NOMBRE DEL TRABAJO

T088A_46966435_T.docx

RECUENTO DE PALABRAS

13404 Words

RECUENTO DE CARACTERES

73042 Characters

RECUENTO DE PÁGINAS

122 Pages

TAMAÑO DEL ARCHIVO

11.3MB

FECHA DE ENTREGA

Jun 27, 2023 4:02 AM GMT-5

FECHA DEL INFORME

Jun 27, 2023 4:03 AM GMT-5

16% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base d

- 16% Base de datos de Internet
- 2% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossr

Excluir del Reporte de Similitud

- Base de datos de trabajos entregados
- Material bibliográfico

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL DE LA UNTELS

(Art. 45° de la ley N° 30220 – Ley)

Autorización de la propiedad intelectual del autor para la publicación de tesis en el Repositorio Institucional de la Universidad Nacional Tecnológica de Lima Sur (https://repositorio.untels.edu.pe), de conformidad con el Decreto Legislativo N° 822, sobre la Ley de los Derechos de Autor, Ley N° 30035 del Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, Art. 10° del Rgto. Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales en las universidades – RENATI Res. N° 084-2022-SUNEDU/CD, publicado en El Peruano el 16 de agosto de 2022; y la RCO N° 061-2023-UNTELS del 01 marzo 2023.

TIPO DE TRABAJO DE INVESTIGACIÓN

1). TESIS ( ) 2). TRABAJO DE SUFICIENCIA PROFESIONAL (X)

DATOS PERSONALES

Apellidos y Nombres:	QUISPE HUARES BORIS JHONATTAN
D.N.I.:	46961435
Otro Documento:	
Nacionalidad:	Peruano
Teléfono:	910552447
e-mail:	boris1604j@gmail.com

DATOS ACADÉMICOS

Pregrado

Facultad:	FACULTAD DE INGENIERIA Y GESTION
Programa Académico:	Trabajo de suficiencia profesional
Título Profesional otorgado:	Ingeniería Electrónica y Telecomunicaciones

Postgrado

Universidad de Procedencia:	
País:	
Grado Académico otorgado:	

Datos de trabajo de investigación

Título:	DISEÑO DE RED WI-FI GESTIONADO EN LA NUBE, PARA EL CONTROL Y MONITOREO DE USUARIOS PARA EL GRUPO ELENDER EN EL DEPARTAMENTO DE LIMA
Fecha de Sustentación:	05 de Diciembre del 2019
Calificación:	Aprobado
Año de Publicación:	2023

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

A través de la presente, autorizo la publicación del texto completo de la tesis, en el Repositorio Institucional de la UNTELS especificando los siguientes términos:

Marcar con una X su elección.

1) Usted otorga una licencia especial para publicación de obras en el REPOSITORIO INSTITUCIONAL DE LA UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR.

Si autorizo __X__ No autorizo _____

2) Usted autoriza para que la obra sea puesta a disposición del público conservando los derechos de autor y para ello se elige el siguiente tipo de acceso.

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO ABIERTO 12.1(*)	**info:eu-repo/semantics/openAccess** (Para documentos en acceso abierto)	(X)

3) Si usted dispone de una **PATENTE** puede elegir el tipo de **ACCESO RESTRINGIDO** como derecho de autor y en el marco de confiabilidad dispuesto por los numerales 5.2 y 6.7 de la directiva N° 004-2016-CONCYTEC DEGC que regula el Repositorio Nacional Digital de CONCYTEC (Se colgará únicamente datos del autor y el resumen del trabajo de investigación).

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO RESTRINGIDO	**info:eu-repo/semantics/restrictedAccess** (Para documentos restringidos)	( )
	info:eu-repo/semantics/embargoedAccess (Para documentos con períodos de embargo. Se debe especificar las fechas de embargo)	( )
	info:eu-repo/semantics/closedAccess (para documentos confidenciales)	( )

(*) http://renati.sunedu.gob.pe

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

Rellene la siguiente información si su trabajo de investigación es de acceso restringido:

Atribuciones de acceso restringido:

Motivos de la elección del acceso restringido:

QUISPE HILARES BORIS JHONATTAN

APELLIDOS Y NOMBRES

46966435

DNI

Firma y huella:

Lima, 04 de Julio del 2023

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERIA ELECTRONICA Y TELECOMUNICACIONES

“DISEÑO DE RED WI-FI GESTIONADO EN LA NUBE, PARA EL CONTROL Y MONITOREO DE USUARIOS PARA EL GRUPO ILENDER EN EL DEPARTAMENTO DE LIMA”

TRABAJO DE SUFICIENCIA PROFESIONAL
Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

QUISPE HILARES, BORIS JHONATTAN

ASESOR
PAEZ ESPINAL, FERNANDO

Villa El Salvador
2019

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

III Programa de la Modalidad de Titulación por Trabajo de Suficiencia Profesional

Facultad de Ingeniería y Gestión

ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

En Villa El Salvador, siendo las 17:45 horas del día jueves 05 de diciembre de 2019, se reunieron en el aula B2-9, los miembros del Jurado Evaluador del Trabajo de Suficiencia Profesional integrado por:

Presidente	: DR. ROMÁN GONZÁLEZ, Avid	CIP N° **97960**
Secretario	: DR. CLEMENTE ARENAS, Mark Donny	CIP N° **181400**
Vocal	: MS.c. ORTEGA GALICIO, Orlando Adrián	CIP N° **79878**

Designados con RESOLUCIÓN DE FACULTAD DE INGENIERÍA Y GESTIÓN N° 630-2019-UNTELS-CO-V.ACAD-FIG, de fecha 26 de noviembre de 2019.

Se da inició al acto público de sustentación y evaluación del Trabajo de Suficiencia Profesional, para obtener el Título Profesional de Ingeniero Electrónico y Telecomunicaciones, bajo la modalidad de Trabajo de Suficiencia Profesional. (Resolución de Comisión Organizadora Nº 176-2019-UNTELS de fecha 17 de setiembre de 2019), en la cual se APRUEBA los documentos de gestión del III Programa de la Modalidad de Titulación por Trabajo de Suficiencia Profesional de la Universidad Nacional Tecnológica de Lima Sur – UNTELS; siendo que el Art. 4º del precitado Reglamento establece que: **"El trabajo de Suficiencia Profesional consiste en la presentación, aprobación y sustentación de un Proyecto que permite demostrar el logro de las competencias adquiridas en el desarrollo de los estudios de pregrado que califican para el ejercicio de la profesión correspondiente. La sustentación del Trabajo de Suficiencia Profesional se realiza en un acto académico público"**, en el cual;

El Bachiller: **QUISPE HILARES, BORIS JHONATTAN**

Sustentó su Trabajo de Suficiencia Profesional: **"DISEÑO DE RED WI-FI GESTIONADO EN LA NUBE, PARA EL CONTROL Y MONITOREO DE USUARIOS PARA DEL GRUPO ILENDER EN EL DEPARTAMENTO DE LIMA"**

Concluida la Sustentación del Trabajo de Suficiencia Profesional, se procedió a la calificación correspondiente según el siguiente detalle:

Condición..APROBADO.....CON 10 PUNTOS....., Equivalencia.....REGULAR.....de acuerdo al Art. 65º del Reglamento General para el Otorgamiento de Grado Académico y Título Profesional de la UNTELS, vigente.

Siendo las .18:30. del día jueves 05 de diciembre de 2019, se dio por concluido el acto de sustentación del Trabajo de Suficiencia Profesional, firmando el presente acta los miembros del Jurado.

SECRETARIO

Mark Donny Clemente Arenas
INGENIERO ELECTRONICO Y TELECOMUNICACIONES
181400

PRESIDENTE

Ph. D. Ing. Avid ROMAN GONZALEZ
Doctor en Procesamiento de Señales e Imagenes
Master en Automatización Industrial y Humana
Ingeniero Electronico & Ingeniero de Sistemas
CIP 97960

PARTICIPANTE

Bachiller: BORIS JHONATTAN QUISPE HILARES

VOCAL

ORLANDO ADRIÁN ORTEGA GALICIO
INGENIERO ELECTRÓNICO
Reg. CIP Nº 79878

Nota: Art. 14°.- La sustentación del Trabajo de Suficiencia Profesional se realizará en un acto público. De faltar algún miembro del Jurado, la sustentación procederá con los dos integrantes presentes. En caso de ausencia del Presidente del jurado, asumirá la presidencia el docente de mayor categoría y antigüedad. En caso de ausencia de dos o más miembros del jurado, la sustentación será reprogramada durante los 05 días siguientes.

DEDICATORIA

Dedicado a mi madre, a mi padre, a mis hermanos, y a una señorita muy especial, a ellos por todo su apoyo y comprensión

AGRADECIMIENTO

Agradezco a buen amigo José Miguel Alvarado, por su apoyo constante y sus muchas lecciones que siempre las recuerdo y aprecio

INDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

INTRODUCCION

El proyecto “Diseño de red Wi-Fi gestionado en la nube, para el control y monitoreo de usuarios para del grupo Ilender en el departamento de lima” es una propuesta de diseño de red inalámbrica administrado desde la nube (internet), en el presente se aborda temas como la evolución de tecnologías derivadas del estándar 802.11, tendencias actuales en los negocios como el uso masivo de aplicaciones móviles en teléfonos, internet de las cosas, administración simplificada. La propuesta de solución permitirá a la empresa tener un control y monitoreo sobre el uso y tipo de las aplicaciones que utilizan los empleados, así como una adecuada política de calidad de servicios que permita una adecuada distribución del ancho de banda; también permitirá gestionar un acceso seguro para los empleados de las diferentes empresas que conforman el grupo Ilender y a todos sus colaboradores externos, permitiendo que mediante una sola autenticación pueda mantener la navegación como un usuario identificado, en la red, con características como la movilidad y asignación de un perfil de usuario con las políticas de acceso y restricciones según su empresa, área y cargo en la sede donde se encuentre. Esto permitirá a la empresa mejora sus operaciones internas, simplificando la gestión de la red y reforzando la seguridad. La plataforma a proponer para el presente proyecto es la solución de administración WLAN en la nube de Alcatel Lucent llamado OmniVista Cirrus. Esta solución se basa en un controlado de punto de acceso inalámbrico siempre disponible y accesible desde cualquier lugar en internet. Este tipo de solución basada en la nube no compromete tráfico del usuario dentro de la red Wi-Fi, debido a la existencia de 03 tipos de “planos” de uso: plano de control, donde él se gestiona los parámetros de asociación entre el AP y la gestión, en el cual la conexión es encriptada; plano de datos, es el tráfico del usuario, el cual no llega hacia el controlador, sino que es manejado por el propio AP y el plano de control, el cual define los parámetros de RF, SSID, y otros entres los AP’s.

El dimensionamiento de AP’s se basa en equipos de tecnología vigente, con soporte del estándar 802.11ac, y con compatibilidad con protocolos antecesores 802.11a/b/g/n. También contarán con la función de inspección profunda de paquetes (DPI), que permitirá monitorear a los usuarios a nivel de capa de aplicación.

CAPITULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

En la actualidad, el grupo Ilender está formado por 7 empresas desplegadas en 04 sedes en Lima.

Sus sedes se encuentran en: San Isidro, Surco, Ate y Lurín:

Siendo las oficinas administrativas San Isidro, Surco, Ate y Lurín

Las sedes en ATE y Lurín son también plantas y almacenes. Los equipos de red existente son de la marca Alcatel Lucent

El despliegue de la red Wi-Fi en todas estas sedes es de forma local con una red Wi-Fi dedicada al uso de empleados y otra para invitados, las cuales presentan problemas de saturación en la red inalámbrica y vulnerabilidad en el acceso, debido a que los usuarios cuentan con el acceso total a la red corporativa desde el momento que ingresan al Wi-Fi con sus desktops/laptop y/o dispositivo móvil de personal, así como del trabajo, esto conlleva a que utilicen todo el ancho de banda digital de conexión a Internet.

Los dispositivos inalámbricos de trabajo de los empleados no están debidamente clasificados por empresa ni catalogados por área haciendo que todos pertenezcan a una sola red.

Mientras que los usuarios invitados al momento de acceder al Wi-Fi ingresan mediante una contraseña diferente a las sedes Una vez dentro, estos solo tienen restricciones para navegación hacia internet al momento que el tráfico generado pasa por un firewall.

Otro aspecto por destacar es el monitoreo de usuarios conectados a la red de la empresa. No se tiene centralizada una base de datos general que identifique a cada usuario, esto genera problemas al momento de dar soporte cuando se presenta problemas de conectividad en el área usuaria

Tampoco se tiene implementado ningún mecanismo para la identificación de tipo tráfico, aplicación (navegación web, Facebook, aplicaciones bancarias, one drive, correo) o categoría (social media, gobierno, banca, streaming) que utilice la para la ejecución de calidad de servicio y/o filtros dentro de la red Wi-Fi de la empresa.

1.2. Justificación del problema

El presente proyecto plantea un modelo de solución que beneficie al Grupo Ilender con lo siguiente: Mejorar el servicio navegación dentro de la red Wi-Fi a través del monitoreo en tiempo real, la identificación de consumo de ancho de banda digital por parte del área usuaria; permitiendo la actualización de las estrategias de calidad de servicio. Resguardar el ingreso a recursos internos mediante políticas de acceso y detección de intrusiones dentro de la red Wi-Fi. Mejorar la experiencia del usuario mediante una primera y única autenticación. Una vez autenticado en la red Wi-Fi, el usuario será identificado y podrá navegar desde cualquier sede de la empresa sin necesidad de volver a autenticarse. Reforzar seguridad uso de la red Wi-Fi a través de la identificación, limitación y/o bloqueo de aplicaciones y/o páginas web no relacionados a la empresa

1.3. Delimitación del proyecto

1.3.1. Teórica

El presente proyecto contempla el diseño de red Wi-Fi gestionada con la marca Alcatel Lucent, bajo el estándar WI-FI 802.11a/b/g/n y 802.11ac wave 1 y wave 2. Se abarcará temas como la movilidad L2 y L3, inspección profunda de paquetes en la red Wi-Fi, autenticación RADIUS y perfiles de acceso a la red, así como la gestión en la nube con la plataforma Omnivista Cirrus de Alcatel Lucent

No forma parte del proyecto el diseño y desarrollo de la infraestructura de acceso, distribución y core.

No forma como parte del proyecto el diseño de la seguridad a nivel externo (internet)

1.3.2. Temporal

La elaboración del proyecto tendrá una duración de 49 días, iniciando el día 11 de octubre del 2019 y culminando el día 29 de noviembre del 2019

Las etapas de proyecto son los siguientes:

Planteamiento del problema: 11/10/2019 hasta el 17/10/2019

Marco teórico: 18/10/2019 hasta el 25/10/2019

Desarrollo:

- Levantamiento de información de la red Wi-Fi del grupo Ilender: 04/11/2019 hasta el 09/11/2019
- Esquema general de la solución: 10/11/2019 hasta el 15/11/2019
- Dimensionamiento de hardware y software: 16/11/2019 hasta el 19/11/2019
- Propuesta de despliegue y configuración de la solución de red gestionada: 20/11/2019 hasta el 25/11/2019

Presentación del proyecto: 28/11/2019

1.3.3. Espacial

La elaboración del diseño de red Wi-Fi gestionado en la nube, para el control y monitoreo de usuario para el grupo Ilender abarcará el departamento de Lima.

1.4. Formulación del problema

1.4.1. Problema General

- ¿Cómo diseñar una red Wi-Fi gestionado en la nube, para el control y monitoreo de usuarios para del grupo Ilender en el departamento de lima?

1.4.2. Problemas Específicos

- ¿Cómo diseñar la topología y dimensionar los componentes de la red Wi-Fi gestionado en la nube, para el control y monitoreo de usuarios para del grupo Ilender en el departamento de lima?

- ¿Cómo elegir los mecanismos de autenticación de usuarios de la red Wi-Fi gestionado en la nube, para el control y monitoreo de usuarios para el grupo Ilender en el departamento de lima?
- ¿Cómo realizar la recolección de datos y monitoreo aplicaciones de los usuarios dentro de la red Wi-Fi gestionado en la nube, para el control y monitoreo de usuarios para el grupo Ilender en el departamento de lima?

1.5. Objetivos

1.5.1. Objetivo General

- Diseñar una red Wi-Fi gestionado en la nube, para el control y monitoreo de usuarios del grupo Ilender en el departamento de lima

1.5.2. Objetivos Específicos

- Diseñar la topología y dimensionar los componentes de la red Wi-Fi gestionado en la nube, para el control y monitoreo de usuarios para del grupo Ilender en el departamento de lima
- Elegir los mecanismos de autenticación de usuarios de red Wi-Fi gestionado en la nube, para el control y monitoreo de usuarios del grupo Ilender en el departamento de lima
- Realizar la recolección de datos y monitoreo aplicaciones de los usuarios dentro de la red Wi-Fi gestionado en la nube, para el control y monitoreo de usuarios del grupo Ilender en el departamento de lima

CAPITULO II: MARCO TEORICO

2.1. Antecedentes

2.1.1. Nacionales

Existen tesis de grado que abordan una problemática similar

LOPEZ, J. R. (2012). "*Diseño e implementación de un sistema de gestión de accesos a una red Wi-Fi utilizando software libre*". Pontificia Universidad Católica del Perú, Lima, Perú.

En la tesis, el autor plantea un meto de acceso inalámbrico, que inicia con ingreso de un dispositivo a una red inalámbrica WI-FI utilizando una credencial de acceso, Donde se primero se autentica el punto de acceso inalámbrico con el servidor de autenticación RADIUS asegurando que sea un agente permitido para permitir el ingreso conexiones de usuarios hacia la red. Luego el punto de acceso inalámbrico realiza la validación del usuario con un servidor de directorio LDAP, las estadísticas y datos de conexión del usuario son enviados hacia un servidor de base de datos MySQL para su almacenamiento.

Y, por último, para la navegación web emplea un servidor web-proxy mediante unas credenciales y autenticada también con el servidor RADIUS. Una vez aceptado el acceso, el control de ancho de banda será gestionado por el servidor web-proxy

BARRENECHEA, T. I. (2011). "*Diseño de una red inalámbrica para una empresa de Lima*". Pontificia Universidad Católica del Perú, Lima, Perú.

En la tesis, el autor plantea un diseño de red inalámbrico Wi-Fi en base a un análisis de cobertura inalámbrica y canales de transmisión, métodos de autenticación y seguridad, densidad de usuarios. También propone la gestión de puntos de acceso inalámbrico a través de conmutadores con capacidades de controlador de puntos de acceso inalámbrico asegurando la movilidad y desplazamiento de los dispositivos inalámbricos sin pérdida de conectividad

MENDOZA, M. G. (2011). "*Diseño y administración centralizada de redes WLAN a nivel nacional para CENTRUM católica*". Pontificia Universidad Católica del Perú, Lima, Perú.

En la tesis, el autor, plantea un diseño de red inalámbrica a nivel nacional para CENTRUM católica, centralizando la gestión con un grupo controladores de punto de acceso como contingencia, mientras que la autenticación, los accesos de usuarios y la administración de políticas de acceso lo realiza con una plataforma del fabricante Cisco llamada "ACS" (Del acrónimo "Cisco Secure Access")

2.1.2. Internacionales

A nivel internacional se tiene:

HERNANDEZ, L. E. (2010). "Diseño de red inalámbrica en el Centro de Convenciones Bolívar". Universidad Central "Marta Abreu" de Las Villas, Santa Clara, Cuba

En la tesis, el autor plantea el dimensionamiento de red Wi-Fi para el centro de convenciones Bolívar, y realiza un análisis de las vulnerabilidades de una red inalámbrica, donde menciona la importancia del uso de un servidor de autenticación RADIUS, 802.1x y encriptación en las comunicaciones inalámbricas entre el dispositivo de usuario y un AP

MORENO, M. (2015). "Análisis, diseño y despliegue de una red Wi-Fi en Santillana del Mar" Universidad Autónoma de Madrid, Madrid, España

En la tesis, el autor propone un diseño de red Wi-Fi tipo malla (mesh) en el municipio de Santillan del Mar, en el cual emplea un método de autenticación por portal cautivo y un gestor de red para el monitoreo de todos los puntos de acceso inalámbrico. Cabe resalar que la autenticación y la gestión es centralizada desde un servidor

2.2. Bases Teóricas

2.2.1. El estándar 802.11

802.11 o Wi-Fi es un protocolo estándar para comunicaciones inalámbricas entre dispositivos móviles, desarrollado por el grupo de trabajo de la IEEE en 1990. El nombre Wi-Fi proviene de Wireless Fidelity Alliance, una organización conformada por las distintas compañías que desarrollan hardware para esta tecnología y cuya principal misión es el de promover su uso en el hogar y en ambientes empresariales. En la Figura 1 se observa los protocolos involucrados en la capa física (L1) y capa de enlace (L2)

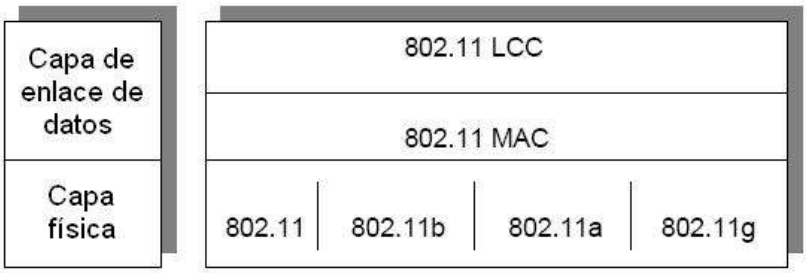


Figura 1. Clasificación del estándar 802.11 dentro del modelo de referencia OSI.
Fuente: Lopez (2008).

Este protocolo sigue evolucionando con el tiempo. En la tabla 1 observamos mejoras significativas en cuanto a capacidad de transmisión, frecuencia de transmisión y radio de cobertura; así como la introducción de estándar 802.11n:

Tabla 1. Resumen de los estándares IEEE 802.11.

Protocolo	Fecha de aparición	Frecuencia de operación	Throughput (Típico)	Tasa de tx (Máx)	Radio de cobertura (interiores) Depende de # y tipo paredes	Rango (exteriores) Atenuación por una pared incluida
802.11 *Legacy*	1997	2.4-2.5 GHz	1 Mbps	2 Mbps	~20 Metros	~100 Metros
802.11a	1999	5.15-5.25/5.25-5.35/5.49-5.725/5.725-5.85 GHz	25 Mbps	54 Mbps	~35 Metros	~120 Metros
802.11b	1999	2.4-2.5 GHz	6.5 Mbps	11 Mbps	~38 Metros	~140 Metros
802.11g	2003	2.4-2.5 GHz	20 Mbps	54 Mbps	~38 Metros	~140 Metros
802.11n	Noviembre 2008 (estimado, actualmente en *draft* 2.0)	2.4 GHz y/o 5 GHz	74 Mbps	248 Mbps = 2x2 ant	~70 Metros	~250 Metros

López (2008).

En la tabla 2 se aprecia que junto con el estándar 802.11n, también aparece una técnica de transmisión llamada MIMO (Del inglés “Multiple Input Multiple Output”) con el que se incrementa la tasa de transferencia teóricas de hasta 300Mbps

Tabla 2. Comparación entre los estándares 802.11 a, b, g y n.

COMPARACIÓN ENTRE LOS ESTANDARES 802.11 A, B, G Y N				
Característica	**IEEE 802.11a**	**IEEE802.11b**	**IEEE 802.11g**	**IEEE 802.11n**
Frecuencia/Ancho de Banda	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz y 5 GHz
Modulación	OFDM	DSSS	OFDM	MIMO
Ancho de Banda por Canal	20 MHz (6 canales utilizables)	22 MHz (3canales)	22 MHz (3 canales)	20 GHz 40 GHz
Tasa de transmisión	54 Mbps	11 Mbps	54 Mbps	300 Mbps
Cobertura Interior/Exterior	30/50 Metros	50/150 Metros	30/50 Metros	
Usuarios Simultáneos	64 usuarios	32 usuarios	50 usuarios	

Fuente: Mendoza (2011).

MENDOZA (2011) concluye que el estándar IEEE 802.11 está diseñado para mejorar el ancho de banda ofrecido por los estándares anteriores a través de del uso de múltiples señales y antenas mediante el uso de tecnología MIMO)(p27).

2.2.2. 802.11ac

802.11ac es un estándar reciente, ratificado por la IEEE en 2013. Entre mejoras significativas, es la utilización de un ancho de banda mayor 20/40/80 (802.11n usa 20/40Mhz). Una diferencia importante es que 802.11ac solo opera en el espectro de los 5Ghz a en comparación a 802.11 que opera en 2.4Ghz y 5Ghz. En la tabla 3 se observa las diferentes configuraciones en velocidad

Tabla 3. Tasas de enlace teórico 802.11ac.

802.11AC THEORETICAL LINK RATES				
Channel bandwidth	Transmit – Receive antennas	Modulation and coding	Typical client scenario	Throughput
40 MHz	1x1	256-QAM 5/6, short guard interval	Smartphone	200 Mbps
40 MHz	3x3	256-QAM 5/6, short guard interval	Laptop	600 Mbps
80 MHz	1x1	256-QAM 5/6, short guard interval	Smartphone, Tablet	433 Mbps
80 MHz	2x2	256-QAM 5/6, short guard interval	Laptop, Tablet	867 Mbps
80 MHz	3x3	256-QAM 5/6, short guard interval	Laptop	1.3 Gbps

Fuente: Aruba Networks (2014).

2.2.2.1. Mejoras de 802.11ac frente a 802.11n

802.11ac se considera un protocolo incluyente, debido a que utiliza mecanismos empleados en de 802.11n

El fabricante líder de tecnología inalámbrica ,Aruba Networks (2014), considera a las nuevas tecnologías en 802.11ac como extensiones de las técnicas inalámbricas en capa 1 presentes en 802.11n, en particular el uso de múltiples antenas en el transmisor/receptor (MIMO) permitiendo el uso de varios flujos de información (p.4)

2.2.2.2. MU-MIMO

802.11 ac emplea una técnica mejorada al MIMO del estándar 802.11n.
Como indica Aruba Networks (2014), Las comunicaciones hasta 802.11n son de punto a punto. Esto cambia con 802.11ac que permite la transmisión de diferentes flujos a varios clientes en simultaneo.

El fabricante Aruba Networks (2014), hace hincapié en que un "Access Point" trabajando en la norma 802.11ac puede generar múltiples transmisiones espaciales a diferentes dispositivos en forma simultánea (p.7)

Esta técnica es MU-MIMO (Del acrónimo “Mult User - Multiple Input Multiple Output”). Aruba Networks (2014), resalta que la compatibilidad con MU-MIMO requiere que los clientes cuenten con hardware con soporte.

MU-MIMO soporta varios tipos de configuraciones y toma como varíales el ancho de banda de canal, el SS (Del acrónimo “Spatial Streams”) (Aruba Networks, 2014)

En la tabla 4, se visualiza las diferentes configuraciones de velocidad en 802.11ac

Tabla 4. Velocidades de datos para varias configuraciones de 802.11ac.

DATA RATES FOR VARIOUS 802.11AC CONFIGURATIONS						
MCS	Lowest rates Mbps (20 MHz channel, 1x SS)		Channel width	Spatial streams	Highest rates Mbps (160 MHz channel, 8x SS)	
	Long GI	Short GI			Long GI	Short GI
0	6.5	7.2	x2.1 for 40 MHz x4.5 for 80 MHz x9.0 for 160 MHz	x2 for 2 SS x3 for 3 SS x4 for 4 SS x5 for 5 SS x6 for 6 SS x7 for 7 SS x8 for 8 SS	468.0	520.0
1	13.0	14.4			939.0	1040.0
2	19.5	21.7			1404.0	1560.0
3	26.0	28.9			1872.0	2080.0
4	39.0	43.3			2808.0	3120.0
5	52.0	57.8			3744.0	4160.0
6	58.5	65.0			4212.0	4680.0
7	65.0	72.2			4680.0	5200.0
8	78.0	86.7			5616.0	6240.0
9	(86.7)	(96.3)			6240.0	6933.3

Fuente: Aruba Networks (2014).

2.2.3. BSS, SID y ESSID

Un BSS es el nombre de la red Wi-Fi, siendo un SSID un Identificador de un conjunto de servicios y un ESSID es una extensión de la red Wi-Fi.

Un BSS (Basic Service Set) es un conjunto de servicio básico, también es conocido como nombre de la red Wi-Fi, con una identificación de 1 a 32 bytes, siendo un SSID (Service Set Identifier) el identificador de un conjunto de servicios y un ESSID en una extensión de la red Wi-Fi (Lopez, 2012).

En redes Wi-Fi de tipo empresariales se utiliza mucho el termino ESS y ESSID y existe para ampliar el área de trabajo de una red Wi-Fi. Así también para la segmentación por medio de vlans.

García y Tejada (2019) señalan como buena práctica segmentar la red para conexiones de tipo cableadas, así mismo resaltan el uso de perfiles para los usuarios para el acceso y restricción a los recursos de red y esto también se trasladan a las redes inalámbricas. Por último, hacen de conocimiento que los diferentes AP's del mercado pueden soportar múltiples SSID y la capacidad de asociar a una VLAN en específico, permitiendo múltiples escenarios de uso para redes de "campus" por ejemplo (p.18)

2.2.4. Punto de acceso inalámbrico (Access Point)

“Dispositivo intermediario entre la red inalámbrica y la red cableada” (López, 2012, p12). También conocido como “AP” (Del acrónimo “Access Point”) Este dispositivo hace realiza la conversión de 802.11 Wi-Fi a tramas Ethernet 802.3, haciendo posible la comunicación con la red.

2.2.5. Roaming L2

Barrenechea (2011) define Romaing L2 como "itinerancia" o movilidad la capa 2 del modelo OSI como la capacidad del dispositivo cliente Wi-Fi de moverse en un entorno de múltiples AP's desasociándose de uno y registrándose al próximo AP manteniendo la conectividad a la red (p.35)

2.2.5.1. Entorno centralizado

Un sistema centralizado de AP’s, estos reciben una IP dentro de un segmento de red para la gestión, mientras que los dispositivos usuarios o clientes reciben direcciones IP de un segmento de IP, donde los datos del usuario viajan encapsulados en paquetes LWAPP y enviados por un túnel hacia el WLC (Wireless Lan Controller), quien se encarga del enrutamiento de los paquetes hacia su destino, esto permite clasificar servicios como voz sobre IP, video, trafico web, entre otros y ejecutar calidad de servicio (priorización de tráfico) . (Mendoza, 2011)

El roaming, solo es posible en un entorno centralizado, donde cada punto de acceso inalámbrico puede “conversar” con otros y elegir el óptimo para brindar conexión a un dispositivo usuario. Un ejemplo es como se visualiza en la figura 2

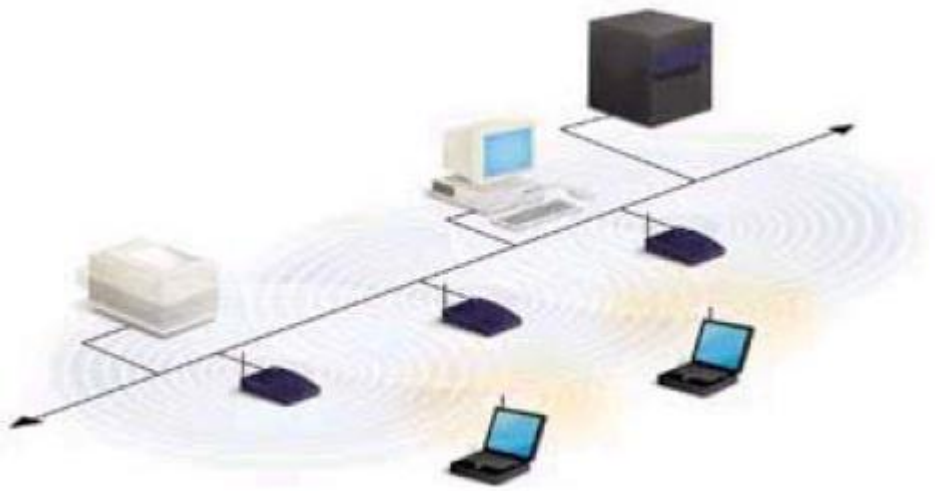


Figura 2. Utilización de varios Puntos de acceso.
Fuente: Barrenechea (2008)

2.2.6. Inspección profunda de paquetes (DPI)

Es un mecanismo de análisis de paquetes para capas superiores del modelo OSI (5-6-7). Siendo muy utilizado por equipos de protección perimetral de la red (Firewall).

Bonilla (2015) declara que el Deep Packet Inspeciton (DPI) es un mecanismo por el cual se detectan el tipo de encabezado (aplicación) del tráfico en la red (se analiza cabeceras de capa 7 del modelo OSI), permitiendo administrar, clasificar y restringir de ancho de banda de la red así como resolver problemas (p. 13)

2.2.6.1. Visibilidad de aplicaciones

El monitoreo típico de usuarios recolecta información de IP, ancho de banda utilizado, entre otros. Realizado por el switch, router y/o firewall.

2.2.6.2. Visibilidad de aplicaciones en redes Wi-Fi

> El fabricante de soluciones inalámbricas, Meraki (2013), hace énfasis en la recolección de información de usuario obtenida mediante la visibilidad de aplicaciones, del cual se presentan muchas ventajas innovadoras como entender el comportamiento del usuario sobre el uso de recursos de red ó navegación internet. Teniendo en cuenta el nivel de detalle (páginas web por categoría/tipo/popularidad, redes sociales, entre otros) las empresas pueden diseñar nuevas estrategias para solventar las necesidades de sus clientes (p. 3)

Proporcionar capacidades de análisis de tráfico a puntos de acceso inalámbricos mediante DPI permite crear bases de datos estadísticos, así como recolectar e identificar nuevas aplicaciones que aparecen con el tiempo y tener un estatus más detallado del comportamiento de sus usuarios (Meraki 2013)

En la figura 3 es un ejemplo de esquema de visualización de aplicaciones del fabricante Meraki

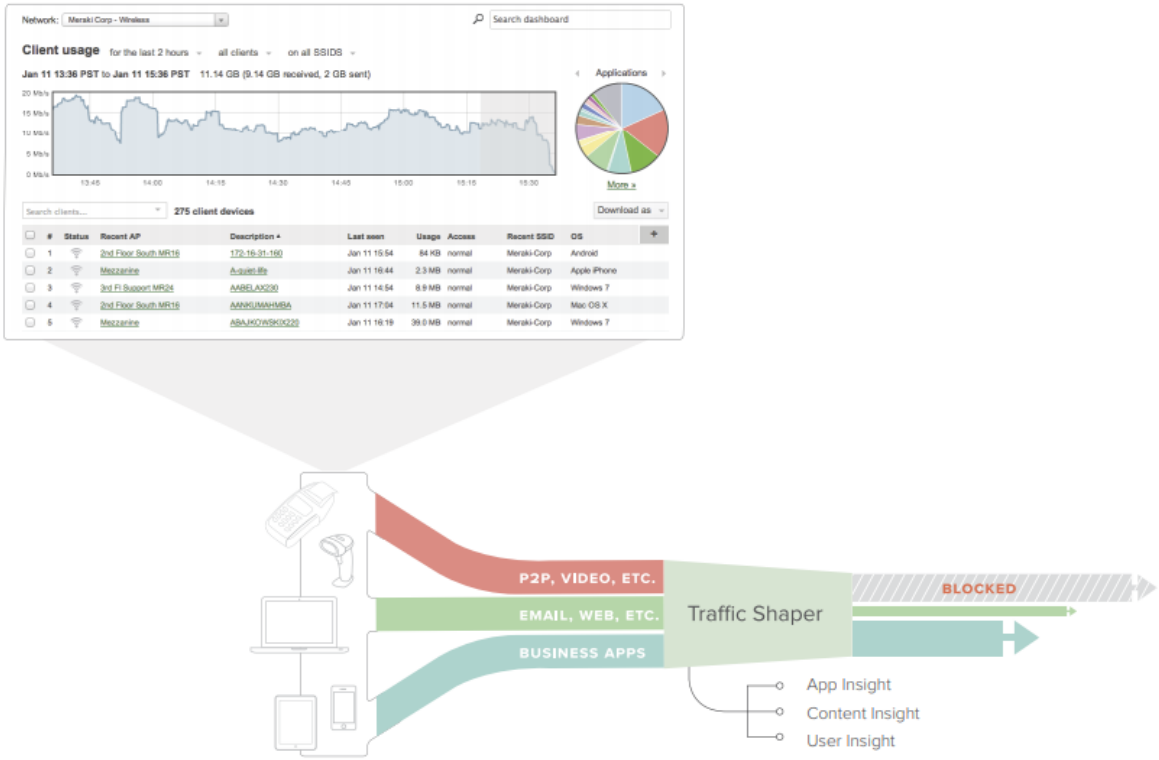


Figura 3. Análisis de tráfico y motor de conformación.
Fuente: Meraki (2013).

