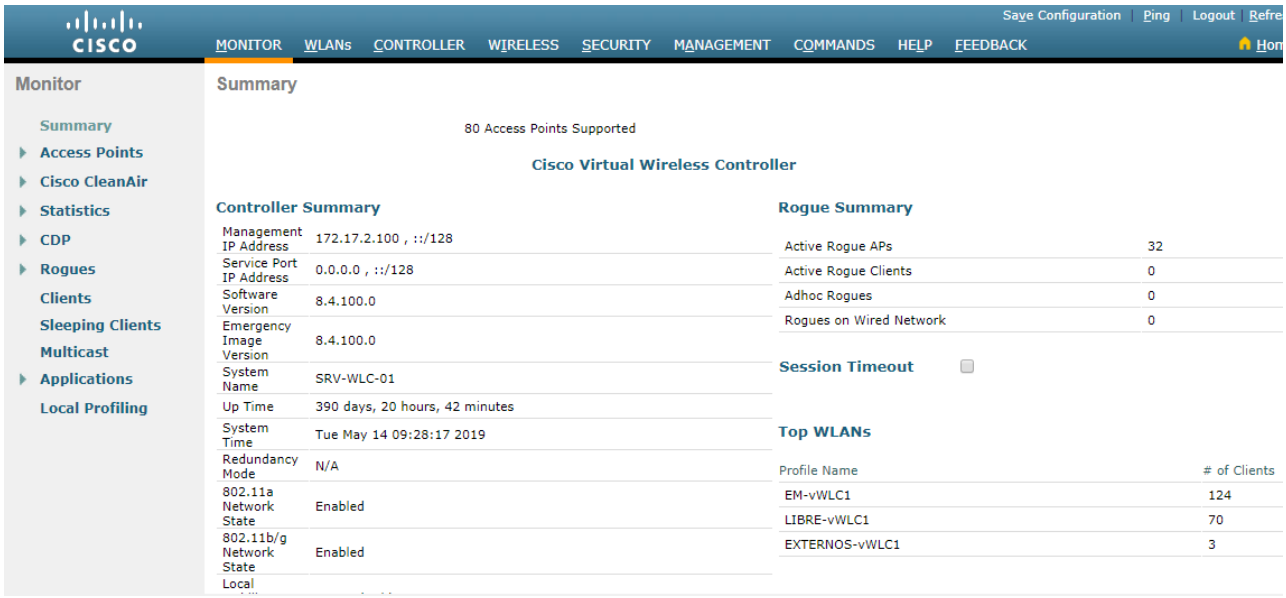


Ilustración 11 - Portal de configuración de vWLC

5.1.1 Configuración básica

5.1.1.1 Credenciales de Acceso

Se acuerda con la organización las credenciales de acceso para usuario admin en los virtual Wireless Controllers.

5.1.1.2 NTP y SNMP

NTP:

Se configura NTP para el servidor externo hora.roa.es (150.214.94.5).

SNMP:

Se definen las siguientes community's (SNMP v2c) siguiendo el standard de cliente para comunicación principalmente con Cisco Prime Infraestructure y el servidor CMX.

Community Name	IP Address	IP Mask	Access Mode
LTd0s	172.17.0.0	255.255.0.0	Read-Only
ETd0s	172.17.0.0	255.255.0.0	Read-Write

Tabla 8 - Configuración vWLC - SNMP

5.1.1.3 Licencias

Se añade licenciamiento para 39 AP's en cada uno de los virtual Wireless Controller.

5.1.2 Configuración avanzada

5.1.2.1 HA N+1

En Virtual Wireless Controller únicamente se soporta configuración N+1 como solución de alta disponibilidad, de tal forma que es necesario vincular los diferentes controladores en un mobility group para soportar la conexión de los AP's en cualquiera de los controladores, pero la configuración no se replica entre los mismos de forma automática, con lo cual se aplicará la configuración que disponga cada uno de los vWLC.

Recordar de replicar la configuración de forma manual en ambos controladores y guardar la configuración para evitar la pérdida de la misma ante cualquier reinicio no controlado.

Se configura el mobility group: **HA_EPC**.

Controller	*MAC Address*	*IP Address*	*Group Name*	*Hash Key*
vWLC01	00:50:56:80:40:51	172.17.2.100	HA_EPC	ab91a7628cfe1e927f0bcddac96035f71226f512
vWLC02	00:50:56:80:5f:d3	172.17.2.101	HA_EPC	5abbfe3367ca1e473c4079e26b6ef05ec72468c9

Tabla 9 - Configuración vWLC – Mobility Group

5.1.2.2 Interfaces

Para el correcto funcionamiento de todas las redes que se quieran configurar, es necesario definir una serie de interfaces lógicas, las cuales se asociarán posteriormente a los SSID's según vlan.

vWLC01

Interface Name	*VLAN Identifier*	*IP Address*	*Interface Type*	*Dynamic AP Management*
management	172	172.17.2.100	Static	Enabled
service-port	N/A	0.0.0.0	DHCP	Disabled
virtual	N/A	1.1.1.1	Static	Not Support
vlan_220_cheste	220	172.40.0.190	Dynamic	Disabled
vlan_290_cheste	290	172.29.0.90	Dynamic	Disabled
vlan_4_torrente	4	10.1.0.190	Dynamic	Disabled
vlan_5_torrente	5	10.2.0.190	Dynamic	Disabled

Tabla 10 - Configuración vWLC - Interfaces vWLC01

vWLC02

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	172	172.17.2.101	Static	Enabled
service-port	N/A	0.0.0.0	DHCP	Disabled
virtual	N/A	1.1.1.1	Static	Not Support
vlan_220_cheste	220	172.40.0.191	Dynamic	Disabled
vlan_290_cheste	290	172.29.0.91	Dynamic	Disabled
vlan_4_torrente	4	10.1.0.191	Dynamic	Disabled
vlan_5_torrente	5	10.2.0.191	Dynamic	Disabled

Tabla 11 - Configuración vWLC - Interfaces vWLC02

5.1.2.3 SSID's

Se definen diferentes SSIDs según necesidades de cliente con las siguientes particularidades y características:

- EM
    - Red de propósito para uso de dispositivos internos (PDA's, Apple TV, Impresoras…) con acceso a la red interna de todas las sedes e internet sin limitaciones.
        - Seguridad: WPA2 – Auth (AES - PSK)
- EM_LIBRE
    - Red de propósito para uso libre por cualquier empleado o visitante con acceso únicamente a internet y con limitación en la velocidad a 5112 kbps.
        - Seguridad: WPA2 - Auth (AES - PSK)
        - QoS: Override Per-SSID Bandwidth Contracts: 5112 kbps.
- EM_EXTERNOS
    - Red de propósito para uso de personal externo con acceso a internet y a los dispositivos Chromecast para la emisión de contenido a las televisiones del cliente, se restringe el acceso al resto de la red interna del cliente.
        - Seguridad: WPA2 - Auth (AES - PSK)

- EM_OPEN
    - Red de propósito para inicialización de dispositivos Chromecast (únicamente necesario para Cheste), deshabilitado por defecto.
        - Seguridad: None
        - Radio Policy: 802.11b/g only. (Requisito Chromecast)
- EM_USUARIOS
    - Red de propósito para uso por usuarios internos con acceso a la red interna de todas las sedes e internet sin limitaciones con la particularidad de que el acceso de cualquier usuario será identificado a través del ISE mediante autenticación con ISE.
        - Seguridad: 802.1X
        - ISE Configuration:
            - Security → AAA Servers:
                - Authentication Servers: IP:172.17.2.81, Port: 1812
                - Accounting Servers: IP:172.17.2.81, Port: 1813
                - Order for authentication: Radius → Local → LDAP
            - Advanced
                - Allow AAA Override: Enable
                - Enable Session Timeout 1800 secs
                - NAC State: None
                - Radius Client Profiling
                    - DHCP and HTTP: Enable

5.1.2.4 AP Groups

Con el fin de separar la publicación de diferentes SSID's según sede y según VLAN, se definen cuatro principales grupos: Cheste, Torrente (Emiten todas salvo la abierta) y Cheste_with_open y Torrente_with_open (Emiten todas incluida la abierta).

- Cheste

WLAN ID	WLAN SSID	Interface
2	EM	Vlan_290_cheste
3	EM_LIBRE	Vlan_220_cheste
4	EM_EXTERNOS	Vlan_220_cheste
6	EM_USUARIOS	Vlan_290_cheste

Tabla 12 - Configuración vWLC - AP Group Cheste

- Torrente

WLAN ID	WLAN SSID	Interface
2	EM	Vlan_4_torrente
3	EM_LIBRE	Vlan_5_torrente
4	EM_EXTERNOS	Vlan_5_torrente
6	EM_USUARIOS	Vlan_4_torrente

Tabla 13 - Configuración vWLC - AP Group Torrente

- Cheste_with_Open

WLAN ID	WLAN SSID	Interface
2	EM	Vlan_290_cheste
3	EM_LIBRE	Vlan_220_cheste
4	EM_EXTERNOS	Vlan_220_cheste
5	EM_OPEN	Vlan_290_cheste
6	EM_USUARIOS	Vlan_290_cheste

Tabla 14 - Configuración vWLC - AP Group Cheste_with_open

- Torrente_with_Open

WLAN ID	WLAN SSID	Interface
2	EM	Vlan_4_torrente
3	EM_LIBRE	Vlan_5_torrente
4	EM_EXTERNOS	Vlan_5_torrente
5	EM_OPEN	Vlan_4_torrente
6	EM_USUARIOS	Vlan_4_torrente

Tabla 15 - Configuración vWLC - AP Group Torrente_with_open

5.1.2.5 Flexconnect

Esta configuración permite que los AP's puedan descargar la configuración del vWLC según su perfil (flexconnect group) y aplique los mapeos correspondientes según sede, pudiendo funcionar de forma independiente de la conexión al controlador.

Para ello es necesario que los AP's sean configurados en modo Flexconnect, y se habilite al mismo tiempo en los SSID's la opción Flexconnect Local Switching. Además, es necesaria la configuración de los siguientes grupos de flexconnect, donde se definirán los mapeos y restricciones correspondientes según sede.

- Flexconnect Group
  - Cheste
    - WLAN VLAN mapping

WLAN ID	WLAN SSID	VLAN	FIREWALL ZONE (SOPHOS)
2	EM	290	LAN
3	EM_LIBRE	220	WI-FI
4	EM_EXTERNOS	220	WI-FI
5	EM_OPEN	290	LAN
6	EM_USUARIOS	290	LAN

Tabla 16 - Configuración vWLC - WLAN VLAN Mapping Cheste

  - Torrente
    - WLAN VLAN mapping

WLAN ID	WLAN SSID	VLAN	FIREWALL ZONE (SOPHOS)
2	EM	4	LAN
3	EM_LIBRE	5	LAN (Flexconnect ACL)
4	EM_EXTERNOS	5	LAN (Flexconnect ACL)
5	EM_OPEN	4	LAN
6	EM_USUARIOS	4	LAN

Tabla 17 - Configuración vWLC - WLAN VLAN Mapping Torrente

    - AAA VLAN-ACL Mapping

VLAN ID	Ingress ACL	Egress ACL
5	Torrente_Internet	Torrente_Internet
5	Torrente_Internet	Torrente_Internet

Tabla 18 - Configuración vWLC - VLAN ACL Mapping Torrente

- Default-flex-group: Es el grupo donde aparecerán los nuevos AP's conectados a los vWLC, conserva por defecto la configuración de Cheste, convendrá reasignar el AP's después de cada nueva inicialización al grupo que corresponda según sede.

- Flexconnect ACLs

Se define el conjunto de reglas ACL que aplican para el mapeo de la VLAN 5 de Torrente para así limitar el acceso a la red interna y solo permitir el acceso a dispositivos del mismo segmento, así como acceso a internet. Las reglas se validarán de forma secuencial siendo la última de ellas la más permisiva.

- Access List Name: Torrente_Internet
- ACL's

Seq	Action	Source	Destination	Protocol	Source Port	DSCP
1	Permit	0.0.0.0/0	10.2.0.0/24	Any	Any	Any
2	Deny	0.0.0.0/0	10.0.0.0/8	Any	Any	Any
3	Deny	0.0.0.0/0	172.16.0.0/20	Any	Any	Any
4	Deny	0.0.0.0/0	192.168.0.0/16	Any	Any	Any
5	Deny	0.0.0.0/0	1.0.0.0/24	Any	Any	Any
6	Deny	0.0.0.0/0	2.0.0.0/24	Any	Any	Any
7	Deny	0.0.0.0/0	3.0.0.0/24	Any	Any	Any
8	Deny	0.0.0.0/0	172.40.0.0/24	Any	Any	Any
9	Deny	0.0.0.0/0	172.45.0.0/24	Any	Any	Any
10	Deny	0.0.0.0/0	172.46.0.0/24	Any	Any	Any
11	Deny	0.0.0.0/0	172.60.0.0/24	Any	Any	Any
12	Permit	0.0.0.0/0	0.0.0.0/0	Any	Any	Any

Tabla 19 - Configuración vWLC - Flexconnect ACL Torrente

5.1.2.6 DHCP

Para la asignación de IP's por DHCP a la interfaz de gestión de los AP's y a los diferentes dispositivos conectados a los SSID's configurados, se realizarán peticiones a los ámbitos definidos en los servidores de DHCP de cheste: **172.26.0.200** y **172.26.0.201**.

Como excepción, los AP's situados en torrente, obtendrán la IP de gestión directamente del servidor de DHCP de dicha sede **1.0.0.250**, debido a la necesidad de propagación de la **opción 43**, para asociación con los vWLC de la sede de Cheste.

