ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

TEMA: ESTUDIO PARA LA IMPLEMENTACIÓN DE REDES DINÁMICAS APLICADAS EN LA RED DE DATOS DE PETROECUADOR, CASO DE ESTUDIO EDIFICIO ALPALLANA

AUTOR: RIVADENEYRA JARAMILLO, TEODORO ENRIQUE

DIRECTOR: ING. MALDONADO STALIN

CO-DIRECTOR: ING. TORRES JÓSE LUIS

SANGOLQUÍ, Junio de 2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

CERTIFICADO

Ing. Stalin Maldonado

Ing. José Luis Torres

CERTIFICAN

Que el trabajo titulado "ESTUDIO PARA LA IMPLEMENTACIÓN DE REDES DINÁMICAS APLICADAS EN LA RED DE DATOS DE PETROECUADOR, CASO DE ESTUDIO EDIFICIO ALPALLANA.", realizado por el Sr. Teodoro Enrique Rivadeneyra Jaramillo, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas por la Universidad de las Fuerzas Armadas – ESPE.

El mencionado trabajo consta de un documento empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (PDF). Se autoriza al Sr. Teodoro Enrique Rivadeneyra Jaramillo, que el material se entregue al Ing. Mauricio Campaña, en su calidad de Director de la Carrera.

Sangolquí, 16 de Junio del 2015.

ING.STALIN MALDONADO
DIRECTOR DE TESIS

ING. JOSÉ LUIS TORRES
CODIRECTOR DE TESIS

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

DECLARACIÓN DE RESPONSABILIDAD

Yo, Teodoro Enrique Rivadeneyra Jaramillo

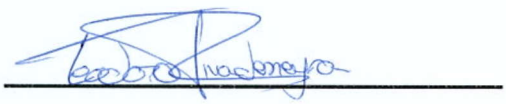
DECLARO QUE:

El proyecto de grado denominado "ESTUDIO PARA LA IMPLEMENTACIÓN DE REDES DINÁMICAS APLICADAS EN LA RED DE DATOS DE PETROECUADOR, CASO DE ESTUDIO EDIFICIO ALPALLANA.", ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan en la bibliografía

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 16 de Junio del 2015



Teodoro Enrique Rivadeneyra Jaramillo

C.C: 1710180322

AUTORIZACIÓN DE PUBLICACIÓN

Yo, Teodoro Enrique Rivadeneyra Jaramillo, autorizo a las Universidad de las Fuerzas Armadas – ESPE la publicación, en la biblioteca virtual de la institución, del trabajo "ESTUDIO PARA LA IMPLEMENTACIÓN DE REDES DINÁMICAS APLICADAS EN LA RED DE DATOS DE PETROECUADOR, CASO DE ESTUDIO EDIFICIO ALPALLANA.", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 16 de Junio del 2015

Teodoro Enrique Rivadeneyra Jaramillo

C.C: 1710180322

DEDICATORIA

Este proyecto va dedicado a cada persona que directa e indirectamente han sido de un gran apoyo. Al Ing. Mauricio Campaña que siempre me ha extendido una mano y ha sido indispensable con su colaboración para la culminación de este proyecto. A mi Esposa Cristina López Brito quien con su amor me apoyado para que todo esto sea posible.

AGRADECIMIENTOS

Agradezco a mis padres por el incondicional apoyo y comprensión brindada durante esta etapa de mi vida se ha hecho todo posible. A los ingenieros Stalin Maldonado y José Luis Torres por haberme guiado en la realización de este proyecto, ofreciéndome su conocimiento, ayuda y sobre todo tiempo. A todos nuestros amigos de carrera con quienes compartimos y disfrutamos ésta importante etapa de nuestras vidas.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Las oficinas de PetroEcuador que funcionan en el edificio Alpallana, presentan un gran inconveniente al momento de realizar mantenimiento o cambio de un conmutador, puesto que no se cuenta con equipos configurados genéricamente, y en cada piso del edificio se manejan diferentes segmentaciones de redes (VLAN). Adicionalmente, se tiene problemas con la movilidad de los equipos móviles, como son Laptops, Celulares y Tablets, porque los equipos de conectividad inalámbrica (Access Point) se encuentran únicamente en ciertos lugares y pisos del edificio. Con el objetivo de dar solución a estos inconvenientes la Institución se ve en la necesidad de realizar un "Estudio para la segmentación de red, enfocado a las VLAN's Dinámicas en la red de datos de PetroEcuador". Esto permitirá, analizar a través de la METODOLOGÍA ELABORADA POR JAMES McCABE, la búsqueda de la mejor solución, misma que a través de la asignación de las DVLAN's permitirá tener conmutadores configurados genéricamente, lo que mejora los tiempos de cambio.