2.2.7. 802.1x

El estándar 802.1X define controles de acceso a la red basados en puertos y proporciona la estructura para autenticar dispositivos físicos conectados a una red. “802.1X nace como forma de poder permitir a cualquier elemento de la red (switches, AP, etc.) pedir un proceso de autenticación para una conexión que se acaba de producir” (Lopez, 2012, p.22)

Su arquitectura de trabajo está conformada por un “suplicante”, “un servidor de autorización” y un “autenticador”. Barrenechea (2011) detalla:

> - El suplicante, o equipo del cliente, que desea conectarse con la red.
> - El servidor de autorización se optó por emplearlos también para autenticación en las LAN.
> - El autenticador, que es el equipo de red (switch, enrutador, servidor de acceso remoto) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza. (p.40)

En la figura 4 se muestra los componentes de una autenticación mediante un servidor RADIUS

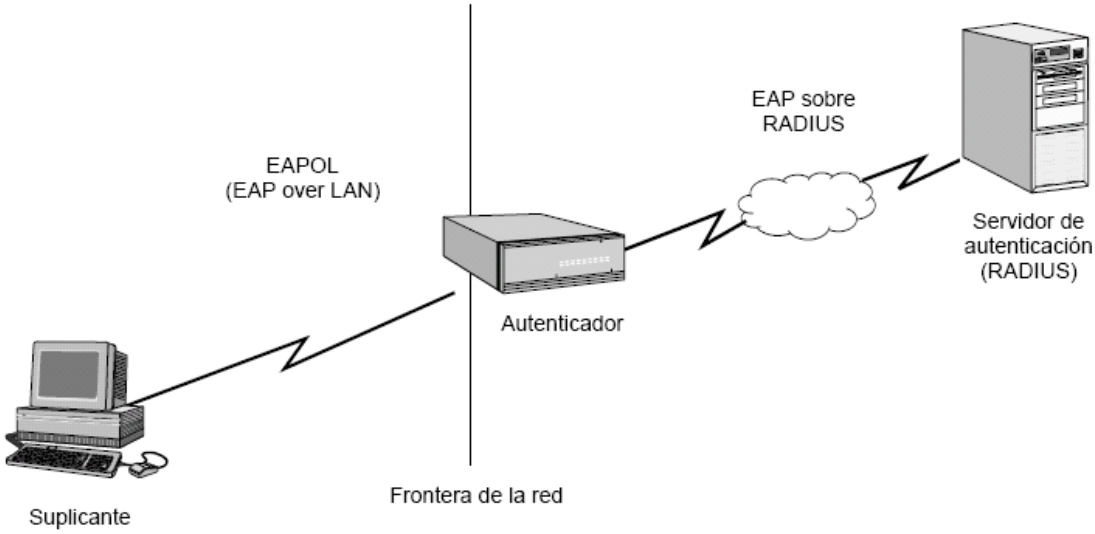


Figura 4. Arquitectura del sistema de autentificación.
Fuente: Barrenechea (2011).

2.2.8. EAP

EAP es un protocolo que ofrece una estructura de soporte para la autenticación.

Mendoza (2011) detalla el protocolo EAP como una "estructura" para la autenticación con 802.1x, lo que permite que los desarrolladores diseñen sus propios métodos EAP que realizan la autenticación (p.42)

López (2012) añade que: “Además de algunos específicos de proveedores comerciales, los definidos por RFC de la IETF incluyen EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, y EAP-AKA” (p.21)

Como se observa en la tabla 5 los tipos de EAP más utilizados tenemos:
Tabla 5. Tipos de EAP.

	Server Authentication	Supplication Authentication	Dynamic Key Delivery	Security Risks
EAP-MD5	None	Password Hash	No	Man-in-the-middle (MitM) attack, Session hijacking
LEAP	Password Hash	Password Hash	Yes	Identity exposed, Dictionary attack.
EAP-TLS	Public Key (Certificate)	Public Key (Certificate or SMART Card)	Yes	Identity exposed
EAP-TTLS	Public Key (Certificate)	CHAP, PAP, MS-CHAP (v2), EAP	Yes	MitM attack
PEAP	Public Key (Certificate)	Any EAP such as EAP-MS-CHAPv2 or Public Key	Yes	MitM attack; identity hidden in phase 2 but potential exposure in Phase 1

Fuente: Allied Telesis (2006).

2.2.8.1. EAP-MD5 (Message Digest)

Es un algoritmo de seguridad EAP, que proporciona soporte EAP nivel básico.

> El fabricante Allied Telesis (2006) señala a EAP-MD5 como un algoritmo autenticación básico para redes cableadas. Contando con un tamaño de mensaje de 128bits y autenticación de una sola vía EAP-MD5 se hace vulnerable para diferentes tipos de ataques en escenarios de redes públicas como detección de estaciones, valores de hash, o suplantación de estaciones. Entiéndase estaciones como los puntos de accesos inalámbricos (p.8)

2.2.8.2. EAP-TLS

Algoritmo propuesto por Microsoft. Mendoza (2011) resalta a EAP-TLS como un método de autenticación de tipo "fuerte", basándose en el uso de credenciales y llaves dinámicas pero también resalta como debilidad el uso masivo de certificados digitales tanto en dispositivos de todos los usuarios y en los servidores de autenticación (RADIUS).(p.43)

2.2.8.3. EAP-TTLS

Algoritmo propuesto por Funk Software y Certicom, Mendoza (2011) lo define como un método de autenticación "fuerte", basándose en credenciales, basado en el uso de credenciales y llaves dinámicas similar a EAP-TLS pero con la diferencia de que no se requiere desplegar certificados digitales en los dispositivos de usuarios, sino solo en los servidores de autenticación (RADIUS).

2.2.8.4. EAP-PEAP

Algoritmo propuesto por Microsoft, Cisco y RSA Security. Mendoza (2011) establece que EAP-PEAP utiliza un túnel para el intercambio de certificados. En este caso la cantidad de certificado disminuye drásticamente debido al uso de un emisor de certificados (p.43)

2.2.9. 802.11i

“El estándar IEEE 802.11i define los mecanismos y protocolos que debe usar una red para estar debidamente asegurada. Define una *Robust Security Network* (RSN) como una WLAN que permite la creación de únicamente asociaciones RSN (RSNA)” (García y Tejada, 2019, p.26)

En la figura 5 se observa los mecanismos bajo el estándar 802.11 Security

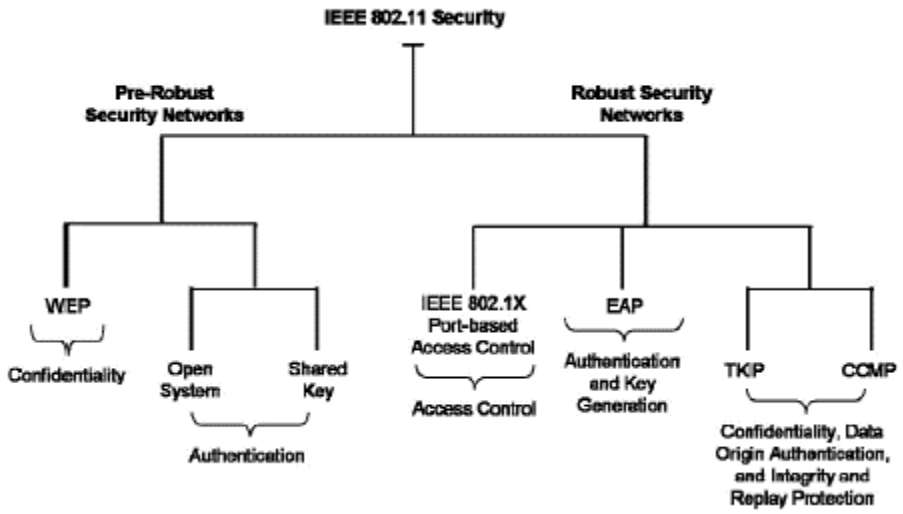


Figura 5. Protocolos y Mecanismos - 802.11i.
Fuente: García y Tejada, (2019)

Sobre las jerarquías de llaves criptográficas para la encriptación, García y Tejada (2019) especifican dos jerarquías de llave para las RSNA's: La "Pairwise Key Hierachy" encargada de proteger el tráfico unicast y la "Group Key Hierarchy" para proteger el tráfico multicast y broadcast (p.27). En la siguiente figura 6 se observa la jerarquía a detalle:

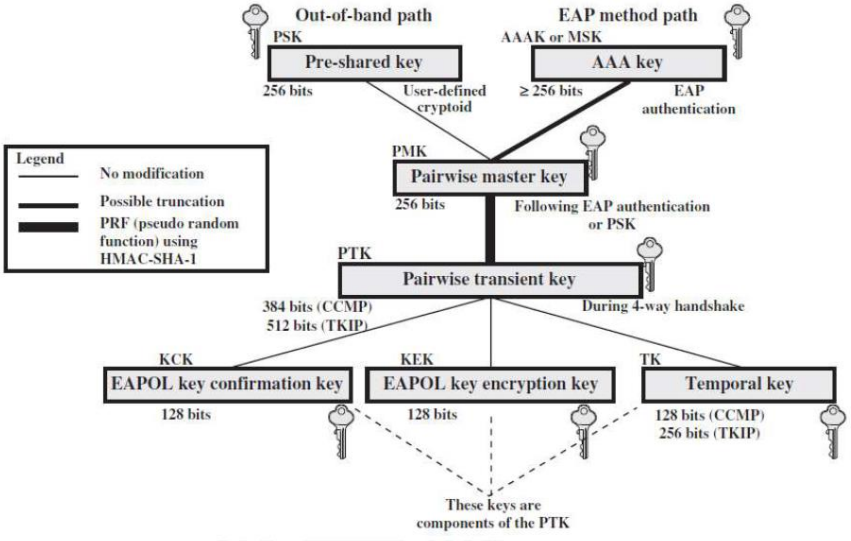


Figura 6. Pairwise Key Hierarchy - 802.11i.
Fuente: García y Tejada, (2019).

2.2.9.1. Pre-Shared Key (PSK)

García y Tejada (2019) Definen Pre-Shared Key como una llave compartida de tipo estática. Esta llave se comparte entre todos los usuarios y son configuradas en los dispositivos de usuario. PSK puede utilizar caracteres hexadecimales de 64 dígitos o de caracteres alfanuméricos, cuando se utiliza con la función HMAC-SHA1 pasa a convertirse en una Pairwise Master Key (PMK) (p.28)

2.2.9.2. Authentication, Authorization, and Accounting Key

> La AAA key también conocida como Master Session Key (MSK) es entregada al usuario mediante el protocolo EAP de un servidor de autenticación cuando se trabaja con 802.1X lo cual implica que el sistema trabaja con una autenticación por usuario a diferencia de la PSK (Garcia y Tejada, 2019, p.28)

Independientemente de usar PSK o AAA, ambas generan una *Pairwise Master Key* (PMK). Garcia y Tejada (2019) mencionan sobre PMK: “es una llave semilla que sirve de entrada al proceso de 4-way-handshake para generar las llaves de encriptación (TK)” (p.29)

2.2.9.3. Group Key Hierarchy

García y Tejada (2019) describen la Group Key Hierachy como una llave única para la encriptación de tráfico multicas/broadcast (GTK). A diferencia de la PMK que es una llave generada entre ambos miembros de la autenticación (suplicante y aunteticador) la Group Key Hierachy es generado solo por el autenticador y distribuido a las demás estaciones (p.29)

En la tabla 6 se observa los diferentes tipos de llaves para Wi-Fi

Tabla 6. Definiciones - Llaves de Encriptación según IEEE 802.11i.

Abbre-viation	Name	Description / Purpose	Size (bits)	Type
AAA Key	Authentication, Accounting, and Authorization Key	Used to derive the PMK. Used with the IEEE 802.1X authentication and key management approach. Same as MSK.	≥ 256	Key generation key, root key
PSK	Pre-Shared Key	Becomes the PMK in pre-shared key environments.	256	Key generation key, root key
PMK	Pairwise Master Key	Used with other inputs to derive the PTK.	256	Key generation key
GMK	Group Master Key	Used with other inputs to derive the GTK.	128	Key generation key
PTK	Pairwise Transient Key	Derived from the PMK. Comprises the EAPOL-KCK, EAPOL-KEK, and TK and (for TKIP) the MIC key.	512 (TKIP) 384 (CCMP)	Composite key
TK	Temporal Key	Used with TKIP or CCMP to provide confidentiality and integrity protection for unicast user traffic.	256 (TKIP) 128 (CCMP)	Traffic key
GTK	Group Temporal Key	Derived from the GMK. Used to provide confidentiality and integrity protection for multicast/broadcast user traffic.	256 (TKIP) 128 (CCMP) 40, 104 (WEP)	Traffic key
MIC Key	Message Integrity Code Key	Used by TKIP's Michael MIC to provide integrity protection of messages.	64	Message integrity key
EAPOL-KCK	EAPOL-Key Confirmation Key	Used to provide integrity protection for key material distributed during the 4-Way Handshake.	128	Message integrity key
EAPOL-KEK	EAPOL-Key Encryption Key	Used to ensure the confidentiality of the GTK and other key material in the 4-Way Handshake.	128	Traffic key / key encryption key
WEP Key	Wired Equivalent Privacy Key	Used with WEP.	40, 104	Traffic key

Fuente: García y Tejada, (2019).

2.2.9.4. TKIP y CCMP

En relación TKIP y CCMP, Garcia y Tejada mencionan: "El estándar IEEE 802.11i define dos protocolos para asegurar la confidencialidad e integridad de la información: *Temporal Key Integrity Protocol* (TKIP) y *Counter Mode with Cipher Block Chaining MAC Protocol* (CCMP)."

Así mismo García y Tejada (2019) describen sobre TKIP, siendo una implementación especifica parar resolver las vulnerabilidades de WEP. Pero al mismo tiempo no es recomendado para entornos de mayor seguridad debido a vulnerabilidades conocidas sobre RC4 y MIC del cual se vale TKIP para funcionar (p.30)

> Por otro lado, CCMP fue desarrollado sin la restricción de usar el hardware anterior (RC4). Es considerado la solución a largo plazo para la seguridad en WLANs. Es obligatorio su uso en un despliegue de RSN. CCMP está basado en CCM, un modo de cifrado por bloques autenticado genérico de AES [12]. CCM combina dos conocidas y comprobadas técnicas para lograr una seguridad robusta. Usa CTR para la confidencialidad y Cipher Block Chaining MAC (CBC-MAC) para proteger la autenticación e integridad de la información. CCMP protege la integridad tanto de las tramas de datos, así como de algunas partes de las cabeceras de las tramas 802.11. (Garcia y Tejada, 2019, p.31)

2.2.10. Certificaciones de seguridad Wi-Fi

Wi-fi Alliance certifica 05 tipos de mecanismo de seguridad: 802.11 Legacy, WPA Personal, WPA Enterprise. WPA2 Personal y WPA2 Enterprise

En la figura 7 se detalla el algoritmo de confidencialidad, cifrado, así como el método de autenticación requerido

Tabla 7. Certificaciones de Seguridad Wi-Fi Alliance.

Certificación Wi-Fi Alliance	802.11 Legacy	WPA		WPA 2	
		Personal	Enterprise	Personal	Enterprise
Método de Autenticación	Open System / Shared Key	PSK	802.1X /EAP	PSK	802.1X/EAP
Algoritmo Confidencialidad	WEP	TKIP	TKIP	CCMP	CCMP
Mecanismo de Cifrado	RC4	RC4	RC4	AES	AES
Tamaño de llaves	40 o 104 bits	128 bits (Encriptación)		128 bits (Encriptación e Integridad)	
		64 bits (Integridad)			
Mecanismo de Integridad	CRC -32	Michael MIC		CCM	
Protección de cabeceras	-	Direcciones MAC de origen y destino protegidas con MIC		Direcciones MAC de origen y destino protegidas con CCM	
Detección de *Replay*	-	Secuenciamiento de IV		Secuenciamiento de IV	

Fuente: García y Tejada, (2019).

2.2.11. RADIUS

Del acrónimo (Remote Authentication Dial-In User Server). es un protocolo de autenticación y contabilidad estándar definido en RFC 2865 y RFC 2866

Su arquitectura es de tipo cliente servidor, siendo los clientes incorporados en dispositivos de red como switches, puntos de acceso inalámbrico, entre otros

El modo de funcionamiento es el que describe Lopez (2012):

> Por ejemplo, cuando se realiza la conexión con un ISP mediante un módem, DSL, cable módem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Network Access Server o Servidor de Acceso a la Red) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autentificación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc. (p.24)

Siendo un protocolo utilizado en redes WPA/WPA2-Empresariales, Barrenechea (2011) señala como requisito indispensable el utilizar servidor RADIUS que generará y compartirá las claves de cifrado que serán solicitadas por los puntos de acceso que empleen WPA/WPA2 (como parte proceso de acceso a la red para dispositivos inalámbrico (autenticación 802.1x y método EAP) (p. 18)

RADIUS no está especificado dentro del estándar 802.11, García y Tejada (2019) menciona lo siguiente “El estándar IEEE 802.11 no obliga o especifica el uso de un servidor RADIUS. (p.18).
Pero 802.1x si se encuentra especificado dentro de 802.11.” Los servidores RADIUS en la práctica son uno de los principales componentes en el esquema de trabajo del 802.1X” (García y Tejada, 2019, p.18).

2.2.12. Perfil de acceso a la red

El perfilamiento de usuarios en la red permite optimizar el uso de las redes de usuario. Barnechea (2011) seña que al definir perfiles de acceso y de rendimiento de aplicaciones, así como de servicios y aplicaciones de red mejora el uso de ancho de banda de la misma (p.59)

2.2.13. Calidad de servicio (QoS)

Son los mecanismos que aseguran la disponibilidad del uso de un servicio en la red

El fabricante Alcatel Lucent (2019), en la documentación de sus equipos, aclara que QoS se refiere a la calidad de la transmisión y a la disponibilidad del servicio de la red.

QoS puede garantizar el tráfico para un tipo particular de paquete que circula en la red. QoS se emplea en redes ATM y también en redes IP a pesar de utilizar mecanismos diferentes (ATM realiza conmutación de circuitos y establece y clasifica el tráfico según la prioridad para enviarlos sobre rutas virtuales mientras que en una transmisión IP que utiliza conmutación de paquetes, se reparten recursos de ancho de banda para el envío de paquetes y se prioriza él envió, también conocido como mejor esfuerzo o "best-effort) (pag.27-3)

Entre los más usados, tenemos QoS de tipo básico, 802.1p, ToS, y DSCP.

El fabricante de equipos, Alcatel Lucent (2019), en su documentación técnica de equipos, describe varios tipos de policitas como ICMP (priorización/limitación de tráfico para aplicaciones ICMP), 802.1p, ToS o DSCP que son mecanismos para marcar y mapear paquetes (clasificar y diferenciar tráfico) (p.27-2)

2.2.14. WLC (Wireless Lan Controller)

Un WLC es un dispositivo que permite la gestión y funcionamiento centralizado de un grupo de AP's. (Mendoza, 2011) menciona sobre un WLC del fabricante Cisco.

Mendoza (2011) describe características esenciales del WLC de cisco como la de administrar de forma centralizada todos los Access point agregados al sistema volviendo el despliegue simple, así como también la de desplegar policitas de acceso seguro para usuarios y priorización de tráfico (QoS). Por ultimo y con lo mencionado se puede desplegar escenarios de redundancia a nivel de servicio (p.51). En la actualidad existen tres tipos de WLC, o también llamados "controladores":

- WLC dedicado: Es un controlador que opera dentro de un chasis o servidor dedicado, también conocido como "controlador virtual"
- WLC embebido: Este puede instalarse dentro de un dispositivo de red como un switch o incluso un AP.
- WLC en la nube: Es un controlador que se encuentra en Internet

2.2.15. Punto de acceso inalámbrico Stellar de Alcatel

Son una familia de AP's que pueden ser gestionados como un WLC dedicado, embebido y en la nube.

2.2.15.1. Stellar AP 1220

Es un punto de acceso inalámbrico de gama empresarial, soporta los estándares IEEE 802.11a/b/g/n/ac.

> La serie 802.11ac AP1220 de alto rendimiento admite una velocidad de datos simultánea máxima de 2.1 Gb / s (1733 Mb / s en 5 GHz y 400 Mb / s en 2.4 GHz), canales de 160 MHz (VHT160 *), MIMO multiusuario (MU -MIMO) y cuatro flujos espaciales (4SS). Proporcionan transmisión de datos de multidifusión simultánea a múltiples dispositivos, maximizando el rendimiento de datos y mejorando la eficiencia de la red. (Alcatel Lucent, OmniAccess Stellar AP1220 Series, 2019, pag.1)

> The high performance 802.11ac AP1220 series supports a maximum concurrent data rate of 2.1 Gb/s (1733 Mb/s in 5 GHz and 400 Mb/s in 2.4 GHz), 160 MHz

channels (VHT160*), multi-user MIMO (MU-MIMO) and four spatial streams (4SS). They provide simultaneous multicast data transmission to multiple devices, maximizing data throughput and improving network efficiency. (Alcatel Lucent, OmniAccess Stellar AP1220 Series, 2019, pag.1)

Existen 02 modelos, el 1221 (AP con antena integrada) y el 1222 (AP con antena externa), tal y como se muestra en la figura 7:

Figura 7. Vista de modelo AP1221 y AP1222.
Fuente: Alcatel-Lucent, OmniAccess Stellar AP1220 Series datsheet, (2019).

2.2.15.2. Stellar AP – 802.1X

Los AP's Stellar 1220 soportan la autenticación basada en MAC (Media Acces Control) y en 802.1X

Alcatel-Lucent Enterprise cumple totalmente este requisito y, de hecho, recomienda utilizar 802.1x para la autenticación de usuario, tanto inalámbrica como con cable. En la autenticación 802.1x participan tres partes: un solicitante, un autenticador y un servidor de autenticación. El solicitante es un dispositivo cliente (como un ordenador portátil o un smartphone) que quiere conectarse a la red WLAN. El servidor de autenticación normalmente es un host que ejecuta software compatible con los protocolos RADIUS y EAP. En el marco de la solución OmniAccess Stellar WLAN, el autenticador es el propio punto de acceso OmniAccess Stellar que actúa como un guarda de seguridad ante la red protegida. El dispositivo cliente inalámbrico no puede acceder a través del autenticador/AP a la parte protegida de la red hasta que su identidad se haya validado y autorizado. (Alcatel Lucent Enterprise (2018). WLAN Alcatel-Lucent Enterprise, 2019, pag.40)

En la figura 8 se muestra el esquema de autenticación entre dispositivo de usuario, AP y el servidor RAIDUS mediante 802.1x

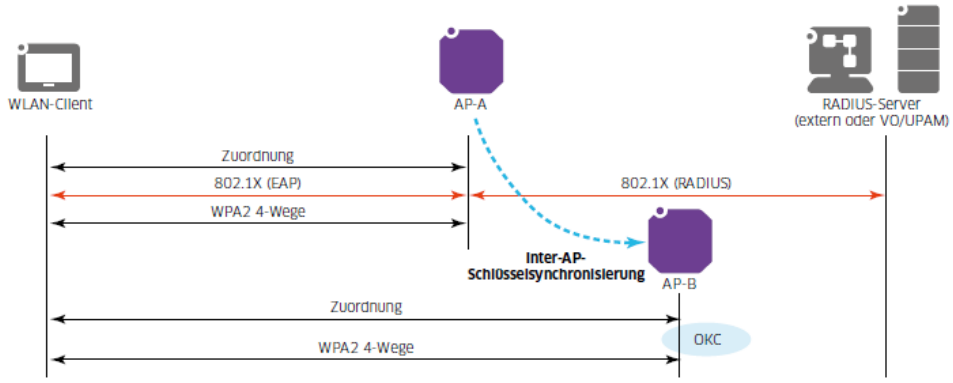


Figura 8. OmniAccess Stellar y 802.1x
Fuente: Alcatel-Lucent, WLAN Alcatel-Lucent Enterprise (2018)

Una característica importante de este AP es la función de DPI integrada al equipo:

El fabricante Alcatel (2019) en su documentación técnica del Access Point modelo OAW-AP1220 especifica que sus dispositivos cuentan con el chip DPI permitiendo la detección, clasificación, filtrado y priorización de trafico de las aplicaciones, y optimizando el tráfico de paquetes en la red inalámbrica (pag.2)

Dentro de la familia 1220 de Stellar, están el modelo AP1221 y AP1222, siendo el primero un AP con antena integrada y el segundo con antena externa.

En la tabla a 8, se podrá observar las características más resaltantes

Tabla 8. Vista de modelo AP1221 y AP1222.

Caracteristica	**AP 1221**	**AP 1222**
Numero de radios	2	2
Bandas soportadas	2.4GHz & 5GHz	2.4GHz & 5GHz
Estandares 802.11	802.11a/b/g/n/ac wave 2	802.11a/b/g/n/ac wave 2
MIMO	MU-MIMO	MU-MIMO
SSID	16	16
maximo numero de clientes asociados por radio	256	256
Potencia de transmisión maxima	18dBm	18dBm
Ganacia de antena	4dBi - 2.4Ghz/6.3dBi - 5Ghz	-
Tipo de antena	Integrada	Externa
Interfaz de red	1GbE	1GbE
Soporte BLE	si	si
Soporte energización PoE	si	si
Soporte DPI	si	si
Soporte WIPS/WIDS	si	si
Potencia maxima de consumo	15.6W	15.6W

Fuente: Propia

2.2.16. Controlador WLAN Omnivista Cirrus

Es una solución de controlador en la nube perteneciente a Alcatel Lucent Dentro de sus cualidades se tiene:

2.2.16.1. Gestión unificada

“Política de acceso basada en roles centralizada con administrador de políticas de autenticación incorporado” (Alcatel Lucent, Omnivista Cirrus, 2019, pag.7)

En la figura 9 se muestra la interfaz de administración de equipos. La solución Omnivista Cirrus soporta la administración de Stellar AP’s, así como switches de acceso, distribución y core del mismo fabricante.

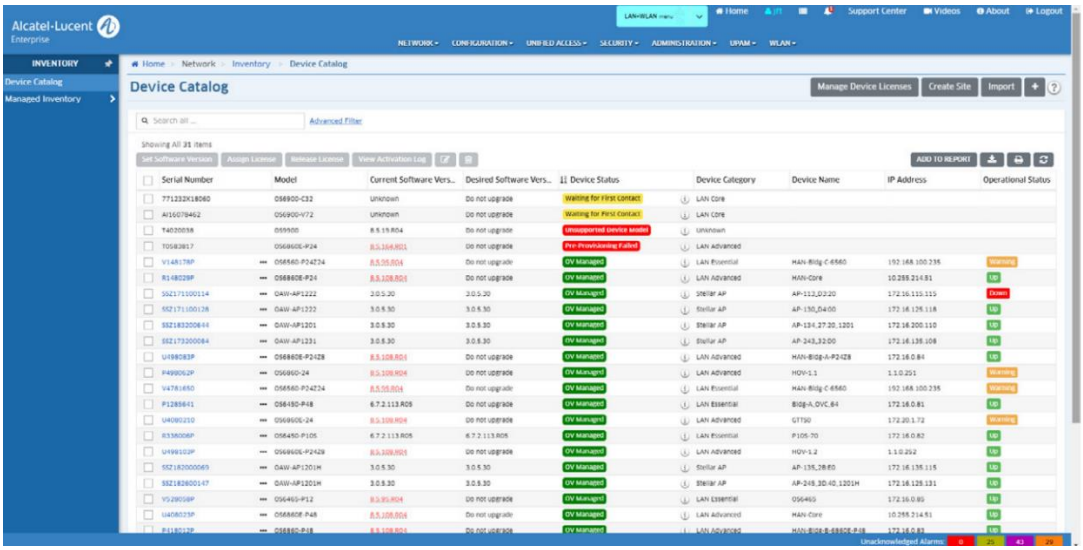


Figura 9. Catálogo de dispositivos
Fuente: Propia

2.2.16.2. Dashboard

"Monitoreo y análisis en tiempo real de los indicadores críticos de rendimiento de la red a través de widgets visuales" (Alcatel Lucent, Omnivista Cirrus, 2019, pag.7)

En la figura 10 se visualiza el Dashboard WLAN, donde se brinda información de SSID, AP Group, AP, clientes, entre otros:

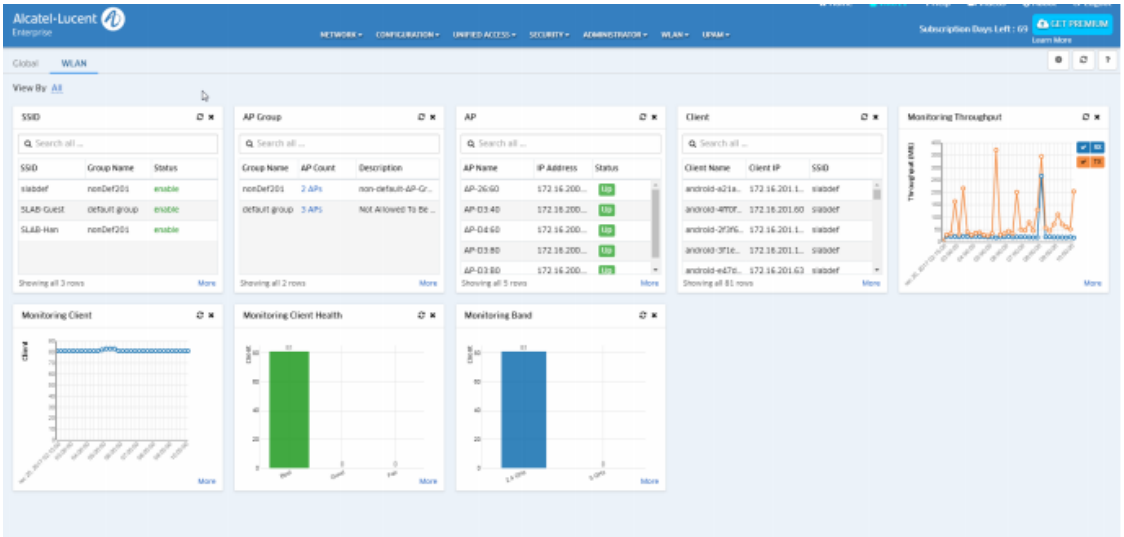


Figura 10. OmniVista Cirrus Dashboard
Fuente: Propia

2.2.16.3. Visibilidad de aplicaciones:

La función de visibilidad provee información para el inventario, monitoreo y uso de aplicaciones en toda la red inalámbrica, lo que permite un mejor entendimiento del consumo de ancho de banda entre los distintos tipos de aplicaciones esenciales como no esenciales (Alcatel Lucent, Omnivista Cirrus, 2019)

2.2.16.4. Gestor de autenticación de políticas unificadas

La solución de servidor RAIUDS de Omnivista Cirrus de Alcatel Lucent es personalizada y enriquecida. Este servidor se llama UPAM (Unified Policy Authentication Manager)

UPAM, opera como servidor RADIUS con funciones enriquecidas, con función gestor de políticas con aplicación de acceso para invitados y para dispositivos visitantes y una solución de acceso BYOD (Bring Your Own Device), trae tu propio dispositivo, para incorporación segura de dispositivos de los empleados (Alcatel Lucent Enterprise, 2019)

En la figura 11 se resume las características de UPAM

Figura 11. Gestor de autenticación de políticas unificadas: modo
Fuente: Alcatel-Lucent WLAN Alcatel-Lucent Enterprise (2018)

Las funciones del módulo UPAM van desde ser un servidor RADIUS de tipo local a interactuar con un servidor RADIUS externo o con un servidor Microsoft Active Directory o LDAP corporativo. La conexión a un origen de autenticación externo permite la gestión centralizada de usuarios con la posibilidad de asignar “perfiles de funciones” de usuario o dispositivo (VLAN, QoS y ACL de seguridad) según los atributos AD/LDAP. (WLAN Alcatel-Lucent Enterprise, 2019)

2.2.16.5. Funcionamiento de controlador en la nube

El controlador en la nube, Omnivista Cirrus, opera en bases a entidades llamadas objetos. Estos objetos contienen las características de funcionamiento de los AP’s en el OmniVista Cirrus, pero no están dentro en los AP’s hasta que se los traslada.

Esta característica de trabajo permite al AP operar de manera independiente en relación a sus parámetros de funcionamiento (SSID, autenticación, perfil, etc.) salvo cuando surge una modificación por parte del usuario.

2.2.16.6. AP Group

En Omnivista Cirrus, un AP Group es un grupo de AP’s los cuales van a operar bajo un dominio de trabajo.

2.2.16.7. WLAN Service

En Omnivista Cirrus el SSID, el tipo de autenticación, y el Acces Role Profile están definidos dentro de un conjunto de servicio, que es llamado WLAN Service.

2.2.16.8. Access Role Profile

Un Access Role Profile (ARP) es un perfil para la conexión, que contiene características como el control de ancho de banda, vlan y asignación de políticas y restricciones

2.2.16.9. Portal Cautivo

El método de acceso para usuarios invitados será realizado sobre un portal cautivo (Portal web personalizado donde el usuario introduce sus nombres de usuario y contraseña, con autenticación MAC y credenciales de acceso, los cuales podrán serán credos en el Omnivista Cirrus

2.2.16.10. Visibilidad de aplicaciones en OmniVista Cirrus

La función de DPI en los Stellar AP1221 se activan dentro del Omnivista Cirrus. La recolección de datos será mostrada en el Dashboard de la interfaz de administración.

Cabe señalar que para la identificación de nuevas aplicaciones es necesario carga una base de datos actualizadas de estas. Omnivista Cirrus lo realiza de forma automática y periódica.

2.3. Definición de términos básicos

AES (Advanced Encryption Standard), Estándar de Encriptación Avanzado
AP (Acces Point) Punto de acceso inalámbrico
Captive Portal, Portal cautivo
Control Plane, Plano de control
Data Plane, Plano de datos
DPI (Deep Packet Inspection) Inspección profunda de paquetes
EAP (Extensible Authentication Protocol), Protocolo de Autenticación Extensible
Management Plane, Plano de gestión
QoS (Quality of Service), Calidad de Servicio
SSID (Service Set Identify), Identificador de Conjunto de Servicios
TKIP (Temporal Key Integrity Protocol), Protocolo de integridad de clave temporal
VC (Virtual Controller) Controlador virtual
VLAN (Virtual LAN), Redes LAN Virtuales
Wi-Fi (Wireless Fidelity), Fidelidad Inalámbrica
WLC (Wireless Lan Controller) Controladores de Puntos de Acceso
WMM (Wi-Fi Multimedia)
WPA Wi-Fi (Protected Access), Acceso Wi-Fi protegido
WPA-2 (Wi-Fi Protected Access), Actualización de Acceso Wi-Fi protegido
AD (Active Directory)
LDAP (Lightweight Directory Access Protocol
UPAM (Unified Policy Authentication Manager)

CAPITULO III DESARROLLO DEL TRABAJO DE SUFICIENCIA PROFESIONAL

3.1. Modelo de solución propuesto

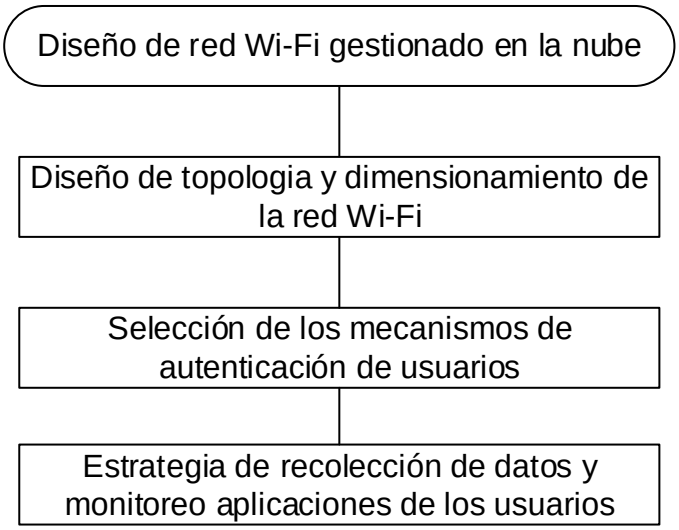


Figura 12. Esquema general de implementación
Fuente: Propia

El desarrollo del diseño de red Wi-Fi gestionado en la nube iniciará con:

1) Diseño de topología y dimensionamiento de la red Wi-Fi:

   Levantamiento de información de los AP's, segmento de red en el cual se administran, así como las vlan de gestión, vlan de usuarios, SSID e identificación de parámetros de calidad de servicio dentro de cada SSID. En esta actividad también se recopilará la cantidad de usuarios concurrentes, las velocidades de conexión inalámbrica establecida para luego proceder con el diseño de la topología de red

   Dimensionamiento de componentes de red como AP's y licenciamiento de plataforma de gestión. Con todos los parámetros definidos se seleccionará un modelo de AP de la marca Alcatel Lucent que cumpla con los requisitos del diseño. Aquí se considerará también la herramienta de inspección de paquetes DPI (Deep Packet Inspection) para la recopilación de información del usuario.