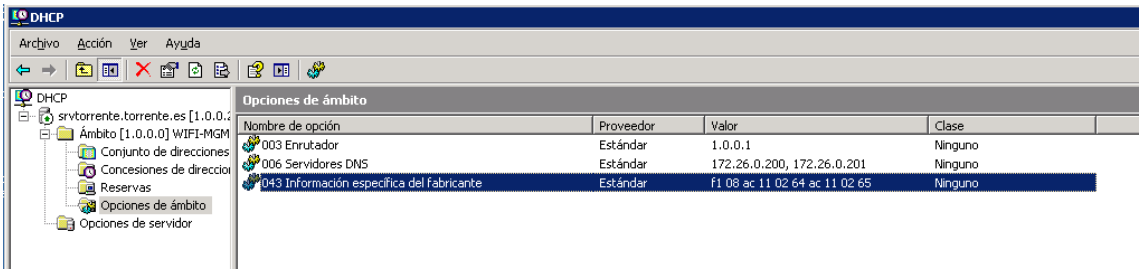


Ilustración 12 - Configuración vWLC - DHCP

5.1.2.7 ISE integration (Radius)

Se configura en los vWLC la conexión al ISE para el registro e identificación de usuarios por Active Directory. Para ello se añade como servidor de autenticación y autorización de conexión al servidor de ISE (el cual se integra con AD) en ambos vWLC mediante el uso del protocolo Radius.

- Security → AAA → Radius → Autentication
    - Server Adress: 172.17.2.81
    - Shared Secret Format: ASCII
    - Shared Secret: Definida en ISE
    - Port Number: 1812

- Security → AAA → Radius → Accounting
    - Server Adress: 172.17.2.81
    - Shared Secret Format: ASCII
    - Shared Secret: Definida en ISE
    - Port Number: 1812

5.2 Cisco Prime Infraestructure

Cisco Prime es la utilidad de Cisco que se encargará de aportar una visión y una gestión centralizada de todos los dispositivos Cisco de la infraestructura tanto de Cheste como de Torrente y Buñol, pudiendo así tener una visión global del estado de la infraestructura, así como la posibilidad de realizar la configuración y administración de los distintos dispositivos de red.

5.2.1 Configuración básica

5.2.1.1 Dashboard

Se ha personalizado un dashboard para la visualización de datos sobre el estado general de la infraestructura denominado EM.

El acceso al mismo se realizará a través de la URL: https://172.17.1.100/webacs/welcomeAction.do.

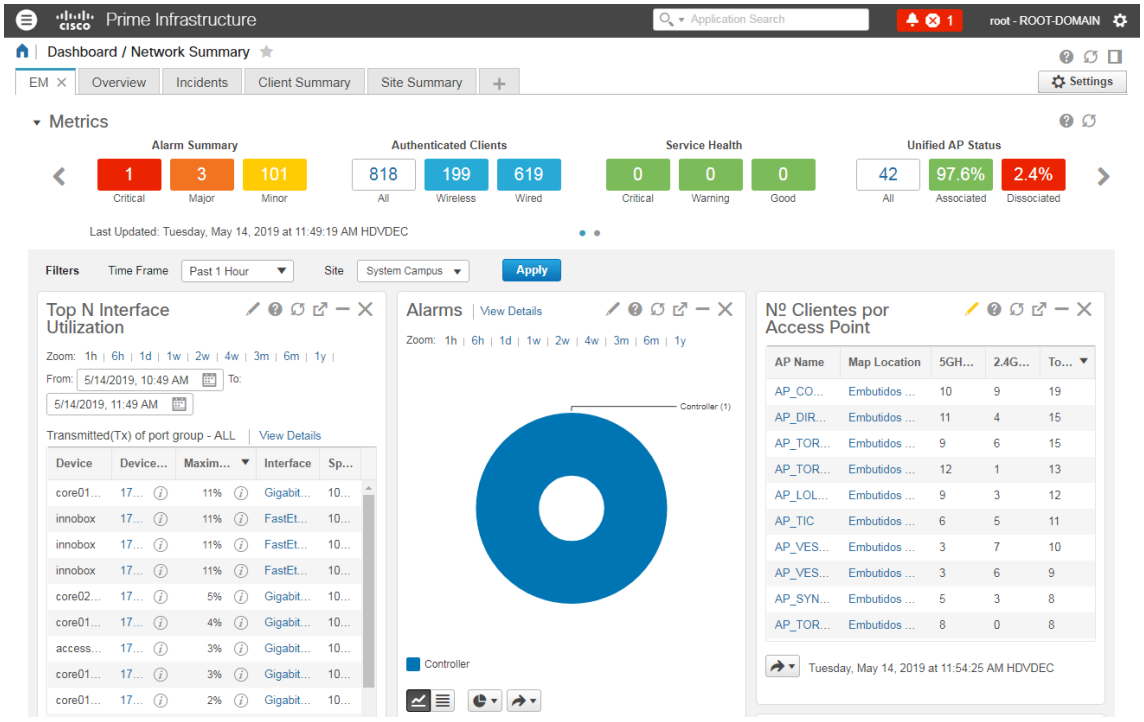


Ilustración 13 - Dashboard Cisco Prime Infraestructure

Adicionalmente, existe otro dashboard especialmente interesante y útil para visualización de clientes conectados y autenticados en la infraestructura tanto por Wi-Fi como por cable a través de switches o routers:

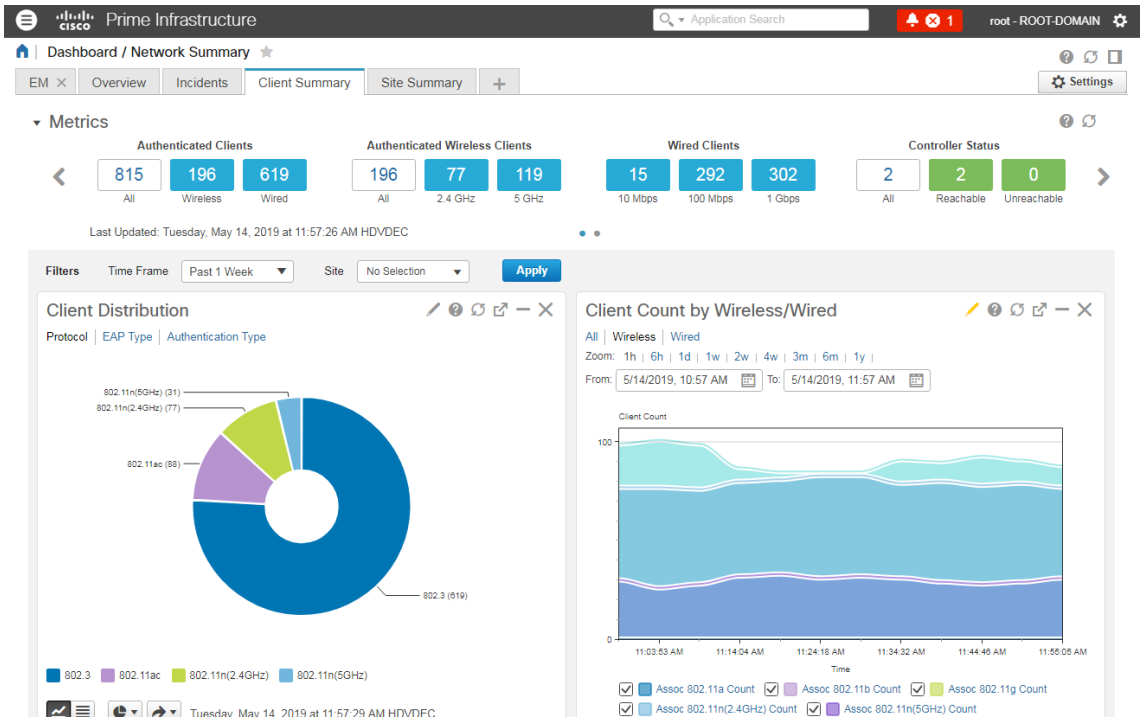


Ilustración 14 - Dashboard de clientes - Cisco Prime

Así mismo, para que la sesión perdure y no se cierre de forma automática vencido un tiempo de timeout, se han desactivado los parámetros de configuración general de sistema referentes al “Global Idle Timeout”.

5.2.1.2 Credenciales de acceso

Se acuerda con cliente las credenciales de acceso SSH para usuario admin, y para acceso WEB con el usuario root.

5.2.1.3 NTP y SMTP

- NTP:

  Se configura NTP para el servidor externo **hora.roa.es** (150.214.94.5).

- SMTP:

  Se define para el envío de correo desde Cisco Prime la siguiente configuración:

Servidor de correo	*Username*	*From*	*To*	*Subject*
172.26.0.149	envio@epc.net	envio@epc.net	sistemas@epc.es	CISCO PRIME

Tabla 20 - Configuración SMTP Cisco Prime

5.2.1.4 Licencias

Se añade licenciamiento para los siguientes dispositivos registrados:

Dev Family	Subtype	Device Count	Tokens per device	Token Count
Switches and Hubs	Cisco Catalyst 2960-24TT Switch	4	1	4
Switches and Hubs	Cisco Catalyst 2960-48TT Switch	3	1	3
Switches and Hubs	Cisco Catalyst 3560-48PS Switch	1	1	1
Switches and Hubs	Cisco Catalyst 3560V2-24PS Switch	1	1	1
Switches and Hubs	Cisco Catalyst 2960-24TC-S Switch	1	1	1
Switches and Hubs	Cisco 3750 Stackable Switches	6	1	9
Switches and Hubs	Cisco Catalyst 2960-Plus 24PC-S Switch	1	1	1
Unified AP	Cisco 1600E Unified Access Point	3	1	3
Unified AP	Cisco 1700I Unified Access Point	28	1	28
Unified AP	Cisco 1600I Unified Access Point	7	1	7

Tabla 21 - Configuración Licencias Cisco Prime

5.2.2 Configuración avanzada

5.2.2.1 Inventario

Se dan de alta en Cisco Prime los siguientes dispositivos de red de la infraestructura:

Device	IP	Model	Firmware
3560_cheste	172.17.1.20	Cisco Catalyst 3560V2-24PS Switch	12.2(55)SE8
access01-cheste	172.17.1.5	Cisco 3750 Stackable Switches	12.2(55)SE11
cheste	172.17.1.3	Cisco Catalyst 2960-48TT Switch	12.2(35)SE5
cheste2	172.17.1.4	Cisco Catalyst 2960-48TT Switch	12.2(50)SE5
core01-cheste	172.17.1.252	Cisco 3750 Stackable Switches	12.2(55)SE11
core01-torrente	1.0.0.252	Cisco 3750 Stackable Switches	12.2(55)SE11
core02-cheste	172.17.1.253	Cisco 3750 Stackable Switches	12.2(55)SE11
core02-torrente	1.0.0.253	Cisco 3750 Stackable Switches	12.2(55)SE11
innobox	172.17.1.13	Cisco Catalyst 2960-24TT Switch	12.2(35)SE5
oficina	172.17.1.8	Cisco Catalyst 2960-24TT Switch	12.2(44)SE6
oficina2	172.17.1.9	Cisco Catalyst 2960-24TT Switch	12.2(50)SE5
rrhh	172.17.1.10	Cisco Catalyst 2960-24TT Switch	12.2(50)SE4
rrhh2	172.17.1.11	Cisco Catalyst 2960-24TC-S Switch	12.2(37)EY
SRV-WLC-01	172.17.2.100	Cisco Virtual Wireless LAN Controller	8.4.100.0
SRV-WLC-02	172.17.2.101	Cisco Virtual Wireless LAN Controller	8.4.100.0

switch_3750	1.0.0.3	Cisco 3750 Stackable Switches	12.2(55)SE8
switch_bunol	192.168.11.1	Cisco Catalyst 3560-48PS Switch	12.2(35)SE5
techo	172.17.1.7	Cisco Catalyst 2960-48TT Switch	12.2(50)SE5
thinking_area	172.17.1.12	Cisco Catalyst 2960-Plus 24PC-S Switch	15.0(2)SE6

Tabla 22 - Configuración Inventario Cisco Prime

Para simplificar el alta de los mismos, se han creado los siguientes perfiles de contraseñas y especificaciones:

- Ap's Standalone (únicamente empleado para la migración de AP's autónomos)
- Switches Capa 2
- Switches Capa 3

5.2.2.2 Templates AP's

Se crean plantillas para la configuración simplificada y automatizada de nuevos AP's. Los parámetros definidos según sede quedan de la siguiente forma:

→ APs Cheste:

- General
  - Location: Cheste
  - Admin Status: Enable
  - AP Mode: FlexConnect
  - Country Code: ES- Spain
  - CDP: Enable
  - AP Led Status: Enable
  - AP Group Name: Cheste
- Controllers Configuration
  - Primary Controller Name: SRV-WLC-01
  - Secondary Controller Name: SRV-WLC-02
  - Primary Controller IP Address: 172.17.2.100
  - Secondary Controller IP Address: 172.17.2.101
- Flexconnect Configuration

- VLAN Support: Enable
- Native VLAN ID: 172
- WLAN VLAN Mapping
  - EM-vWLC1 → 290
  - EM-vWLC2 → 290
  - EXTERNOS-vWLC1 → 220
  - EXTERNOS-vWLC2 → 220
  - LIBRE-vWLC1 → 220
  - LIBRE-vWLC2 → 220
  - EM_USUARIOS-vWLC1 → 290
  - EM_USUARIOS-vWLC2 → 290

→ APs Torrente:

- General
  - Location: Torrente
  - Admin Status: Enable
  - AP Mode: FlexConnect
  - Country Code: ES- Spain
  - CDP: Enable
  - AP Led Status: Enable
  - AP Group Name: Torrente
- Controllers Configuration
  - Primary Controller Name: SRV-WLC-01
  - Secondary Controller Name: SRV-WLC-02
  - Primary Controller IP Address: 172.17.2.100
  - Secondary Controller IP Address: 172.17.2.101
- Flexconnect Configuration
  - VLAN Support: Enable
  - Native VLAN ID: 1
  - WLAN VLAN Mapping
    - EM-vWLC1 → 4
    - EM-vWLC2 → 4

- EXTERNOS-vWLC1 → 5
- EXTERNOS-vWLC2 → 5
- LIBRE-vWLC1 → 5
- LIBRE-vWLC2 → 5
- EM_USUARIOS-vWLC1 → 4
- EM_USUARIOS-vWLC2 → 4

Una vez configuradas dichas plantillas, tendremos posibilidad de desplegarlas y programar su despliegue según corresponda su ubicación una vez estas sean visibles en la red desde el apartado *Configuration / Templates / Lightweight Access Points*:

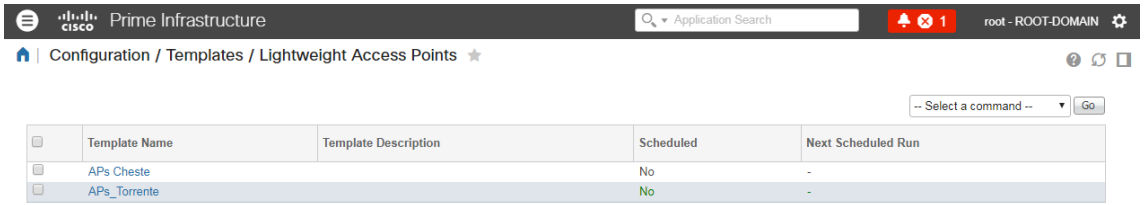


Ilustración 15 - Plantillas configuración AP's - Cisco Prime

Al seleccionar cualquiera de ellas, por defecto ya veremos la configuración precargada sobre la plantilla:

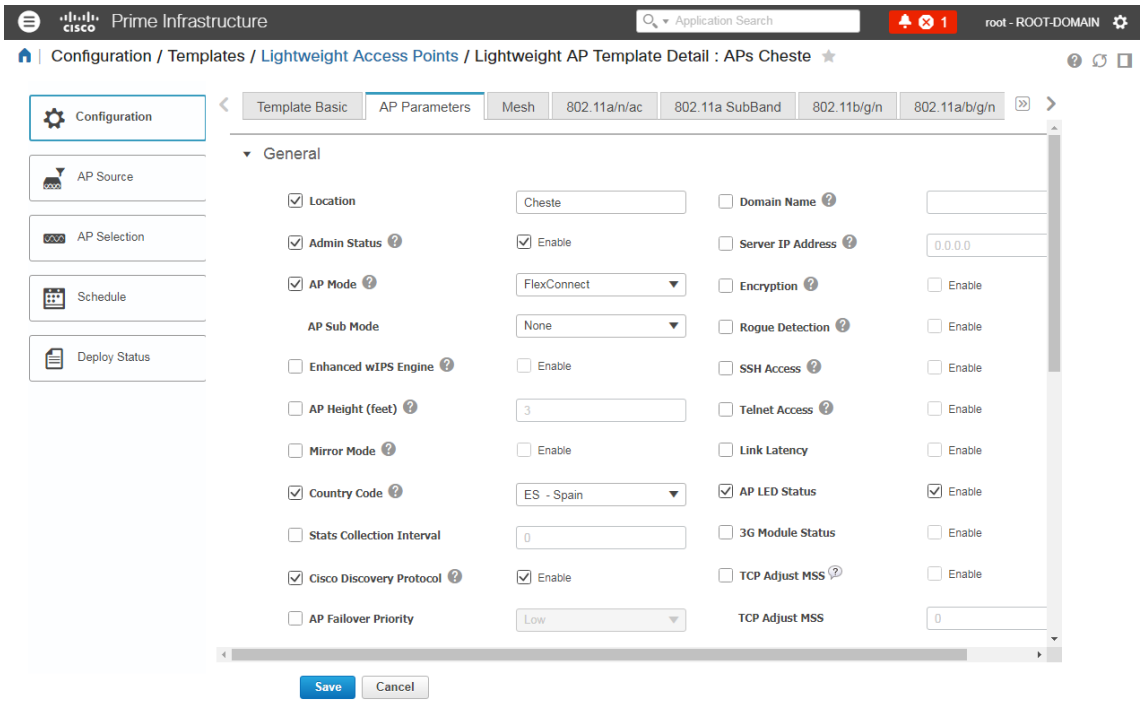


Ilustración 16 - Configuración Plantillas - Cisco Prime

Por lo que únicamente será necesario seleccionar los AP's sobre los cuales desplegar la configuración y planificar el despliegue de la plantilla según el horario que interese o inclusive de forma inmediata.

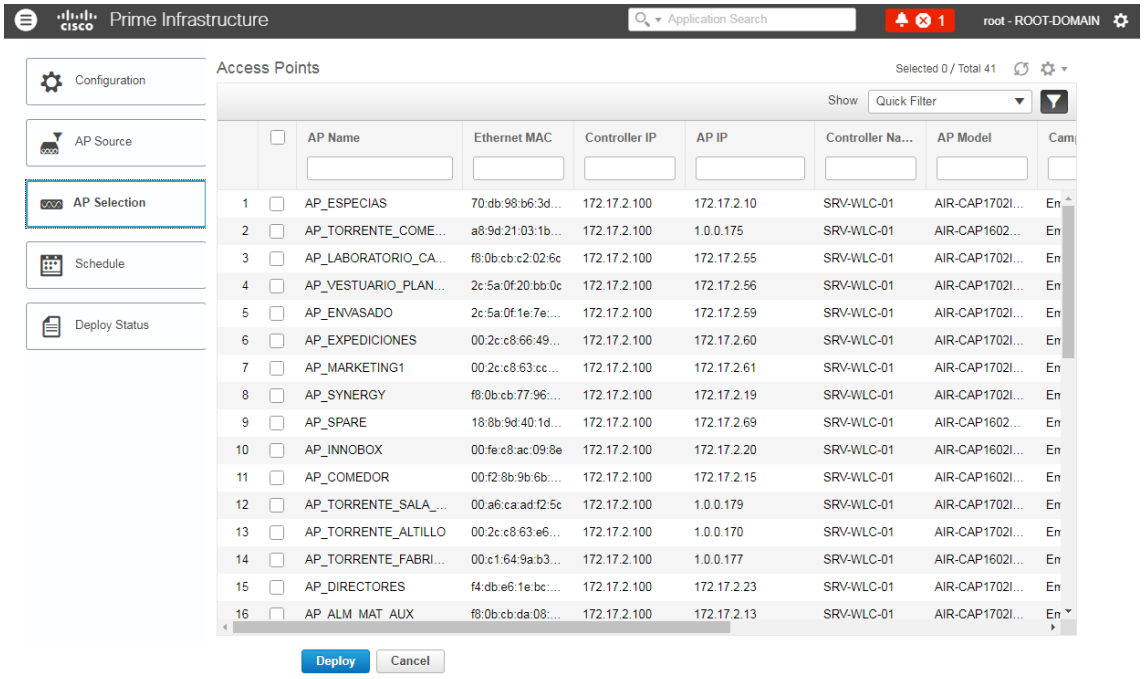


Ilustración 17 - Despliegue de plantillas - Cisco Prime

5.2.2.3 Configuración Jobs Backup

Se configura una tarea de backup dedicada para el respaldo diario de todos los dispositivos inventariados en Cisco Prime.

Dicha tarea se ejecutará todas las noches a las 22 h y se mantendrá hasta un máximo de 14 archivos de configuración por dispositivo o en su defecto hasta un máximo de 14 días.

No será necesaria la modificación de dicha tarea ante alta de nuevos dispositivos.

Además, se configura y se parametriza el prime para realizar un autoguardado de la configuración cuando se detecten cambios en los dispositivos conectados, para ello, en el switch se requiere la adición y ejecución del comando:

```
logging 172.17.1.100
```

Posteriormente, ajustaremos el valor de Hold Off timer en "*Admininistration / Settings /system Settings / Inventory / configuration Archive*" a 1 minuto para reducir el tiempo de espera que Cisco Prime respetará para detectar los cambios realizados y guardar la configuración.

5.2.2.4 Mapas

Se importan los mapas para poder situar los AP's de las sedes de Cheste y Torrente.

Cheste P0 – Contiene todos los AP's situados en la planta cero de la sede de Cheste.

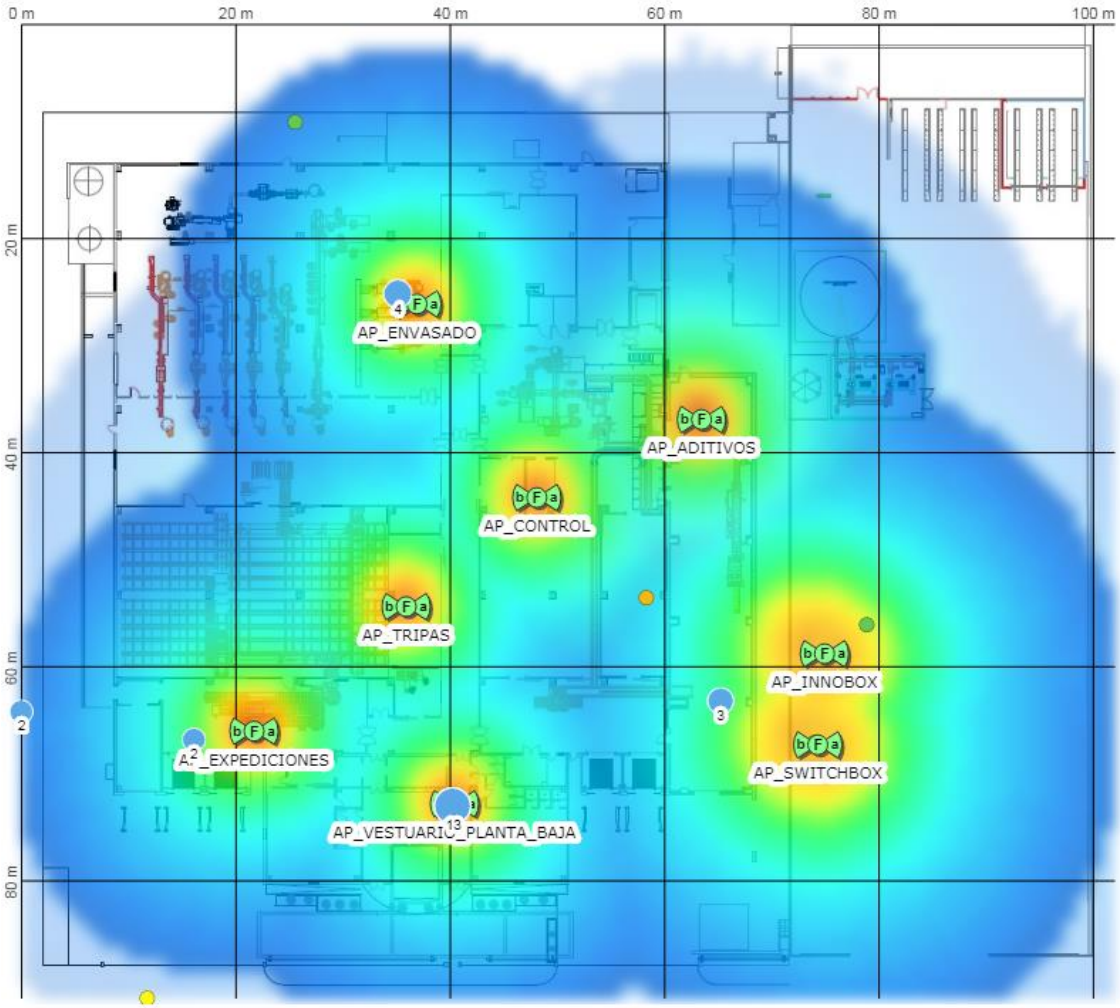


Ilustración 18 - Configuración Mapa Cheste P0 - Cisco Prime

Cheste P1 y P2 – Contiene todos los AP's situados en la planta uno de la sede de Cheste y también de la entreplanta.

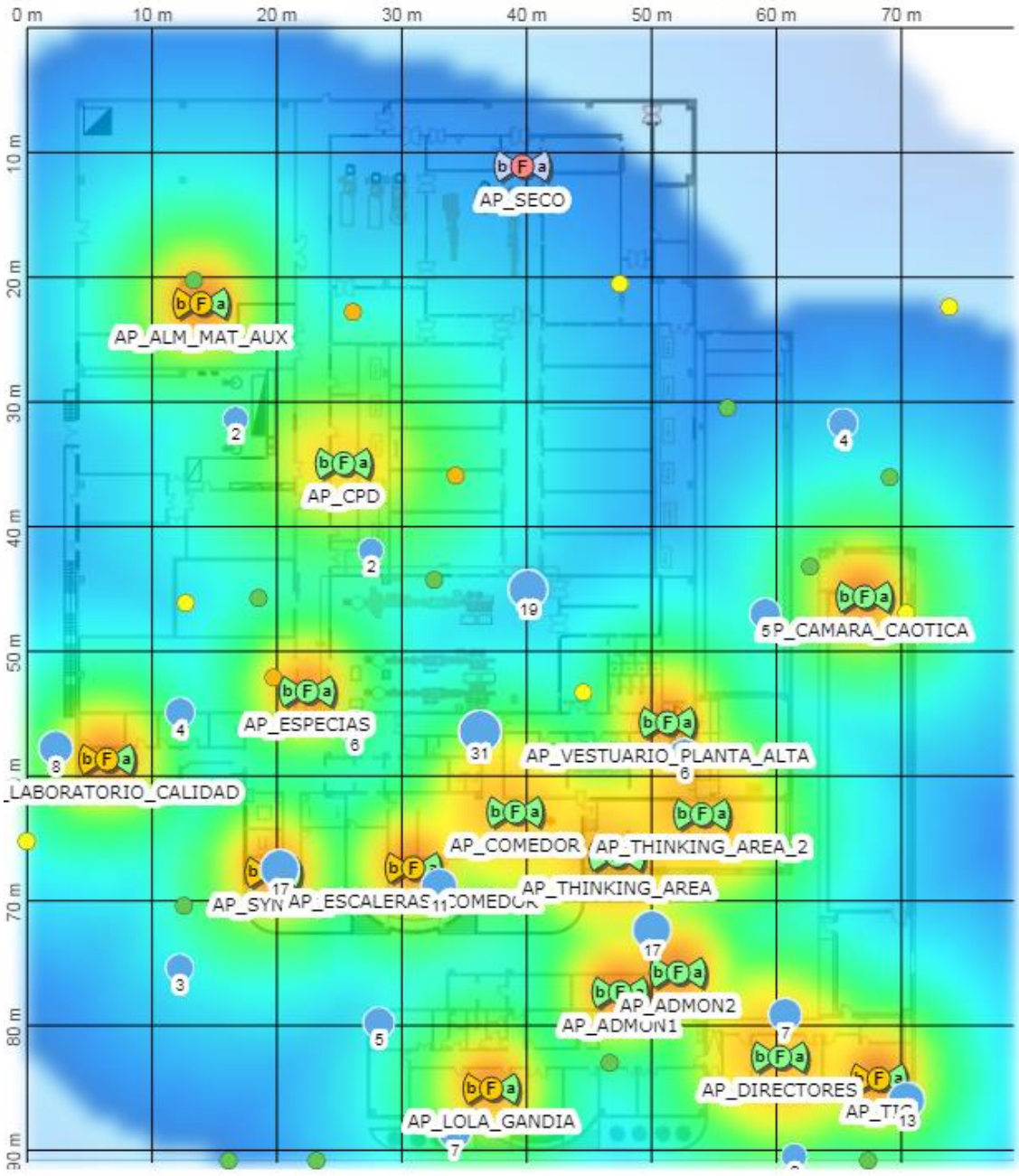


Ilustración 19 - Configuración Mapa Cheste P1 y P2 - Cisco Prime

Torrente P0 – Contiene todos los AP's situados en la planta cero de la sede de Torrente.