Palabras Claves:

- **DVLAN**
- **Conmutador**
- **VLAN**
- **MAC**

ABSTRACT

PetroEcuador´s offices that work in Alpallana building have a major drawback when performing maintenance or changing switches, given that they do not have generically configured computers, and in each floor of the building, different network segmentations (VLAN) are handled. Additionally, they have mobility problems with mobile equipment as Laptops, Cellphones and Tablets, because wireless connectivity equipment (Access Point) are found only in certain places and floors of the building. In order to solve these problems the Institution needs to perform a “Study for network segmentation, focusing on Dynamic VLAN’s in PetroEcuador’s data network”. This will allow analysis by Top-Down Network Design methodology, the search of the best solution, which through DVLAN’s assignment, allows to have generically configured switches, this will improve change time.

Keywords:

- **DVLAN**
- **SWITCH**
- **VLAN**
- **MAC**

CAPÍTULO 1: Introducción

1.1 Título

Estudio para la implementación de redes dinámicas aplicadas en la red de datos de PETROECUADOR, caso de estudio en el edificio ALPALLANA.

1.2 Definición

PETROECUADOR se ha obligado a mejorar drásticamente las seguridades a nivel de redes de datos, por tal motivo, la Institución se encuentra en una etapa de elaboración de un proyecto de seguridad informática a gran escala.

Como parte del proyecto se realizará la implementación de VLAN's dinámicas, las cuales permitirán optimizar recursos humanos y técnicos, en actividades como: reubicación de equipos networking, mantenimiento preventivo, rectificativo y reemplazo de equipos. La implementación de VLAN's dinámicas permitirá tener un control a nivel de usuarios restringiendo acceso a información confidencial de la Institución.

Para ofrecer una mayor movilidad a usuarios se optimizará la red inalámbrica existente con la finalidad de tener mayor control sobre estos, quienes seguirán trabajando transparentemente bajo el sistema de VLAN's dinámicas. Con los avances tecnológicos, en la actualidad se encuentran una variedad de equipos de interconexión inalámbrica (Access Point) que poseen mayor amplitud de onda, que permitirán trasladarse a usuarios de una ubicación física dentro del edificio ALPALLANA a otra ubicación dentro del mismo edificio, sin perder la conectividad con los sistemas informáticos de la Institución.

1.3 Planteamiento del Problema

Las oficinas de PETROECUADOR se encuentran en el edificio ALPALLANA, en el cual existe una red de datos, la misma que en la actualidad funciona bajo la modalidad de VLAN's estáticas, esto ha producido inconvenientes al momento de realizar reubicaciones de usuarios debido a que la red de datos se encuentra segmentada por departamentos, los cuales se encuentran configurando permisos a la red, produciendo la necesidad de comunicarse con el departamento de sistemas para la configuración adecuada del nuevo segmento de red.

La red de datos inalámbrica actual está configurada de tal manera que el usuario al momento de trasladarse físicamente de un piso a otro del edificio ALPALLANA, pierde la conectividad con los sistemas informáticos.

Se ha detectado que usuarios externos pueden ingresar a la red de datos de la Institución accediendo a información confidencial.

1.4 Justificación e Importancia

La importancia de mejorar los niveles de seguridad y minimizar la administración de recursos informáticos a través de redes dinámicas, se solventarán los problemas que actualmente se presentan en la Institución.

Minimizando la administración se permitirá que cualquier persona del departamento técnico pueda realizar cambios de acuerdo a las necesidades presentadas, eliminando la centralización de la administración en una sola persona.

Con el estudio de éste proyecto se ayudara a la Institución, a conseguir mejor rendimiento, confiabilidad, administración en cualquier circunstancia presentada dentro de PETROECUADOR.

1.5 Objetivos

1.5.1 Objetivo General

- Realizar el estudio de la segmentación de red, enfocado a las VLAN's Dinámicas en la red de datos de PETROECUADOR, caso de estudio en el edificio ALPALLANA.

1.5.2 Objetivos Específicos

- Realizar el levantamiento de la información de la infraestructura física y lógica de la red actual.

- Analizar las variables necesarias para recomendar la implementación de las VLAN's Dinámicas.

- Realizar una propuesta de estudio en el edificio ALPALLANA, utilizando Segmentación Dinámica de la red.

1.6 Alcance

Se realizará la investigación de la tecnología con el fin de proveer una guía práctica para su análisis y/o futura implementación de redes dinámicas. Se podrá crear VLAN's dinámicas con el objetivo de los usuarios absorban permisos y privilegios independientemente del segmento.