2) Selección de los mecanismos de autenticación de usuarios:
   En este apartado se clasificará y analizará los tipos de usuarios y se seleccionará el método de autenticación

3) Estrategia de recolección de datos y monitoreo de aplicaciones de los usuarios:
   Aquí se definirá la estrategia del uso de la herramienta de inspección profunda de paquetes, así como las herramientas dentro de la plataforma de gestión que realizan la función de monitoreo

3.1.1. Desarrollo 01: Diseño de topología y dimensionamiento de los componentes de red Wi-Fi gestionado en la nube

3.1.1.1. Levantamiento de información de la red Wi-Fi

El grupo Ilender cuenta con 04 sedes, las cuales son:

1) San Isidro: En esta sede se encuentran las oficinas administrativas de las empresas Corporación Ilender, Fructus Terrum, Labot, +futuro, Animal Pharm, cdtel y Ummana
2) Surco: Oficinas En esta sede se encuentran oficinas administrativas de las empresas Corporación Ilender
3) Ate: En esta sede se encuentra oficinas almacenes de la empresa Corporación Ilender
4) Lurín: En esta sede se encuentra oficinas y almacenes de la empresa Labot

3.1.1.2. San Isidro

En esta sede se accedió a la interfaz web de administración de los AP's como se muestra en la figura 13, que está conformado por los AP's y un controlador embebido dentro de 01 AP con rol de maestro.

De la imagen mostrada, se puede observar que la IP de administración (Controlador Virtual) es 192.168.10.141, así mismo también se identifica 04 AP's y 03 SSID: "GRUPO_ARMEJOR", GRUPO_ARMEJO_VISITANTES" y "CAPTIVE_PORTA" (Este último se encuentra deshabilitado)

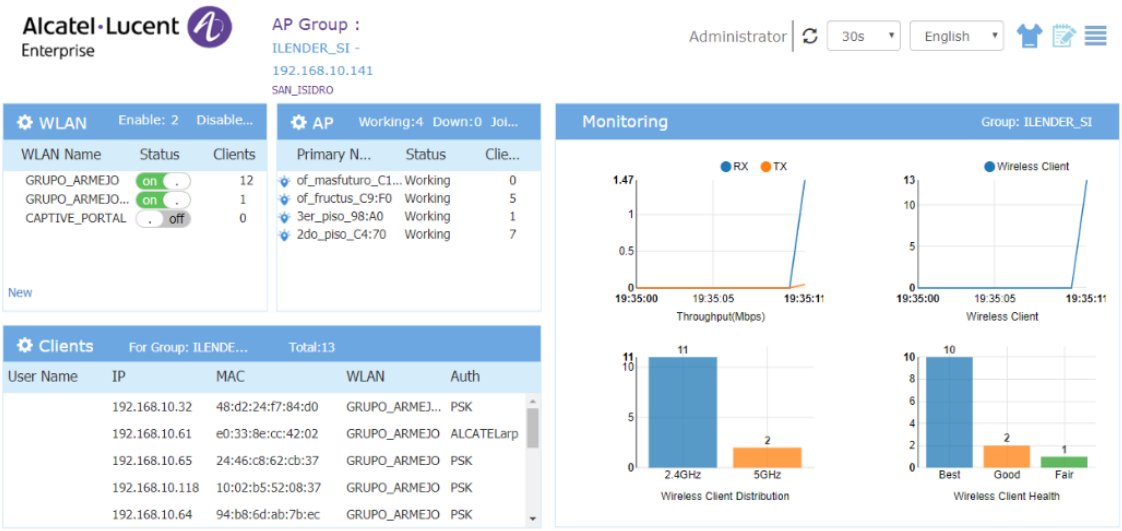


Figura 13. Interfaz de gestión de AP's en San Isidro
Fuente: Propia

En la imagen 14, se explora en la ventana "AP Configuration" donde se muestra las direcciones IP de cada AP:

- 192.168.10.141 (AP): IP de controlador virtual
- 192.168.10.142 (AP): IP de dispositivo AP
- 192.168.10.143 (AP): IP de dispositivo AP
- 192.168.10.144 (AP): IP de dispositivo AP
- 192.168.10.145 (AP): IP de dispositivo AP

Los parámetros básicos de conexión a otras redes:

DNS: 8.8.8.8

Gateway: 192.168.10.200

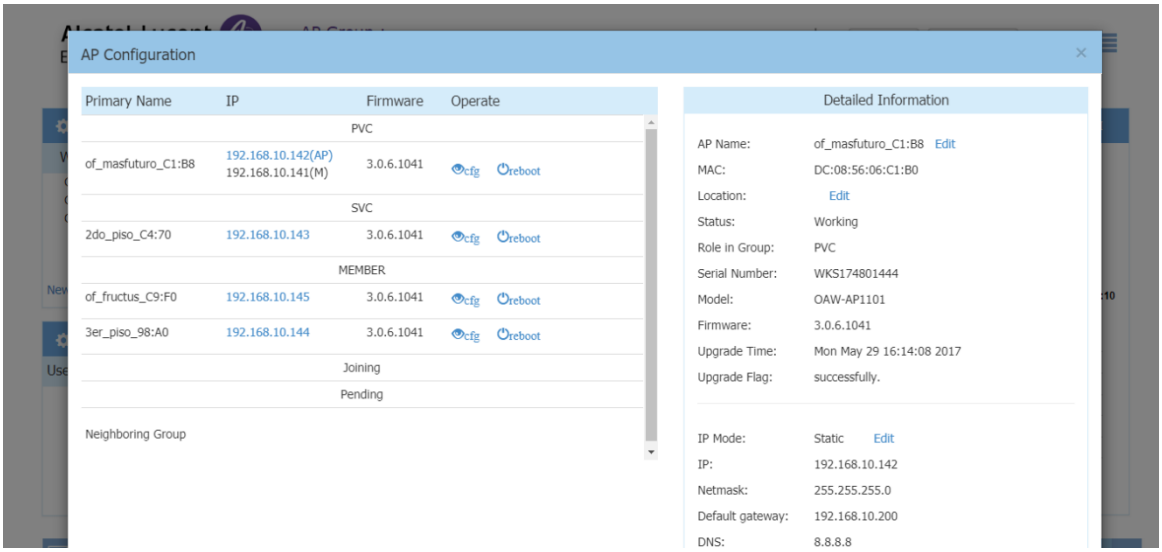


Figura 14. Lista de AP's en San Isidro
Fuente: Propia

En la siguiente figura 15, en la ventana "WLAN Configuration" se observa los parámetros de configuración del SSID "GRUPO_ARMEJO"

En el campo "VLAN ID" esta con el valor "0", que indica que el SSID no se etiqueta con una vlan (Untagged)

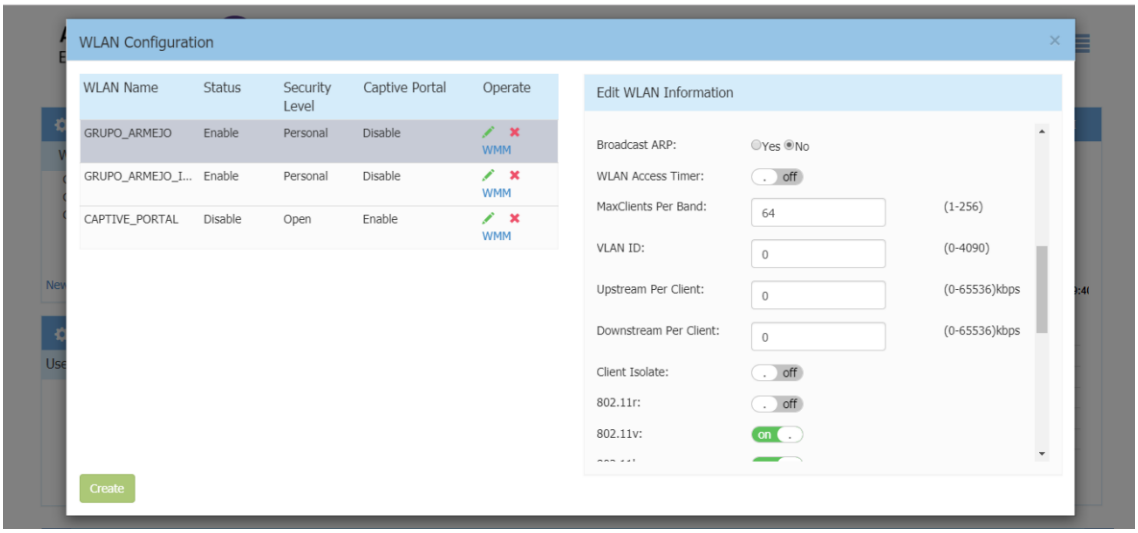


Figura 15. SSID's GRUPO_ARMEJO
Fuente: Propia

En la siguiente figura 16 se observa los parámetros de configuración del SSID “GRUPO_ARMEJO_INVITADOS”

En el campo “VLAN ID” esta con el valor “0”, que indica que el SSID no se etiqueta con una vlan (Untagged)

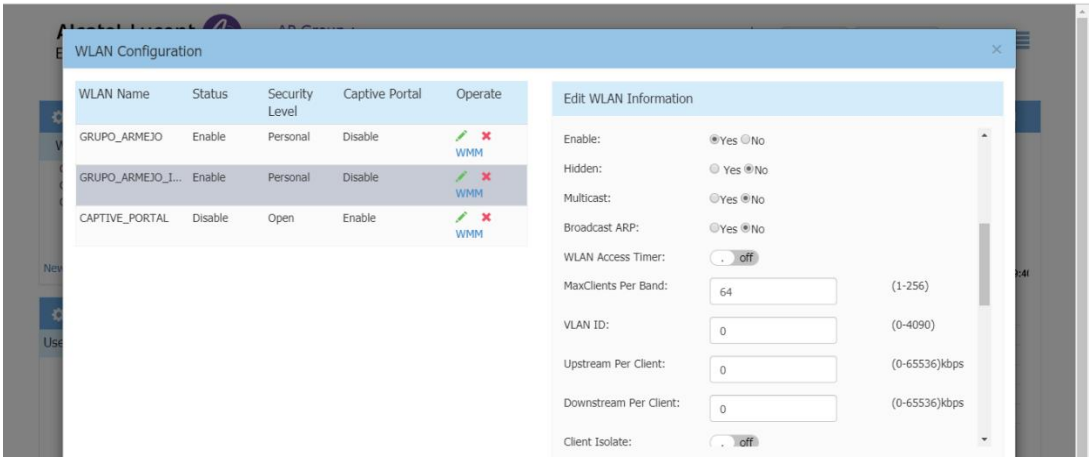


Figura 16. SSID’s GRUPO_ARMEJO_ INVITADOS
Fuente: Propia

En la siguiente figura 17 se observa en la ventana “Clients” que las direcciones IP de los usuarios están dentro del rango 192.168.10.0/24 , este segmento de red está siendo utilizado por el SSID “GRUPO_ARMEJO” y “GRUPO_ARMEJO_INVITADOS” debido a que estos están definidos con la misma vlan por defecto y no etiquetada

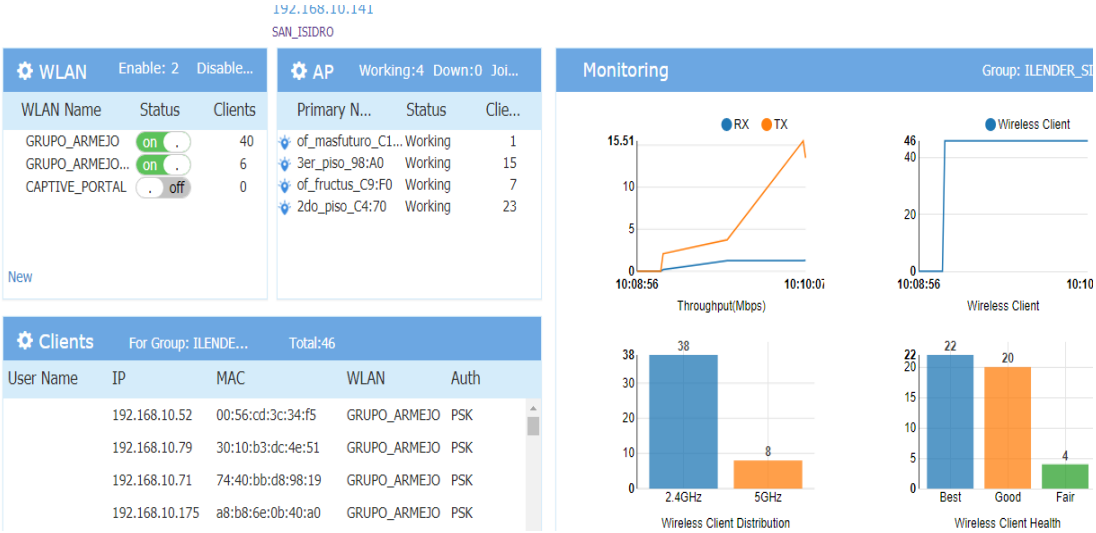


Figura 17. Clientes conectados San Isidro
Fuente: Propia

La información sobre parámetros de los AP's en la red Wi-Fi de la sede San Isidro se resume en la tabla 9:

Tabla 9. Inventario de AP's sede San Isidro

Nro	Marca	Modelo	Nombre	IP	SSID - Vlan asociada	User	Password	Vlan "Untagged"
1	Alcatel	AP-1101	of_masfuturo_C1:B8	192.168.1.142	"GRUPO_ARMEJO" vlan id=0 "GRUPO_ARMEJO_INVITADOS" vlan id=0	admin	Alcatel2019	10
2	Alcatel	AP-1101	2do_piso_C4:70	192.168.1.143	"GRUPO_ARMEJO" vlan id=0 "GRUPO_ARMEJO_INVITADOS" vlan id=0	admin	Alcatel2019	10
3	Alcatel	AP-1101	3er_piso_98:A0	192.168.1.144	"GRUPO_ARMEJO" vlan id=0 "GRUPO_ARMEJO_INVITADOS" vlan id=0	admin	Alcatel2019	10
4	Alcatel	AP-1101	of_fructus_C9:F0	192.168.1.145	"GRUPO_ARMEJO" vlan id=0 "GRUPO_ARMEJO_INVITADOS" vlan id=0	admin	Alcatel2019	10

Fuente: Propia

En la figura 18 se visualiza 04 dispositivos conectados al SSID GRUPO_ARMEJO_INVITADOS y el resto a GRUPO_ARMEJO

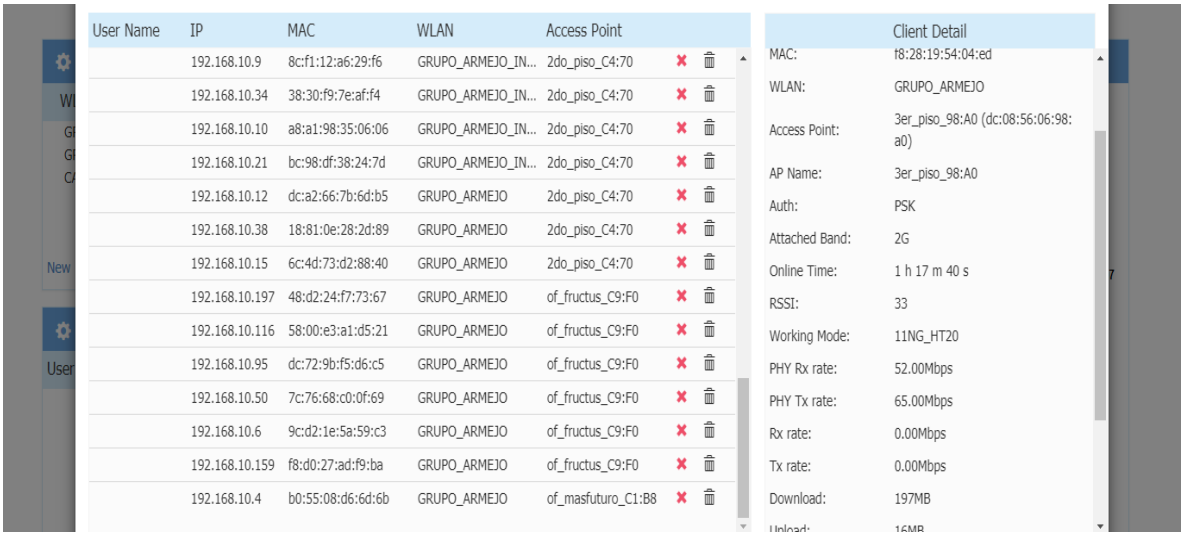


Figura 18. Clientes conectados por SSID en San Isidro
Fuente: Propia

La información sobre usuarios en la red Wi-Fi de la sede San Isidro se resume en la tabla 10:

Tabla 10. Lista de SSID y usuarios concurrentes sede San Isidro

	SSID	Usuarios concurrentes
1	GRUPO_ARMEJO	42
2	GRUPO_ARMEJO_INVITADOS	4

Fuente: Propia

3.1.1.3. Surco

En esta sede se accedió a la interfaz web de administración de los AP's como se muestra en la imagen 19, que está conformado por los AP's y un controlador embebido dentro de 01 AP con rol de maestro.

De la imagen mostrada, se puede observar que la IP de administración (Controlador Virtual) es 192.168.8.123, así mismo también se identifica 06 AP's y 02 SSID: "Ilender-Qubo" e "Ilender_Visitantes"

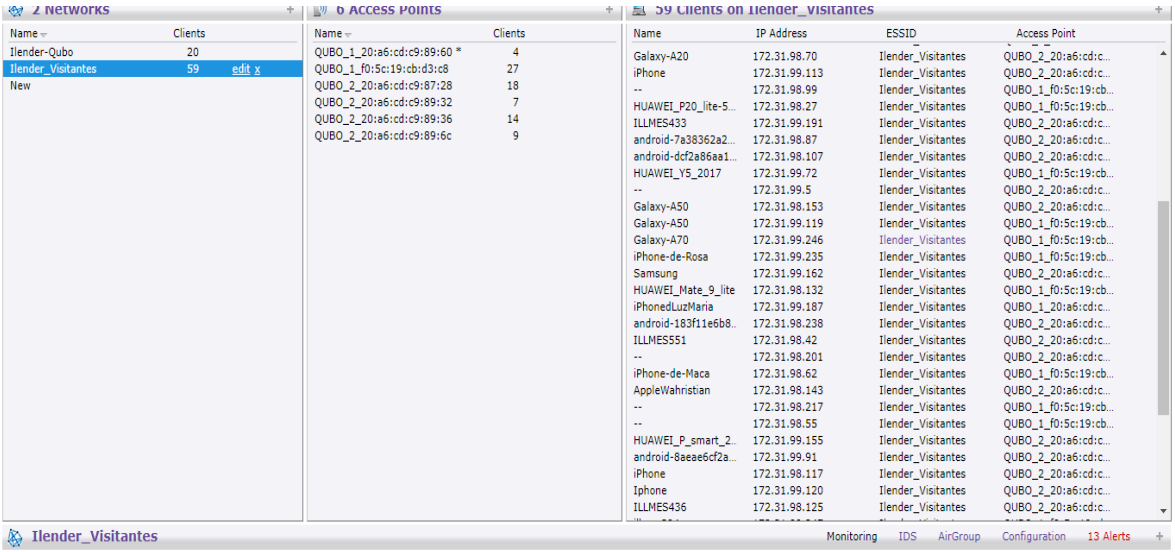


Figura 19. Interfaz de gestión de AP's en conectados Surco
Fuente: Propia

En la siguiente figura 20, en la ventana "AP Configuration" se aprecia las direcciones IP de cada AP:

- 192.168.8.122 (AP): IP de dispositivo AP y controlador virtual
- 192.168.8.121 (AP): IP de dispositivo AP
- 192.168.8.118 (AP): IP de dispositivo AP
- 192.168.8.119 (AP): IP de dispositivo AP
- 192.168.8.125 (AP): IP de dispositivo AP
- 192.168.8.124 (AP): IP de dispositivo AP

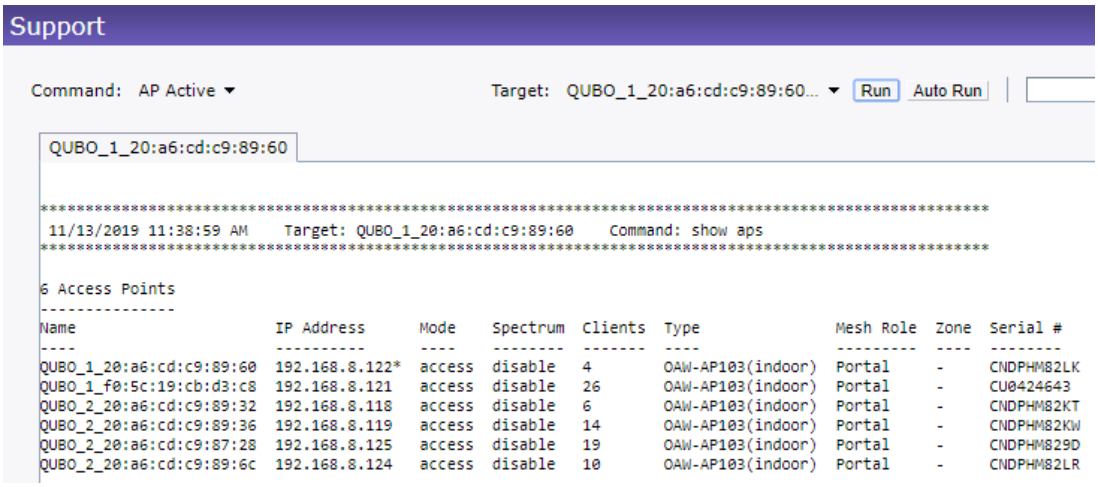


Figura 20. Lista de AP's en Surco
Fuente: Propia

De la figura 21, se obtuvo los parámetros básicos de conexión a otras redes:

DNS: 192.168.8.101

Gateway: 192.168.168.8.100

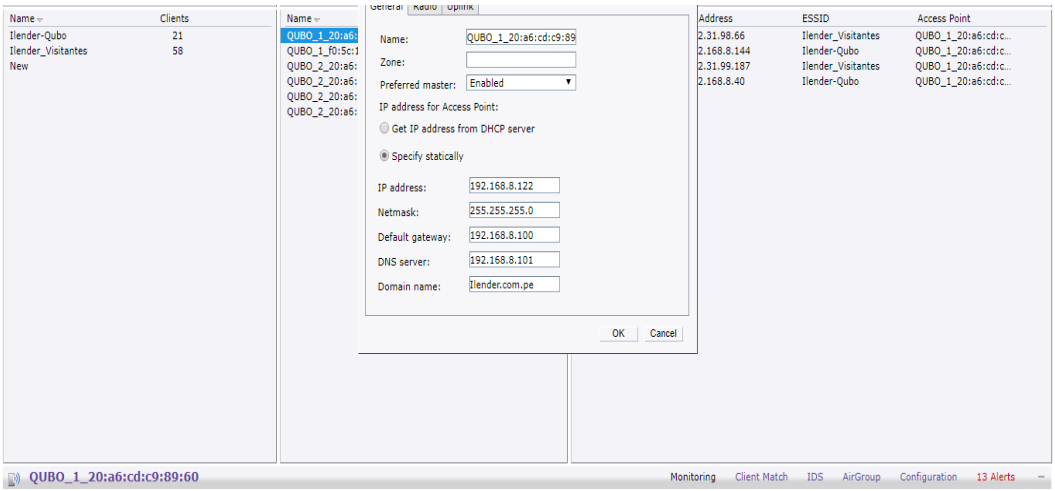


Figura 21. Parámetros de red de AP's en Surco
Fuente: Propia

Para el SSID “Ilender-Qubo”:

En la figura 22 se tiene

- Name: Nombre de SSID
- Primary usage: Uso principal, en este caso esta seleccionado como “Employe” (empleados)

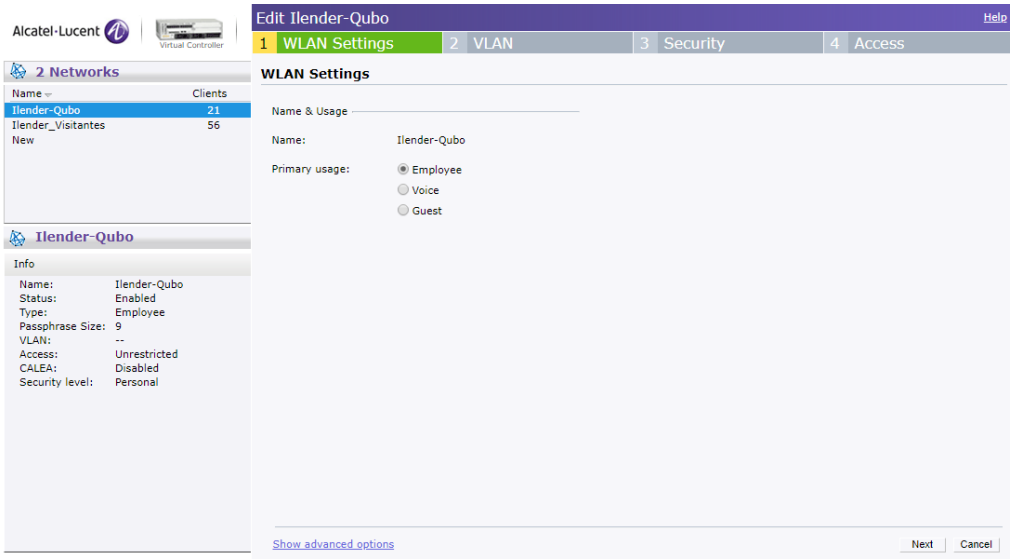


Figura 22. Parámetros SSID Ilender-Qubo en Surco: WLAN Settings
Fuente: Propia

En la figura 23 se tiene

Client IP Assigment: La asignación de direcciones IP’s es brindado por la red

Client VLAN Assigment: Vlan asignada a usuarios de este SSID

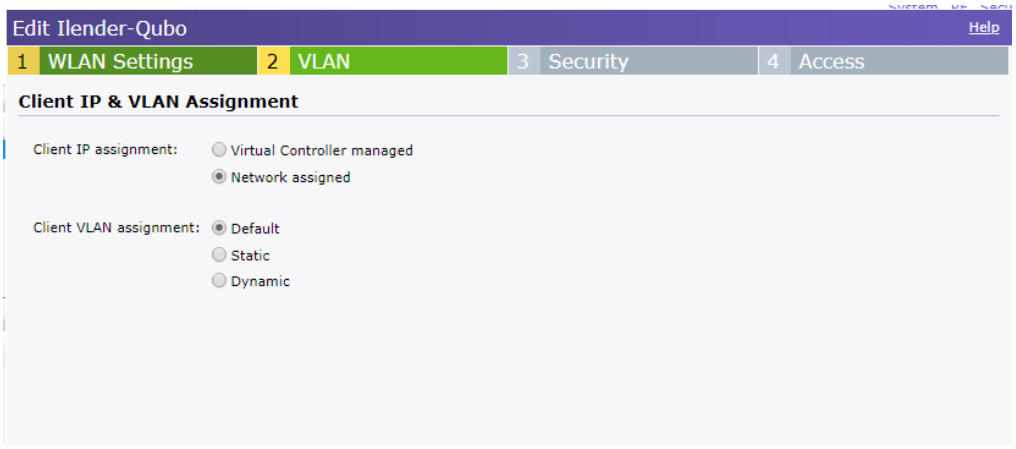


Figura 23. Parámetros SSID Ilender-Qubo en Surco: VLAN
Fuente: Propia

En la figura 24 se muestra el campo “Security”, donde se tiene seleccionado la autenticación “WPA-2 y WPA”

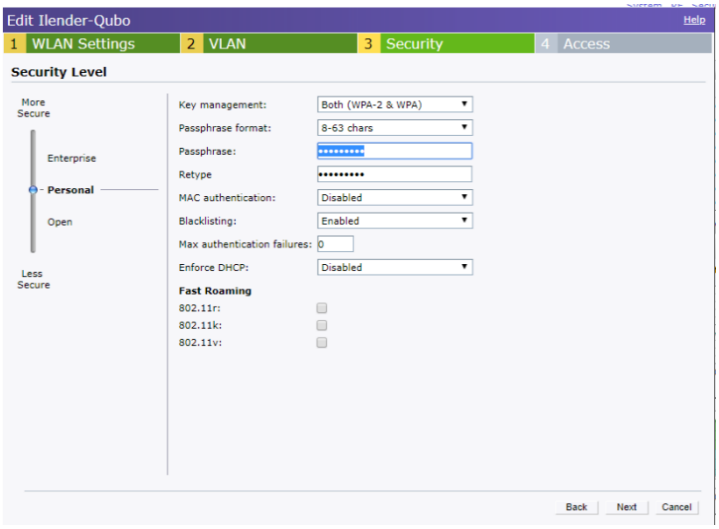


Figura 24. Parámetros SSID Ilender-Qubo en Surco: Security
Fuente: Propia

En la figura 25 se muestra el campo “Access”, donde no se tiene ninguna regla de acceso habilitado “Unrestriced”

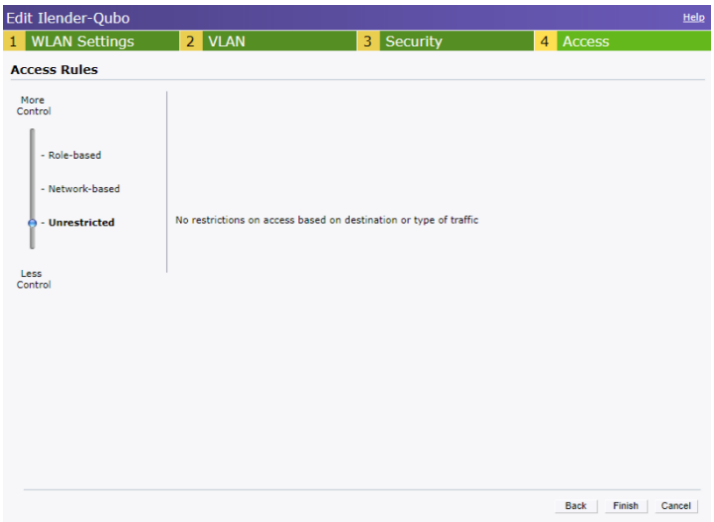


Figura 25. Parámetros SSID Ilender-Qubo en Surco: VLAN
Fuente: Propia

Para el SSID “Ilender-Visitantes”:

En la figura 26 se tiene

- Name: Nombre de SSID

- Primary usage: Uso principal, en este caso esta seleccionado como “Employe” (empleados)

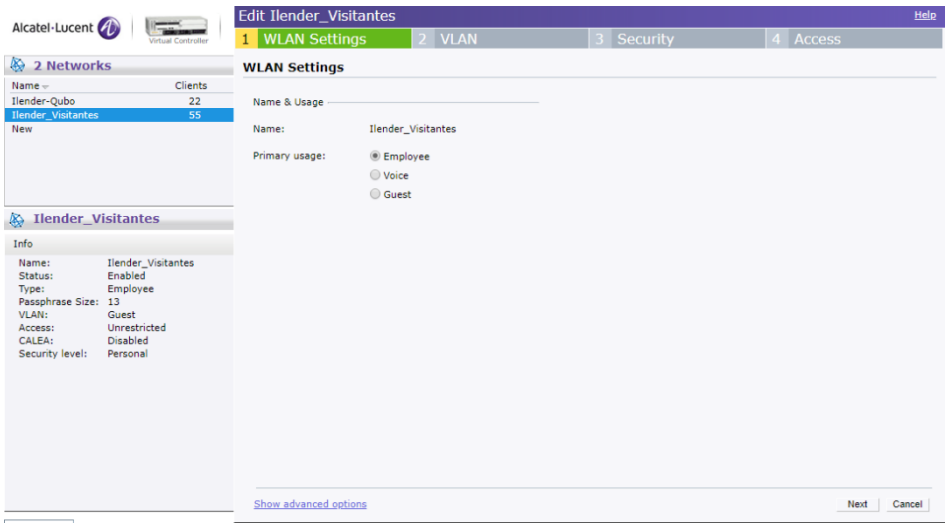


Figura 26. Parámetros SSID Ilender-Visitantes en Surco: WLAN Settings
Fuente: Propia

En la figura 27 se tiene

Client IP Assigment: La asignación de direcciones IP’s es brindado por el controlador virtual (Virtual Controller Managed)

Client VLAN Assigment: Vlan asignada a usuarios de este SSID

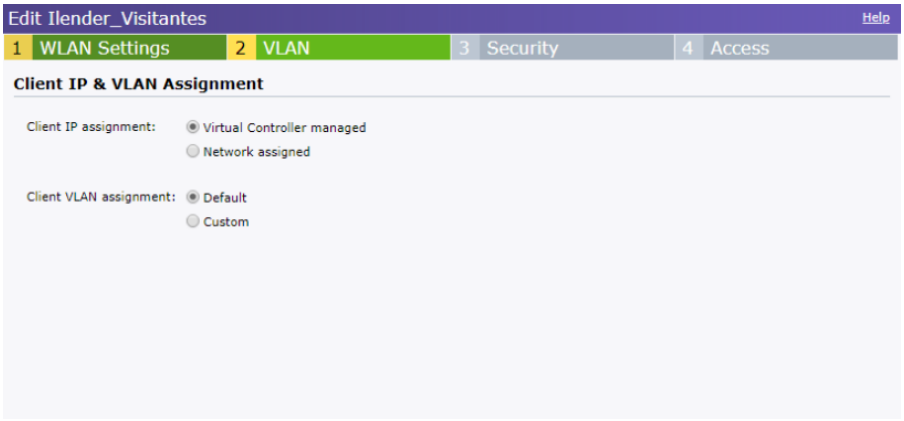


Figura 27. Parámetros SSID Ilender-Visitantes en Surco: VLAN
Fuente: Propia

En la figura 28 se muestra el campo “Security”, donde se tiene seleccionado la autenticación “WPA-2 y WPA”

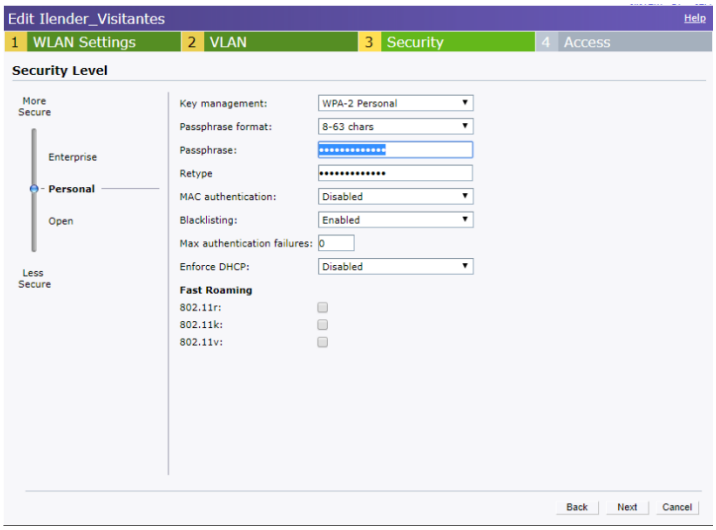
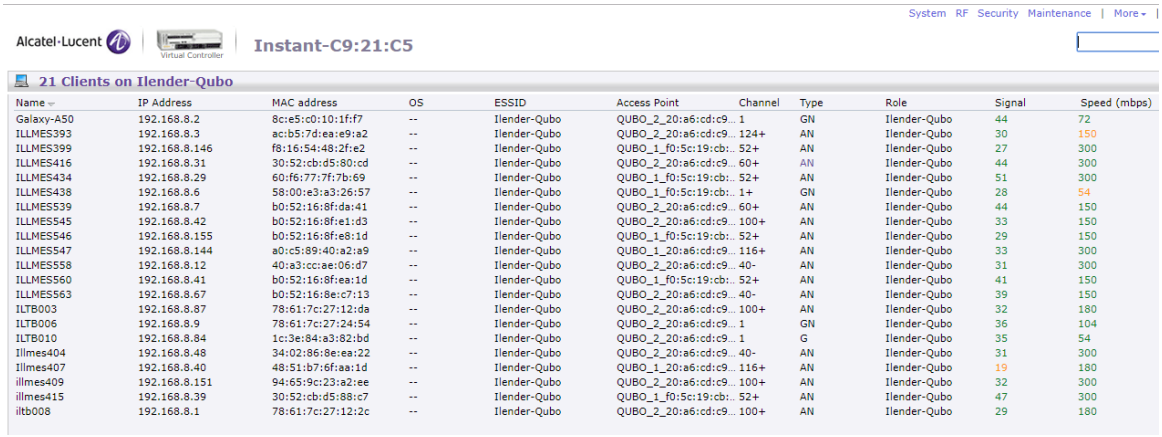


Figura 28. Parámetros SSID Ilender-Visitantes en Surco: Security
Fuente: Propia

En la figura 29 se muestra el campo “Access”, donde no se tiene ninguna regla de acceso habilitado “Unrestriced”