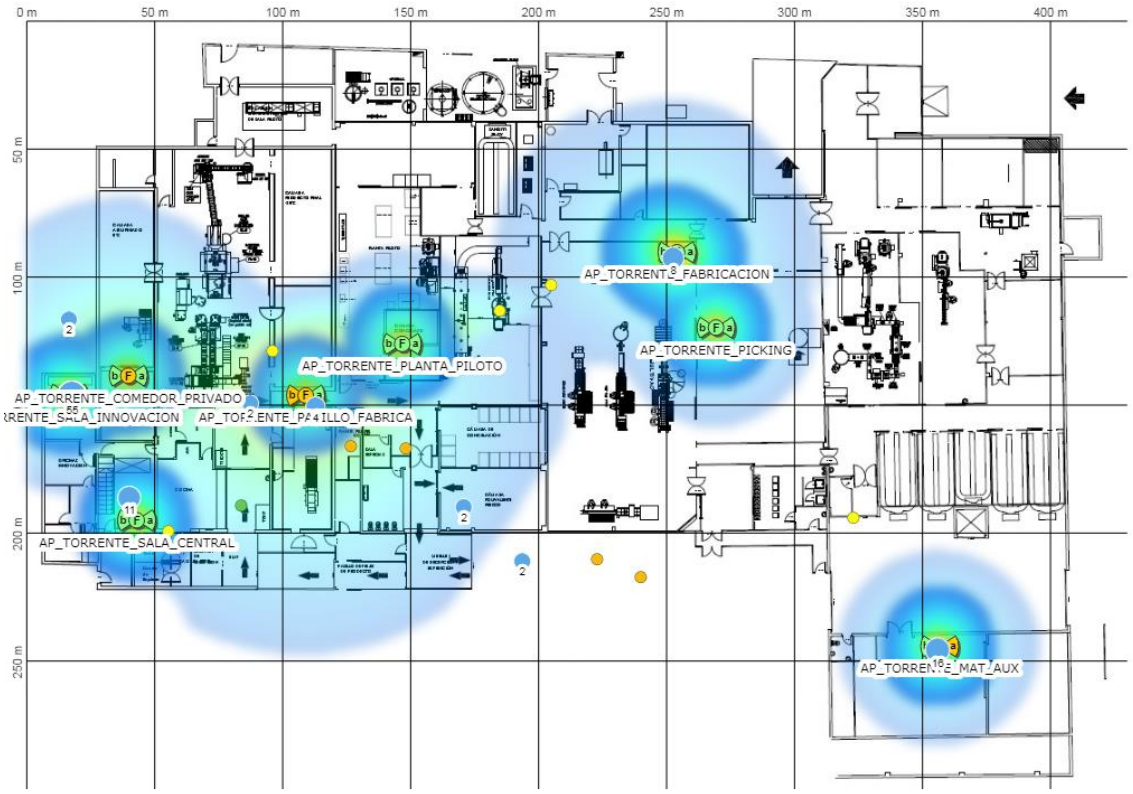


Ilustración 20 - Configuración Mapa Torrente P0 - Cisco Prime

Torrente P1 – Contiene todos los AP's situados en la planta uno de la sede de Torrente.

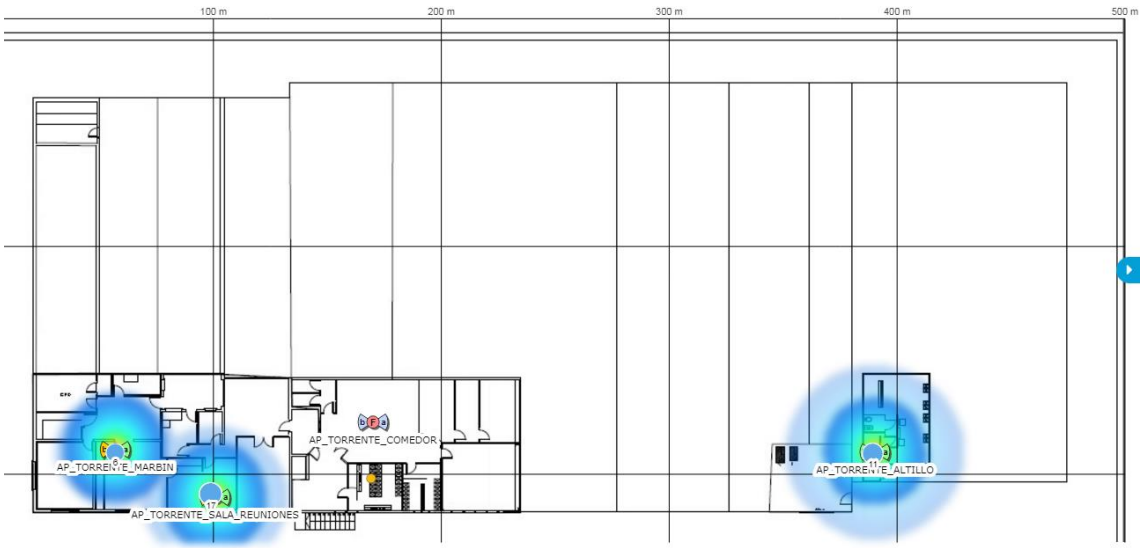


Ilustración 21 - Configuración Mapa Torrente P1 - Cisco Prime

5.2.2.5 Políticas de notificación

Se configuran las siguientes políticas de notificación para recibir alertas por correo ante la producción de ciertas alarmas.

- AP Apagado
    - Se notificará cuando el estado de un AP que está en producción se desasocie del vWLC o cambie de estado alguna interfaz del dispositivo. En concreto se generarán notificaciones cuando:
        - AP Ethernet interface down
        - AP disassociated from controller
        - AP has no radios
        - AP radio interface down due to failure
        - Autonomous AP Admin Status Down
        - Autonomous AP Link Down
        - Flexconnect AP disassociated from controller but reachable by ping
        - Invalid radio
        - POE status
        - Radio administratively up and operationally down
- Config Changed
    - Producirá alertas cuando se modifique cualquier configuración sobre cualquier dispositivo inventariado en Cisco Prime y modificado desde el mismo. En concreto se notificará ante la producción de las siguientes alarmas:
        - Config Archive : Device Config Changed
        - Config Change from Prime Infrastructure
        - Configuration Archive
        - Configuration not in Sync

5.2.2.6 Integración ISE

Se integra el servidor ISE en Cisco Prime para sincronización de información.

- Server Adress: 172.17.2.81
- Port: 443
- Username: Admin
- Password: (convenido con cliente)

5.3 CMX

El CMX (Connected Mobile Experience) es el encargado de detectar, registrar y analizar todas las señales detectadas desde los puntos de acceso, así como mantener información sobre los clientes asociados a ellos y los no asociados. Además de ser analizada en tiempo real, además permite la visualización y generación de reportes en informes según restricciones de horarios o ubicación.

Mostramos a continuación los principales dashboard con información sobre la infraestructura que nos ofrece Cisco CMX:

- Dashboard principal con información de usuarios/dispositivos detectados por día y tiempo de actividad:

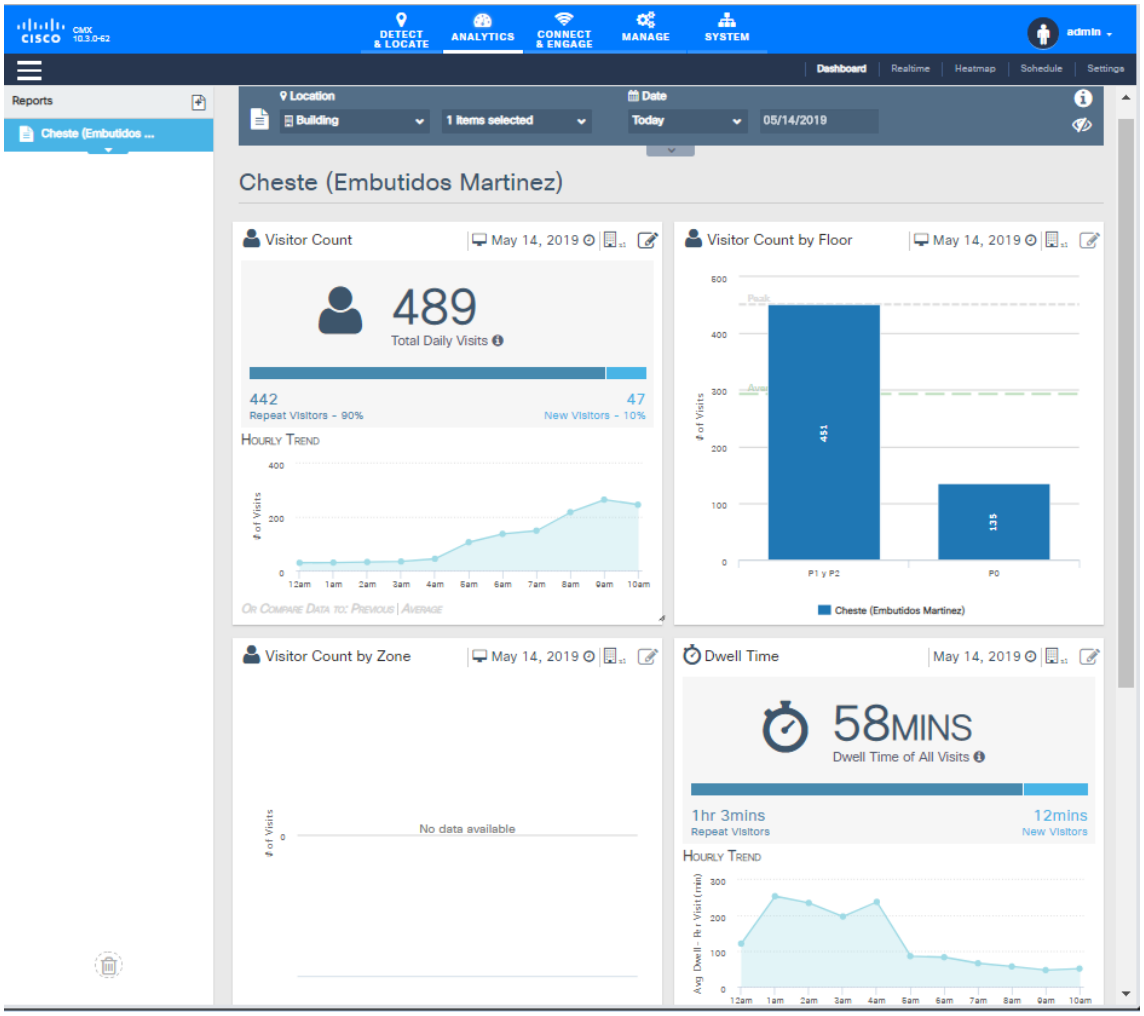


Ilustración 22 - Dashboard CMX

- Mapa de calor según actividad:

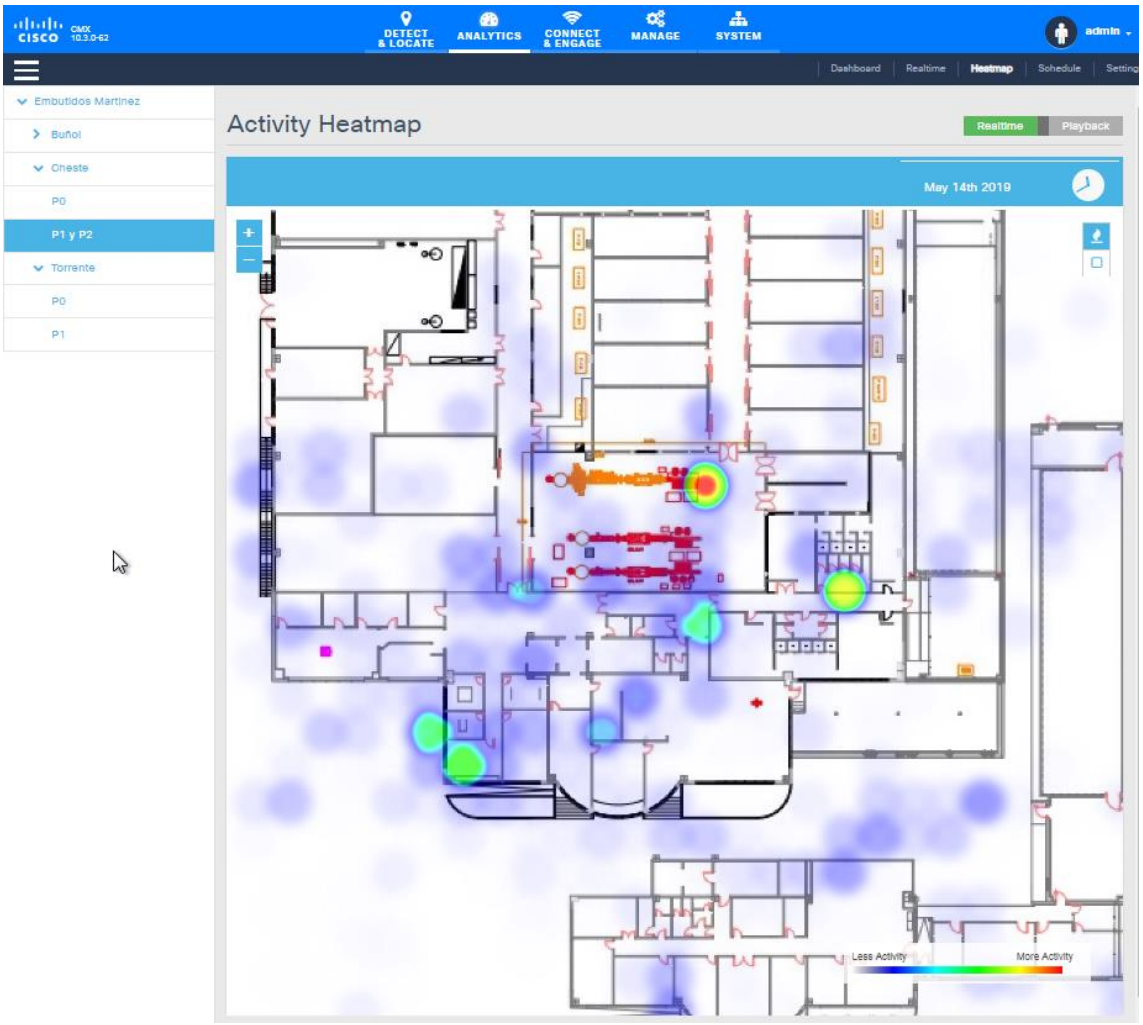


Ilustración 23 - Mapa de calor - Cisco CMX

5.3.1 Configuración básica

5.3.1.1 Portal de acceso

Para acceder a la gestión de la herramienta web CMX, será necesario entrar en la URL: https://172.17.2.80/login/

5.3.1.2 Credenciales de acceso

Se acuerda con cliente las credenciales de acceso **SSH** para usuario **cmxadmin**, y para acceso **WEB** con el usuario **admin**.