El implementar un equipo centralizado para la administración de equipos de networking, como por ejemplo Access Point, permitirá que los usuarios obtengan conectividad aunque exista un usuario móvil.

Se mejorarán los niveles de seguridad en la red de datos, debido a que los equipos externos de la Institución serán asignados con niveles de privilegios netamente limitados para obtener acceso al servicio de internet.

El proyecto tiene como objetivo ofrecer mayores beneficios y ventajas en movilidad y en el uso de redes inalámbricas, las que existen no cumplen las necesidades de cobertura, ni las necesidades del personal que labora en el edificio ALPALLANA.

Se detallan algunos puntos importantes en la elaboración de este proyecto:

- Ofrecer mayor agilidad para los usuarios móviles dentro de la Institución.
- Mejorar la seguridad a nivel de acceso por medio de la creación de VLAN's Dinámicas.

CAPÍTULO 2: Marco Teórico

2.1 Introducción de VLAN's

Una VLAN (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.

Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas y limitaciones de dirección), ya que se define una segmentación lógica basada en el agrupamiento de equipos según determinados criterios (direcciones MAC, números de puertos y protocolo). [1]

2.2 DVLAN (VLAN's Dinámicas)

Las VLAN's dinámicas son puertos del conmutador que automáticamente determinan a que VLAN pertenece a cada puesto de trabajo. El funcionamiento de estas VLAN's se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados. Cuando un puesto de trabajo pide autorización para conectarse a la VLAN, el conmutador chequea la dirección MAC ingresada previamente por el administrador en la base de datos de las mismas y automáticamente se configura el puerto al cual corresponde por la configuración de la VLAN. El mayor beneficio de las DVLAN's es el menor trabajo de administración dentro del armario de comunicaciones, cuando se cambian de lugar las estaciones de trabajo o se agregan, y también la notificación centralizada cuando un usuario desconocido pretende ingresar en la red.

En la siguiente Tabla 2.1 se presenta un ejemplo práctico de algunas máquinas de la unidad de sistemas, de cómo se generan las tablas MAC para la asignación de las DVLAN's.

Tabla 2.1.

Ejemplo real de asignación de DVLAN

MAC	VLAN
00-0B-CD-26-D7-31	10
00-0E-7F-64-A6-F2	10
00-11-OA-96-EB-87	10
00-1C-C4-A0-AE-D8	19
00-11-0A-3F-36-22	28

2.3 Ventajas y Desventajas de las DVLAN

Ventajas:

- Facilidad de movimiento: En caso de que una terminal de trabajo cambie de lugar la reconfiguración del switch.
- Multiprotocolo.
- Se pueden tener varios miembros en múltiples VLAN's.

Desventajas:

- Problemas de rendimiento y control de Broadcast: el tráfico de paquetes de tipo Multicast y Broadcast se propagan por todas las VLAN's.

- Complejidad en la administración: En un principio para todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo.

2.4 Equipos y características del funcionamiento técnico

2.4.1 Equipos:

- **Servidor TFTP:** Almacena la base de datos (archivo plano) que contiene información necesaria para la asignación dinámica de VLAN's. Ésta base es leída por el conmutador central.
- **Conmutador central:** Aquí se encuentra configurado el servidor VMPS que es el encargado de realizar la asignación dinámica de VLAN's.
- **Servidor VMPS (VLAN Membership Policy Server):** Permite asignar a un puerto una VLAN en forma dinámica, basándose en la dirección MAC de los hosts junto con la VLAN asociada perteneciente a dicha dirección MAC, de esta forma se obtiene un mapa de direcciones VLAN-MAC.

2.4.2 Funcionamiento:

Para que se asigne dinámicamente una VLAN a un host, éste se conecta a la red y ejecuta los siguientes pasos:

- Envía un DHCP request (petición al servidor DHCP) para obtener una dirección IP.
- La dirección MAC del host es enviada al conmutador de acceso.
- El conmutador de acceso envía la dirección MAC al conmutador central.
- El conmutador central ubica la dirección MAC en su bases de datos y determina a que VLAN pertenece dicha dirección MAC.
- Finalmente, el identificador de la VLAN es enviado al conmutador de acceso para que se configure el puerto con la VLAN correspondiente.