Figura 29. Parámetros SSID Ilender-Visitantes en Surco: Access
Fuente: Propia

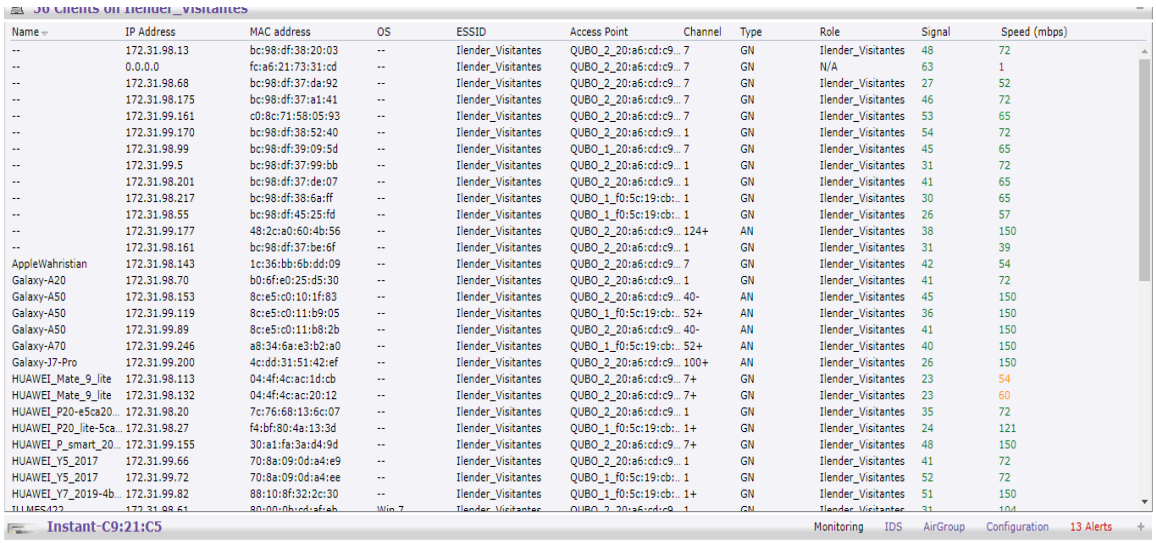
En la siguiente figura 30 se observa la ventana “Clients on Ilender-Qubo” (Clientes en SSID “Ilender-Qubo”) que las direcciones IP de los usuarios están dentro del rango 192.168.8.0/24, con vlan por defecto



Name	IP Address	MAC address	OS	ESSID	Access Point	Channel	Type	Role	Signal	Speed (mbps)
Galaxy-A50	192.168.8.2	8c:e5:c0:10:1f:f7	--	Ilender-Qubo	QUBO_2_20:a6:cd:c9...	1	GN	Ilender-Qubo	44	72
ILLMES393	192.168.8.3	ac:b5:7d:ea:e9:a2	--	Ilender-Qubo	QUBO_2_20:a6:cd:c9...	124+	AN	Ilender-Qubo	30	150
ILLMES399	192.168.8.146	f8:16:54:48:2f:e2	--	Ilender-Qubo	QUBO_1_f0:5c:19:cb:...	52+	AN	Ilender-Qubo	27	300
ILLMES416	192.168.8.31	30:52:cb:d5:80:cd	--	Ilender-Qubo	QUBO_2_20:a6:cd:c9...	60+	AN	Ilender-Qubo	44	300
ILLMES434	192.168.8.29	60:f6:77:7f:7b:69	--	Ilender-Qubo	QUBO_1_f0:5c:19:cb:...	52+	AN	Ilender-Qubo	51	300
ILLMES438	192.168.8.6	58:00:e3:a3:26:57	--	Ilender-Qubo	QUBO_1_f0:5c:19:cb:...	1+	GN	Ilender-Qubo	28	54
ILLMES539	192.168.8.7	b0:52:16:8f:da:41	--	Ilender-Qubo	QUBO_2_20:a6:cd:c9...	60+	AN	Ilender-Qubo	44	150
ILLMES545	192.168.8.42	b0:52:16:8f:e1:d3	--	Ilender-Qubo	QUBO_2_20:a6:cd:c9...	100+	AN	Ilender-Qubo	33	150
ILLMES546	192.168.8.155	b0:52:16:8f:e8:1d	--	Ilender-Qubo	QUBO_1_f0:5c:19:cb:...	52+	AN	Ilender-Qubo	29	150
ILLMES547	192.168.8.144	a0:c5:89:40:a2:a9	--	Ilender-Qubo	QUBO_1_20:a6:cd:c9...	116+	AN	Ilender-Qubo	33	300
ILLMES558	192.168.8.12	40:a3:cc:ae:06:d7	--	Ilender-Qubo	QUBO_2_20:a6:cd:c9...	40-	AN	Ilender-Qubo	31	300
ILLMES560	192.168.8.41	b0:52:16:8f:ea:1d	--	Ilender-Qubo	QUBO_1_f0:5c:19:cb:...	52+	AN	Ilender-Qubo	41	150
ILLMES563	192.168.8.67	b0:52:16:8e:c7:13	--	Ilender-Qubo	QUBO_2_20:a6:cd:c9...	40-	AN	Ilender-Qubo	39	150
ILTB003	192.168.8.87	78:61:7c:27:12:da	--	Ilender-Qubo	QUBO_2_20:a6:cd:c9...	100+	AN	Ilender-Qubo	32	180
ILTB006	192.168.8.9	78:61:7c:27:24:54	--	Ilender-Qubo	QUBO_2_20:a6:cd:c9...	1	GN	Ilender-Qubo	36	104
ILTB010	192.168.8.84	1c:3e:84:a3:82:bd	--	Ilender-Qubo	QUBO_2_20:a6:cd:c9...	1	G	Ilender-Qubo	35	54
Illmes404	192.168.8.48	34:02:86:8e:ea:22	--	Ilender-Qubo	QUBO_2_20:a6:cd:c9...	40-	AN	Ilender-Qubo	31	300
Illmes407	192.168.8.40	48:51:b7:6f:aa:1d	--	Ilender-Qubo	QUBO_1_20:a6:cd:c9...	116+	AN	Ilender-Qubo	19	180
illmes409	192.168.8.151	94:65:9c:23:a2:ee	--	Ilender-Qubo	QUBO_2_20:a6:cd:c9...	100+	AN	Ilender-Qubo	32	300
illmes415	192.168.8.39	30:52:cb:d5:88:c7	--	Ilender-Qubo	QUBO_1_f0:5c:19:cb:...	52+	AN	Ilender-Qubo	47	300
iltb008	192.168.8.1	78:61:7c:27:12:2c	--	Ilender-Qubo	QUBO_2_20:a6:cd:c9...	100+	AN	Ilender-Qubo	29	180

Figura 30. Clientes conectados en SSID Ilender-Qubo en Surco
Fuente: Propia

En la figura 31 se puede observar en ventana “Clients on Ilender_Visitantes” (Clientes en SSID “Ilender_Visitantes”) que las direcciones IP de los usuarios están dentro del rango 172.31.X.X/16. Estas direcciones IP son entregadas por el controlador, el cual realiza NAT entre sus direcciones (192.168.8.122) y las direcciones 172.31.X.X para permitir la comunicación con la red externa.



Name	IP Address	MAC address	OS	ESSID	Access Point	Channel	Type	Role	Signal	Speed (mbps)
--	172.31.98.13	bc:98:df:38:20:03	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	7	GN	Ilender_Visitantes	48	72
--	0.0.0.0	fc:a6:21:73:31:cd	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	7	GN	N/A	63	1
--	172.31.98.68	bc:98:df:37:da:92	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	7	GN	Ilender_Visitantes	27	52
--	172.31.98.175	bc:98:df:37:a1:41	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	7	GN	Ilender_Visitantes	46	72
--	172.31.99.161	c0:8c:71:58:05:93	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	7	GN	Ilender_Visitantes	53	65
--	172.31.99.170	bc:98:df:38:52:40	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	1	GN	Ilender_Visitantes	54	72
--	172.31.98.99	bc:98:df:39:09:5d	--	Ilender_Visitantes	QUBO_1_20:a6:cd:c9...	7	GN	Ilender_Visitantes	45	65
--	172.31.99.5	bc:98:df:37:99:bb	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	1	GN	Ilender_Visitantes	31	72
--	172.31.98.201	bc:98:df:37:de:07	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	1	GN	Ilender_Visitantes	41	65
--	172.31.98.217	bc:98:df:38:6a:ff	--	Ilender_Visitantes	QUBO_1_f0:5c:19:cb:...	1	GN	Ilender_Visitantes	30	65
--	172.31.98.55	bc:98:df:45:25:fd	--	Ilender_Visitantes	QUBO_1_f0:5c:19:cb:...	1	GN	Ilender_Visitantes	26	57
--	172.31.99.177	48:2c:a0:60:4b:56	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	124+	AN	Ilender_Visitantes	38	150
--	172.31.98.161	bc:98:df:37:be:6f	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	1	GN	Ilender_Visitantes	31	39
AppleWahristian	172.31.98.143	1c:36:bb:6b:dd:09	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	7	GN	Ilender_Visitantes	42	54
Galaxy-A20	172.31.98.70	b0:6f:e0:25:d5:30	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	1	GN	Ilender_Visitantes	41	72
Galaxy-A50	172.31.98.153	8c:e5:c0:10:1f:83	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	40-	AN	Ilender_Visitantes	45	150
Galaxy-A50	172.31.99.119	8c:e5:c0:11:b9:05	--	Ilender_Visitantes	QUBO_1_f0:5c:19:cb:...	52+	AN	Ilender_Visitantes	36	150
Galaxy-A50	172.31.99.89	8c:e5:c0:11:b8:2b	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	40-	AN	Ilender_Visitantes	41	150
Galaxy-A70	172.31.99.246	a8:34:6a:e3:b2:a0	--	Ilender_Visitantes	QUBO_1_f0:5c:19:cb:...	52+	AN	Ilender_Visitantes	40	150
Galaxy-J7-Pro	172.31.99.200	4c:dd:31:51:42:ef	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	100+	AN	Ilender_Visitantes	26	150
HUAWEI_Mate_9_lite	172.31.98.113	04:4f:4c:ac:1d:cb	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	7+	GN	Ilender_Visitantes	23	54
HUAWEI_Mate_9_lite	172.31.98.132	04:4f:4c:ac:20:12	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	7+	GN	Ilender_Visitantes	23	60
HUAWEI_P20-e5ca20...	172.31.98.20	7c:76:68:13:6c:07	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	1	GN	Ilender_Visitantes	35	72
HUAWEI_P20_lite-5ca...	172.31.98.27	f4:bf:80:4a:13:3d	--	Ilender_Visitantes	QUBO_1_f0:5c:19:cb:...	1+	GN	Ilender_Visitantes	24	121
HUAWEI_P_smart_20...	172.31.99.155	30:a1:fa:3a:d4:9d	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	7+	GN	Ilender_Visitantes	48	150
HUAWEI_Y5_2017	172.31.99.66	70:8a:09:0d:a4:e9	--	Ilender_Visitantes	QUBO_2_20:a6:cd:c9...	1	GN	Ilender_Visitantes	41	72
HUAWEI_Y5_2017	172.31.99.72	70:8a:09:0d:a4:ee	--	Ilender_Visitantes	QUBO_1_f0:5c:19:cb:...	1	GN	Ilender_Visitantes	52	72
HUAWEI_Y7_2019-4b...	172.31.99.82	88:10:8f:32:2c:30	--	Ilender_Visitantes	QUBO_1_f0:5c:19:cb:...	1+	GN	Ilender_Visitantes	51	150

Figura 31. Clientes conectados en SSID Ilender-Visitantes en Surco
Fuente: Propia

La información sobre parámetros de los AP’s en la red Wi-Fi de la sede Surco se resume en la tabla 11:

Tabla 11. Inventario de AP's en Surco

Nro	Marca	Modelo	Nombre	IP	SSID - Vlan asociada	User	Password	Vlan "Untagged"
1	Alcatel	IAP-103	QUBO_1_20:a6:cd:c9:89:60	192.168.8.122	"Ilender-Qubo" vlan id=0 "Ilender_Visitantes" vlan id=0	admin	admin	1
2	Alcatel	IAP-103	QUBO_1_f0:5c:19:cb:d3:c8	192.168.8.121	"Ilender-Qubo" vlan id=0 "Ilender_Visitantes" vlan id=0	admin	admin	1
3	Alcatel	IAP-103	QUBO_2_20:a6:cd:c9:89:32	192.168.8.118	"Ilender-Qubo" vlan id=0 "Ilender_Visitantes" vlan id=0	admin	admin	1
4	Alcatel	IAP-103	QUBO_2_20:a6:cd:c9:89:3	192.168.8.119	"Ilender-Qubo" vlan id=0 "Ilender_Visitantes" vlan id=0	admin	admin	1
5	Alcatel	IAP-103	QUBO_2_20:a6:cd:c9:87:28	192.168.8.125	"Ilender-Qubo" vlan id=0 "Ilender_Visitantes" vlan id=0	admin	admin	1
6	Alcatel	IAP-103	QUBO_2_20:a6:cd:c9:89:6c	192.168.8.124	"Ilender-Qubo" vlan id=0 "Ilender_Visitantes" vlan id=0	admin	admin	1

Fuente: Propia

La información sobre usuarios en la red Wi-Fi de la sede San Surco se resume en la tabla 12:

Tabla 12. Lista de SSID y usuarios concurrentes en Surco

	SSID	Usuarios concurrentes
1	Ilender-Qubo	21
2	Ilender_Visita	56

Fuente: Propia

3.1.1.4. Ate

En esta sede se accedió a la interfaz web de administración de los AP's como se muestra en la figura 32, que está conformado por los AP's y un controlador embebido dentro de 01 AP con rol de maestro.

De la imagen mostrada, se puede observar que la IP de administración (Controlador Virtual) es 172.20.0.71, así mismo también se identifica 20 AP's y 02 SSID: "Ilender-SantaClara" e "Ilender-Invitados".

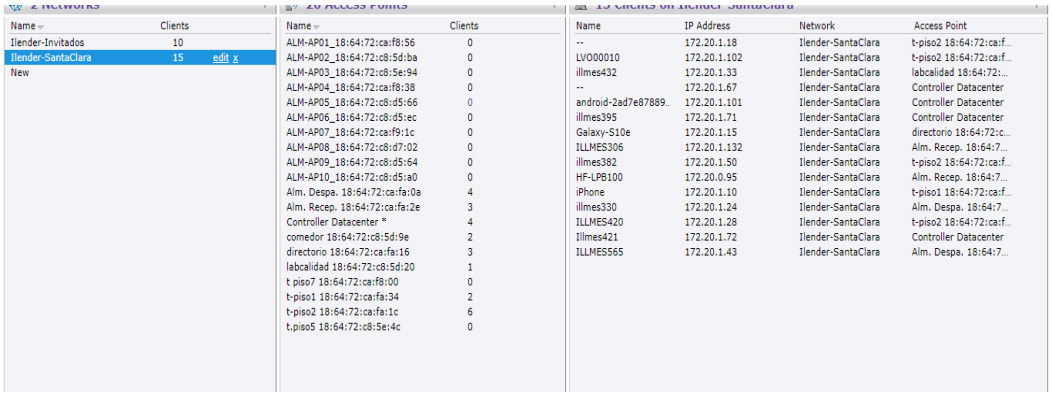


Figura 32. Interfaz de gestión de AP's en Ate
Fuente: Propia

En la figura 33, en la ventana "AP Configuration" se aprecia las IP's de cada AP.

172.20.0.71 (AP): IP de dispositivo AP y controlador virtual
172.20.0.89 (AP): IP de dispositivo AP
172.20.0.70 (AP): IP de dispositivo AP
172.20.0.75 (AP): IP de dispositivo AP
172.20.0.74 (AP): IP de dispositivo AP
172.20.0.81 (AP): IP de dispositivo AP
172.20.0.86 (AP): IP de dispositivo AP
172.20.0.84 (AP): IP de dispositivo AP
172.20.0.69 (AP): IP de dispositivo AP
172.20.0.77 (AP): IP de dispositivo AP
172.20.0.79 (AP): IP de dispositivo AP
172.20.0.87 (AP): IP de dispositivo AP
172.20.0.83 (AP): IP de dispositivo AP
172.20.0.82 (AP): IP de dispositivo AP
172.20.0.88 (AP): IP de dispositivo AP
172.20.0.85 (AP): IP de dispositivo AP
172.20.0.76 (AP): IP de dispositivo AP
172.20.0.73 (AP): IP de dispositivo AP

172.20.0.78 (AP): IP de dispositivo AP

172.20.0.80 (AP): IP de dispositivo AP

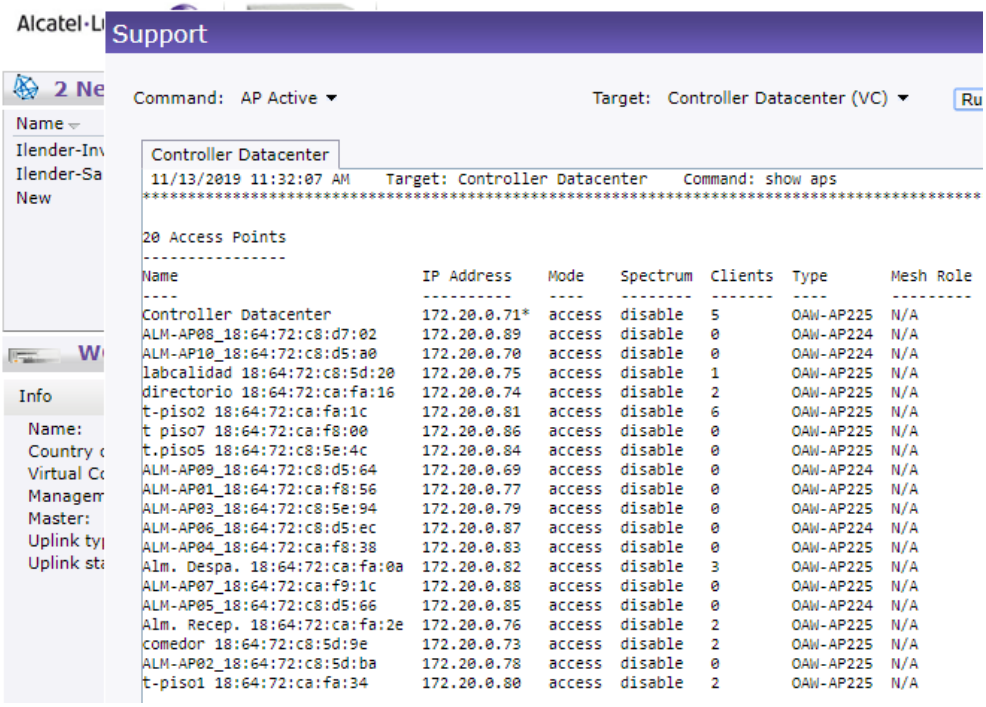


Figura 33. Lista de AP's en Ate
Fuente: Propia

De la figura 34, se obtuvo los parámetros básicos de conexión a otras redes:

DNS: 172.20.0.10

Gateway: 172.20.0.1

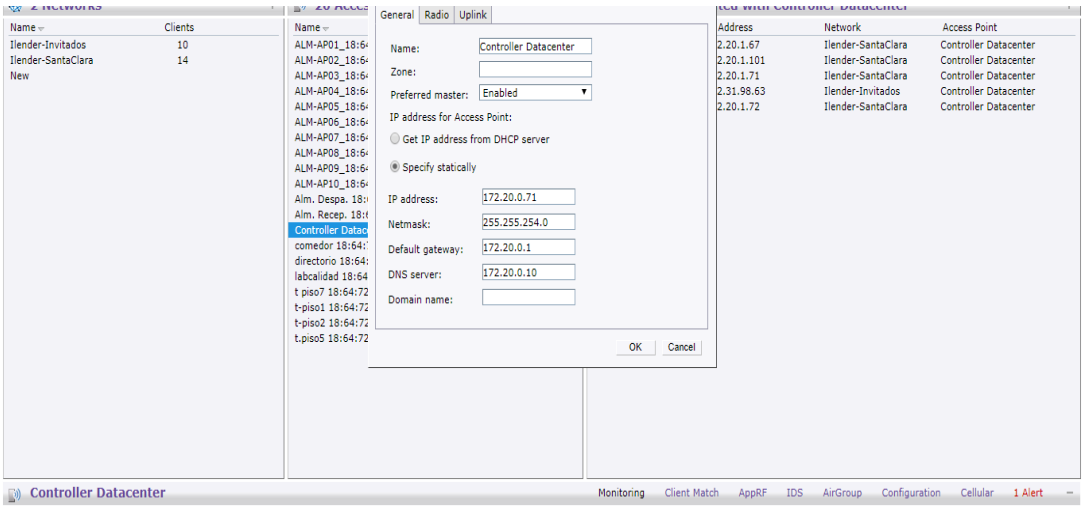


Figura 34. Interfaz de gestión de AP's en Ate
Fuente: Propia

Para el SSID “Ilender-SantaClara”

En la figura 35 observa:

- Name: Nombre de SSID
- Primary usage: Uso principal, en este caso esta seleccionado como “Employe” (empleados)

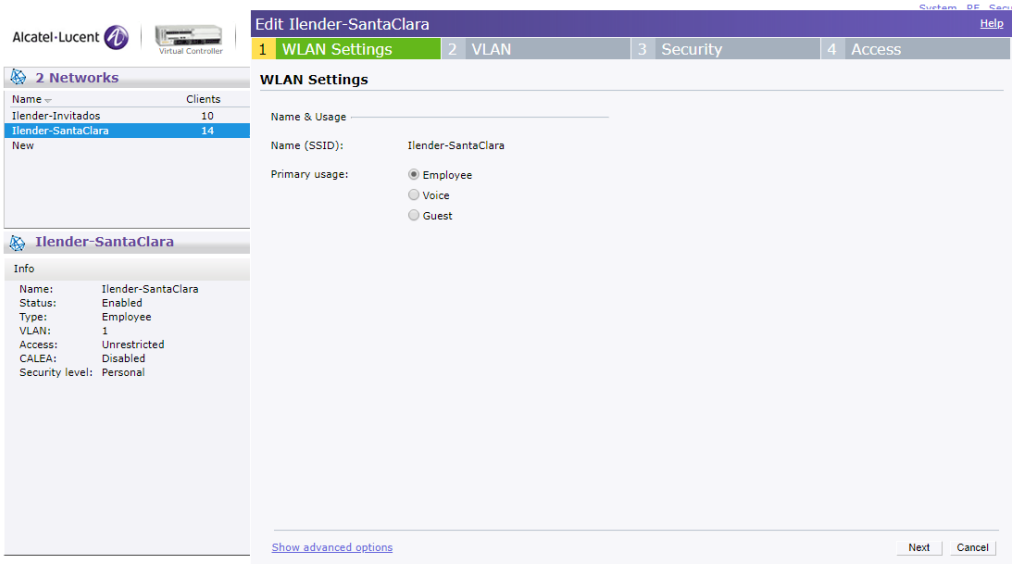


Figura 35. Parámetros SSID Ilender-SantaClara en Ate: WLAN Settings
Fuente: Propia

En la figura 36 se observa:

Client IP Assigment: La asignación de direcciones IP’s es brindado por la red

Client VLAN Assigment: Vlan asignada a usuarios de este SSID (VLAN:1)

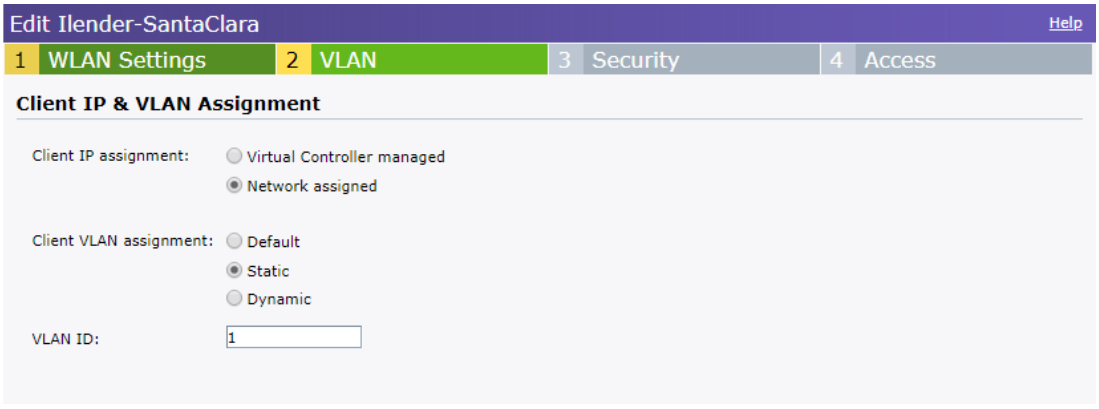


Figura 36. Parámetros SSID Ilender-SantaClara en Ate: VLAN
Fuente: Propia

En la figura se muestra el campo “Security”, donde se tiene seleccionado la autenticación “WPA-2 y WPA”

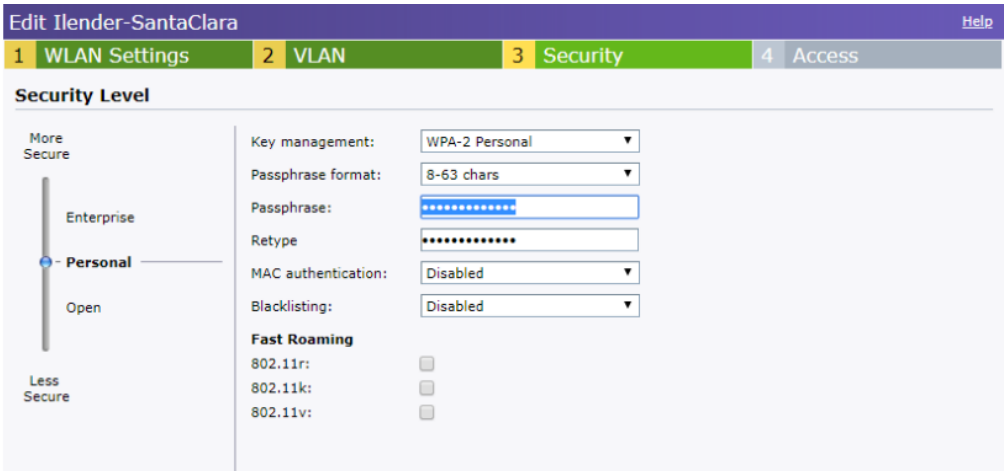


Figura 37. Parámetros SSID Ilender-SantaClara en Ate: Security
Fuente: Propia

En la figura 38 se muestra el campo “Access”, donde no se tiene ninguna regla de acceso habilitado “Unrestriced”

Figura 38. Parámetros SSID Ilender-SantaClara en Ate: Security
Fuente: Propia

Para el SSID “Ilender-Visitantes”:

En la figura 39 se tiene

- Name: Nombre de SSID
- Primary usage: Uso principal, en este caso esta seleccionado como “Employe” (empleados)

Figura 39. Parámetros SSID Ilender-Invitados en Ate: Security
Fuente: Propia

En la figura 40 se tiene:

Client IP Assigment: La asignación de direcciones IP's es brindado por el controlador virtual (Virtual Controller Managed)

Client VLAN Assigment: Vlan asignada a usuarios de este SSID

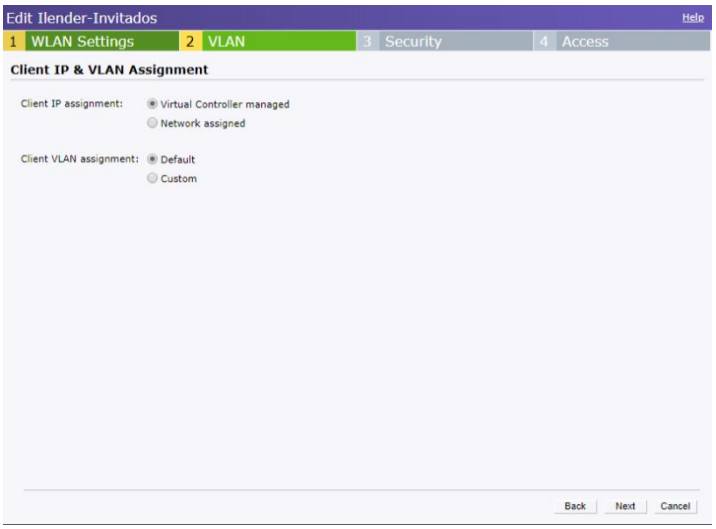


Figura 40. Parámetros SSID Ilender-Invitados en Ate: VLAN
Fuente: Propia

En la figura 41 se muestra el campo "Security", donde se tiene seleccionado la autenticación "WPA-2 y WPA"

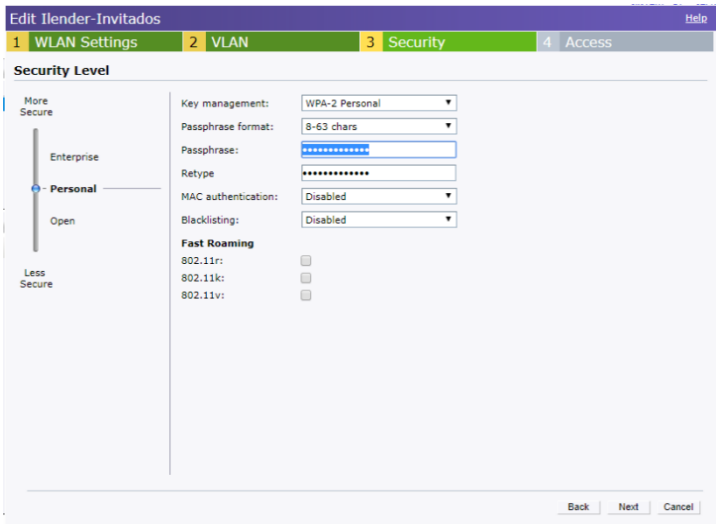


Figura 41. Parámetros SSID Ilender-Invitados en Ate: Security
Fuente: Propia

En la figura 42 se muestra el campo “Access”, donde no se tiene ninguna regla de acceso habilitado “Unrestriced”

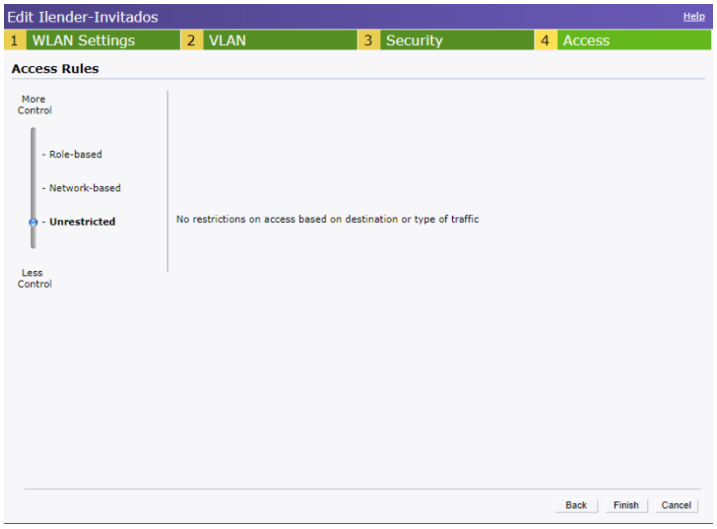


Figura 42. Parámetros SSID Ilender-Invitados en Ate: Access
Fuente: Propia

En la figura 43 se puede observar en ventana “Clients on Ilender-SantaClara” (Clientes en SSID “Ilender-SantaClara”) que las direcciones IP de los usuarios están dentro del rango 172.20.10.0/24 con vlan por defecto (VLAN ID:0)

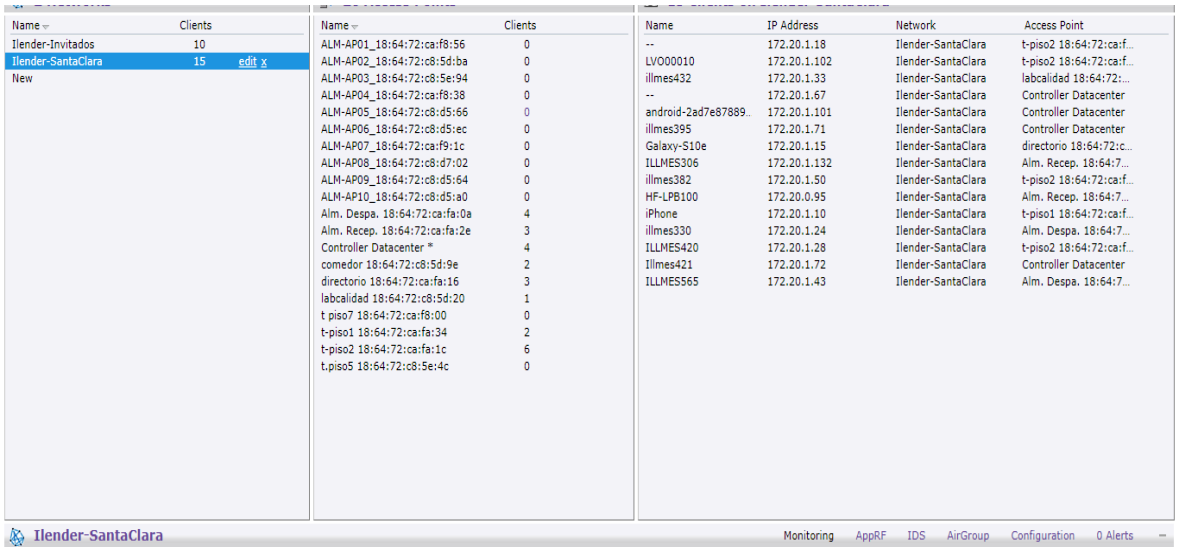


Figura 43. Clientes conectados en SSID Ilender-Qubo en Ate
Fuente: Propia

En la siguiente figura se puede observar en ventana “Clients on Ilender-Invitados” (Clientes en SSID “Ilender_Visitantes”) que las direcciones IP de los usuarios están dentro del rango 172.31.X.X/16. Estas direcciones IP son entregadas por el controlador, el cual realiza NAT entre sus direcciones (172.20.0.71) y las direcciones 172.31.X.X para permitir la comunicación con la red externa.

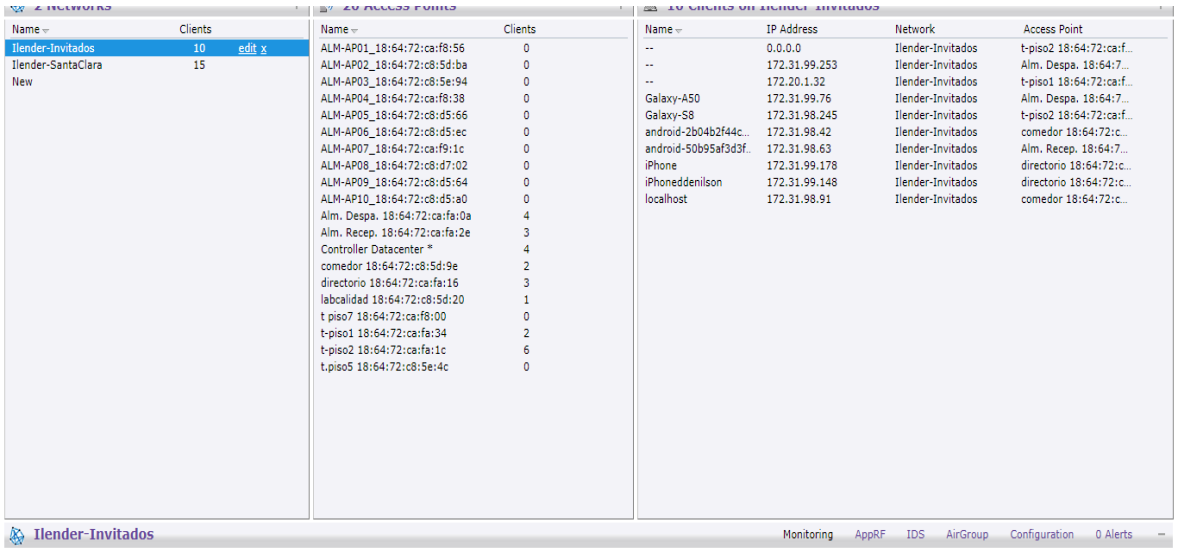


Figura 44. Clientes conectados en SSID Ilender-Invitados en Ate
Fuente: Propia

La información sobre parámetros de los AP's en la red Wi-Fi de la sede Ate se resume en la tabla 13:

Tabla 13. Inventario de AP's en Ate

Nro	Marca	Modelo	Nombre	IP	SSID - Vlan asociada	User	Password	Vlan "Untagged"
1	Alcatel	OAW-AP225	Controller Datacenter	172.20.0.71	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
2	Alcatel	OAW-AP224	ALM-AP08_18:64:72:c8:d7:02	172.20.0.89	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
3	Alcatel	OAW-AP224	ALM-AP10_18:64:72:c8:d7:a0	172.20.0.70	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
4	Alcatel	OAW-AP225	Labcalidad 18:64:72:c8:5d:20	172.20.0.75	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
5	Alcatel	OAW-AP225	directorio 18:64:72:ca:fa:16	172.20.0.74	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
6	Alcatel	OAW-AP225	t-piso2 18:64:72:ca:fa:1c	172.20.0.81	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
7	Alcatel	OAW-AP225	t-piso7 18:64:72:ca:f8;00	172.20.0.86	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
8	Alcatel	OAW-AP225	t-piso5 18:64:72:c8:5e:4c	172.20.0.84	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
9	Alcatel	OAW-AP224	ALM-AP09_18:64:72:c8:d5:64	172.20.0.69	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
10	Alcatel	OAW-AP225	ALM-AP01_18:64:72:c8:f8:56	172.20.0.77	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
11	Alcatel	OAW-AP225	ALM-AP03_18:64:72:c8:5e:94	172.20.0.79	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
12	Alcatel	OAW-AP224	ALM-AP06_18:64:72:c8:d5:ec	172.20.0.87	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
13	Alcatel	OAW-AP225	ALM-AP04_18:64:72:c8:f8:38	172.20.0.83	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
14	Alcatel	OAW-AP225	Alm. Despa. 18:64:72:ca:fa:0a	172.20.0.82	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
15	Alcatel	OAW-AP225	ALM-AP07_18:64:72:ca:f9:1c	172.20.0.88	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
16	Alcatel	OAW-AP224	ALM-AP05_18:64:72:c8:d5:66	172.20.0.85	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
17	Alcatel	OAW-AP225	Alm. Recep.. 18:64:72:ca:fa:2e	172.20.0.76	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
18	Alcatel	OAW-AP225	comedor 18:64:c8:5d:9e	172.20.0.73	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
18	Alcatel	OAW-AP225	ALM-AP02_18:64:72:c8:5d:9e	172.20.0.78	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1
18	Alcatel	OAW-AP225	t-piso1 18:64:72:ca:fa:34	172.20.0.80	"llender-SantaClara" vlan id=1 "llender-Invitados" vlan id=0	admin	admin	1

Fuente: Propia

La información sobre usuarios en la red Wi-Fi de la sede San Surco se resume en la siguiente tabla:

Tabla 14. Usuarios concurrentes por SSID en Ate

	SSID	Usuarios concurrentes
1	Ilender-SantaClara	15
2	Ilender-Invitados	10

Fuente: Propia

3.1.1.5. Lurín

La Sede Lurín es una planta nueva, pero aún no se encuentra en operación.