5.3.1.3 NTP

- NTP:

  Se configura NTP para el servidor externo **hora.roa.es** (150.214.94.5).

5.3.2 Configuración avanzada

5.3.2.1 Gestión de mapas

La importación de los mapas debe realizarse cada vez que se sitúe un nuevo AP en cisco prime o se realice la modificación sobre alguno ya previamente situado.

Desde Cisco se recomienda la exportación e importación de los mapas directamente desde Cisco Prime (Services / Mobility Services / Connected Mobile Experiences)

5.3.2.2 vWLC

CMX requiere de conexión con los vWLC para la detección de los clientes por los AP's asociados en él. Es por ello que se registran en el CMX empleando la Read and Write community v2c definida en los vWLC.

5.4 ISE

El ISE (Identity Service Engine) es el encargado de identificar y obtener información sobre los clientes asociados al SSID: EM_USUARIOS mediante autenticación 802.1X. Para ello se integra dicha plataforma con el AD de la organización. Además, también es capaz de detectar dispositivos presentes pero no conectados a la red y registrar la MAC e IP de los dispositivos finales conectados a los vWLC.

El dashboard principal nos ofrece la siguiente información general de los dispositivos y los registros de inicios de sesión:

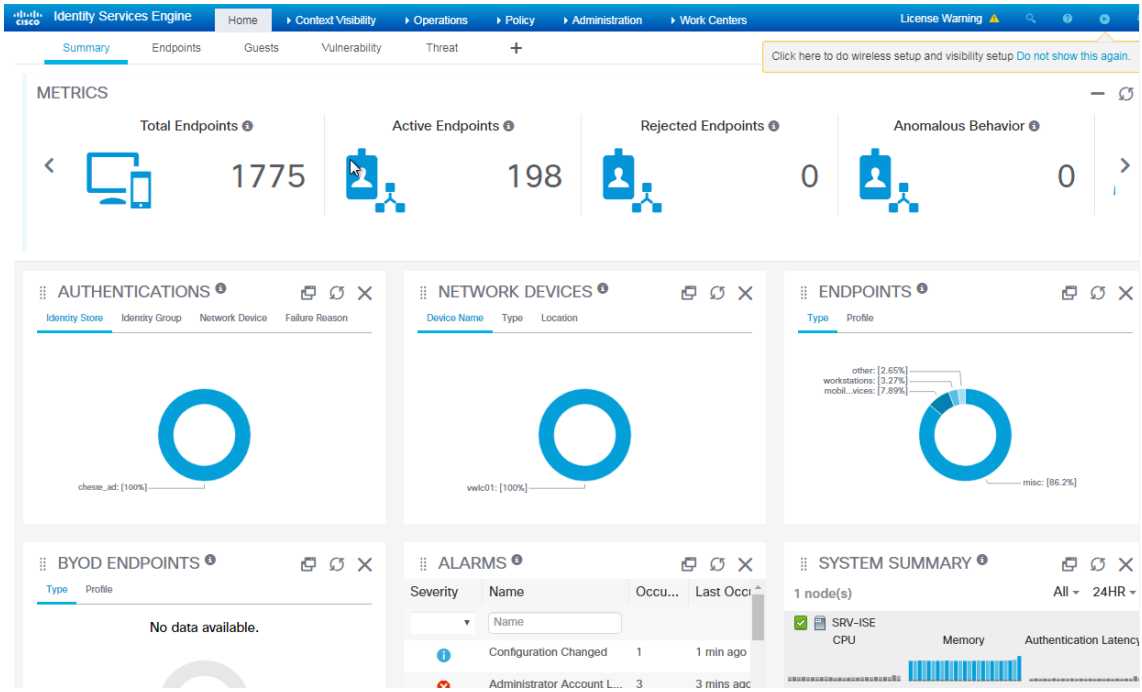


Ilustración 24 - Dashboard Cisco ISE

5.4.1 Configuración básica

5.4.1.1 Portal de acceso

Para acceder a la gestión de la herramienta web Identity, será necesario entrar en la URL: https://172.17.2.81

5.4.1.2 Credenciales de acceso

Se acuerda con cliente las credenciales de acceso para acceso **WEB** con el usuario **admin**.

5.4.1.3 NTP

- NTP:

  Se configura NTP para el servidor externo **hora.roa.es** (150.214.94.5).

5.4.2 Configuración avanzada

5.4.2.1 Integración con AD

Para la correcta autenticación con el Dominio de central Cheste, se requiere la configuración e integración de Active Directory como fuente externa de indentidad en el vWLC.

- Join Point Name: CHESTE_AD
- Active Directory Domain: CENTRALC.EPC.ES

5.4.2.2 vWLC (Radius)

Identity requiere de conexión con los vWLC para la detección de los clientes que utilicen 802.1X como método de autenticación. Es por ello que se dan de alta los vWLC con la siguiente configuración:

vWLC01/vWLC02

- Device Profile: Cisco
- IP: 172.17.2.100/32 (vWLC01)
- IP: 172.17.2.101/32 (vWLC02)
- Radius Authentication Settings
  - UDP Settings
    - Shared Secret: XXXX (Contraseña convenida con cliente)
    - CoA Port: 1700
- SNMP Settings
  - SNMP Version: 2c
  - SNMP RO Community: Lembutid0s

5.4.2.3 Políticas de autorización y autenticación

ISE implementa adicionalmente ciertas reglas para permitir los accesos de cualquier dispositivo en dos fases, primero requiere la fase de autenticación que consiste en validar que el usuario que intenta conectarse lo hace con sus credenciales correctas y su cuenta existe y no está deshabilitada en AD. Una vez superada esta fase existen políticas de autorización para denegar el acceso a la red y redirigir al usuario a un portal web específico si se precisa. Para ello se evalúan una serie de condiciones que se deberán superar de forma automática en cada intento de inicio de sesión.

Dado los requisitos actuales para la organización en los que únicamente se requiere la identificación de los dispositivos conectados a la red Wi-Fi por usuario y contraseña de AD, la configuración de las políticas se define de forma lo más permisiva posible, siempre y cuando se cumplan los requisitos mínimos de seguridad.

- Políticas de Autenticación:

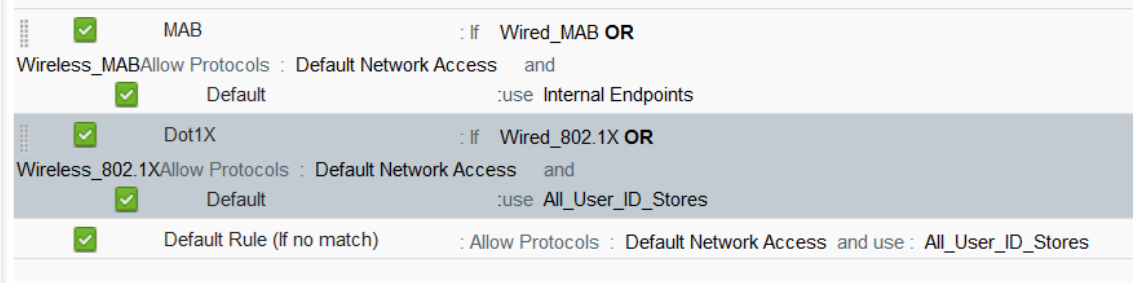


Ilustración 25 - Configuración políticas de autenticación – ISE

- Políticas de Autorización:

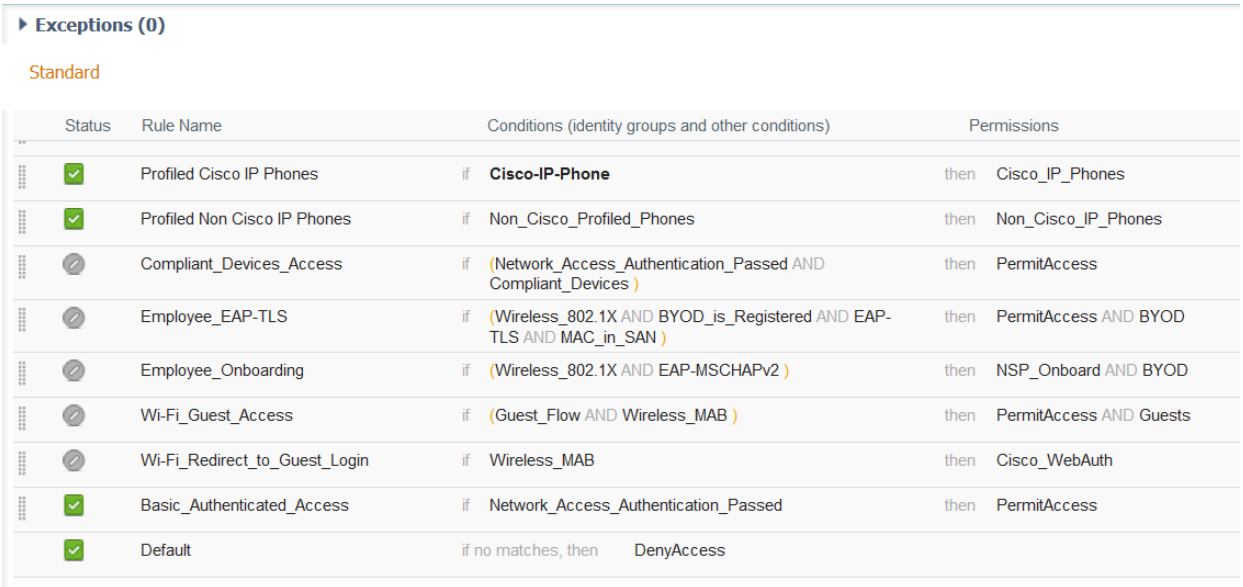


Ilustración 26 - Configuración políticas de autorización - ISE

5.5 Configuración Netflow

Con el fin de monitorizar con mayor precisión el flujo de datos en la red, teniendo en cuenta que Netflow es un protocolo de red propietario de Cisco para el análisis de información en los flujos de comunicación IP de la red, se valora la activación de netwflow en la infraestructura aprovechando que los dispositivos instalados y adquiridos son Cisco.

Para validar que dispositivos son actualmente compatibles con Netflow, se consulta la *Support Matrix* de Netflow para dispositivos Cisco [26] , siendo que los switches de la organización no son compatibles con la funcionalidad requerida:

- Cisco Catalyst 3750G-48PS
- Cisco Catalyst 2960-24TT
- Cisco Catalyst 3560-48PS

No obstante, se verifica que el firewall Sophos XG 330 de la organización si soporta la exportación de datos de Netflow a otros servidores de Netflow [27], por lo que configura el envío de dichas métricas al servidor de monitorización PRTG para el análisis de la información de red.

- Configuración en Sophos firewall:

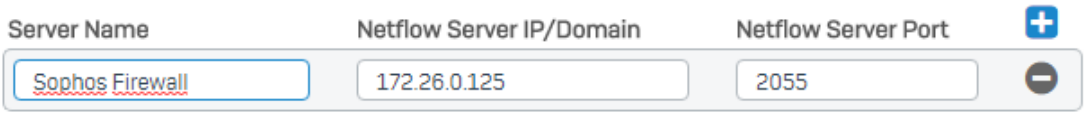


Ilustración 27 - Netflow Sophos XG 330

Además de la configuración del servidor netflow, Sophos requiere la activación de "Log Firewall Traffic" en aquellas reglas de firewall donde se requiere monitorización de tipo netflow. Con lo que se activa dicho parámetro en las siguientes reglas:

- LAN (CLIENTLESS) -> WAN[ID : 9]
- LAN (VIP) -> WAN[ID : 22]
- LAN (TIC-USERS) -> WAN[ID : 11]
- LAN (USERS) -> WAN[ID : 8]
- LAN -> WAN[ID : 1]

- VPN -> ALL VLANS[ID : 5]
- VPN -> VLAN1 & VLAN200[ID : 6]
- VPN -> VLAN1 Y BUÑOL[ID : 7]
- VPN -> VLAN1 Y TORRENTE[ID : 30]

- Configuración en servidor PRTG
  - Se configura un device para definir el objeto Firewall y sobre él se define un sensor de tipo netflow v5, que estará escuchando en el puerto 2055.

A partir de este momento, es posible consultar en el servidor de monitorización PRTG todo el tráfico y las conexiones que atraviesan las reglas con Netflow activas en el firewall para hacer *troubleshooting* cuando se generen incidencias en la red, especialmente problemas de rendimiento o sobrecarga de la red.

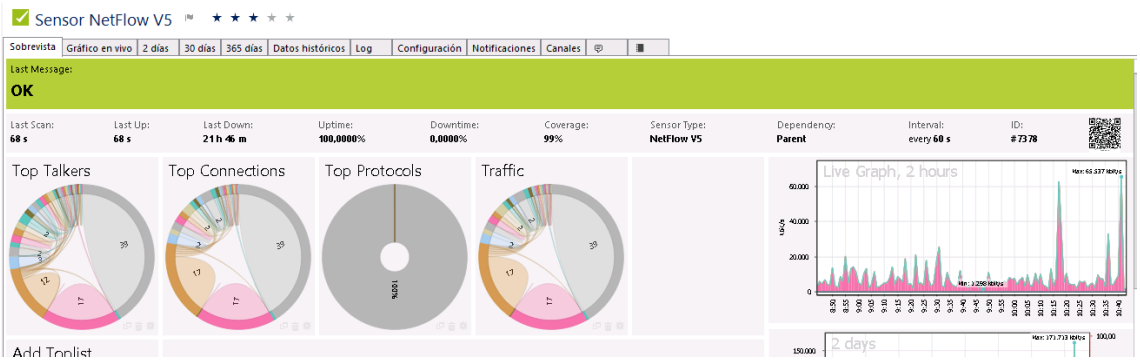


Ilustración 28 - Graficas Netflow - PRTG

5.6 Configuración interfaces switch para AP's

Aquellos puertos de los switches que formar parte de la red de la organización donde se quiera conectar un AP requiere de una configuración especial para el correcto funcionamiento del mismo.

Se deberá configurar/especificar:

- Establecer puerto en modo trunk.
- Especificar la vlan nativa para trunk según sede.
  - VLAN 1 para Torrente, VLAN 172 para Cheste.

- Habilitar spanning-tree portfast trunk.

5.7 Configuración Cisco Prime para migración de los AP's Autónomos

Para la migración de los AP's autónomos se han configurado plantillas para dispositivos de la gama 1600 y 1700 de Cisco (*ver apartado 5.2.2.2*).

En los mismos se ha habilitado el soporte para DHCP, se han especificado los valores según del controlador principal (172.17.2.100), y se ha especificado el fichero de firmware adecuado según versión light-weight según el modelo de AP (*ap1g2-k9w8-tar.153-3.JF.tar o ap3g2-k9w8-tar.153-3.JF.tar*) que previamente se ha dejado subido al servidor TFTP de la organización.

Con ello, se ha realizado una tarea programada para el upgrade de firmware de dichos AP's de su versión actual (AP autónomo) a (AP ligero), y posteriormente se ha programado el despliegue de su configuración de forma automática gracias a las plantillas configuradas según su ubicación.

6. Incidencias

6.1 Análisis incidencia con dispositivos Apple:

Tras la fase del proceso de implementación, la organización nos traslada que existen dos problemáticas con los dispositivos Apple de la compañía:

- Los móviles y portátiles no realizan correctamente los inicios de sesión en la red y toleran bien los cambios de lugar por el edificio por problemas con el Roaming.
- Algunos Apple TV de la sede de Cheste se desconectan pasados unos minutos de uso (especialmente frecuente con la herramienta Airparrot para Windows, no de la misma manera con Airplay en Apple). Los Apple TV de Torrente no experimentan desconexiones. Otros dispositivos similares como Google ChromeCast no experimentan tampoco este tipo de problemas.
    - Versión Apple TV: 11.2
    - Versión Airparrot: 2.7.4.369

Es por ello que se realiza un análisis de la problemática para identificar y corregir los fallos detectados.

Siguiendo la documentación de referencia de cisco al respecto (RF Design Recommendations for Apple Devices on Cisco WLAN [26]), se separa el análisis en diferentes bloques.
Además, se consultan para la resolución de las incidencias las siguientes fuentes de información:

- Compatibilidad de iOS con QoS Fastlane y Adaptive 802.11r de Cisco [27]
- Release notes Airparrot2 para Windows [28]

Monitorización

1. The use of 802.11a/n/ac 5GHz based design for all Apple devices
2. Optimal Cell edge recommendation for Apple Devices is -67 dBm or better (-65 dBm is better for typical high density enterprise deployments). An optimal

WLAN deployment will require minimum of 2 APs in 5 GHz at -67 dBm as measured by the Apple client

3. Average Channel Utilization should be less than 40%
4. Maintain a minimum Signal to Noise Ratio (SNR) of 25 dB
5. 802.11 retransmissions should be kept under 15%
6. Packet Loss should remain under 1 percent and jitter should be kept to less than 100 ms
7. Cisco recommends that at all times an Apple client device observes a minimum of 2 APs with an RSSI measurement of -67 dBm
8. Cisco recommends monitoring for peer-to-peer communication activity on UNII
9. Cisco recommends monitoring for APs changing channels frequently, and take action to resolve identified 5 GHz Wi-Fi channels that are most affected by known sources of interference on a regular basis.

- **Validaciones:**
    a. Se valida que los dBm se encuentran por encima de -67.
    b. Se valida que la conexión de los apple tv y resto de dispositivos Apple TV están empleando la frecuencia de 5GHz.
    c. La prueba de conexión de Wireless controllers otorga una calidad de un 100% para los apple TV.
    d. Tramas ICMP también muestran unos tiempos de respuesta óptimos.
    e. Actualmente los canales asignados son en la banda U-NII-1 (34 to 48)
    f. Herramienta de testing de Apple para medir las señales, AirPort Utility [31]

Roaming

10. Cisco and Apple recommend that you configure an 802.11r mix mode WLAN for fast transition 802.1X or WPA2 PSK capable clients and 802.11r-compatible clients to join the same network
11. For high density enterprise environments, Cisco and Apple recommend to use 802.11r with Over the air transition for optimal 11r-FT performance.

12. Cisco recommends configuring 802.11k on the WLAN to provide Apple devices with a neighbor list response. Cisco v8.0MR3 and v8.1.120.0 and Apple iOS 8.0 is the minimum version recommended for 802.11k
13. Cisco and Apple recommend the use of 802.11v BSS Transition Management to help balance client load across access points

- **Validaciones:**
    a. Es necesario aplicar y activar los protocolos de roaming 802.11r, 802.11k y 802.11v.

Tunning Data Rates (DFS and DCA)

14. Cisco recommends managing data rates to provide the coverage that is suitable for the number of clients needed in the coverage of a channel, with bandwidth needed in the coverage of the channel
15. Cisco and Apple recommends a minimum data rate of 12Mbps and 24 Mbps as the mandatory rate as a general best practice for Apple devices on
16. Cisco Wireless LAN. If the 5GHz coverage is marginal, set 6Mbps as the lowest mandatory rate, and make sure that 12 and 24Mbps are enabled as well
17. 3 band channels in a high client density environment. If high number of Apple devices are expected to perform peer-to-peer activity, excluding channels 149, 153 from DCA can be considered as a last resort measure
18. Cisco highly recommends leaving all MCS rates enabled
19. Cisco recommends for Channel Bonding: use 20 MHz when channel density (e.g., high number of APs in environment) is needed, and consider 40 MHz when client traffic uses heavy bandwidth (e.g., video) and DFS Channels are available

- **Validaciones:**
    a. Maximizing range vs Maximizing performance (5Ghz):
        1. > Rango – Habilitar low data rates
        2. > Performance – Deshabilitar low data rates (mandatory – unicast and multicast, supported – only unicast) Cisco

and Apple recommends a minimum data rate of 12 Mbps, and enabling 12 Mbps and 24 Mbps as the two mandatory data rates as a general best practice for Apple devices on Cisco Wireless LAN. If the 5GHz coverage is marginal, setting 6 Mbps as the lowest mandatory rate could potentially resolve issues.

b. Cambiar la configuración del Channel Bonding en modo auto o forzado a 20Mhz (actualmente está forzado a 40Mhz).

QoS

20. Cisco recommends all Apple devices to be connected to a WLAN with a QoS value of platinum (Voice) and with WMM set to required.
21. Cisco recommends using DSCP 46 for voice traffic based applications, translates to 802.11e - UP 6

- **Validaciones**:
    a. Dado que los dispositivos Apple no requieren servicios de voIP, se omiten estos correctivos.

Versionado

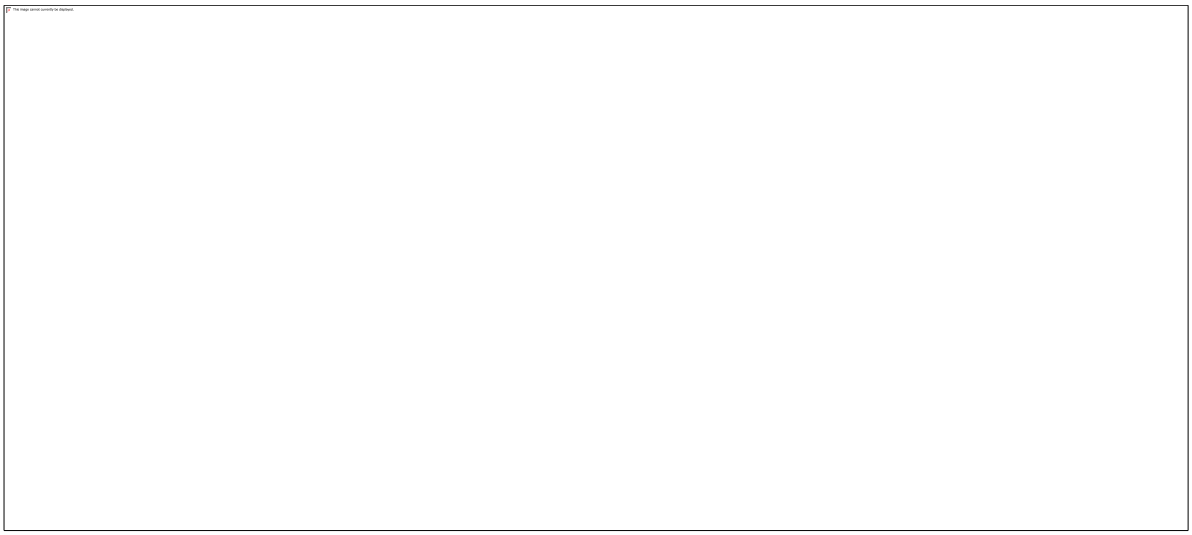
22. Apple recommends upgrading all devices to the latest iOS 9 or above operating System

Otras comprobaciones

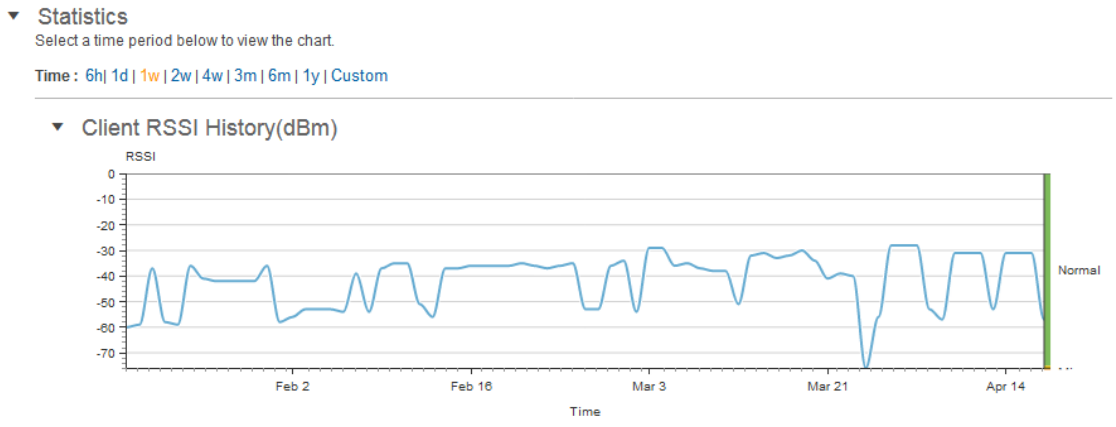
Revisión logs Airparrot, adjuntamos extracto en el momento se produce la desconexión aleatoria:

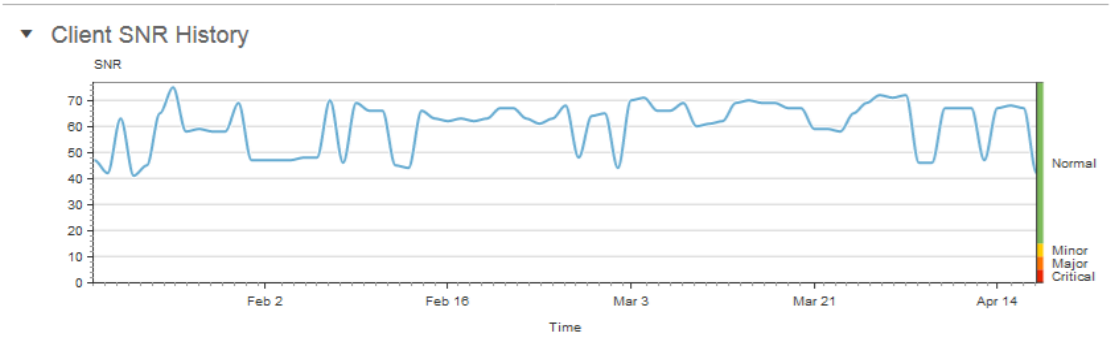
```
[2018-03-15 09:15:42.100] DNSService Finished getting devices
[2018-03-15 09:15:42.101] UI: Destination list updated, populate list for window
[2018-03-15 09:15:42.101] UI: Populating Destinations
[2018-03-15 09:53:04.298] Non optional sock tag: 199 disconnect. on 2028
[2018-03-15 09:53:04.298] APS Closing (disconnect error 12296)
[2018-03-15 09:53:04.298] AirPlay: Left connected loop shutting down!
[2018-03-15 09:53:04.299] AirPlay: Past Socket Close!
[2018-03-15 09:53:04.299] AirPlay: Finished Disconnecting
```

Pruebas monitorización con el APPLETV de las salas afectadas (Switchbox y thinking):



Realizando la medición de los últimos 3 meses de la señal emitida y recibida, parece que se mantiene en rangos razonables, observando únicamente un pico puntual a final de Marzo.





Comprobación de estado mDNS

- Se verifica que está habilitado a nivel global, se usa para que cualquier dispositivo pueda descubrir el Apple TV, en esto no se detectan problemas, se suele configurar en casos en los que los Apple TV se encuentran en redes diferentes.

Conclusiones:

Tras las revisiones del entorno oportunas se determina que entre el controlador y los AP's no existen problemas de conectividad, y tampoco en las redes presentadas por los AP's. No existe ningún problema de señal débil ni interferencias, y tampoco existen problemas con el autodescubrimiento de dispositivos Apple en la red. Por lo que se ha procedido con aplicar cambios identificados en los bloques anteriores para resolver los problemas experimentados por los usuarios.