En esta sede se accedió a la interfaz web de administración de los AP's como se muestra en la figura 45, que está conformado por varios AP's y un controlador embebido dentro de 01 AP con rol de maestro.

De la imagen mostrada, se puede observar que la IP de administración (Controlador Virtual) es 192.168.10.141, así mismo también se identifica 02 AP's y 01 SSID: "LABOT".

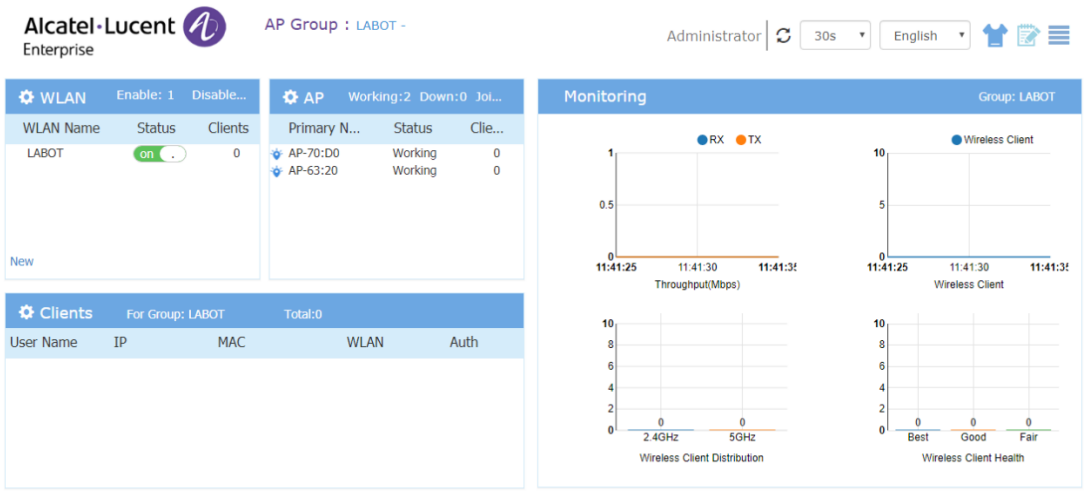


Figura 45. Interfaz de gestión de AP's en Lurín
Fuente: Propia

En la siguiente imagen, en la ventana “AP Configuration” se aprecia las IP’s de cada AP siendo:

- 172.21.1.13 (AP): IP de controlador virtual
- 172.21.1.12 (AP): IP de dispositivo AP

Los parámetros básicos de conexión a otras redes:

DNS: 8.8.8.8

Gateway: 172.21.0.5

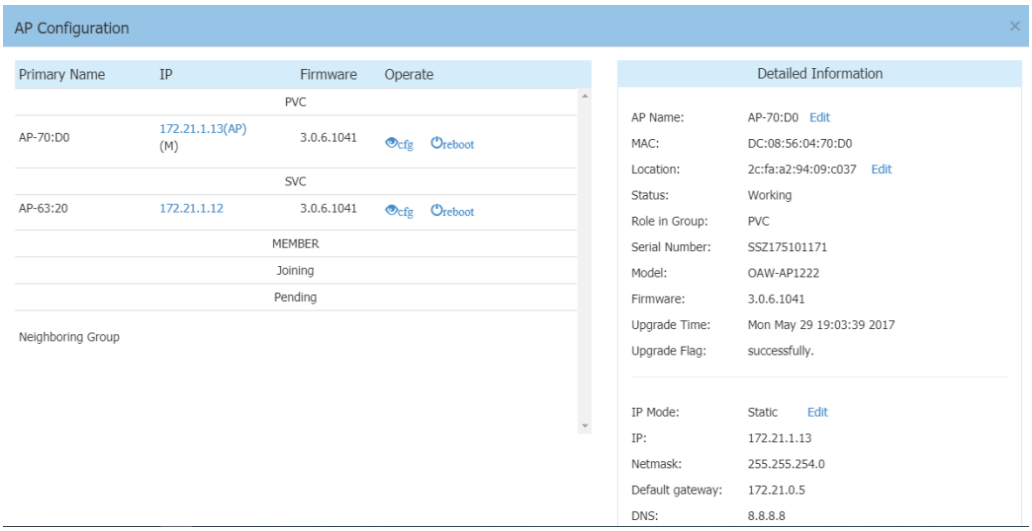


Figura 46. Lista de AP’s en Lurín
Fuente: Propia

La información sobre parámetros de los AP’s en la red Wi-Fi de la sede Lurín se resume en la siguiente tabla:

Tabla 15. Inventario de AP’s en Lurín

Nro	Marca	Modelo	Nombre	IP	SSID - Vlan asociada	User	Password	Vlan "Untagged"
1	Alcatel	AP-1222	AP-70:D0	172.20.0.71	"LABOT" vlan id=0	admin	admin	1
2	Alcatel	AP-1222	AP-63:20	172.20.0.89	"LABOT" vlan id=0	admin	admin	1

Fuente: Propia

La información sobre usuarios en la red Wi-Fi de la sede Lurín se resume en la siguiente tabla:

Tabla 16. Lista de SSID y usuarios concurrentes en Lurín

	SSID	Usuarios proyectados
1	LABOT	50
2	INVITADOS	30

Fuente: Propia

3.1.1.6. Inventario de AP’s

De lo contabilizado en los apartados anteriores, se obtuvo el inventario actualizado de equipos desplegados en las 04 sedes, según se muestra en la tabla 17 (32 AP’s):

Tabla 17. Lista de AP's por sede

Item	SEDE	Modelo	Marca
1	San Isisdro	AP-1101	Alcatel Lucent
2	San Isisdro	AP-1101	Alcatel Lucent
3	San Isisdro	AP-1101	Alcatel Lucent
4	San Isisdro	AP-1101	Alcatel Lucent
5	Surco	IAP-103	Alcatel Lucent
6	Surco	IAP-103	Alcatel Lucent
7	Surco	IAP-103	Alcatel Lucent
8	Surco	IAP-103	Alcatel Lucent
9	Surco	IAP-103	Alcatel Lucent
10	Surco	IAP-103	Alcatel Lucent
11	Ate	OAW-AP225	Alcatel Lucent
12	Ate	OAW-AP224	Alcatel Lucent
13	Ate	OAW-AP224	Alcatel Lucent
14	Ate	OAW-AP225	Alcatel Lucent
15	Ate	OAW-AP225	Alcatel Lucent
16	Ate	OAW-AP225	Alcatel Lucent
17	Ate	OAW-AP225	Alcatel Lucent
18	Ate	OAW-AP225	Alcatel Lucent
19	Ate	OAW-AP224	Alcatel Lucent
20	Ate	OAW-AP225	Alcatel Lucent
21	Ate	OAW-AP225	Alcatel Lucent
22	Ate	OAW-AP224	Alcatel Lucent
23	Ate	OAW-AP225	Alcatel Lucent
24	Ate	OAW-AP225	Alcatel Lucent
25	Ate	OAW-AP225	Alcatel Lucent
26	Ate	OAW-AP224	Alcatel Lucent
27	Ate	OAW-AP225	Alcatel Lucent
28	Ate	OAW-AP225	Alcatel Lucent
29	Ate	OAW-AP225	Alcatel Lucent
30	Ate	OAW-AP225	Alcatel Lucent
31	Lurin	AP-1222	Alcatel Lucent
32	Lurin	AP-1222	Alcatel Lucent

Fuente: Propia

Se tiene un total de 32 Puntos de acceso inalámbrico de la marca Alcatel Lucent, de los cuales desde el ítem 01 hasta el 30 pertenecen a la familia de APs' OMNIACCESS INSTANT (descontinuada) y del 31 al 32 pertenecen a la familia de AP's OMNIACCESS STELLAR

3.1.1.7. Diseño existente

Del levantamiento de información de las 04 sedes de la empresa Ilender, se tiene una topología como se muestra en la figura 47.

Para la red LAN, las 04 sedes del Grupo Ilender una red LAN operan sobre la VLAN 1, con un servidor DHCP que asigna IP, mascará y gateway a los usuarios.

La red Wi-Fi también está desplegada sobre la vlan 1, los usuarios y los AP's también están dentro del mismo segmento de red, lo que hace posible que cualquier usuario pueda comunicarse con el AP's e ingresar a su interfaz de gestión (Salvo en el caso de la red de ATE, donde los AP's se encuentran en otro segmento.

La seguridad está controlada del lado de conexión hacia internet a través del firewall.

Todos los accesos están configurados a través de WPA/WPA2

- La empresa tiene un segmento de red para usuarios Wi-Fi
- Solo existen hasta 02 SSID (para invitados y para usuarios)
- Solo existe una VLAN sobre la cual accedes los usuarios de las redes Wi-Fi
- No cuenta con ningún tipo de QoS aplicado
- Ambos SSID se encuentran en la misma vlan
- La autenticación es a través de WPA y WPA-2
- La conexión entre sedes es a través de un router del proveedor CLARO vía VPN
- Los AP's en cada sede son gestionados por un controlador virtual, el cual opera un AP denominado "MASTER"

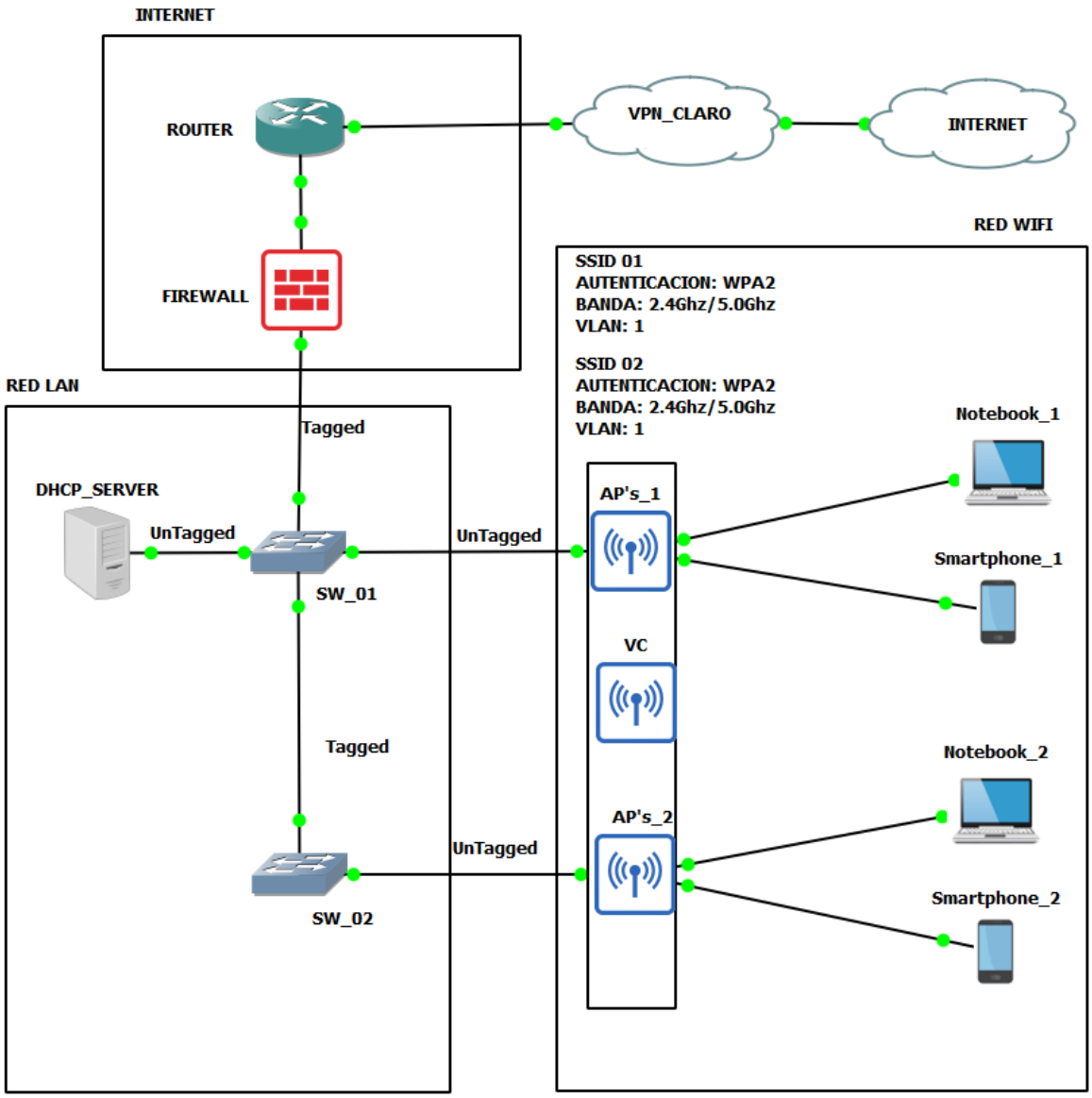


Figura 47. Diseño existente en las 4 sedes
Fuente: Propia

3.1.1.8. Propuesta de diseño Wi-Fi gestionado en la nube

El nuevo diseño, se centra en crear un SSID por cada empresa del Grupo Ilender, e invitados como se muestra en la figura 48
Consideraciones del diseño:

RED WIFI: Se utilizará 01 SSD por cada empresa del grupo (en total existen 07 empresas) y 01 SSD para usuarios invitado, es decir se tendrán 08 SSID con una subred. Esto permitirá un espacio de trabajo definido para cada empresa, limitando el dominio de broadcast y permitiendo tener su propia característica en cuanto a consumo de ancho de banda, así como acceso y restricciones en la navegación o al ingreso a otras redes de la empresa.
En la figura 475 se observa el DPI, esta función de inspección de paquete irá embebido en el equipo, esto permitirá a los AP's analizar el tráfico que envía cada usuario, permitiendo el monitoreo a nivel profundo de las actividades realizadas por los usuarios.

RED LAN: Al existir 08 SSID, se requiere modificar la red LAN existente, esto se logra creando 08 Vlans adicionales (uno por cada SSID) y una vlan de administración de equipos.
De la figura 47, las interfaces de los AP's que conectan a los switches deben estar configuradas como Troncales (vlan 201 hasta vlan 208) salvo la vlan de gestión de AP's que será la nativa o "default", es decir no se etiquetará dentro de la troncal.
Para la asignación de IP's en todas subredes (vlan 201-208), en el servidor DHCP server se declararán 09 nuevos segmentos de red (8 de Wi-Fi, 1 para la gestión de AP's, con su respectivo pool, mascara, dns y gateway. De la misma forma, en el router se debe configurar las gateway y el enrutamiento, también se deberá configurar la opción "relay" o "IP helper" para el router coordine con el DHCP server la asignación de IP's para asignación de IP's para cada segmento.

CONTROLADOR CLOUD: Es el controlador que gestionará los AP's de forma remota, así como también permitirá la autenticación a través de su módulo de UPAM (Servidor RADIUS embebido) para usuarios internos; para usuarios invitados utilizará la función de portal cautivo.

La utilización de este controlador en la nube permitirá al personal de TI administrar la red Wi-Fi completa en todo momento y en cualquier lugar

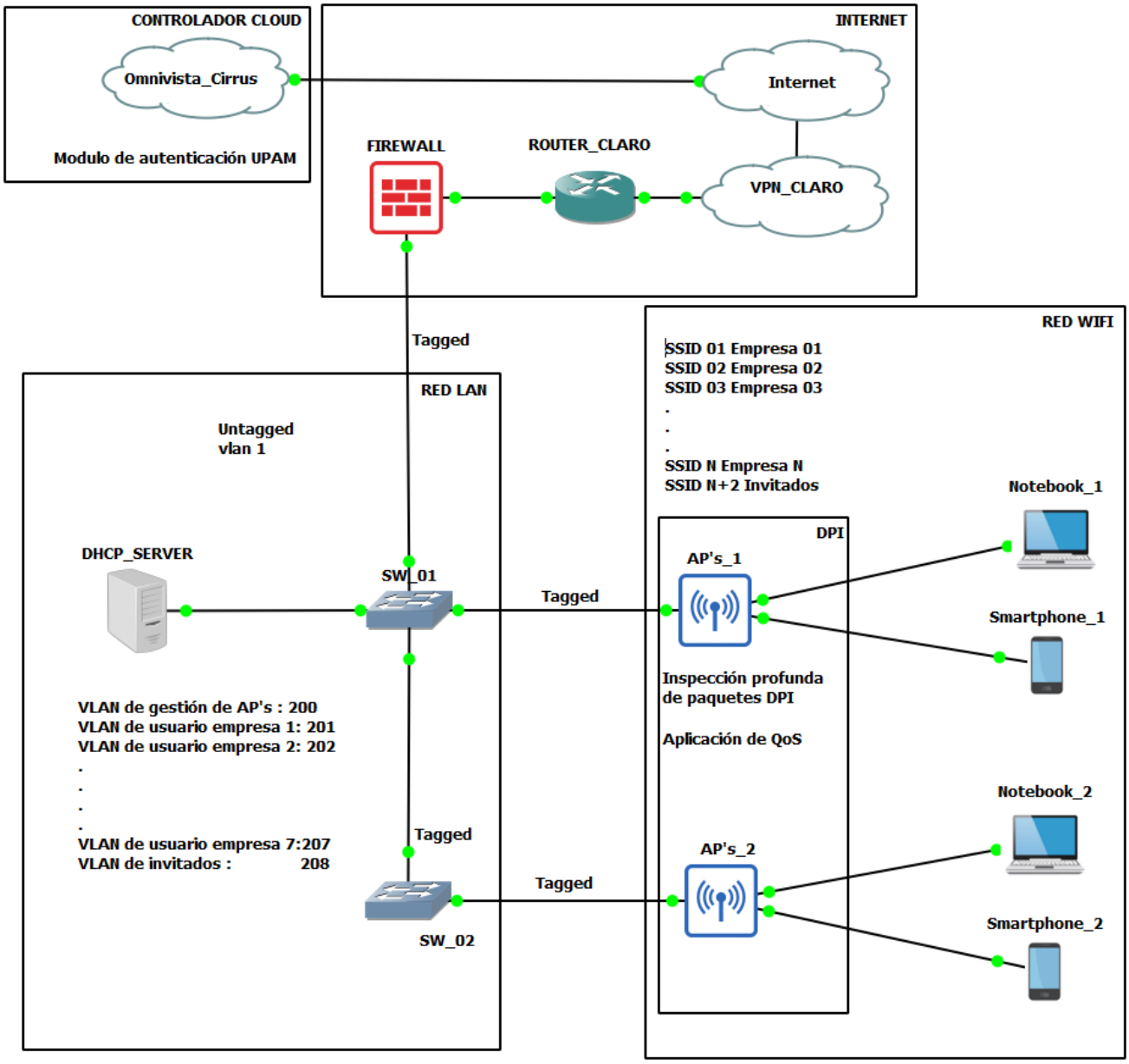


Figura 48. Interfaz de gestión de AP's en Lurín
Fuente: Propia

En la tabla18, se nombra 08 SSID’s para cada empresa del grupo.

Tabla 18. Lista de SSID propuesto.

SSID
llender
Furctus_Terrum
Labot
+futuro
Animal Pharm
Ummana
CDTEL
Invitados

Fuente: Propia

En la figura 49 se plantea la topología para las 04 sedes

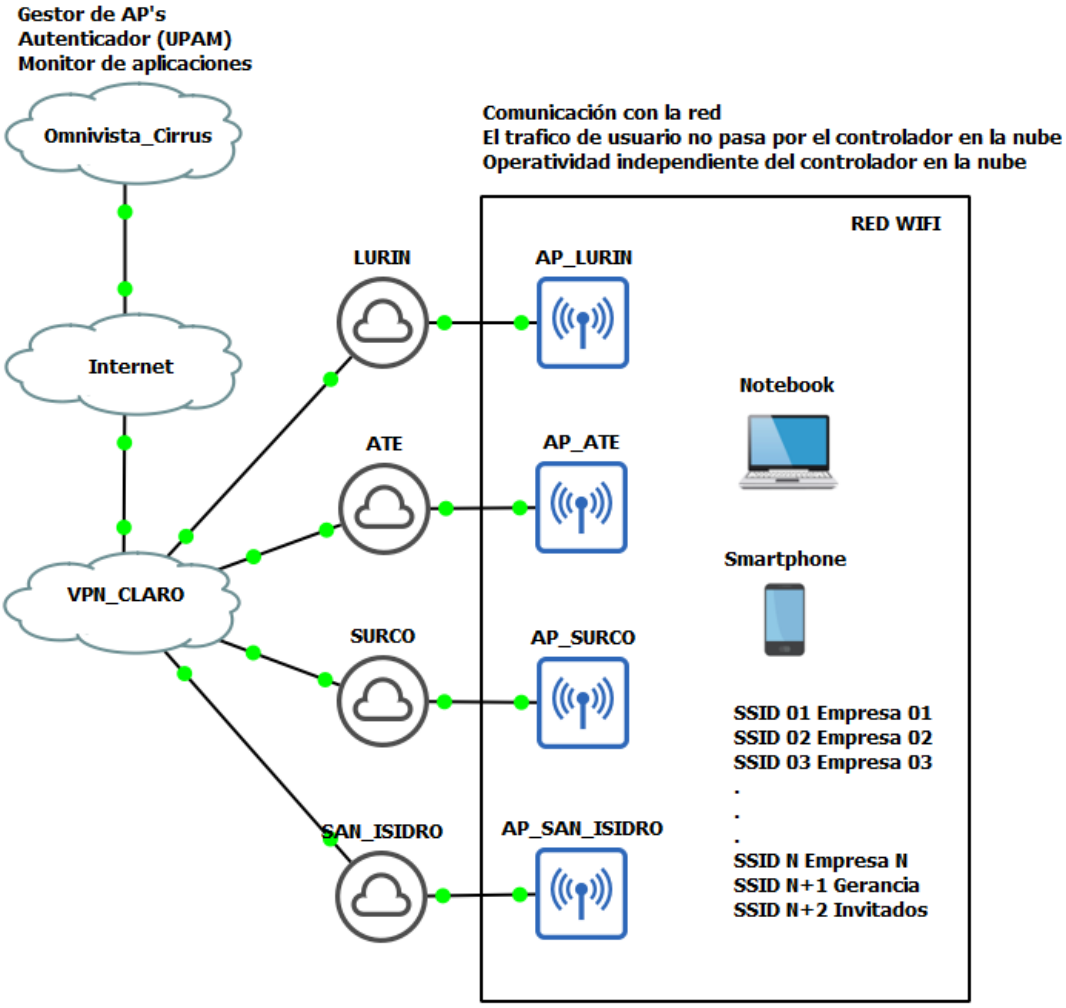


Figura 49. Interfaz de gestión de AP’s en Lurín

Fuente: Propia

3.1.1.9. Dimensionamiento de componentes de red: AP’s

El modelo de AP’s a utilizar es el Stellar AP-1221 de Alcatel Lucent. Este equipo cuenta con las siguientes prestaciones descritas en la tabla 19:

Tabla 19. Características del AP 1221

Caracteristica	**AP 1221**
Numero de radios	2
Bandas soportadas	2.4GHz & 5GHz
Estandares 802.11	802.11a/b/g/n/ac wave 2
MIMO	MU-MIMO
SSID	16
maximo numero de clientes asociados por radio	256
Potencia de transmisión maxima	18dBm
Ganacia de antena	4dBi - 2.4Ghz/6.3dBi - 5Ghz
Tipo de antena	Integrada
Interfaz de red	1GbE
Soporte BLE	si
Soporte energización PoE	si
Soporte DPI	si
Soporte WIPS/WIDS	si
Potencia maxima de consumo	15.6W

Fuente: Propia

El punto importante para mencionar es que soporta MU-MIMO, el estándar 802.11a/b/g/n/ac y cuenta con el DPI para la visualización de aplicaciones.
Así mismo también cuenta con soporte de hasta 16 SSID en total, es decir 8 SSID por Radio (2.4Ghz y 5Ghz), y la capacidad de soportar hasta 256 usuarios por radio.

En la tabla 20 se observa la cantidad de usuarios concurrentes por SSID, excepto el SSID en Lurín, donde no se cuenta con ningún usuario conectado

Tabla 20. Cantidad de usuarios concurrentes en SSID existentes

Sede	SSID	Usuarios concurrentes
San Isidro	GRUPO_ARMEJO	42
San Isidro	GRUPO_ARMEJO_INVITADOS	4
Surco	Ilender-Qubo	21
Surco	Ilender-Qubo	56
Ate	Ilender-SantaClara	15
Ate	Ilender-Invitados	10
Lurin	LABOT	NA

Fuente: Propia

La cantidad de usuarios se establecerá a 254 usuarios por SSID, asociados a una vlan como se muestra en la tabla 21:

Tabla 21. Cantidad de usuarios concurrentes en nuevo diseño

VLAN	SSID	Usuarios concurrentes
101	Ilender	254
102	Furctus_Terrum	254
103	Labot	254
104	+futuro	254
105	Animal Pharm	254
106	Ummana	254
107	CDTEL	254
108	Invitados	254

Fuente: Propia

En la tabla 22 se muestra el modelo de AP a remplazar, exceptuando AP 1222 existentes en la sede de Lurín:

Tabla 22. Nueva lista de AP's

Item	SEDE	Modelo	Nuevo modelo
1	San Isisdro	AP-1101	AP-1221
2	San Isisdro	AP-1101	AP-1221
3	San Isisdro	AP-1101	AP-1221
4	San Isisdro	AP-1101	AP-1221
5	Surco	IAP-103	AP-1221
6	Surco	IAP-103	AP-1221
7	Surco	IAP-103	AP-1221
8	Surco	IAP-103	AP-1221
9	Surco	IAP-103	AP-1221
10	Surco	IAP-103	AP-1221
11	Ate	OAW-AP225	AP-1221
12	Ate	OAW-AP224	AP-1221
13	Ate	OAW-AP224	AP-1221
14	Ate	OAW-AP225	AP-1221
15	Ate	OAW-AP225	AP-1221
16	Ate	OAW-AP225	AP-1221
17	Ate	OAW-AP225	AP-1221
18	Ate	OAW-AP225	AP-1221
19	Ate	OAW-AP224	AP-1221
20	Ate	OAW-AP225	AP-1221
21	Ate	OAW-AP225	AP-1221
22	Ate	OAW-AP224	AP-1221
23	Ate	OAW-AP225	AP-1221
24	Ate	OAW-AP225	AP-1221
25	Ate	OAW-AP225	AP-1221
26	Ate	OAW-AP224	AP-1221
27	Ate	OAW-AP225	AP-1221
28	Ate	OAW-AP225	AP-1221
29	Ate	OAW-AP225	AP-1221
30	Ate	OAW-AP225	AP-1221
31	Lurin	AP-1222	No aplica
32	Lurin	AP-1222	No aplica

Fuente: Propia

3.1.1.10. Dimensionamiento de componentes de red: Controlador en la nube

La plataforma de gestión a proponer es OmniVista Cirrus de Alcatel Lucent, el cual opera por suscripción de 1,3 o 5 años.

Cuenta con 03 tipos de planes (Basico, Negocios y Premium). La versión a utilizar es negocios (incluye asistencia técnica remota y reposición de equipos en garantía por la duración del servicio).

Omnivista Cirrus utiliza posee 04 tipos de licencias para sus productos como se muestra en la tabla 23:

Tabla 23. Licenciamiento OmniVista Cirrus

SKU	Description
OVC-AP-BAS-nY	OmniVista Cirrus - Cloud network administration for one Stellar Access Point model (covers OAW-AP1101, AP1201, AP1201H, AP1221, AP1222, AP1231, AP1232, AP1251 series) for the selected subscription duration (options are one, three or five years). Include Base Service and Support Bundle for the device under subscription.
OVC-ESS-BAS-nY	OmniVista Cirrus - Cloud network administration for one Essential OmniSwitch model (covers OS6350, OS6450, OS6465, OS6560 series) for the selected subscription duration (options are one, three or five years). Include Base Service and Support Bundle for the device under subscription.
OVC-ADV-BAS-nY	OmniVista Cirrus - Cloud network administration for one Advanced OmniSwitch model (covers OS6860, OS6860-E, OS6865 series) for the selected subscription duration (options are one, three or five years). Include Base Service and Support Bundle for the device under subscription.
OVC-CORE-BAS-nY	OmniVista Cirrus - Cloud network administration for one Core OmniSwitch model (covers OS6900 series) for the selected subscription duration (options are one, three or five years). Include Base Service and Support Bundle for the device under subscription.

Fuente: Propia

De lo anterior, el tipo de licencia a utilizar es la OVC-AP-VAS-nY, licencia que permite gestionar AP's de la familia Stellar. Debido a que la solución es por servicio de suscripción, se elegirá al mayor tiempo, que es de 05 años.

3.1.1.11. Provisionamiento

La configuración inicial de los AP's requiere del envió de la dirección del controlador cloud (Omnivista Cirrus) a través de DHCP opción 138 sobre la vlan de gestión de AP's, como se describe en la figura 50. Cabe señalar que la comunicación esa encriptada mediante MQTT-TLS. Para el proceso de Provisionamiento, es necesario que la vlan de gestión de AP's tenga acceso a internet para la comunicación con el Gestor Omnivista

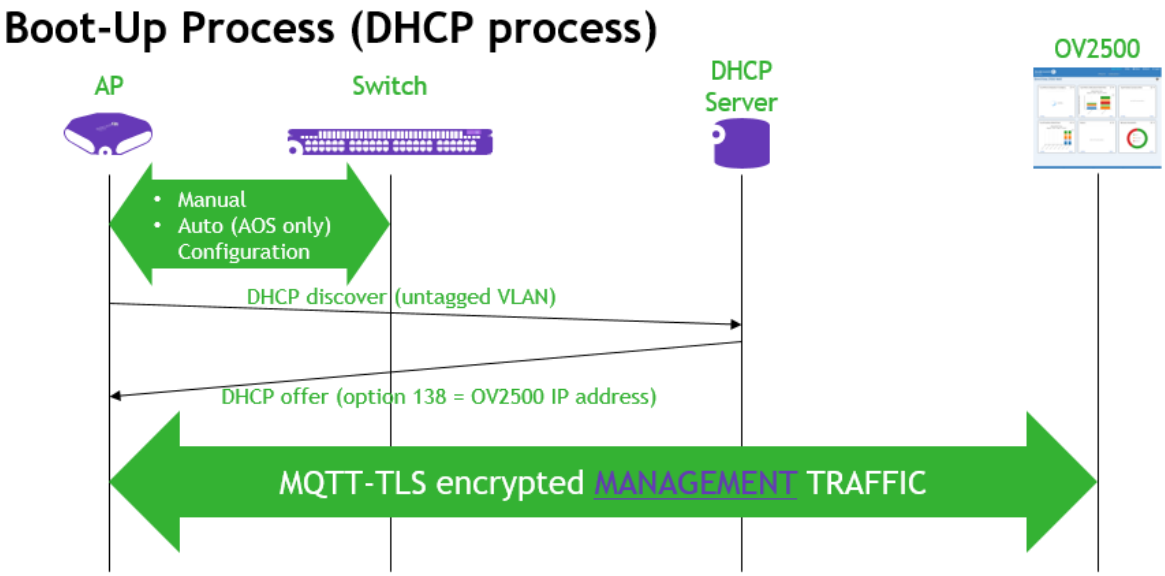


Figura 50. Provisionamiento
Fuente: Propia

3.1.1.12. Plantilla

OmniVista Cirrus, al manejar en base a objetos, permite tener un sinfín de plantillas predeterminadas para el despliegue y modificaciones en los AP's con la ejecución en pocos pasos

3.1.1.13. Resumen de equipamiento y software

3.1.1.14. Equipos

- 30 AP modelo Stellar AP1221

3.1.1.15. Accesorios

- 30 Kits de montaje para Stellar AP1221

3.1.1.16. Software y licenciamiento

- Licencia Omnivista Cirrus para 32 AP's modelo Stellar AP1221
-

3.1.1.17. Instalación

- Servicio de reemplazo de 30 AP's

- Servicio de despliegue de e implementación de AP’s
- Capacitación para personal de TI

3.1.1.18. Soporte

- Bolsa de horas para atención de emergencia anual, por un periodo de 05 años: 16

3.1.1.19. Propuesta económica

En la tabla 24 se muestra una cotización realizada por un socio de negocio de la empresa Alcatel Lucent en Perú:

Tabla 24. Cotización de Wi-Fi gestionado

	Descripción	Cantidad	Precio unitario	Subtotal
OMNI Data I/00 (YAYDZ)				**756.72**
Mounting kit, Type A wall mount and ceiling mount with screws. Applicable for OmniAccess Stellar AP1101, AP122x and AP123x series.	OAW-AP-MNT-W	30	25.22	756.72
OMNI Data I/01 (YAYEA)				**14,446.43**
OAW-AP1221-RW OmniAccess Stellar AP1221. Dual radio 2x22 4x44 802.11a/b/g/n/ac MU-MIMO AP, integrated antenna, 1x GbE, 1x USB opt BLE), 1x 48V DC power interface, 1x Console. Unrestricted Regulatory Domain. MUST NOT be used for US, Japan or Israel.	OAW-AP1221-RW	30	481.55	14,446.43
OMNI Data D/00 Services (YBYBL)				**9,085.46**
OmniVista Cirrus - 5 YR SaaS administration for one Stellar Access point model (Covers all Stellar Access Points). Business Service Support Bundle per Licensed device. See e-Buy Portal for ordering	OVC-AP-BIZ-5Y	32	283.92	9,085.46
Instalación				**3,842.80**
instalación de 30 AP's y despliegue de solución Omnivista Cirrus		30	64.21	1,926.19
Capacitación de 16 horas		1	1,916.61	1,916.61
Soporte tecnico				**7,154.42**
Bola de 12 horas anuales x 05 años		1	7,154.42	7,154.42
Precio total en dólares + IGV, financiado en modalidad de alquiler por 05 años, incluye intereses				**35,285.82**

Fuente: Propia

3.1.2. Desarrollo 02: Selección de los mecanismos de autenticación de usuarios de red Wi-Fi

3.1.2.1. Clasificación de usuarios

Los usuarios se clasificarán por usuarios internos (pertenecientes a la empresa) y usuarios externos (usuarios invitados)

3.1.2.2. Autenticación usuarios internos

La autenticación de usuario internos será realizada mediante autenticación 802.1x a través del UPAM (Servidor Radius interno) y con la creación de credenciales por cada usuario. Con ello se tendrá identificado a cada usuario

En la figura 51, se muestra el uso del módulo UPAM, en la pestaña "Authentication Record" se observa el histórico sobre inicio de sesión, en la columna "Account Type" se identifica el usuario interno como "Employee".