Para la conexión correcta de dispositivos IOS con un perfil móvil, ha sido necesaria la configuración a nivel de vWLC de los protocolos de roaming 802.11r, 802.11k y 802.11v. De ellos la característica más relevante es la conocida como: Fast SSID change. Esto permite que el vWLC no elimine el registro de los clientes conectados y por tanto la reconexión a otro SSID es inmediata. Cuando Fast SSID change está deshabilitado el propio controlador fuerza un delay cada vez que un cliente quiere cambiar de SSID.

Con lo que respecta al problema con los Apple TV, se han probado a aplicar los cambios identificados previamente sobre la configuración para lograr el tunning de la solución sin lograr cambios sobre el origen del problema. No obstante, se identifican unas antenas de telefonía cercanas sobre los dispositivos con problemas que podrían llegar a

generar interferencias, no obstante, se verifica que tampoco son causante del problema ya que la problemática se reproduce con las mismas apagadas.

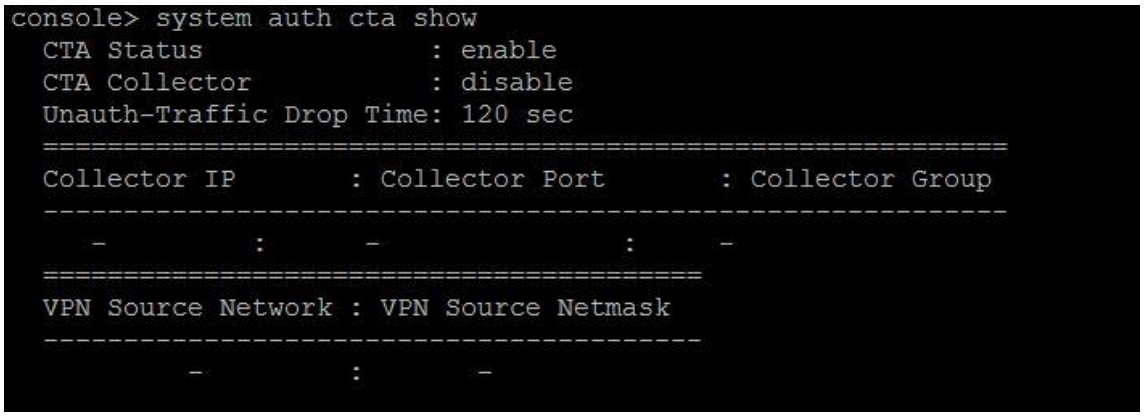
Finalmente se realizan pruebas con un Apple TV con una versión de tvOS inferior (10.2) verificando que no se reproduce el problema. A pesar de que según las release notes de Airparrot tvOS 11 debería estar soportado, parece que en la versión 11.2 de tvOS algo ha cambiado que puede estar provocando estas desconexiones. Tras la apertura y revisión del caso por el soporte de Airparrot, no se ofrece ninguna solución a corto plazo, por lo que se opta por cablear por Apple TV en versión 11.2 de la organización validando que ya no se experimentan desconexiones aleatorias al emitir contenido desde un equipo Windows.

6.2 Análisis incidencia con integración firewall Sophos de la organización.

Tras finalización del proyecto, se identifica un comportamiento extraño en algunos dispositivos, especialmente móviles o equipos externos a la organización, ya que estos en la primera conexión a la red no tienen posibilidad a navegar hasta pasados 120 segundos. No obstante, los usuarios que emplean dispositivos en dominio no experimentan este tipo de problemas.

En el caso de esta infraestructura, descubrimos que los firewalls de la organización emplean un software para la identificación transparente de usuarios de la organización llamado STAS, para así, mediante reglas de firewall priorizar y incluso regular el tráfico de usuarios desconocidos y usuarios desconocidos de la organización.

Tras revisar el comportamiento de STAS según su misma guía de implementación [31], se verifica que existe una parametrización por defecto por la que todo tráfico no autenticado mediante algún usuario de la organización es automáticamente bloqueado durante 120 segundos, tiempo mientras en cual el tráfico generado por dicho dispositivo está siendo analizado por el firewall para verificar si es tráfico lícito o puede ser un ataque de intrusión a la red.



Finalmente, para minimizar este tipo de bloqueos, se decide la configuración de un periodo de drop de 1 segundo, mediante la ejecución del siguiente comando en sophos.

```
system auth cta unauth-traffic drop-period 1
```

Tras aplicar los cambios en el firewall se verifica que el comportamiento de los dispositivos al conectar con la red Wi-Fi vuelve a ser el esperado, pudiendo navegar inmediatamente desde el momento que se establece la conexión.

6.3 Problemas inicialización de Chromecast

Se ha detectado tras la implementación de la red Wi-Fi, que los dispositivos Chromecast de Google, no son capaces de inicializarse correctamente en ninguna de las redes configuradas por los virtual Wireless controllers a pesar de cumplir con las consideraciones de implementación de la documentación de Cisco para estos dispositivos [32].

Se experimenta un problema en la conexión a dichas redes para su configuración inicial, es por ello por lo que se implementa la red EM_Open sin autenticación, la cual permite la correcta conexión, configuración e inicialización del dispositivo.

Una vez inicializado cada chromecast, es posible su correcto funcionamiento cambiando la red del mismo a cualquiera de las ofrecidas por los Wireless controllers y por tanto, tras configuración inicial de los chromecast, la red EM_Open es retirada de la emisión de los AP’s por motivos de seguridad.

7. Conclusiones

Este proyecto ha permitido la implementación de una red Wi-Fi en malla, la cual permite administrar desde los vWLC desplegados en la sede central todos los puntos de acceso distribuidos en la sede de Cheste y Torrente sin tener que realizar cambios por cada punto de acceso individualmente. Tras la implementación del mismo, se ha observado una mejora considerable en la señal y calidad del acceso a la red inalámbrica en las sedes donde se han implementado los nuevos AP's. Sin embargo, también se han detectado incidentes con dispositivos Apple, los cuales han requerido una configuración adicional sobre los vWLC para su correcto funcionamiento en la red implementada.

En lo que respecta a los sistemas desplegados para la dotación de funcionalidades extra a la red, en el caso del sistema de monitorización, su implementación ha sido un éxito siendo el producto más empleado por la organización para identificación de usuarios por *mac-address*, revisión consumo de red por usuario, detección de mal funcionalidades en la red y errores hardware en los dispositivos añadidos al mismo. No obstante, el resto de herramientas como el CMX a pesar de seguir en funcionamiento tras su implementación apenas es consultada ya que la misma está orientada quizás para usos en escenarios con más movilidad de personal como lugares públicos o aeropuertos. Además, la implementación de ISE ha permitido crear una red en la que los usuarios pudieran autenticar con las credenciales de *Active Directory*, pero que sin embargo, de cara a la organización no se ha decidido poder en producción. Finalmente, el sistema HA (N+1) de los vWLC no ha cumplido con las expectativas, siendo necesario aplicar los cambios de configuración en ambos nodos manualmente ya que no replican la configuración, a pesar que si cumplen con su función, y en caso de caída de un nodo, el otro asume el control sin incidentes. Esto puede ocasionar problemas si en un futuro se realizan cambios únicamente sobre el nodo productivo sin tener presente el nodo de backup, no obstante, existe también respaldo por las funcionalidades de alta disponibilidad de *VMware* lo que minimiza el riesgo de pérdida de servicio, y se cuenta con respaldo de *Veeam Backup* para su respaldo en caso de corrupción de las máquinas virtuales.

El proyecto desarrollado ha sido posible ejecutarlo según la planificación planteada en la fase inicial del mismo y con resultados satisfactorios cumpliendo con los propósitos y requisitos planteados por la organización. Si bien, ha sido necesario dedicar un tiempo adicional tras finalizar las tareas de implementación, para el análisis y resolución de incidencias tras la detección de problemas con dispositivos Apple.

De cara a futuros proyectos, sería recomendable la explotación de funcionalidades de la herramienta de monitorización Cisco Prime Infraestructure, habilitado características de *Netflow* para mayor visibilidad de tráfico sobre la red y añadiendo en el inventario todos los dispositivos de red Cisco con los que cuenta la organización, para ello habría que considerar realizar cambios sobre la infraestructura actual de red ya que los switches actuales no soportan *Netflow*. Además, dado que la solución adoptada es escalable y aún no ha alcanzado los límites de la misma, sería posible la ampliación y despliegue de nuevos puntos de acceso en nuevas sedes de la organización que actualmente siguen funcionando con puntos de acceso independientes.

8. Glossario

- **AAA** → Acrónimo que corresponde a las funciones autenticación, autorización y contabilización.
- **ACL** → Acrónimo empleado en la seguridad informática correspondiente a la definición de listas de control de acceso.
- **Active directory (AD)** → Servicio propietario de Microsoft para la gestión centralizada múltiples elementos de una red (usuarios, servidores, equipos, impresoras…).
- **AES** → Sistema de encriptación por bloques.
- **AP** → Punto de acceso empleado para dotar de conexión inalámbrica a dispositivos a diferentes redes.
- **Appliance** → Dispositivo hardware o software diseñado con un propósito específico.
- **ASCII** → Standard de codificación de caracteres para comunicaciones electrónicas.
- **Bandwith** → Termino inglés para definir el ancho de banda
- **CDP** → Protocolo propietario de Cisco para descubrimiento de dispositivos.
- **Cloud** → Infraestructura IT que forma una red única capaz de ofrecer servicios, puede ser pública, privada o híbrida.
- **Cluster** → Unión de más de un dispositivo de idénticas características para la dotación de servicios de alta disponibilidad o aumentar las capacidades de los mismos.
- **CMX** → Sistema propietario de Cisco destinado a la recopilación y análisis de dispositivos conectados a una red inalámbrica.
- **Community** → Término conocido dentro de SNMP para la definición de un usuario o contraseña de dicho servicio.
- **Controller** → Dispositivo capaz de centralizar la gestión de multitud de puntos de acceso.
- **Core** → Representa los dispositivos de red centrales con funciones lógicas de capa 3 que unen entre si las diferentes redes de una organización.

- **Datasheet** → Documento técnico de referencia de cualquier dispositivo.
- **dBi** → Indicador medidor de decibelios de ganancia de una antena.
- **dBm** → Indicador medidor de decibelios relativa a un milivatio.
- **DHCP** → Servidor para asignación de direccionamiento IP dinámico.
- **Ethernet** → Standard para la definición de características de cableado y señalización de una red de área local.
- **Firewall** → Sistema de seguridad encargado de restringir los accesos no autorizados a una red mediante la implementación de reglas de acceso.
- **Firmware** → Software de bajo nivel para el control del circuito electrónico de cualquier dispositivo.
- **Flexconnect** → Tecnología propietaria de Cisco para la conexión y gestión remota de puntos de acceso de la red.
- **HA** → Siglas empleadas para definir la capacidad de alta disponibilidad.
- **HTTP** → Protocolo de comunicación que permite la transferencia de hipertexto.
- **IP** → Identificador numérico, lógico y jerárquico, empleado para la identificación de interfaces de red.
- **ISE** → Sistema propietario de Cisco empleado para la identificación, seguimiento y securización de accesos a una red.
- **kBps** → Unidad de medida representada en Kilobytes por segundo, un Kilobyte es equivalente a 1024 bytes.
- **Kbps** → Unidad de medida representada en kilobits por segundo, un Kilobit es equivalente a 1000 bits.
- **LAN** → Red de área local.
- **LDAP** → Protocolo empleado para la conexión y acceso a servicios de directorio activo.
- **Lightweight** → Versión ligera de firmware para puntos de acceso que posibilitan la unión a un controlador.
- **MAC** → Identificador numérico hexadecimal, empleado para la identificación de tarjetas de red físicas.
- **Macrolan** → Servicio de red privada virtual basado en tecnología MPLS ofrecido por proveedores de servicios de internet.

- **Netflow** → Protocolo de red propietario de Cisco para la recolección de información e identificación de tráfico IP.
- **NTP** → Protocolo que permite la sincronización horaria de los dispositivos que lo implementan.
- **On-premise** → Término empleado para situar la implementación de sistemas dentro de la infraestructura de una organización.
- **PoE** → Tecnología capaz de suministrar alimentación eléctrica a dispositivos que lo implementan.
- **PSK** → Clave secreta compartida, empleado para sistemas Wi-Fi para la conexión a un SSID que implemente sistemas de cifrado como WEP y WPA.
- **QoS** → Se emplea para medir y configurar ratios de rendimiento de calidad de servicio de red.
- **Radius** → Protocolo de autenticación y autorización de aplicaciones por la red.
- **Roaming** → Capacidad de itinerancia, permite la movilidad de un dispositivo manteniendo la conectividad a una red independientemente de la fuente de la misma.
- **Router** → Dispositivo capaz de proporcionar conexión de capa 3 y encaminar los paquetes entre diferentes redes.
- **RSSI** → Indicador medidor de nivel de potencia de una señal Wi-Fi.
- **SNMP** → Protocolo que permite el intercambio de información de administración de los dispositivos que lo habilitan.
- **Spare** → Dispositivo provisionado cuya finalidad no es dar servicio, sinó servir de reemplazo inmediato en caso de fallo de un dispositivo en producción.
- **SSID** → Identificador de una red inalámbrica.
- **Standalone** → Versión pesada de firmware para puntos de acceso que posibilitan su uso de forma independiente de un controlador.
- **Switch** → Dispositivo capaz de proporcionar conexión de capa 2 y distribuir los paquetes entre los diferentes dispositivos conectados al mismo.
- **TCP** → Protocolo de control de transmisión.
- **UDP** → Protocolo de datagramas de usuario.

- **Uplink** → Suele referir al enlace de telecomunicación efectuado entre dos dispositivos.
- **vLAN** → Red de área local virtual.
- **vWLC** → Servidor virtual propietario de Cisco, cuyo propósito es centralizar la gestión de los puntos de acceso de una red.
- **Wi-Fi** → Tecnología que permite la interconexión inalámbrica de dispositivos electrónicos.
- **WLAN** → Red de área local inalámbrica.
- **WPA** → Sistema de seguridad informática empleado para proteger el acceso a una red Wi-Fi mediante la autenticación con una clave precompartida.
- **WPA2** → Sistema de seguridad equivalente a WPA pero mejorado mediante el uso de cifrado AES.