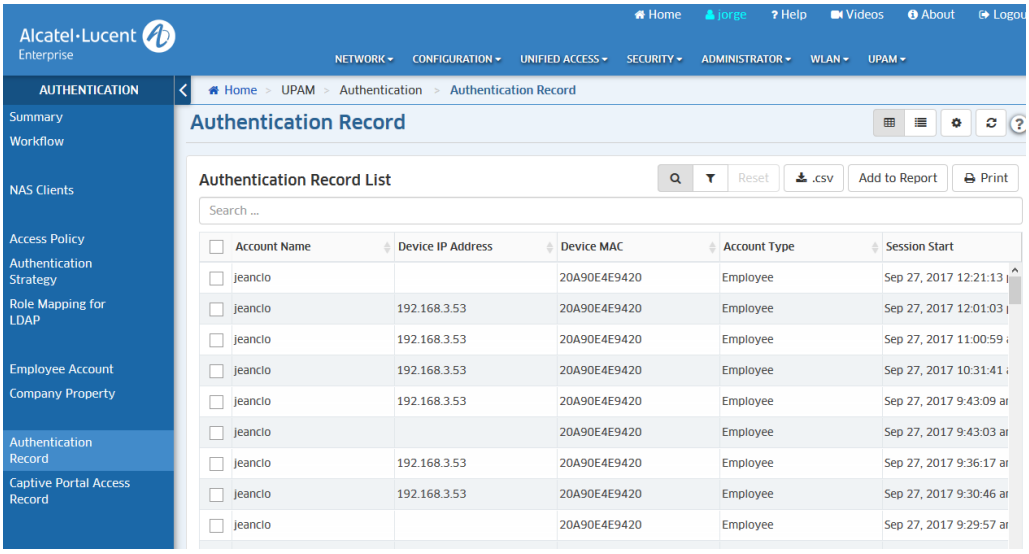


Figura 51. Histórico de autenticación
Fuente: Propia

3.1.2.3. Autenticación usuarios externos

La autenticación de usuarios externos (invitados) será realizada mediante autenticación MAC, y Portal Cautivo.

En la figura 52 se observa la “Pestaña Captive Portal Page” dentro del modulo “UPAM”, donde se puede personalizar la página de inicio de sesión para usuarios invitados. En la figura 53 se observa a modo de ejemplo la página del portal

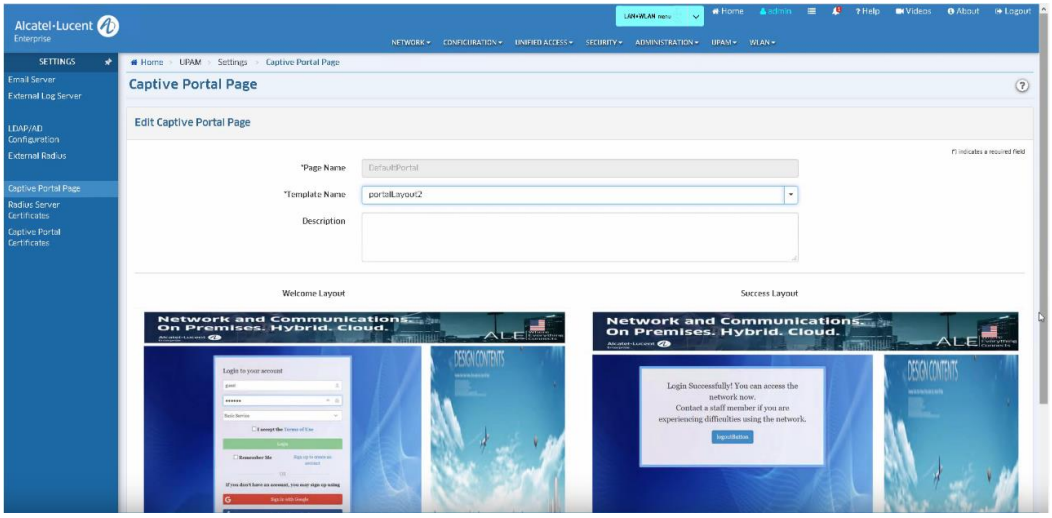


Figura 52. Plantilla personalizable de portal cautivo
Fuente: Propia

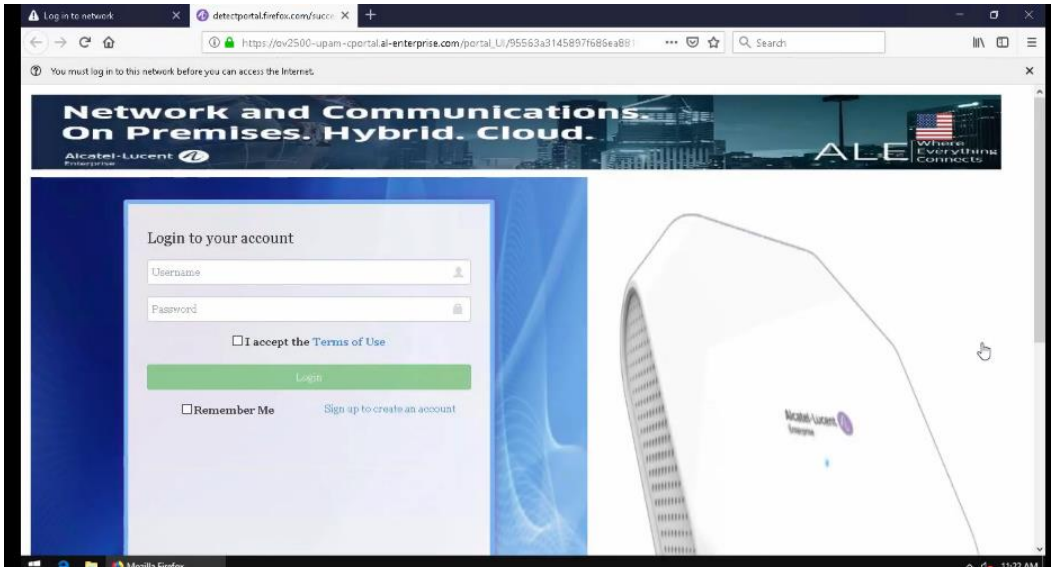


Figura 53. Ejemplo de funcionamiento de portal cautivo
4. Fuente: Propia

3.1.3. Desarrollo 03: Estrategia de recolección de datos y monitoreo aplicaciones de los usuarios dentro de la red Wi-Fi

3.1.3.1. Inspección profunda de paquetes

La inspección de paquetes será realizada mediante los AP's, el cual enviará la información recopilada hacia el controlador en la nube para el registro y análisis En la figura 54, se observa la pestaña "Summary View", dentro del módulo "ANALYTICS"

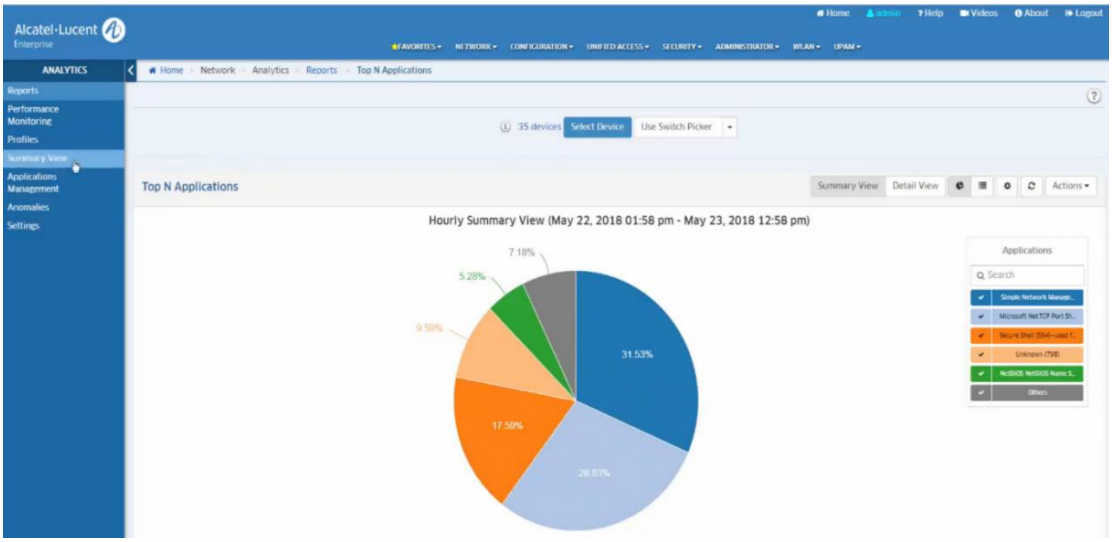


Figura 54. Visor de aplicaciones
Fuente: Propia

En la figura 55, se observa la opción "Global" donde se muestra la información de aplicaciones como estadístico.

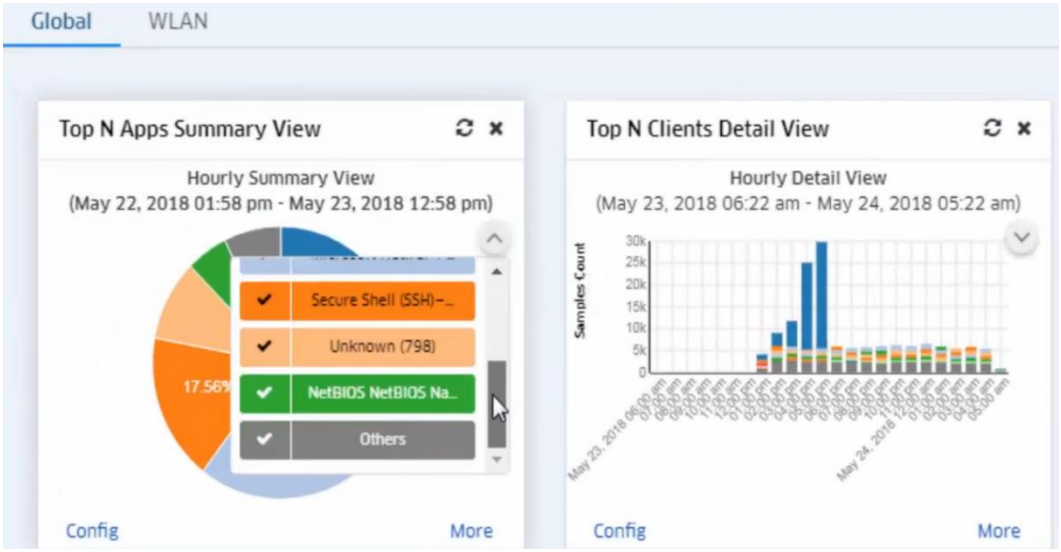


Figura 55. Visor de aplicaciones expandido
Fuente: Propia

3.1.3.2. Calidad de servicio

La calidad de servicio será por tipo de aplicación, siguiente el estándar WMM (IEEE 802.11e) y DSCP

• Background:

Uplink DSCP= 10

Downlink DSCP= 10

•Best Effort:

Uplink DSCP=0

Downlink DSCP=0

• Video:

Uplink DSCP=40

Downlink DSCP=40

• Voice:

Uplink DSCP=56

Downlink DSCP=56

3.2. Pruebas

El en siguiente apartado se explorará una versión de prueba del controlador en la nube OmniVista Cirrus, detallando las características relevantes a los objetivos del proyecto:

En la figura 56 se tiene las credenciales de acceso a la DEMO OmniVista Cirrus

Link: https://edemocirrus.ov.ovcirrus.com/login.html

User: edemocirrus

Contraseña: Ale2018!

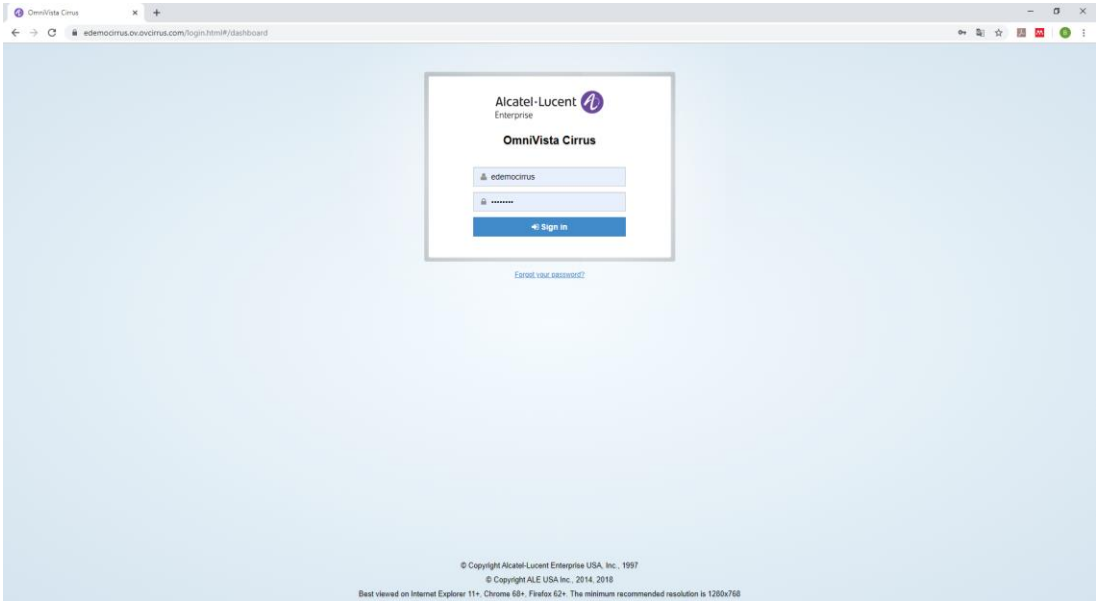


Figura 56. Interfaz web OmniVista Cirrus
Fuente: Propia

3.2.1. Gestión y administración unificada

3.2.2. Dashboard: WLAN Advanced

Dashboard es la página principal de la interfaz del OmniVista Cirrus, aquí se mostrará ventanas informativas llamadas “Widget”. Cada Widget contiene información sobre AP’s, clientes, Grupos, SSID, Densidad de usuarios entre otros.

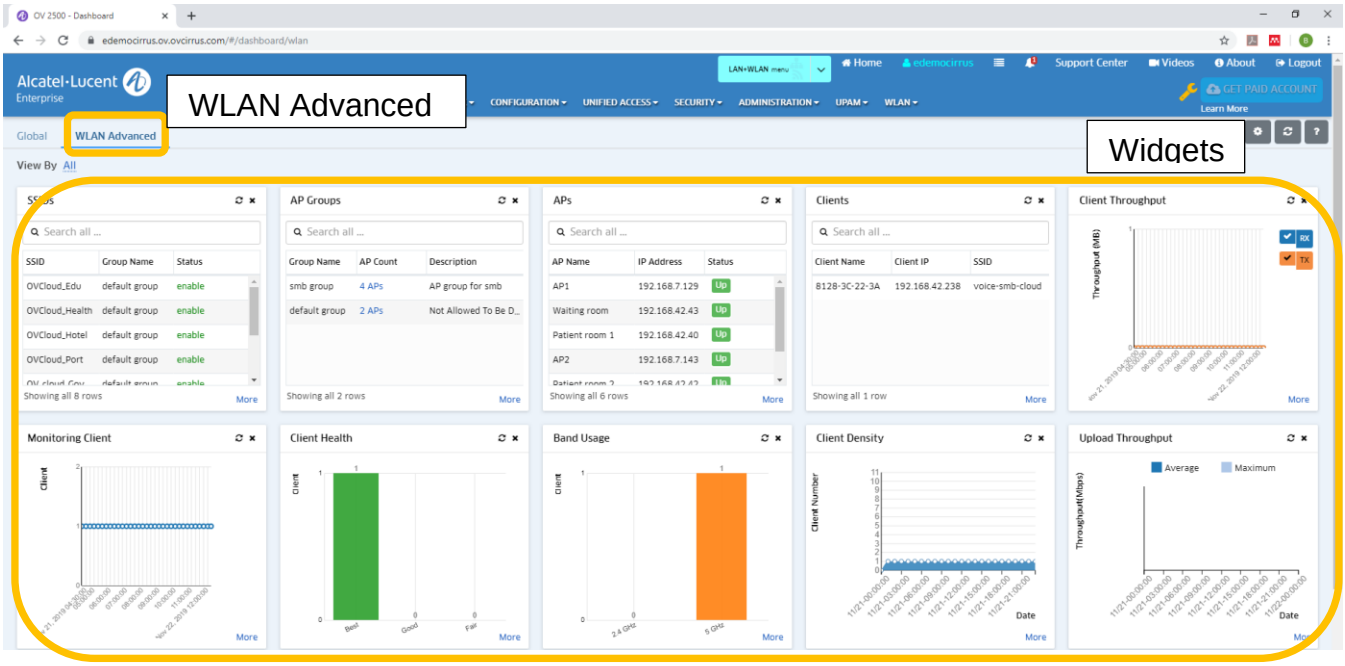


Figura 57. Visor de aplicaciones expandido
Fuente: Propia

Al hacer en la opción “more” de un widget, por ejemplo, el Widget “AP’s”, inmediatamente nos dirige a una nueva ventada donde nos brinda información sobre los AP’s como se muestra en la figura 58:

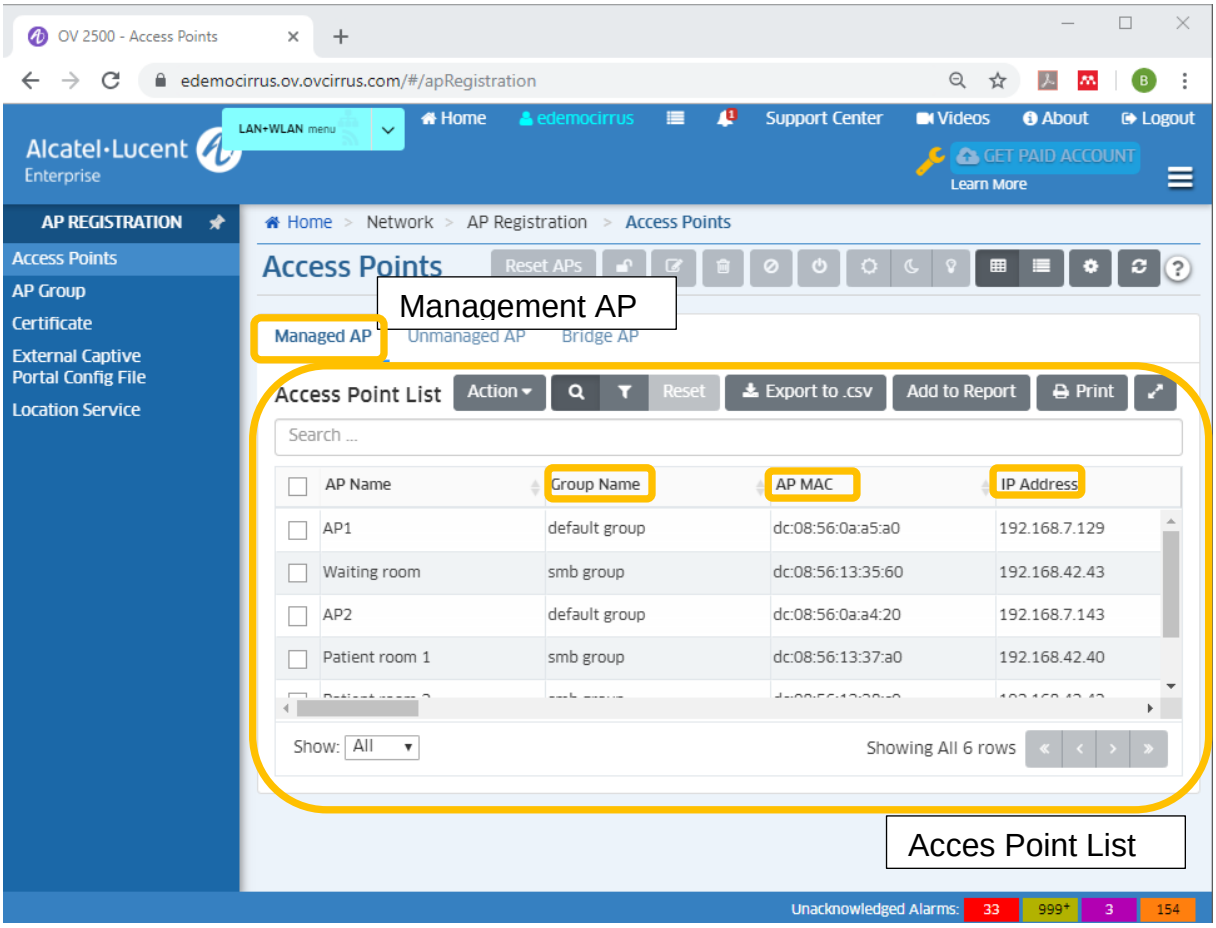


Figura 58. Ventana Ap Registration>Access Points
Fuente: Propia

En la figura 58 se observa información sobre los Apps gestionados, cada uno con su nombre, grupo al que pertenece, dirección IP entre otros

3.2.2.1. Modulo Network: AP registration

Este módulo contiene información de los AP's gestionados y los grupos a los que pertenecen (AP Group).

En la figura 59 se observa 02 AP groups definidos.

Se debe señalar que, para nuestro diseño, existirán 04 grupos de AP's, uno grupo para cada sede (San Isidro, Surco, Ate, Lurín).

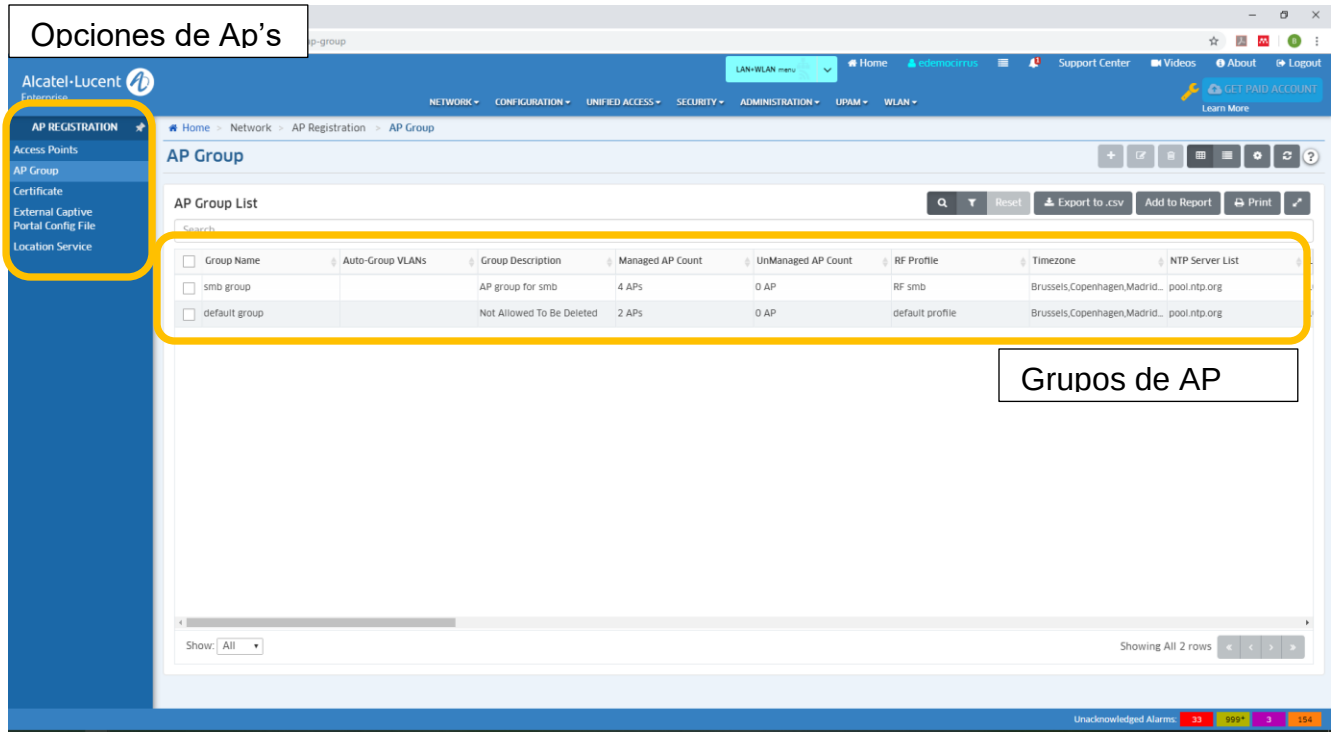


Figura 59. Ventana Ap Registration> AP group
Fuente: Propia

3.2.2.2. Modulo Network: Topology

Este módulo nos brinda un mapa topológico de cada AP activo.

Por cada "AP Group" activo, se creará un mapa topológico donde se conectarán los AP's.

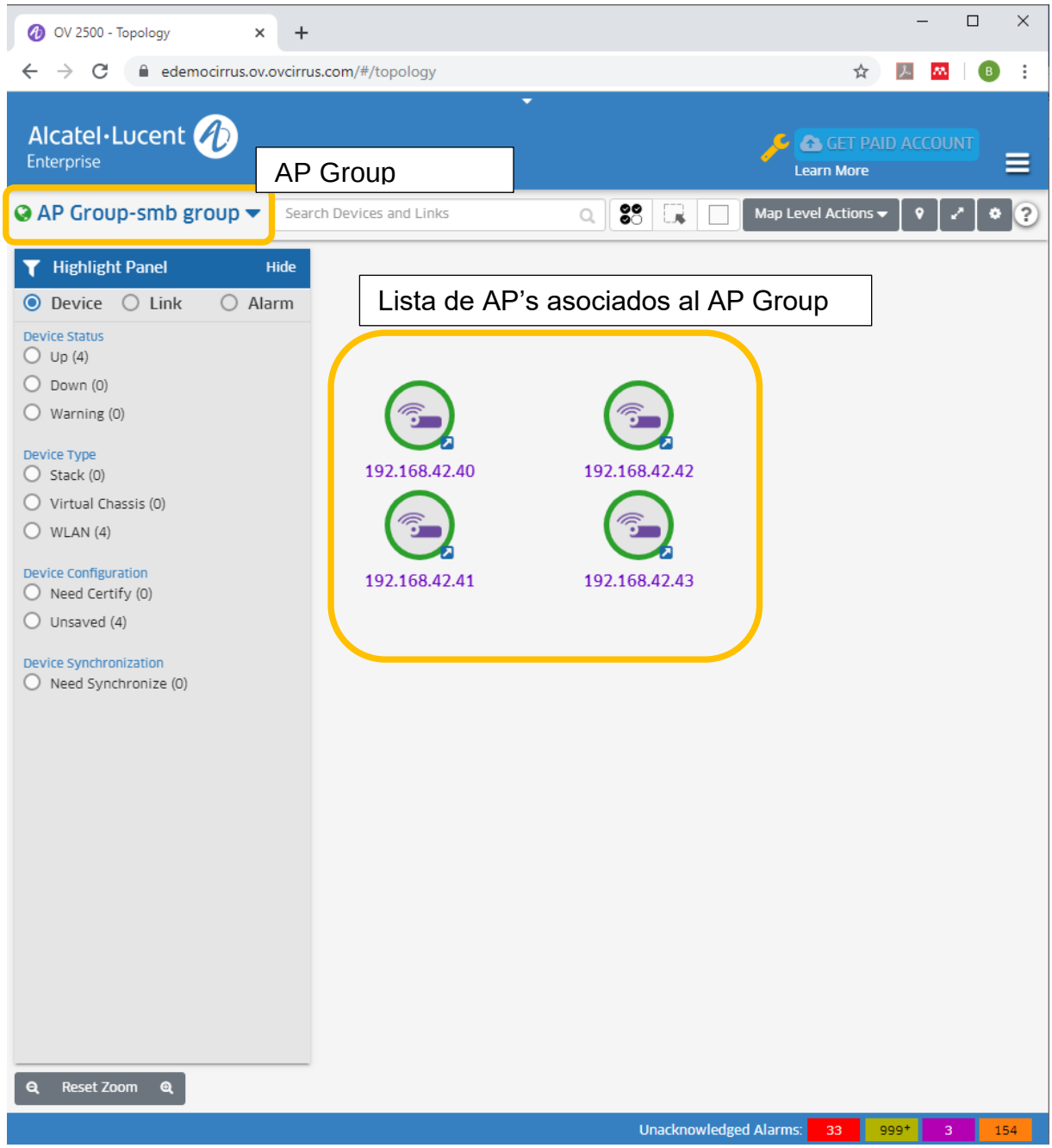


Figura 60. Ventana Topology
Fuente: Propia

3.2.2.3. Modulo Network: Inventory

Este módulo (ver figura) es utilizado para inventariar todos los AP's y equipos del fabricante Alcatel Lucent. Aquí es donde se puede observar el estado de la adopción del controlador OmniVista Cirrus con los AP's.

Para el propósito del diseño de la red del grupo Ilender, se tendrá 32 AP's gestionados por el controlador

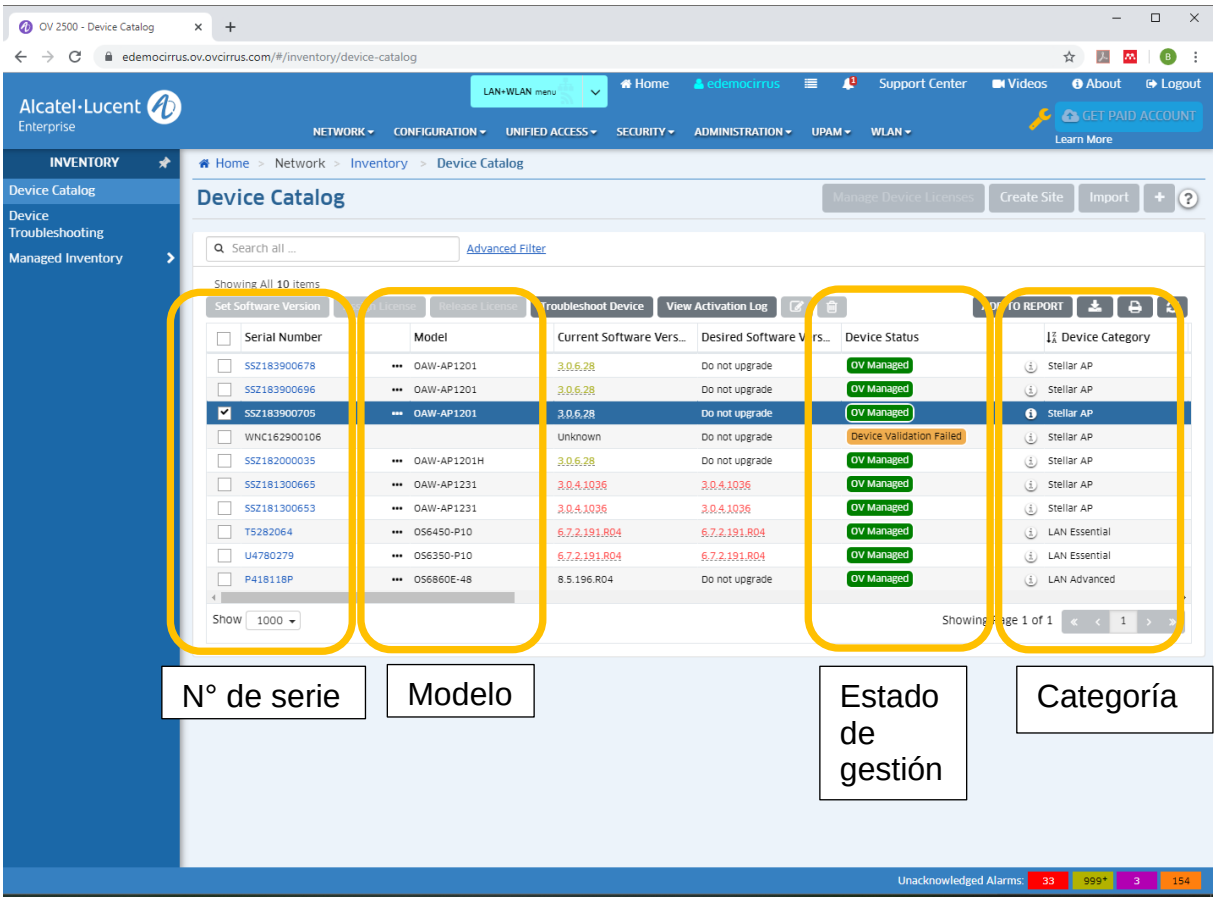


Figura 61. Ventana Device Catalog
Fuente: Propia

3.2.2.4. Modulo WLAN: SSID

En este apartado se visualizan todas las SSID activas, también se menciona todas las características asociadas, como el tipo de seguridad, autenticación, vlan, ARP (Access Role Profile), etc. En la figura se observa 02 SSID, uno para invitado y otro para usuarios (Guest). Para el diseño de la red Wi-Fi del grupo se tendrá creado 08 SSID's con sus respectivas vlans.

Figura 62. Ventana SSID
Fuente: Propia

3.2.2.5. Modulo WLAN: WLAN Service

WLAN Service es el módulo donde se crean y definen los parámetros de SSID como seguridad, autenticación, roaming, QoS y control de clientes tal y como se muestra en la figura 61, donde se tiene aprecia los parámetros del WLAN Servie “OVCloud_Health”

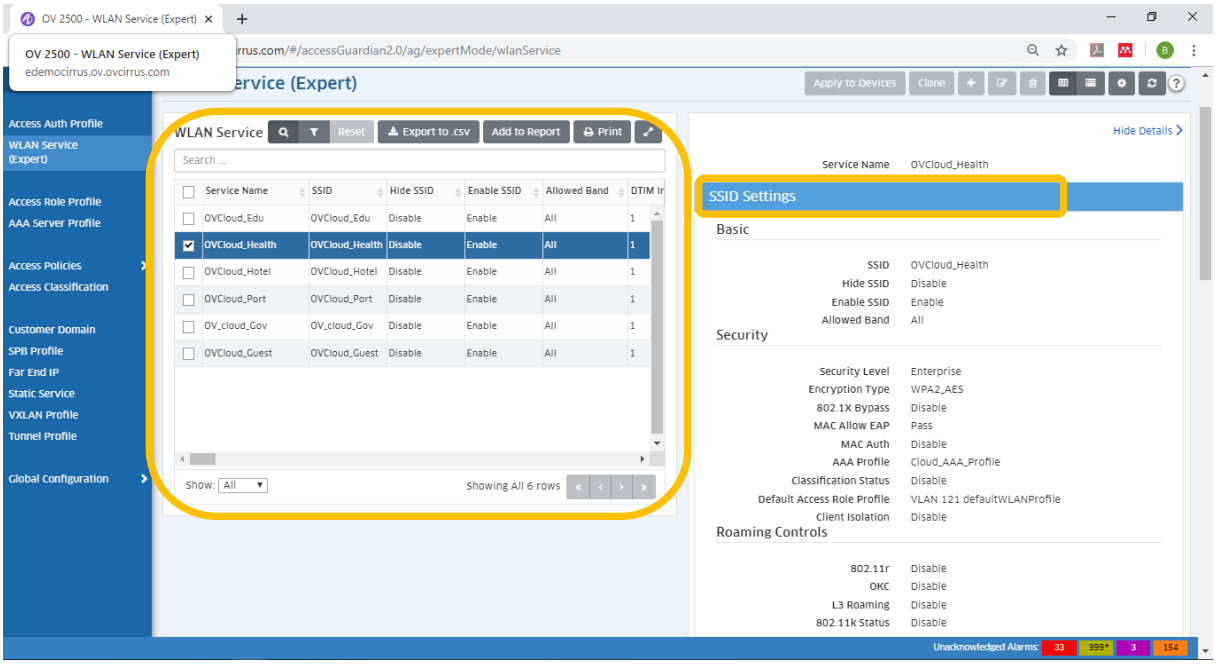


Figura 63. WLAN Service – SSID
Fuente: Propia

Para el diseño de la solución del grupo Ilender, se tendrán habilitados 01 WLAN Service por cada SSID, es decir habrán 08 WLAN Service creados

En la figura 64 se observa los parámetros de QoS

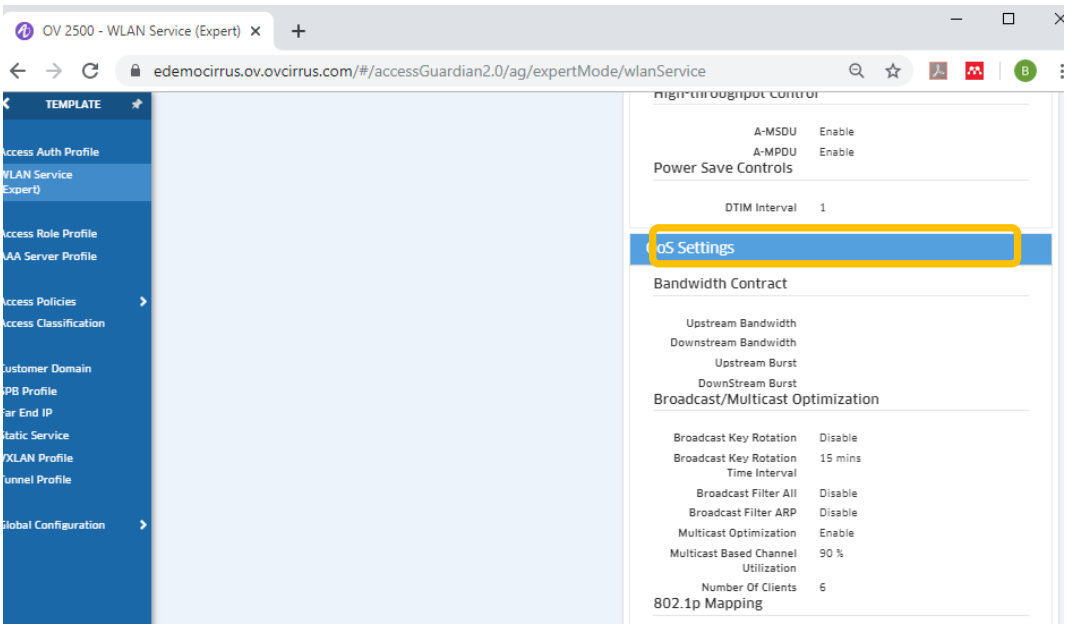


Figura 64. Ventana WLAN Service - Qos
Fuente: Propia

3.2.3. Autenticación

3.2.3.1. Modulo UPAM: Authentication

Para la autenticación de usuarios, se cuenta con el módulo UPAM, en este apartado se declaran los usuarios internos, pudiendo clasificarlos en base al tipo de departamento como se muestra en la figura 65

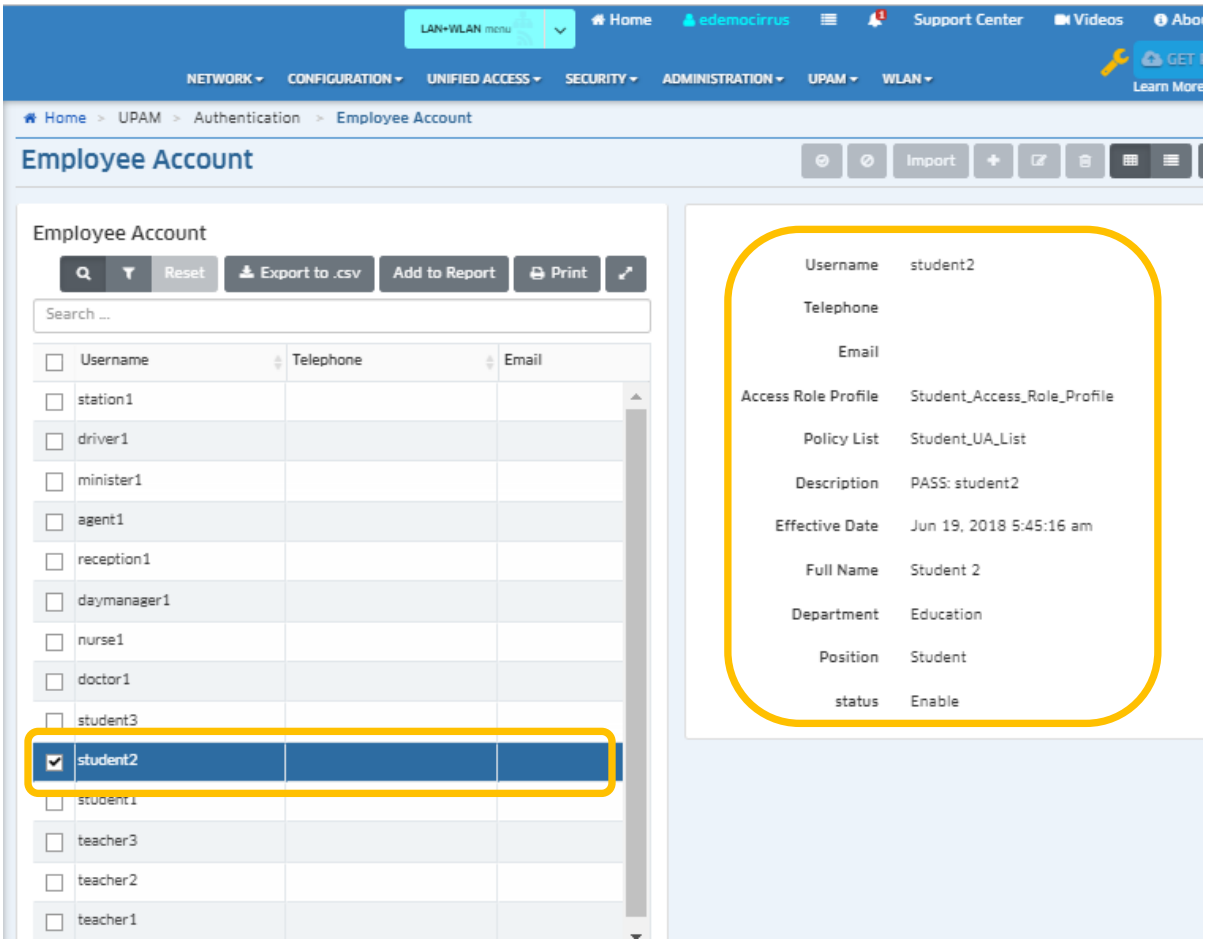


Figura 65. Ventana UPAM> Authentication>Employee Account
Fuente: Propia

Cabe señalar, aquí se define el tipo de servidor a utilizar como se muestra en la figura 64, al utilizar un servidor RADIUS interno en la pestaña “Authentication Strategy”, se define como Authenticación Source “Local Database”

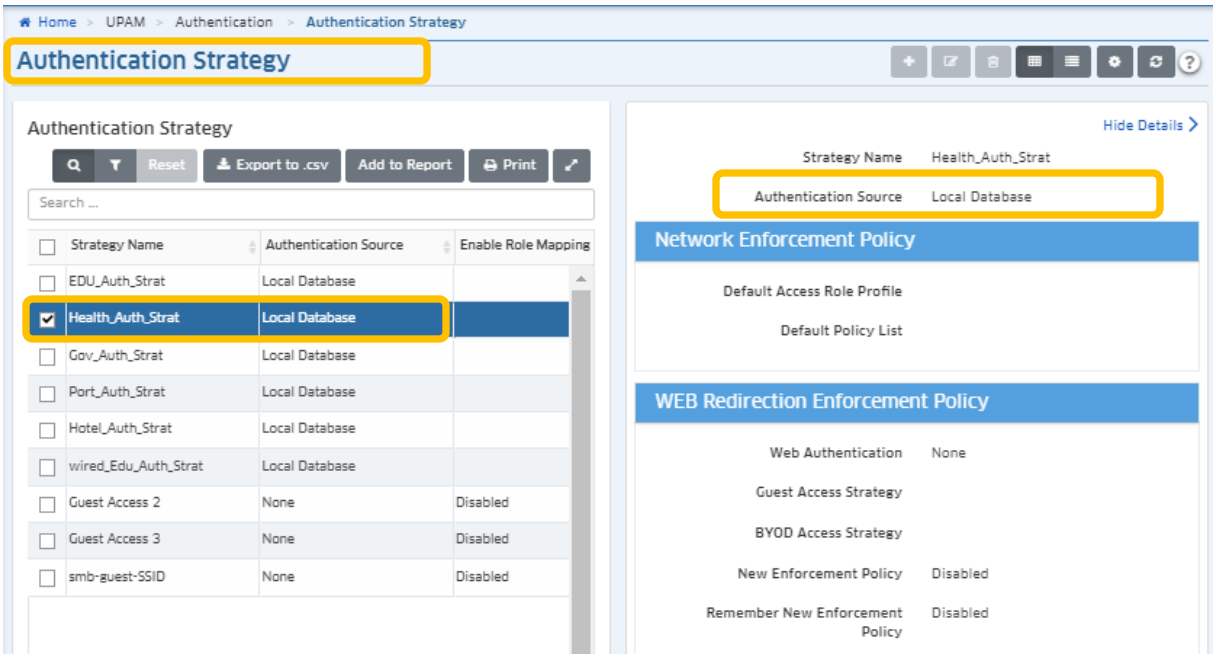


Figura 66. Ventana Authentication Strategy
Fuente: Propia

3.2.3.2. Modulo UPAM: Guest Access

Guest Access es el módulo donde se consolidad los usuarios de tipo invitados. Aquí se podrá crear, modificar y eliminar las credenciales. En la figura 67 se observa los usuarios creados:

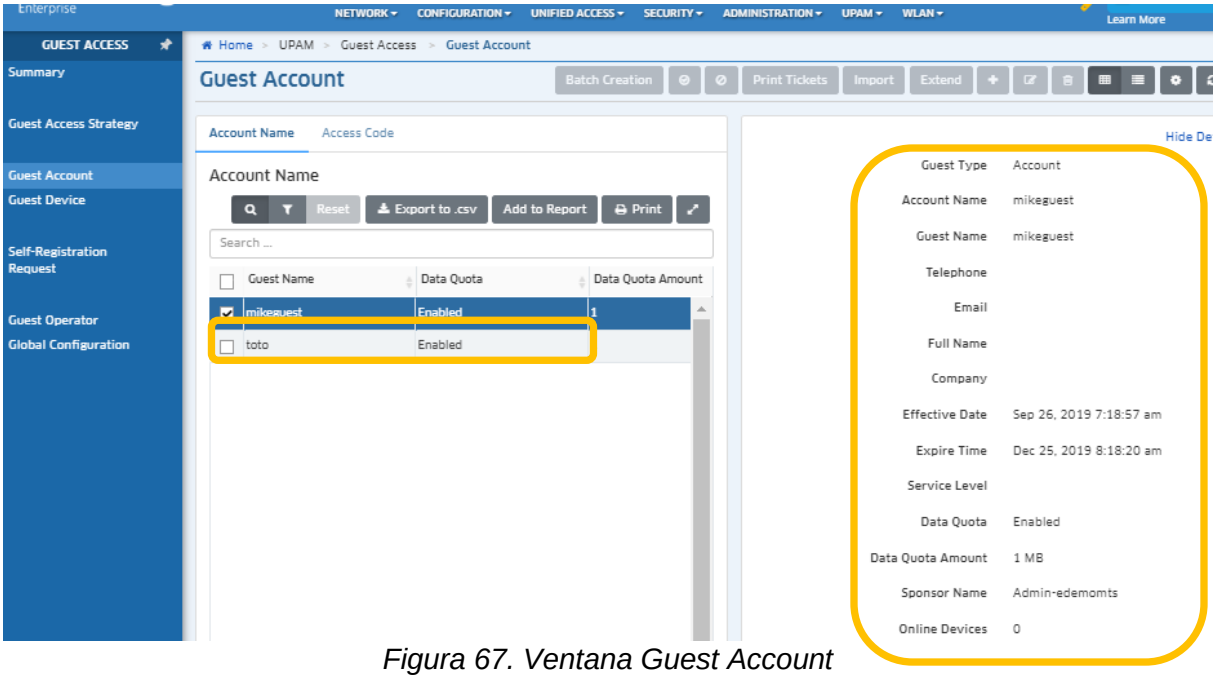


Figura 67. Ventana Guest Account
Fuente: Propia

3.2.3.3. Modulo Configuration: Captive Portal

En la figura 68, se tiene lo siguiente la interfaz de personalización del portal cautivo, aquí se personalizará con el logo de Grupo Ilender. También se editarán los términos y condiciones de ingreso. En nuestro diseño, solo se considera un Portal Cautivo con una página personalizada para el acceso de usuarios invitados.

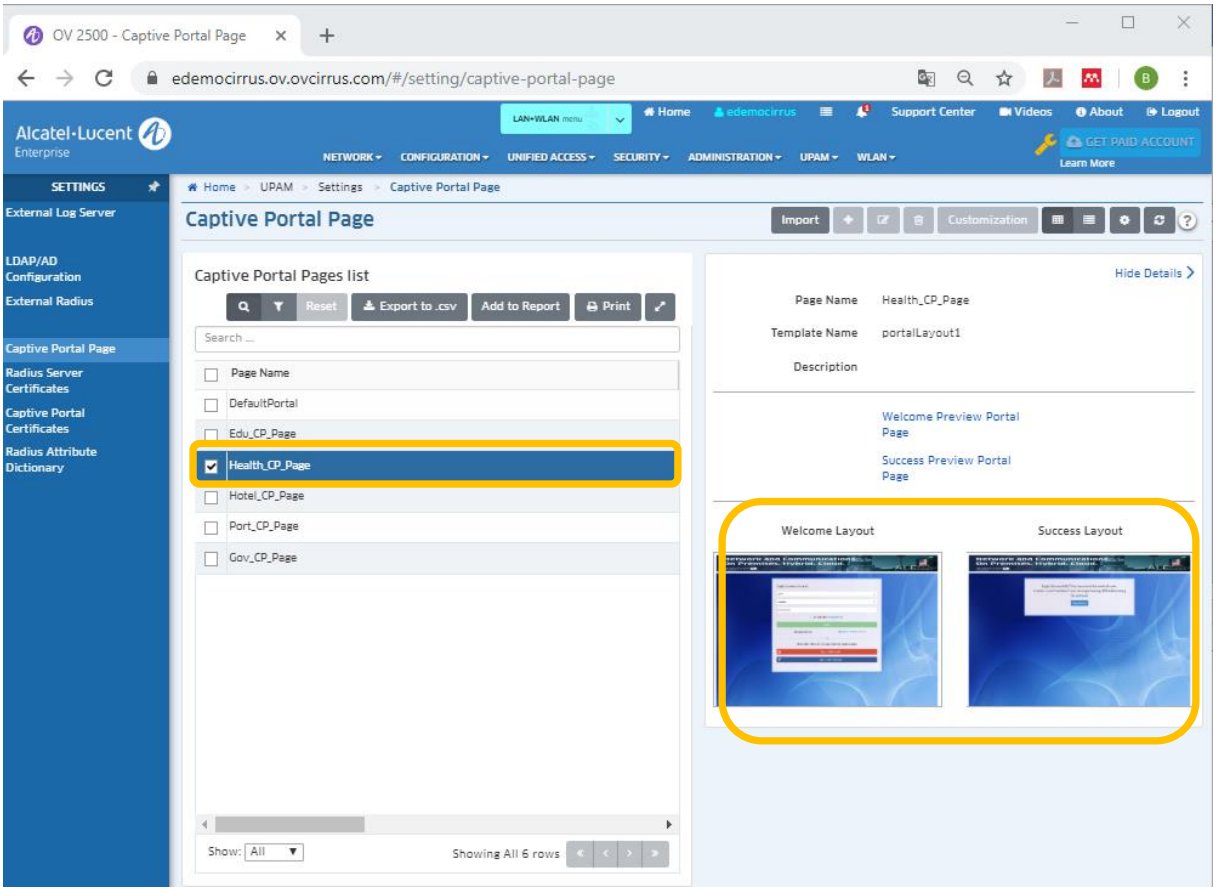


Figura 68. Ventana Guest Captive Portal
Fuente: Propia

3.2.4. Estrategia de recolección de datos y monitoreo de aplicaciones

3.2.4.1. Modulo Network: Application Visibility

Este módulo permite la identificación de datos a través de los AP's con la herramienta DPI embebida
Se cargará una "Signature Profile" (figura 69) al AP's. Este perfil contiene todos los grupos de aplicaciones actualizados a la fecha (base de datos con el que el DPI comparará e identificará. Los datos obtenidos son mostrados en el Dashboard

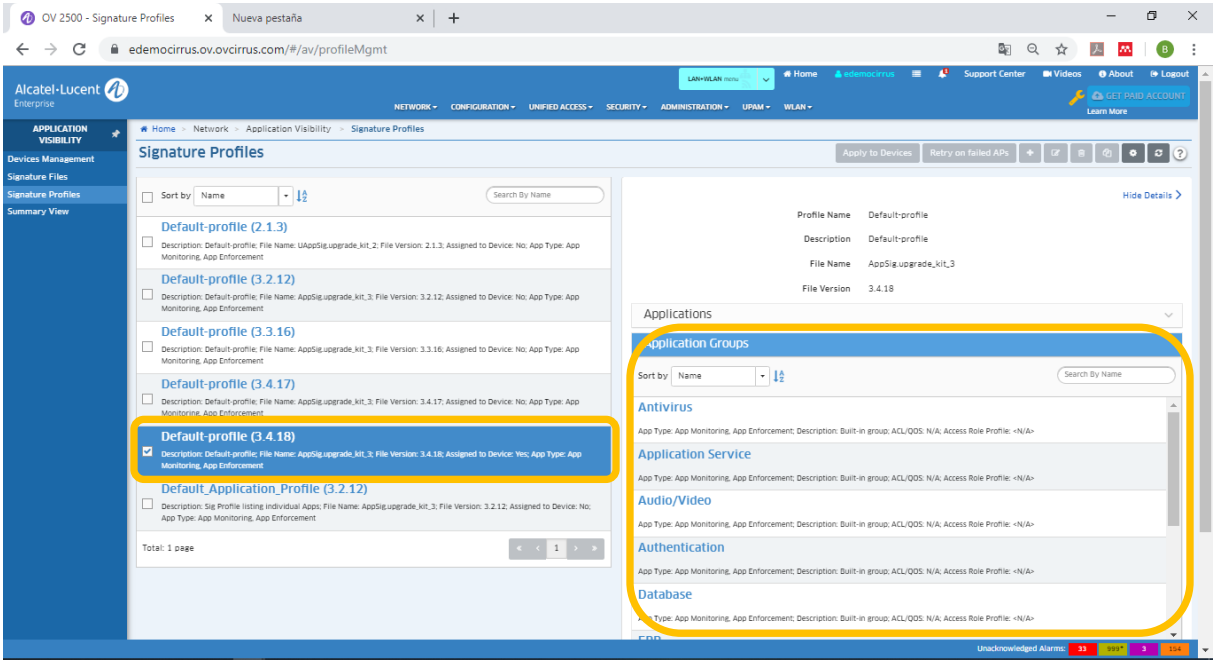


Figura 69. Ventana Application Visibility
Fuente: Propia

3.3. Resultados

1) Se logró diseñar una red Wi-Fi gestionado en la nube que permitirá el control y monitoreo de usuarios de forma centralizada y disponible en todo momento para el grupo Ilender en el departamento de Lima

2) A nivel de diseño de la topología y dimensionamiento de red Wi-Fi, se logró determinar que el diseño permitirá una clasificación de usuarios por cada empresa del grupo con su respectivo SSID y credenciales de usuario. Así mismo también se logró determinar que los AP's modelo Stellar 1221 y el controlador en la nube OmniVista Cloud, de la marca Alcatel Lucent, soportarán el funcionamiento y la gestión en la nube, respectivamente de la red Wi-Fi propuesta

3) Se eligió mecanismo de autenticación de usuarios de red Wi-Fi la autenticación por 802.1x a través del servidor RADIUS embebido dentro del módulo UPAM (Unified Policy Authentication Management), modulo que incorpora el controlador en la nube OmniVista Cirrus.

4) Se logró realizar la recolección de datos y monitoreo de aplicaciones de los usuarios dentro de la red Wi-Fi gestionado en la nube utilizando la herramienta DPI embebida en los AP's Stellar AP1221 propuestos, los cuales envían el tráfico identificado hacia el controlador en la nube OmniVista Cirrus para su almacenamiento y tratamiento.

CONCLUSIONES

1) El diseño de la red Wi-Fi gestionado en la nube para el grupo Ilender simplificará la administración, asegurará la integridad de los usuarios de cada empresa del grupo Ilender mediante la autenticación y monitoreo en tiempo de real del tráfico a nivel de aplicación sobre la red Wi-Fi

2) El diseño de topología y dimensionamiento de la red Wi-Fi soportará el control y monitoreo de usuarios de forma ordenada y permitirá el crecimiento tanto en despliegue de nuevos AP's como en usuarios conectados manteniendo la gestión centralizada en la nube.

3) La autenticación a través del servidor RADIUS embebido dentro del controlador en la nube OmniVista Cirrus permitirá llevar el control de acceso integro de los usuarios del grupo Ilender en el departamento de Lima de forma unificada y segura, debido a que el servidor se encuentra en la nube y siempre estará disponible para la autenticación de los dispositivos de usuario

4) La característica del AP modelo Stellar AP1221 de contar con una la herramienta DPI integrada permitirá la identificación del tipo de tráfico de usuario hasta el nivel de capa de aplicación del modelo OSI. Esto permitirá distribuir el flujo de trabajo para la inspección profunda de paquetes sobre tráfico de datos dentro de la red Wi-Fi.

RECOMENDACIONES

1) Se debe considerar un segundo enlace de respaldo hacia internet a fin de asegurar la disponibilidad del servicio de conexión a internet para la gestión en la nube.

2) Para el asegurar el correcto funcionamiento, despliegue, compatibilidad y comunicación de los componentes de red (AP's y controlador), se recomienda que estos sean de la misma marca; en este caso, Alcatel Lucent.

3) Es recomendable realizar una validación periódica de todos los usuarios autenticados en la red Wi-Fi a fin de llevar el control actualizado de todos los dispositivos asociados por cada usuario. También se recomienda actualizar una lista negra para aquellos dispositivos no identificados.

4) Se recomienda mantener siempre actualizado la base de datos de aplicaciones dentro del servidor Omnivista Cirrus y trasladarlo al AP, esto permitirá identificar las aplicaciones nuevas para su posterior análisis y tratamiento.

BIBLIOGRAFIA

Alcatel Lucent Enterprise. (2018). *Network Strategy and Vision for the Enterprise - Where Everything Connects*.
Recuperado de: https://www.al-enterprise.com/-/media/assets/internet/documents/network-strategy-whitepaper-en.pdf

Alcatel Lucent Enterprise (2018) *User Guide for OmniVista 2500 NMS Enterprise Version 4.3R1*
https://support.alcadis.nl/Support_files/Alcatel-Lucent/OmniVista//OmniVista_2500_Data/Software/OmniVista%202500%20NMS%20v4.x/OmniVista%202500%20NMS%20v4.3%20R01%20build%2051%20GA/OmniVista_2500_NMS_v4.3%20R01_build_51_GA_Release_Notes.pdf

Alcatel Lucent Enterprise (2018). *WLAN Alcatel-Lucent Enterprise OmniAccess® Stellar – Golden RFP.* Recuperado de: https://www.al-enterprise.com/en/-/media/assets/internet/documents/omniaccess-stellar-wlan-golden-rfp-es.pdf

Alcatel Lucent Enterprise (2019) "*Alcatel-Lucent OmniVista Cirrus Simple, secure cloud-based network management as a service"*
Recuperado de:
https://www.al-enterprise.com/-/media/assets/internet/documents/ov-cloud-datasheet-en.pdf

Alcatel Lucent Enterprise (2019). *Alcatel Lucent Stellar AP1220 series.*
Recuperado de:
https://www.al-enterprise.com/-/media/assets/internet/documents/oaw-ap1220-series-datasheet-en.pdf

Alcatel Lucent Enterprise. (2019). *Mobile Campus Network Solution: Transform your business with a network infrastructure that supports digital technologies, seamless mobility and the Internet of Things.* Recuperado de:
https://www.al-enterprise.com/en/-/media/assets/internet/documents/h-to-m/mobile-campus-solution-white-paper-en.pdf

Alcatel Lucent Enterprise (2019). *OmniSwitch AOS Release 8 Network Configuration Guide.*
Recuperado de:
https://support.alcadis.nl/Support_files/Alcatel-Lucent/OmniSwitch//OS6465/Manuals/OS6465%20AOS%208.5.1.R01/OS6465_AOS_8.5.1.R01_Network_Configuration_Guide.pdf

Alcatel Lucent Enterprise. (2019). *The perfect fit for business Enterprise wireless LAN reliability with operational simplicity*. Recuperado de: https://www.al-enterprise.com/en/-/media/assets/internet/documents/a-to-g/generic-at-a-glance-techbrief-stellar-en.pdf

Allied Telesis (2006) *802.1x White Paper*. Recuperado de: https://www.alliedtelesis.com/sites/default/files/documents/white-papers/8021x_wp.pdf

Aruba Networks (2009). *Optimizing Aruba WLANs for Roaming Devices* Recuperado de: https://community.arubanetworks.com/aruba/attachments/aruba/Aruba-VRDs/152/1/Optimizing%20Aruba%20WLANs%20for%20Roaming%20Devices.pdf

Aruba Networks. (2014). *802.11ac In-Depth. Recuperado de https://www.um.es/documents/378246/2964900/Normas+APA+Sexta+Edici%C3%B3n.pdf/27f8511d-95b6-4096-8d3e-f8492f61c6dc*

Aruba Networks. (2014). *migration guide 802.11ac.* Recuperado de https://www.arubanetworks.com/pdf/technology/MG_80211ac.pdf

BARRENECHEA, T. I. (2011). "*Diseño de una red inalámbrica para una empresa de Lima*". Pontificia Universidad Católica del Perú, Lima, Perú.
MENDOZA, M. G. (2011). "*Diseño y administración centralizada de redes WLAN a nivel nacional para CENTRUM católica*". Pontificia Universidad Católica del Perú, Lima, Perú.

BONILLA, M. A. (2016) "*Análisis y diseño de un sistema de seguridad en red perimetral en la empresa aseguradora del Sur – Matriz".* Pontificia Universidad Católica de Ecuador, Quito, Ecuador

GARCIA, J., y TEJADA , J. (2019). "*Diseño y validación de un método de roaming rápido en capa 2 para una red Wi-Fi con autenticación 802.1X".* Pontificia Universidad Católica del Perú, Lima, Perú.

HERNANDEZ L. E. (2010). "*Diseño de red inalámbrica en el Centro de Convenciones Bolívar"*. Universidad Dentral Marta Abreu De Las Villa, Santa Clara, Cuba

JENRY, L. V. (2015) "*diseño de una red de sensores de espectro para la selección de canales de operación óptimos en la red wifi del campus pucp".* Pontificia Universidad Católica del Perú, Lima, Perú.

LOPEZ, J. R. (2012). "*Diseño e implementación de un sistema de gestión de accesos a una red Wi-Fi utilizando software libre*". Pontificia Universidad Católica del Perú, Lima, Perú.

MORENO, M. (2015). *"Análisis, diseño y despliegue de una red WiFi en Santillana del Mar".* Universidad Autónoma de Madrid, Madrid, España

Telecom Engineering Centre. *Deep Packet Inspection*. Recuperado de http://tec.gov.in/pdf/Studypaper/White%20paper%20on%20DPI.pdf.

ANEXOS

ANEXO A: ALCATEL LUCENT STELLAR AP 1220 SERIES
ANEXO B: ALCATEL LUCENT OMNIVISTA CIRRUS

ANEXO A

ALCATEL LUCENT STELLAR AP 1220 SERIES

ALE | Where Everything Connects

Alcatel-Lucent OmniAccess Stellar AP1220 Series

Indoor high performance 802.11ac Wave 2 wireless access points

Multifunctional Alcatel-Lucent OmniAccess® Stellar AP1220 series access points are mid-end 802.11ac Wave 2 APs for medium density and large business deployments. The OmniAccess Stellar AP1220 series indoor Wi-Fi access point provides high throughput and a seamless user experience.

AP1221

AP1222

The high performance 802.11ac AP1220 series supports a maximum concurrent data rate of 2.1 Gb/s (1733 Mb/s in 5 GHz and 400 Mb/s in 2.4 GHz), 160 MHz channels (VHT160*), multi-user MIMO (MU-MIMO) and four spatial streams (4SS). They provide simultaneous multicast data transmission to multiple devices, maximizing data throughput and improving network efficiency.

Featuring enhanced WLAN technology with RF Radio Dynamic Adjustment, a distributed control Wi-Fi architecture, secure network admission control with unified access, built in application intelligence and analytics, making it ideal for enterprises of all sizes demanding a simple, secure and scalable wireless solution.

Cloud enabled with OmniVista Cirrus

The AP1220 series APs can be managed by Alcatel-Lucent OmniVista® Cirrus cloud platform. OmniVista® Cirrus powers a secure, resilient and scalable cloud-based network management platform. It offers hassle free network deployment and easy service rollout with advanced analytics for smarter decision making. Offers IT friendly Unified Access with secure authentication and policy enforcement for users and devices.

Alcatel·Lucent Enterprise

OmniVista 2500 managed deployment

The AP1220 series APs can be managed by Alcatel-Lucent OmniVista® 2500 on premise Network Management System. The access points are managed as one or more access point (AP) groups (a logical grouping of one or more access points). The OmniVista 2500 next generation management suite embeds a visionary controller-less architecture, providing user friendly workflows for unified access together with an integrated unified policy authenticati on manager (UPAM) which helps define authentication strategy and policy enforcement for employees, guest management and BYOD devices. The AP1220 series has built-in DPI technology providing real-time Application Monitoring and enforcement. The network administrator can obtain a comprehensive view of applications running in the network and apply adequate control to optimize the performance of the network for business critical applications. OmniVista 2500 provides advanced options for RF management, WIDS/WIPS for intrusion detection and prevention, and a heat map for WLAN site planning.

Plug and Play: Secure Web managed (HTTPS) cluster deployment

The AP1220 series by default operates in a cluster architecture to provide simplified plug-and-play deployment. The access point cluster is an autonomous system that consists of a group of OmniAccess Stellar APs and a virtual controller, which is a selected access point, for cluster management. One AP cluster supports up to 64 APs.

The access point cluster architecture ensures simplified and quick deployment. Once the first AP is configured using the configuration wizard, the remaining APs in the network will come up automatically with an updated configuration. This ensures the whole network is up and functional within a few minutes.

The AP1220 series also supports secure zero-touch provisioning with Alcatel- Lucent OXO Connect R2, a mechanism by which all access points in a cluster will obtain bootstrap data securely from an on-premise OXO Connect.

Integrated guest management

The AP1220 series supports role based management access to the AP cluster which includes Admin, Viewer and GuestOperator access. GuestOperator access simplifies guest account creation and management, and can be used by any non-IT person such as a front desk worker or receptionist. The AP1220 series access points also support a built-in customizable captive portal which enables customers to offer unique guest access.

Quality of service for unified communication apps

The OmniAccess Stellar AP1220 series access points support fine tuned, quality of service (QoS) parameters to differentiate and provide appropriate QoS for each application such as voice, video and desktop sharing. Application aware RF scanning avoids interruption of real-time applications.

RF management

Radio Dynamic Adjustment (RDA) technology automatically assigns channels and power settings, provides DFS/TPC, and ensures that access points stay clear of all radio frequency interference (RFI) sources to deliver reliable, high-performance wireless LANs. The OmniAccess Stellar AP1220 series APs can be configured to provide part-time or dedicated air monitoring for spectrum analysis and wireless intrusion protection.

Product specifications

Radio specification

- AP type: Indoor, dual radio, 5 GHz 802.11ac 4x4:4 MU-MIMO and 2.4 GHz 802.11n 2x2:2 MIMO
- 5 GHz: Four spatial stream single user (SU) MIMO for up to 1733 Mb/s wireless data rate to individual 4x4 VHT80 or 2x2 VHT160* client devices
- 5 GHz: Four spatial stream multi user (MU) MIMO for up to 1733 Mb/s wireless data rate to up to three MU-MIMO capable client devices simultaneously
- 2.4 GHz: Two spatial stream single user (SU) MIMO for up to 400 Mb/s wireless data rate to individual 2x2 VHT40 client devices (300 Mb/s for HT40 802.11n client devices)
- Supported frequency bands (country-specific restrictions apply):
  - 2.400 to 2.4835 GHz
  - 5.150 to 5.250 GHz
  - 5.250 to 5.350 GHz
  - 5.470 to 5.725 GHz
  - 5.725 to 5.850 GHz
- Frequencies fixed at factory for Middle East models OAW-AP1221-ME and OAW-AP1222-ME
  - 2400 - 2483.5 MHz
  - 5150 - 5350 MHz
- Available channels: Dependent on configured regulatory domain
- DFA (dynamic frequency adjustment) optimizes available channels and provides proper transmission power
- Short guard interval for 20 MHz, 40 MHz, 80 MHz and 160 MHz* channels
- Transmit beam forming (TxBF) for increased signal reliability and range
- 802.11n/ac packet aggregation: Aggregated Mac Protocol Data Unit (A-MPDU), Aggregated Mac Service Data Unit (A-MSDU)
- Supported data rates (Mb/s):
  - 802.11b: 1, 2, 5.5, 11
  - 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
  - 802.11n: 6.5 to 600 (MCS0 to MCS31)
  - 802.11ac: 6.5 to 1,733 (MCS0 to MCS9, NSS = 1 to 4 for
  - VHT20/40/80, NSS = 1 to 2 for VHT160)*
- Supported modulation types:
  - 802.11b: BPSK, QPSK, CCK
  - 802.11a/g/n/ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM

*160 MHz channel support will be available in the future

- 802.11n high-throughput (HT) support: HT 20/40
- 802.11ac very high throughput (VHT) support: VHT 20/40/80/160*
- Advanced Cellular Coexistence (ACC) Minimizes interference from 3G/4G cellular networks, distributed antenna systems, and commercial small cell/ femtocell equipment

Interfaces

- 1x 10/100/1000Base-T autosensing (RJ-45) port, Power over Ethernet (PoE)
- 1x USB 2.0 (Type A connector)
- 1x management console port (RJ-45)
- Reset button: Factory reset
- Kensington security slot
- AP1222: 4x RP-SMA antenna connectors

Visual Indicators (Tri-color LEDs)

- For system and radio status
  - Red flashing: System abnormal, link down
  - Red light: System startup
  - Red and blue rotate flashing: System running, OS upgrading
  - Blue light: System running, dual bands working
  - Green flashing: System running, no SSID created
  - Green light: System running, single band working
  - Red, blue and green rotate flashing: System running, use for location of an AP

Antenna

- AP1221: Built-in 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz
  - Integrated dual-band down tilt omni-directional antennas for 4x4 MIMO with maximum antenna gain of 3.61 dBi in 2.4 GHz and 4.45 dBi in 5 GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP.
- AP1222 External 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz
  - Four RP-SMA connectors for external dual band antennas.
- Optional external antenna (sold separately)
  - Offer includes broad selection of antennas, delivering optimal coverage for a variety of deployment scenarios.

Receive sensitivity (per chain)

	2.4 GHz	5 GHz
1 Mb/s	-96	
11 Mb/s	-88	
6 Mb/s	-92	-91
54 Mb/s	-74	-74
HT20 (MSC 0/8)	-91	-91
HT20 (MSC 7/15)	-71	-70
HT40 (MSC 0/8)	-88	-88
HT40 (MSC 7/15)	-68	-68
VHT20 (MSC 0)	-91	-91
VHT20 (MSC 8)	-67	-67
VHT40 (MSC 0)	-88	-88
VHT40 (MSC 9)	-63	-63
VHT80 (MCS0)		-85
VHT80 (MCS9)		-58
VHT160* (MCS0)		-84
VHT160* (MCS9)		-58

Maximum transmit power (per chain)

	2.4 GHz	5 GHz
1 Mb/s	18 dBm	
11 Mb/s	18 dBm	
6 Mb/s	18 dBm	18 dBm
54 Mb/s	17 dBm	17 dBm
HT20 (MSC 0/8)	18 dBm	18 dBm
HT20 (MSC 7/15)	16 dBm	17 dBm
HT40 (MSC 0/8)	18 dBm	18 dBm
HT40 (MSC 7/15)	16 dBm	17 dBm
VHT20 (MSC 0)	18 dBm	18 dBm
VHT20 (MSC 8)	16 dBm	17 dBm
VHT40 (MSC 0)	18 dBm	18 dBm
VHT40 (MSC 9)	15 dBm	16 dBm
VHT80 (MCS0)		18 dBm
VHT80 (MCS9)		16 dBm
VHT160* (MCS0)		18 dBm
VHT160* (MCS9)		16 dBm

Chile: Regulatory compliance. Maximum transmit power of 150mW including antenna gain.

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

Power

- Supports direct DC power and Power over Ethernet (PoE)
- When both power sources are available, DC power takes priority over PoE
- Maximum (worst case) power consumption:
  - <15.6 W (802.3at PoE or DC)
  - Excludes power consumed by external USB device; USB with 500mA load can add up to 2.9 W
  - Maximum power consumption in idle mode: 7.5 W

- Direct DC source: 48 V DC nominal, ± 5%
- Power over Ethernet (PoE):
  - 48 V DC (nominal) 802.3af/802.3at compliant source
  - Unrestricted functionality with 802.3at PoE
  - The USB port is disabled and the 5 GHz radio is restricted to 2*2:2 when the AP is powered by 802.3af PoE source

Mounting

- The AP ships with two (white) mounting clips to attach to a 9/16-inch or 15/16- inch flat T-bar drop-tile ceiling.
- Optional mount kits for Open Silhouette and Flanged Interlude.
- Optional mount kits for flat-surface (wall).