9. Bibliografia

[1] Cisco, «Cisco Aironet 1130AG Series Access Point Hardware Installation Guide,» [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/wireless/access_point/1130/installation/guide/1130-TD-Book-Wrapper/113h_c2.html. [Último acceso: 25 03 2019].

[2] A. Networks, «Aruba Mobility Controller Virtual Appliance Datasheet,» [En línea]. Available: https://www.arubanetworks.com/assets/ds/DS_VMC.pdf. [Último acceso: 25 03 2019].

[3] A. Networks, «MOBILITY CONTROLLER VIRTUAL APPLIANCE Datasheet,» Aruba Networks, [En línea]. Available: https://www.arubanetworks.com/assets/ds/DS_VMC.pdf. [Último acceso: 25 03 2019].

[4] A. Networks, «ARUBA 207 SERIES Datasheet,» Aruba Networks, [En línea]. Available: https://www.arubanetworks.com/assets/ds/DS_AP207Series.pdf. [Último acceso: 25 03 2019].

[5] Huawei, «AC6003-8 Wireless Access Controller Datasheet,» Huawei, [En línea]. Available: http://files.rakurs.su/IT/WLAN/Huawei/AC6003/Huawei%20AC6003-8%20Wireless%20Access%20Controller%20Datasheet.pdf. [Último acceso: 25 03 2019].

[6] Huawei, «AP1050DN-S Access Point Datasheet,» Huawei, [En línea]. Available: https://e.huawei.com/en/material/onLineView?MaterialID=2b4fd557e436423e99059250ccaa9281. [Último acceso: 25 03 2019].

[7] AeroHive, «HiveManager Classic On-Premises Datasheet,» AeroHive, [En línea]. Available: https://www.aerohiveworks.com/datasheets/Aerohive_Datasheet_HiveManager_Classic_OnPrem.pdf. [Último acceso: 25 03 2019].

[8] AeroHive, «AP130 Access Point Datasheet,» AeroHive, [En línea]. Available: https://www.aerohive.com/wp-content/uploads/Aerohive_Datasheet_AP130.pdf. [Último acceso: 25 03 2019].

[9] Cisco, «Cisco Virtual Wireless Controller Data Sheet,» Cisco, [En línea]. Available: https://www.cisco.com/c/en/us/products/collateral/wireless/virtual-wireless-controller/data_sheet_c78-714543.html. [Último acceso: 25 03 2019].

[10] Cisco, «Cisco Aironet 1700 Series Access Point Data Sheet,» Cisco, [En línea]. Available: https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1700-series/datasheet-c78-732347.html. [Último acceso: 25 03 2019].

[11] I. Price, «Controlador Aruba MC-VA-50 P/N: H5UA9E,» ITprice, [En línea]. Available: https://itprice.com/hp/h5ua9e.html. [Último acceso: 31 03 2019].

[12] Senetic, «Access Point Aruba AP-207 P/N: JX952A,» Senetic, [En línea]. Available: https://www.senetic.es/product/JX952A?gclid=Cj0KCQjwyoHlBRCNARIsAFjKJ6Du3BMxORo85KPQ4a_EWzMY7SV5W2-sXUZnsr-ry8C53ZlyNg5uRHIaAp3jEALw_wcB. [Último acceso: 31 03 2019].

[13] 4Gltemall, «Controlador Huawei AC6003-8-8AP P/N: AC6003-8-8AP,» 4Gltemall, [En línea]. Available: https://www.4gltemall.com/huawei-ac6003-8-8ap-wireless-access-controller.html. [Último acceso: 31 03 2019].

[14] YoyCart, «Access Point ap1050dn-s P/N: ap1050dn-s,» YoyCart , [En línea]. Available: https://www.yoycart.com/Product/569851765887/. [Último acceso: 31 03 2019].

[15] Aerohiveworks, «HiveManager NMS Virtual Appliance P/N: AH-HM-VA,» Aerohiveworks, [En línea]. Available: http://www.aerohiveworks.com/HiveManager.asp. [Último acceso: 31 03 2019].

[16] Amazon, «Aerohive HiveAP 130 Access Point P/N: AH-AP-130,» Amazon, [En línea]. Available: https://www.amazon.com/Aerohive-HiveAP-Access-Point-Indoor/dp/B072YTJHDG/ref=sr_1_2?keywords=Aerohive+HiveAP+130&qid=1554922617&s=electronics&sr=1-2-spell. [Último acceso: 31 03 2019].

[17] ItPrice, «Controlador Cisco virtual Wireless Controller P/N: L-AIR-CTVM-5-K9,» ItPrice, [En línea]. Available: https://itprice.com/cisco-gpl/l-air-ctvm-5-k9. [Último acceso: 31 03 2019].

[18] UsedCisco, «Cisco Access Point P/N: AIRCAP1702I-E-K9,» UsedCisco, [En línea]. Available: https://www.usedcisco.de/en/wireless/cisco-1700-access-point-series/123/air-cap1702i-e-k9?number=10110080-014&gclid=Cj0KCQjwnKHlBRDLARIsAMtMHDGJRUc7Eo-ZKJWW6BILYnmr_QkJzNOPURxGqSdqDu_-i2g1PjfkBUwaAtKcEALw_wcB. [Último acceso: 31 03 2019].

[19] Provantage, «Licencia Controlador P/N: JY902AAE,» Provantage, [En línea]. Available: https://www.provantage.com/hpe-jy902aae~7DECC4XL.htm. [Último acceso: 31 03 2019].

[20] 4Gltemall, «Licencia Controlador+AP P/N: L-AC6003-8AP-S,» 4Gltemall, [En línea]. Available: https://www.4gltemall.com/huawei-l-ac6003-8ap-s-huawei-ac6003-8-8ap-controller-8ap-authorization-software.html. [Último acceso: 31 03 2019].

[21] Myriad360, «Licencia para Access Point P/N: AH-HM-LIC-1AP,» Myriad360, [En línea]. Available: https://myriad360.com/product/aerohive-ah-hm-lic-1ap/. [Último acceso: 31 03 2019].

[22] Connection, «Hardware y Licencia Access Point P/N: AH-ERATE-HMOL-1YR-130-FCC,» Connection, [En línea]. Available: https://www.connection.com/product/aerohive-ap130-w-fcc-domain-

hivemanager-6-online-select-support-1-year/ah-erate-hmol-1yr-130-fcc/32200592. [Último acceso: 31 03 2019].

[23] ItPrice, «Licencia Controlador Cisco vWLC P/N: L-AIR-CTVM-5-K9,» ItPrice, [En línea]. Available: https://itprice.com/cisco-gpl/l-air-ctvm-5-k9. [Último acceso: 31 03 2019].

[24] Zones, «Licencia Cisco One por AP P/N: C1FPAIRK9,» Zones, [En línea]. Available: http://www.zones.com/site/product/index.html?id=102698320. [Último acceso: 31 03 2019].

[25] «Ocellum Consultoria TIC,» [En línea]. Available: https://ocellum.net/tarifa-general-de-precios/. [Último acceso: 2019 05 14].

[26] «NetFlow Support Matrix,» [En línea]. Available: https://community.cisco.com/t5/security-documents/netflow-support-matrix/ta-p/3644638. [Último acceso: 14 05 2019].

[27] «Sophos XG Firewall: How to connect with Netflow,» [En línea]. Available: https://community.sophos.com/kb/en-us/132762. [Último acceso: 14 05 2019].

[28] «Enterprise Best Practices for iOS devices and Mac,» [En línea]. Available: https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/8-6/Enterprise_Best_Practices_for_iOS_devices_and_Mac_computers_on_Cisco_Wireless_LAN.pdf. [Último acceso: 14 05 2019].

[29] «Compatibilidad de iOS con QoS Fastlane y Adaptive 802.11r de Cisco,» [En línea]. Available: https://support.apple.com/es-es/HT207308. [Último acceso: 14 05 2019].

[30] «AIRPARROT FOR WINDOWS RELEASE NOTES,» [En línea]. Available: https://www.airsquirrels.com/airparrot/release-notes/win. [Último acceso: 14 05 2019].

[31] «AirPort Utility,» [En línea]. Available: https://itunes.apple.com/us/app/airport-utility/id427276530?mt=8. [Último acceso: 16 05 2019].

[32] «Sophos XG Firewall: How to Implement Clientless SSO with multiple Active Directory Domain Controllers,» [En línea]. Available: https://community.sophos.com/kb/en-us/123154. [Último acceso: 16 05 2019].

[33] «Chromecast Deployment Guide, Release 7.6,» [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/7-6/chromecastDG76/ChromecastDG76.html. [Último acceso: 16 05 2019].

10. Anexos

10.1 Inventario Unified Access Point's.

Se detallan todos los AP's configurados para funcionar en modo Flexconnect a través de los virtual Wireless Controllers.

AP Name	Ethernet MAC Address	AP Model	POE Status	AP Serial Number
AP_ADITIVOS	2c:5a:0f:20:aa:98	AIR-CAP1702I-E-K9	External	FCW2106NQYV
AP_ADMON1	00:2c:c8:63:cc:2c	AIR-CAP1702I-E-K9	Normal	FCW2106NR2V
AP_ADMON2	2c:5a:0f:20:bb:f4	AIR-CAP1702I-E-K9	Normal	FCW2107N9HK
AP_ALM_MAT_AUX	f8:0b:cb:da:08:28	AIR-CAP1702I-E-K9	Normal	FCW2116N5FD
AP_CAMARA_CAOTICA	2c:5a:0f:1e:6c:00	AIR-CAP1702I-E-K9	External	FCW2106NQYW
AP_COMEDOR	00:f2:8b:9b:6b:4b	AIR-CAP1602I-E-K9	Normal	FGL2015X045
AP_CONTROL	a0:e0:af:e1:cf:10	AIR-CAP1702I-E-K9	External	FCW2107NH08
AP_CPD	a8:9d:21:03:1a:45	AIR-CAP1602E-E-K9	Normal	FGL1909X9PQ
AP_DIRECTORES	00:c1:64:9a:b4:b2	AIR-CAP1602I-E-K9	External	FGL2015X03N
AP_ENVASADO	2c:5a:0f:1e:7e:90	AIR-CAP1702I-E-K9	External	FCW2107N98S
AP_ESCALERAS_COMEDOR	70:db:98:b6:37:e4	AIR-CAP1702I-E-K9	External	FCW2116N5F6
AP_ESPECIAS	70:db:98:b6:3d:34	AIR-CAP1702I-E-K9	Normal	FCW2116N3GY
AP_EXPEDICIONES	00:2c:c8:66:49:08	AIR-CAP1702I-E-K9	Normal	FCW2107N9CV
AP_INNOBOX	00:fe:c8:ac:09:8e	AIR-CAP1602I-E-K9	Normal	FGL2009X6KF
AP_LABORATORIO_CALIDAD	f8:0b:cb:c2:02:6c	AIR-CAP1702I-E-K9	Normal	FCW2116N3FQ
AP_LOLA_GANDIA	2c:5a:0f:20:aa:f8	AIR-CAP1702I-E-K9	Normal	FCW2106NREA
AP_SECO	f8:0b:cb:7c:15:78	AIR-CAP1702I-E-K9	Normal	FCW2106NQZ8
AP_SPARE	18:8b:9d:40:1d:08	AIR-CAP1602E-E-K9	External	FGL1933X9KE
AP_SWITCHBOX	00:fe:c8:ac:04:f2	AIR-CAP1602I-E-K9	Normal	FGL2009X6MM
AP_SYNERGY	f8:0b:cb:77:96:54	AIR-CAP1702I-E-K9	External	FCW2106NNJ7
AP_THINKING_AREA	00:f2:8b:9b:6a:42	AIR-CAP1602I-E-K9	Normal	FGL2015X046
AP_THINKING_AREA_2	00:c1:64:9a:b2:bc	AIR-CAP1602I-E-K9	Normal	FGL2015X047
AP_TIC	2c:5a:0f:1e:54:f4	AIR-CAP1702I-E-K9	Normal	FCW2106NR32
AP_TORRENTE_ALTILLO	00:2c:c8:63:e6:7c	AIR-CAP1702I-E-K9	Normal	FCW2107N9E6
AP_TORRENTE_COMEDOR	a8:9d:21:03:1b:c6	AIR-CAP1602E-E-K9	Normal	FGL1909X9Q1
AP_TORRENTE_COMEDOR_PRIVADO	00:a2:ee:91:c8:7c	AIR-CAP1702I-E-K9	Normal	FCW2037NRC5
AP_TORRENTE_FABRICACION	00:c1:64:9a:b3:8e	AIR-CAP1602I-E-K9	Normal	FGL2015X04A
AP_TORRENTE_MARBIN	00:a2:ee:60:22:10	AIR-CAP1702I-E-K9	Normal	FCW2037NR83
AP_TORRENTE_MAT_AUX	00:2c:c8:66:2d:94	AIR-CAP1702I-E-K9	Normal	FCW2106NR30
AP_TORRENTE_PASILLO_FABRICA	a0:e0:af:e1:b5:58	AIR-CAP1702I-E-K9	Normal	FCW2106NR2Z
AP_TORRENTE_PICKING	f8:0b:cb:c1:f0:18	AIR-CAP1702I-E-K9	Normal	FCW2116N3PB
AP_TORRENTE_PLANTA_PILOTO	00:a2:ee:bb:06:24	AIR-CAP1702I-E-K9	Normal	FCW2037NRQB
AP_TORRENTE_SALA_CENTRAL	00:a6:ca:ad:f2:5c	AIR-CAP1702I-E-K9	Normal	FCW2037NRMG
AP_TORRENTE_SALA_INNOVACION	00:a2:ee:bb:06:d8	AIR-CAP1702I-E-K9	Normal	FCW2037NRLN
AP_TORRENTE_SALA_REUNIONES	00:a2:ee:bb:07:ec	AIR-CAP1702I-E-K9	Normal	FCW2037NRQ4
AP_TRIPAS	00:2c:c8:63:e6:3c	AIR-CAP1702I-E-K9	External	FCW2107N9J7
AP_VESTUARIO_PLANTA_ALTA	2c:5a:0f:20:bb:0c	AIR-CAP1702I-E-K9	Normal	FCW2107N9AK
AP_VESTUARIO_PLANTA_BAJA	2c:5a:0f:20:ab:04	AIR-CAP1702I-E-K9	Normal	FCW2106NRDU