Environmental

- Operating:
  - Temperature: 0°C to 45°C (+32°F to +113°F)
  - Humidity: 10% to 90% non-condensing
- Storage and transportation:
  - Temperature: -40°C to +70°C (-40°F to +158°F)

Dimensions/Weight

- Single AP excluding packing box and accessories:
  - 180 mm (W) x 180 mm (D) x 36 mm (H) -7.08" (W) x 7.08" (D) x 1.41" (H)
  - 700 g/1.54 lb
- Single AP including packing box and accessories:
  - 228 mm (W) x 198 mm (D) x 66 mm (H) -8.97" (W) x 7.79" (D) x 2.59"(H)
  - 920 g/2.02 lb

Reliability

- MTBF: 916,666h (104.6 years) at +25°C operating temperature

Capacity

- Up to 8 SSID per radio (total 16 SSID)
- Support for up to 512 associated client devices per AP

Software features

- Up to 4K APs when managed by OV2500. There is no limit on the number of AP groups
- Up to 64 APs per web-managed (HTTP/ HTTPS) cluster
- Auto channel selection
- Auto transmit power control
- Bandwidth control per SSID
- L2 roaming
- L3 roaming with OmniVista 2500
- Captive portal (Internal/ External)
- Guest self-registration (optional SMS notification) with OmniVista 2500
- Internal user database
- RADIUS client
- Guest social-login with OmniVista 2500
- RADIUS proxy authentication OmniVista 2500
- LDAP/AD proxy authentication OmniVista 2500
- Wireless QoS
- Band steering
- Client smart load balance
- Client sticky avoidance
- User behavior tracking
- White/black list
- Zero-touch provisioning (ZTP)
- NTP server client
- ACL
- DHCP/DNS/NAT
- Wireless MESH P2P/P2MP
- Wireless Bridge
- Rogue AP location and containment
- System log report
- Dedicated Scanning AP
- SNMPv2
- SNMP Trap Notification with OmniVista 2500
- Wireless attack detection with OmniVista 2500
- Floor plan and heat map with OmniVista 2500
- Stanley Healthcare/Aeroscout RTLS support

Note: Some features are limited by local regulatory settings

Security

- 802.11I, WI-FI Protected Access 2 (WPA2), WPA, AES 128-256 bits
- 802.1X
- WEP, Advanced Encryption Standard (AES), Temporal Key Integrity Protocol (TKIP)
- Firewall: ACL, wIPS/wIDS and DPI application policy enforcement with OmniVista™
- Portal page authentication
- Integrated Trusted Platform Module (TPM) for secure storage of credentials and keys

IEEE standard

- IEEE 802.11a/b/g/n/ac Wave 2
- IEEE 802.11e WMM
- IEEE 802.11h, 802.11I, 802.11e QoS
- IEEE 802.1Q (VLAN tagging)
- 802.11k Radio Resource Management
- 802.11v BSS Transition Management
- 802.11r Fast Roaming

Regulatory & certification

- CB Scheme Safety, cTUVus
- WI-FI Alliance (WFA) certified 802.11a/b/g/n/ac
- FCC
- CE marked
- RoHS, REACH, WEEE
- UL2043 plenum rating
- EMI and susceptibility (Class B)

Ordering information

Item	Description
OAW-AP1221-RW	Indoor Mid-end Enterprise 802.11ac MU-MIMO AP, Dual-Radio, 11n 2x2:2 + 11ac 4x4:4, 1x GbE, 1x USB, 1x Console, and integrated antennas. Unrestricted Regulatory Domain. These products should be considered as Rest of World products and MUST NOT be used for deployments in the United States, Japan or Israel
OAW-AP1221-US	Indoor Mid-end Enterprise 802.11ac MU-MIMO AP, Dual-Radio, 11n 2x2:2 + 11ac 4x4:4, 1x GbE, 1x USB, 1x Console, and integrated antennas. Restricted regulatory domain: United States
OAW-AP1221-ME	Indoor Mid-end Enterprise 802.11ac MU-MIMO AP, Dual-Radio, 11n 2x2:2 + 11ac 4x4:4, 1x GbE, 1x USB, 1x Console, and integrated antennas. Restricted regulatory domain: Middle East (Israel, Egypt)
OAW-AP1222-RW	Indoor Mid-end Enterprise 802.11ac MU-MIMO AP, Dual-Radio, 11n 2x2:2 + 11ac 4x4:4, 1x GbE, 1x USB, 1x Console, and 4x antenna connectors. Unrestricted Regulatory Domain. These products should be considered as Rest of World products and MUST NOT be used for deployments in the United States, Japan or Israel
OAW-AP1222-US	Indoor Mid-end Enterprise 802.11ac MU-MIMO AP, Dual-Radio, 11n 2x2:2 + 11ac 4x4:4, 1x GbE, 1x USB, 1x Console, and 4x antenna connectors. Restricted regulatory domain: United States
OAW-AP1222-ME	Indoor Mid-end Enterprise 802.11ac MU-MIMO AP, Dual-Radio, 11n 2x2:2 + 11ac 4x4:4, 1x GbE, 1x USB, 1x Console, and 4x antenna connectors. Restricted regulatory domain: Middle East (Israel, Egypt)

Accessories	Description
OAW-AP-MNT-B	OmniAccess indoor mounting kit, for AP1101, AP122X, AP123X, Type B1(9/16") and B2(15/16") for T-shaped ceiling rail mounting. Standard configuration in the product packaging. Optional for customer ordering
OAW-AP-MNT-W	OmniAccess indoor mounting kit, for AP1101, AP122X, AP123X, Type W wall and ceiling mounting with screws. Optional for customer ordering
OAW-AP-MNT-C	OmniAccess indoor mounting kit, for AP1101, AP122X, AP123X, Type C1 (Open Silhouette) and C2 (Flanged Interlude), for other shaped ceiling rail mounting. Optional for customer ordering
PD-9001GR/AT/AC	1-Port IEEE 802.3at PoE Midspan. Port speed 10/100/1000M PoE power 30W. No power cord included. Please order PWR-CORD-XX for country specific power cord.
ADP-30HRBD	48V/30W AC-to-DC Power Adapter with Type A DC plug 2.1*5.5*9.5mm circular, straight. Please order PWR- CORD-XX for country specific power cord.
ANT-O-6	Dual band 2.4/5 GHz, 1-element direct mount , omni-directional antenna, 6dBi (box includes QTY 4)
ANT-O-M4-5	Dual band 2.4/5 GHz, 4-element, Ceiling-mount , Downtilt omni-directional antenna, MIMO 4*4, max gain 4.8dBi (1X); includes 4 element 30in RF cable
ANT-S-M4-60	Dual band 2.4/5 GHz, 4-element, Wall-mount, sector antenna , >5dBi, 60°Hx60°V (1x); includes 4 element 30in RF cable

Warranty

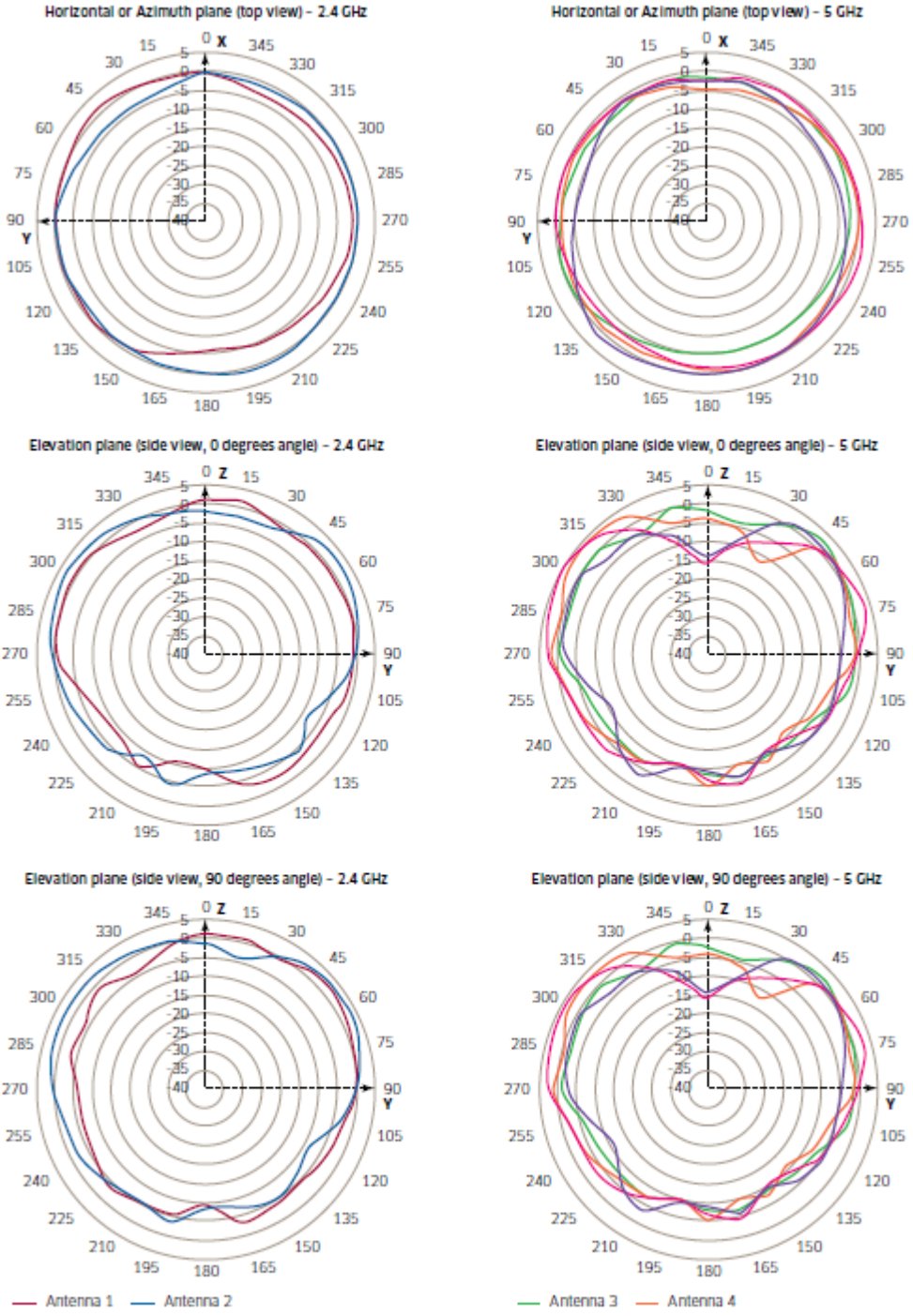
OmniAccess Stellar Access Points come with Hardware Limited Lifetime Warranty (HLLW)

Services and support

OmniAccess Stellar Access Points include 1 year of complementary SUPPORT Software for partners. For more information about our Professional services, Support services, and Managed services, please go to

http://enterprise.alcatel-lucent.com/?services=EnterpriseServices&page=directory

Figure 1. OmniAccess Stellar AP1221 antenna pattern plots



ANEXO B

ALCATEL LUCENT OMNIVISTA CIRRUS

Alcatel·Lucent
Enterprise

Alcatel-Lucent OmniVista Cirrus

Simple, secure cloud-based network management as a service

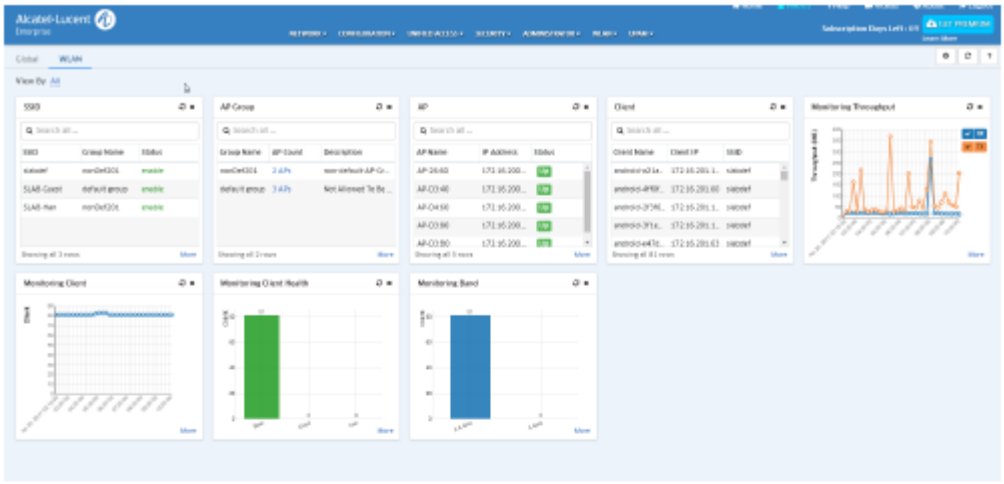
Alcatel-Lucent OmniVista® Cirrus is a scalable, resilient, secure cloud-based network management for unified access offered as a subscription service. OmniVista Cirrus offers an easy to deploy, effective way to manage and monitor Alcatel-Lucent Enterprise switches and Alcatel-Lucent OmniAccess® Stellar access point infrastructure. It provides advanced policy capabilities for guest access and BYOD as well as advanced analytics for smarter decision making.
OmniVista Cirrus is a subscription-based service, facilitating alignment with your new business imperatives. Ease of purchasing, provisioning and ongoing daily operations are at the core of OmniVista Cirrus. This facilitates your digital transformation, allowing you to be quick to respond to new business needs such as IoT visibility and identification of network connected devices, but without high upfront costs or complex infrastructure changes or software deployments. Shifting to a cloud based network management solution with OmniVista Cirrus simplifies digital transformation by reducing cost and administrative IT burden.

OmniVista Cirrus sets a new IT experience standard for simple yet powerful capabilities. OmniVista Cirrus can scale and adapt to your business requirements. It offers advanced visibility and control over users and applications. By focusing on core IT operations OmniVista Cirrus comprehensive management solution makes it easy to improve application performance and troubleshoot issues in deployments with distributed locations and limited IT staff. OmniVista Cirrus protects your network infrastructure investment by adapting to changing business needs without expensive “rip and replace.”

Datasheet

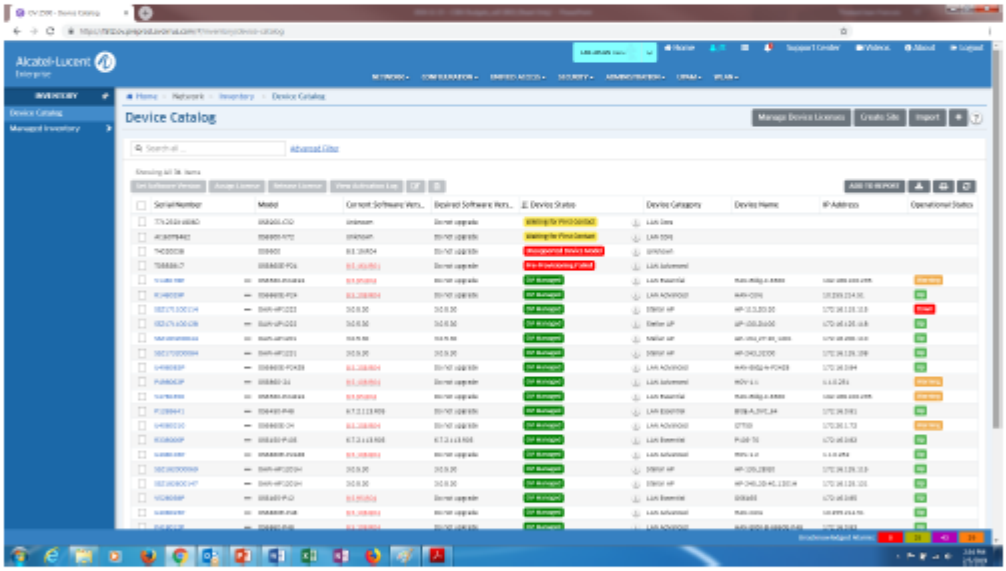
Features	Benefits
Investment protection	• ALE wired and wireless network devices can be migrated from on-premises network management to the cloud with OmniVista Cirrus with just an appropriate firmware version • Quickly adapt your network infrastructure to meet the changing needs of your business without costly hardware replacement or complex network re-architecture for maximum business alignment
Operational simplification	• Continuous feature updates delivered from the cloud, reducing IT daily involvement and costs • Intuitive interface eliminating Costly training or added staff
Multi-site management	• Provides centralized management of multiple virtual or physical sites • Consolidates critical management information from across the entire network for a global and consistent network experience
Multi-tenancy services	• Multi-client level with simplified Administration • Easily control who has access to which client network and tenant with the appropriate administrative network administration credentials • See all key management status and all-important network events and alerts from a single Dashboard
Highly scalable	• Provide cloud scalability from small to large network deployments without network reconfiguration • Designed to scale and adapt to your business transformation imperatives during subscription
Highly available	• Hosted in multiple regional data centers with optimal 99.99% availability • Maximum availability ensured with backup and redundant services and disaster recovery provided by each data center
Highly secure	• OmniVista Cirrus with separation of out of band control plane (management traffic) and user data • Secure communications with the highest level of protection using certificates ranging from a mutual cloud to device authentication
Easy to deploy	• Simplified device catalog and cloud on-boarding with mobile apps (IOS and Android) • Faster service roll-out with Zero-touch provisioning of managed network devices • Minimal network expertise required for initial enterprise network set up and daily operations, offloading IT resource
Template based Provisioning	• Automates roll-out of consistent device configuration and translates into deployment of specific device configuration based on adapted network services • Allows off-the shelf OmniSwitches to be provisioned simply by connecting to the network • Policy-driven provisioning and automation allowing compliance enforcement for provisioning best practices • Lower costs by enabling deployment of new devices in minutes, and without onsite support visits, eliminates repetitive tasks and onsite support visits
IoT visibility	• Know your network with a single pane of glass for Inventory view- from traditional IT managed devices up to hard to detect endpoints • Real-time wired-wireless endpoints inventory with Cloud based device fingerprinting solution for most diversified network environments with advanced contextual information • IoT focus dashboard widgets facilitate the operational management for faster time to decision
Lifecycle management	• Optimal device firmware selection with remote update over the cloud for network element under subscription
Easy wireless configuration with integrated Guest access and BYOD support	• Reduced administration time and effort while providing consistent network experience across LAN and WLAN services • Extensive guest access and BYOD support for on-boarding and management of visitor and employee personal devices • Fully customizable Captive Portal with integrated credentials management for email, sms,social Login (Facebook, Google, WeChat)
Application visibility and control	• Ensure consistent user experience to support all business requirements across the network infrastructure • Control usage on the network of recreational applications • Optimized network application performances for professional applications and network services
Real-time network monitoring	• Network Operating Center (NOC) style topology provides global visibility of all network equipment in a single view with real-time view of devices, clients, alarms and events • Real-time monitoring and analysis of critical network performance indicators through visual widgets

OmniVista Cirrus dashboard



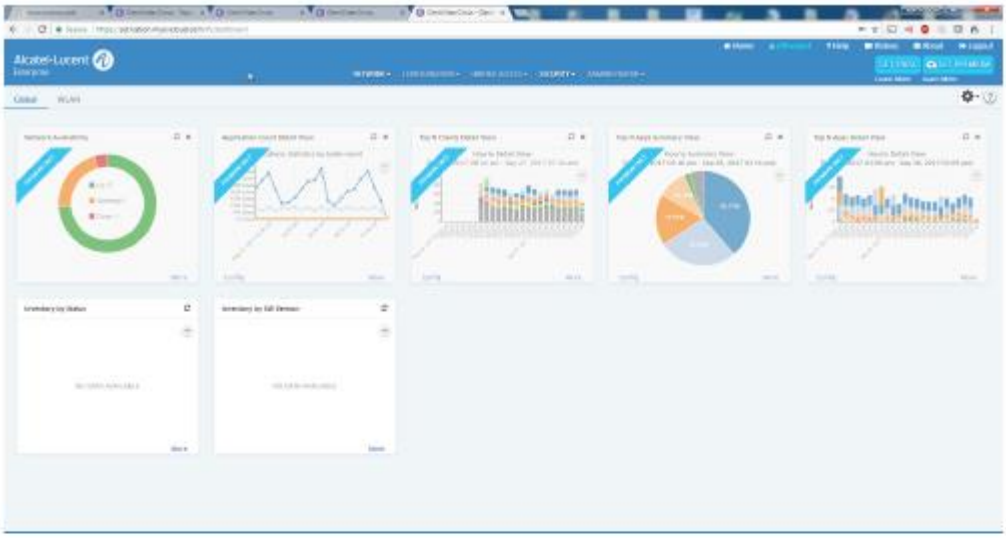
OmniVista Cirrus Dashboard offers Real-time monitoring and analysis of critical network performance indicators through intuitive visual widgets.

OmniVista Cirrus device on-boarding



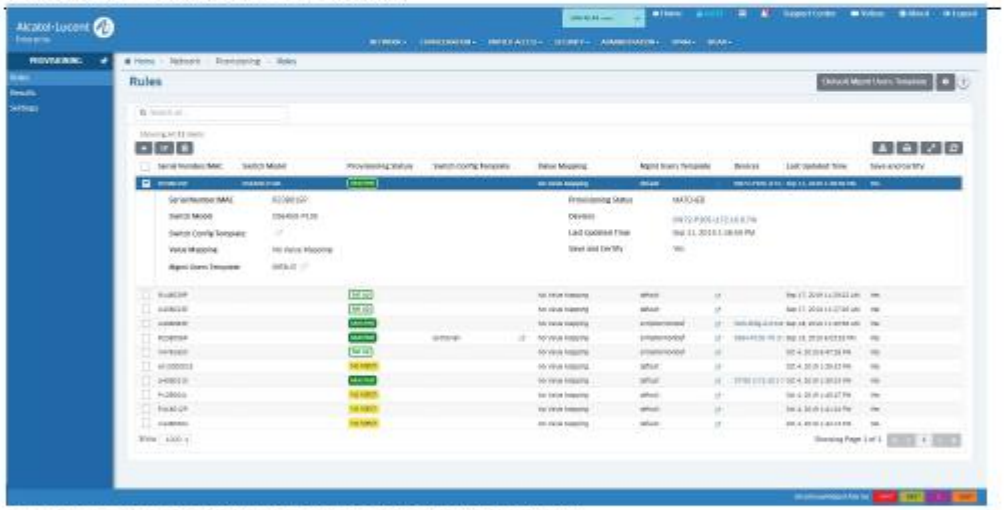
Easy, intuitive registration and activation for Alcatel-Lucent Enterprise portfolio from OmniVista Cirrus device catalog.

OmniVista Cirrus Freemium



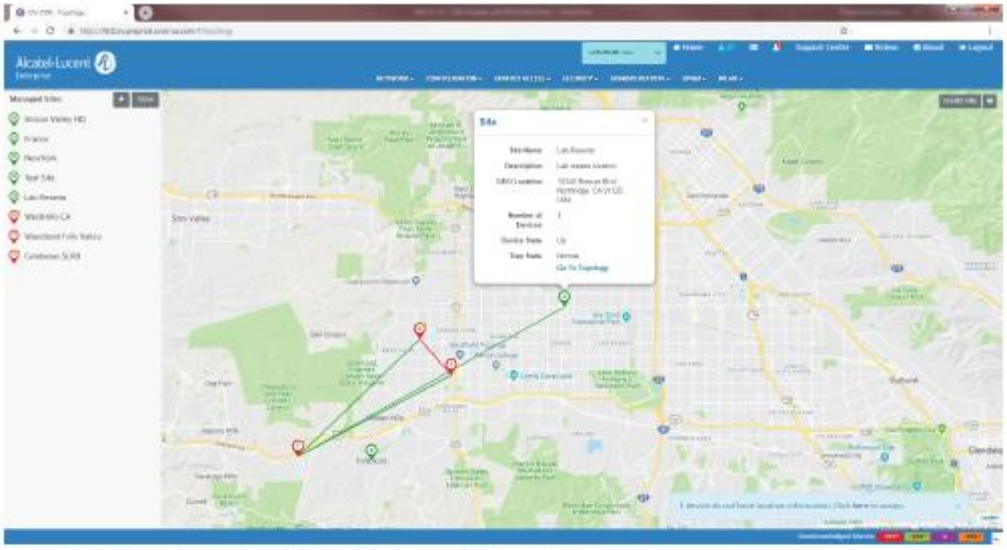
OmniVista Cirrus Freemium mode allows Alcatel-Lucent Enterprise customers easy access to the latest software and firmware versions for their network devices.

OmniVista Cirrus Template Based Provisioning



Policy-driven provisioning and automation reduce cost of new device deployment.

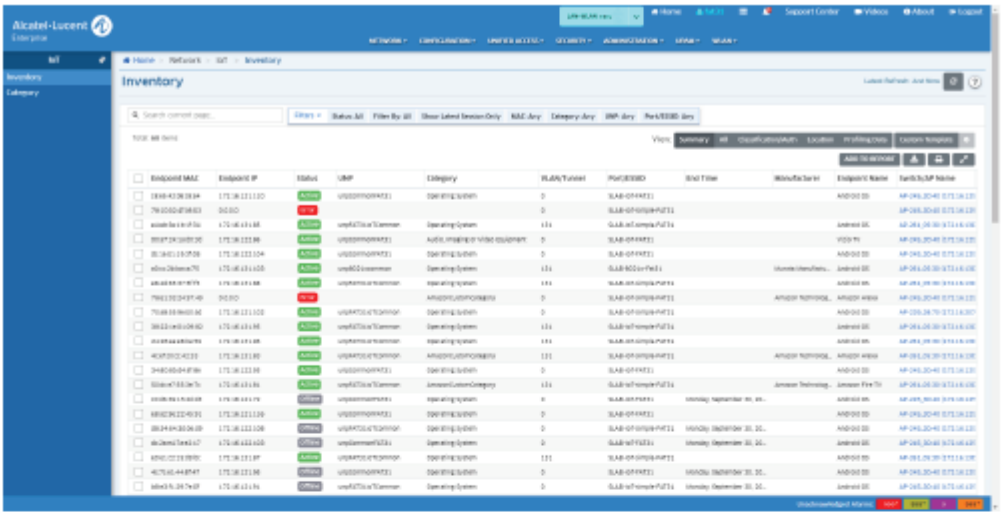
Geo-Location Topology



Geo-location node map shows nodes and device status in geographical context using Google map

OmniVista Cirrus Network Topology

OmniVista Cirrus real-time detailed topology for each tenant across multi-site deployment.



Single Pane of glass for IoT endpoints inventory view

Product specifications

Simplified ordering and activation

- Portal for customer self- registration and subscription activation
- Pay-as-you-go subscription model with flexible duration (1, 3, 5 years) to accommodate business OPEX imperatives
- Flexible Service and Support bundle for device under subscription
- Easy subscription renewal process to avoid service interruption

Simplified deployment

- Network devices automatically connect to OmniVista Cirrus out of the box
- Optimal firmware update for device cloud registration
- Configuration template for devices and Access Points for auto-provisioning
- Template for devices and access points bulk provisioning and configuration modeling

Secure

- No customer data crossing the Internet – only traffic management over encryption
- Layer 2 VPN IPSec encryption and tunneling services between a network device and OmniVista Cirrus
- Administrative management is secured over HTTPS/SSL with different levels of administration
- Role-based administration for mapping network administration credentials to a specific subset of customer organization
- Firewall friendly, eliminating complex local infrastructure changes
- Strong password policy

Multi-tenancy services

- Allow MSPs and large organizations to effectively managed and monitor multiple associated customers, subsidiaries from one Master management account while maintaining separation and good level of security
- User management control for easy control and devices access with role based access profiles
- Advanced Dashboard capabilities for Multi-Tenancy Services including devices inventory, alerts and devices status

Geo-location topology

- Google map integration by displaying devices or network sites by its physical location address or by its GPS coordinates
- Register automatically device GPS coordinates, through OV Cirrus Mobile Assistant application (iOS and Android)
- Display device list, equipment status associated to a geographical site

Network topology

- Detailed discovery of the Alcatel-Lucent Enterprise portfolio with overlay display for wired/ wireless devices and virtual chassis
- Network visualization for logical and physical infrastructure and live device status
- Dynamic, customizable, logical map based on user-defined filters (IP subnet, location, model, user provided descriptive info)
- Hierarchical multi-site topology display
- Wireless heatmap with RF planner

Configuration lifecycle

- Extensive Life cycle operations for device configuration change
- Create infrastructure wide, device software image update for baseline version management
- Configuration life cycle operations (backup & restore) with scheduling and remote reboot
- Optimal device firmware selection reducing IT involvement

Template based Provisioning

- Automatically roll-out consistent provisioning policies and pushed device configuration
- Allows off the-shelf OmniSwitches devices to be provisioned simply by connecting to the network
- Enforce Golden configuration and best practices by monitoring compliance and audit reporting

Unified management

- Single pane of glass management for Alcatel-Lucent Omni Switch® and Stellar Access Points for wireless services provisioning and monitoring
- Centralized role based access policy with built-in authentication policy manager
- Advanced BYOD and guest access mobility features including configuration and monitoring (each Stellar Access Point comes bundled with 50 Guest Access and 50 BYOD licenses allowances)
- Integrated Captive Portal including Social Login Authentication (Facebook™, Google™, Rainbow™)

Dashboard

- Graphical widgets for device status with drill-down capabilities
- Real-time monitoring and analysis of critical network performance indicators through visual widgets
- Full choice of displays, data and other important network and device information with advanced reporting capabilities
- WLAN focus widgets providing extensive view for live reporting on wireless operations (SSID, AP and Clients) and WiFi performances (throughput, band utilization and client health)
- IoT focus widgets helps to visualize real-time and historical graphical views of your endpoints

Network Analytics

- Provides insight in the network health with advanced graphical analytics on most problematic switches based on device state (CPU, memory, temperature)
- Enables automatic generation of business centric, CIO-oriented graphical analytics reports for network

IoT visibility

- IoT inventory assisted with cloud-based Endpoints fingerprinting service gives a full spectrum visibility of all connected devices across the network with complete contextual information
- Contextual information of all connected devices including Key attributes such as device type, vendor, hardware version, network location and time information
- Dashboard IoT with focus Endpoint analytics summary provide real-time and historical summary view of IoT activity for better informed analysis and reporting

Application visibility

- Provides application analytics for network wide application inventory, monitoring and use, allowing a better understanding of bandwidth consumption between business critical and non- professional applications
- Allows centralized policy enforcement and application-use policy by applying QoS policy enforcement such as rate limiting, blocking and application prioritization
- Improves user experience and business outcome with embedded analytics engine, showing in depth application use reports and key measurement indicators

Privacy and regulatory compliance

- OmniVista Cirrus hosted in regional data centers based on customer location
- Compliant with applicable data privacy, security and regulatory framework in US, EU and abroad
- Compliant with General Data Protection Regulation (GDPR)

Technical specifications

OmniVista Cirrus ready network devices

- Alcatel-Lucent OmniSwitch® 6350, OS6450 models with minimum release AOS 6.7.2R03 MR
- Alcatel-Lucent OmniSwitch® OS6465 models with minimum release AOS 8.5R2
- OmniSwitch 6560, OS6860, OS6860-E, OS6865, OS6900 models with minimum release AOS release 8.4.1R03
- Stellar access points AP1101, AP1201, AP1201H, AP1221, AP1222, AP1231, AP1251 models with minimum AWOS release 3.0.7

Minimum browser requirements

- Google Chrome minimum version 63, Mozilla Firefox minimum version 56

Mobile apps

- OmniVista Cirrus Assistant (iOS min 8.0 & Android min 4.2)

Feature comparison

	Freemium	Paid subscription
Customer sign-on through portal	✓	✓
Number of devices supported	Limited to customer device inventory	Based on subscription terms
Duration of service	No limitation	Based on subscription duration (1, 3, 5 years)
Service and Support bundle included with subscription	Only Community Support	Different levels of Service and Support bundle available
Extended software support and device hardware maintenance (AVR)	—	Based on subscribed service and Support level bundle
Functionalities level	Customer device inventory One time device software update	Complete features No restrictions
Guided workflows and simplified network provisioning	—	✓
Advanced monitoring and topology services	—	✓
Unified Access for LAN and WLAN	—	✓
Guest access with Captive Portal and BYOD	—	✓
Smart Analytics and reporting	—	✓
Application visibility Monitoring and enforcement	—	✓

Ordering information

OmniVista Cirrus is available with 3 different Service and Support bundles (Base, Business, Premium)

Base Bundle Includes:

- OmniVista Cirrus Network Administration SaaS for all licensed devices
- Community support access

SKU	Description
OVC-AP-BAS-nY	OmniVista Cirrus – Cloud network administration for one Stellar Access Point model (covers OAW-AP1101, AP1201, AP1201H, AP1221, AP1222, AP1231, AP1232, AP1251 series) for the selected subscription duration (options are one, three or five years). Include Base Service and Support Bundle for the device under subscription.
OVC-ESS-BAS-nY	OmniVista Cirrus – Cloud network administration for one Essential OmniSwitch model (covers OS6350, OS6450, OS6465, OS6560 series) for the selected subscription duration (options are one, three or five years). Include Base Service and Support Bundle for the device under subscription.
OVC-ADV-BAS-nY	OmniVista Cirrus – Cloud network administration for one Advanced OmniSwitch model (covers OS6860, OS6860-E, OS6865 series) for the selected subscription duration (options are one, three or five years). Include Base Service and Support Bundle for the device under subscription.
OVC-CORE-BAS-nY	OmniVista Cirrus - Cloud network administration for one Core OmniSwitch model (covers OS6900 series) for the selected subscription duration (options are one, three or five years). Include Base Service and Support Bundle for the device under subscription.

Replace n with 1,3,5 for duration terms (1, 3, 5 years)

Business Bundle Includes:

- OmniVista Cirrus Network Administration SaaS for all licensed devices
- ALE Business Partner Access to the Global Welcome center for OmniVista Cirrus SaaS Service and support
- Firmware update and upgrade for all licensed devices
- ALE Partner TAC Access for OmniVista Cirrus SaaS and node support assistance

- ALE Partner hardware service (AVR/Advanced replacement) and support for all licensed devices

SKU	Description
OVC-AP-BIZ-nY	OmniVista Cirrus - Cloud network administration for one Stellar Access Point model (covers OAW-AP1101, AP1201, AP1201H, AP1221, AP1222, AP1231, AP1232, AP1251 series) for the selected subscription duration (options are one, three or five years. Include Business Service and Support Bundle for the device under subscription.
OVC-ESS-BIZ-nY	OmniVista Cirrus - Cloud network administration for one Essential OmniSwitch model (covers OS6350, OS6450, OS6465, OS6560 series) for the selected subscription duration (options are one, three or five years). Include Business Service and Support Bundle for the device under subscription.
OVC-ADV-BIZ-nY	OmniVista Cirrus - Cloud network administration for one Advanced OmniSwitch model (covers OS6860, OS6860-E, OS6865 series) for the selected subscription duration (options are one, three or five years). Include Base Service and Support Bundle for the device under subscription.
OVC-CORE-BIZ-nY	OmniVista Cirrus - Cloud network administration for one Core OmniSwitch model (covers OS6900 series) for the selected subscription duration (options are one, three or five years). Include Business Service and Support Bundle for the device under subscription.

Replace n with 1,3,5 for duration terms (1, 3, 5 years)

Premium Bundle Includes:

- OmniVista Cirrus Network Administration SaaS for all licensed devices
- End Customer Access to the Global Welcome center for OmniVista Cirrus SaaS Service and support
- Firmware update and upgrade for all licensed devices
- End-user support access for OmniVista Cirrus SaaS and node support assistance
- End-user hardware service (AVR/Advanced replacement) and support for all licensed devices

SKU	Description
OVC-AP-nY	OmniVista Cirrus - Cloud network administration for one Stellar access point model (covers OAW-AP1101, AP1201, AP1201H, AP1221, AP1222, AP1231, AP1232, AP1251 series) for the selected subscription duration (options are one, three or five years). Include Premium Service and Support Bundle for the device under subscription.
OVC-ESSENT-nY	OmniVista Cirrus - Cloud network administration for one Essential OmniSwitch model (covers OS6350, OS6450, OS6465, OS6560 series) for the selected subscription duration (options are one, three or five years). Include Premium Service and Support Bundle for the device under subscription.
OVC-ADV-nY	OmniVista Cirrus - Cloud network administration for one Advanced OmniSwitch model (covers OS6860, OS6860-E, OS6865 series) for the selected subscription duration (options are one, three or five years). Include Premium Service and Support Bundle for the device under subscription.
OVC-CORE-nY	OmniVista Cirrus - Cloud network administration for one Core OmniSwitch model (covers OS6900 series) for the selected subscription duration (options are one, three or five years). Include Premium Service and Support Bundle for the device under subscription.

Replace n with 1,3,5 for duration terms (1, 3, 5 years)

Visit ALE OmniVista Cirrus.

Alcatel·Lucent Enterprise