- Luego de eso el tráfico de la red continua, permitiendo que se complete la petición al servidor DHCP.
- En el caso que una dirección MAC no se encuentre registrada, se le asigna una VLAN por defecto o de invitado, para que tenga acceso limitado a dicha red.[2]

2.5 Introducción a las redes inalámbricas

2.5.1 Características:

De acuerdo al rango de frecuencias utilizado para transmitir, el medio de transmisión pueden ser ondas de radio, microondas terrestres o por satélite, por ejemplo los infrarrojos. Dependiendo del medio, la red inalámbrica tendrá unas características u otras:

- **Ondas de radio:** Las ondas electromagnéticas son omnidireccionales, así que no son necesarias las antenas parabólicas. La transmisión no es sensible a las atenuaciones producidas por la lluvia ya que se opera en frecuencias no demasiado elevadas. En este rango se encuentran las bandas desde la ELF que va de 3 a 30 Hz, hasta la banda UHF que va de 300 a 3000 MHz, es decir, comprende el espectro radioeléctrico de 30 - 3000000 Hz.

- **Microondas terrestres:** Se utilizan antenas parabólicas con un diámetro aproximado de tres metros. Tienen una cobertura de kilómetros, pero con el inconveniente de que el emisor y el receptor deben estar perfectamente alineados. Por eso, se acostumbran a utilizar en enlaces punto a punto en distancias cortas. En este caso, la atenuación producida por la lluvia es más importante ya que se opera a una frecuencia más elevada. Las microondas comprenden las frecuencias desde 1 hasta 300 GHz.

- **Microondas por satélite:** Se hacen enlaces entre dos o más estaciones terrestres que se denominan estaciones base. El satélite recibe la señal (denominada señal ascendente) en una banda de frecuencia, la amplifica y la retransmite en otra banda (señal descendente). Cada satélite opera en unas bandas concretas. Las fronteras frecuenciales de las microondas, tanto terrestres como por satélite, con los infrarrojos y las ondas de radio de alta frecuencia, se mezclan, así que pueden existir interferencias con las comunicaciones en determinadas frecuencias.

- **Infrarrojos:** Se enlazan transmisores y receptores que modulan la luz infrarroja no coherente. Deben estar alineados directamente o con una reflexión en una superficie. No pueden atravesar las paredes. Los infrarrojos van desde 300 GHz hasta 384 THz.[3]

2.5.2 Tipos

Según su cobertura como se presenta en la figura 2.1, se pueden clasificar en diferentes tipos:

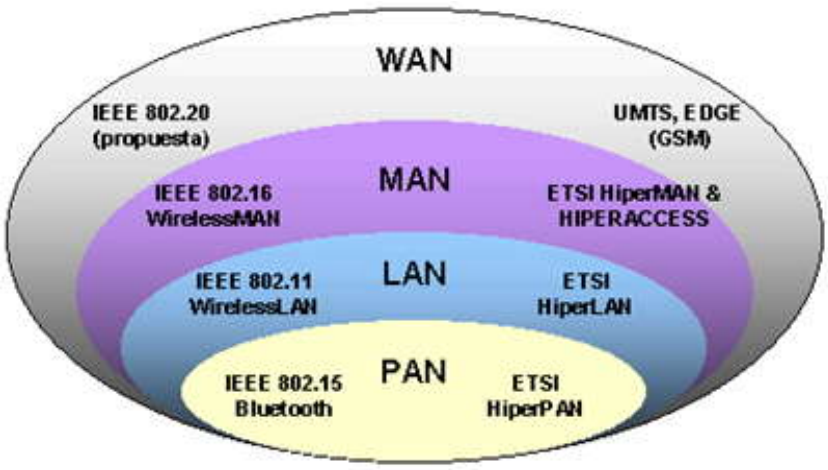


Figura 2.1. Posicionamiento Estándares Wireless. [3]

2.5.2.1 WPAN (Wireless Personal Area Network)

En este tipo de red de cobertura personal, existen tecnologías basadas en HomeRF (estándar para conectar todos los teléfonos móviles de la casa y los ordenadores mediante un aparato central); Bluetooth, ZigBeeque siguen el estándar IEEE 802.11 con diferentes variantes y utilizado en aplicaciones como la domótica, que requieren comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías, bajo consumo); RFID (sistema remoto de almacenamiento y recuperación de datos) con el propósito de transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.

2.5.2.2 WLAN (Wireless Local Area Network)

En las redes de área local se puede encontrar tecnologías inalámbricas basadas en HiperLAN (High Performance Radio LAN), un estándar del grupo ETSI, o tecnologías basadas en Wi-Fi, que siguen el estándar IEEE 802.11 con diferentes variantes.

2.5.2.3 WMAN (Wireless Metropolitan Area Network, Wireless MAN)

Para redes de área metropolitana se encuentran tecnologías basadas en WiMax (World wide Interoperability for Microwave Access, es decir, Interoperabilidad Mundial para Acceso con Microondas), un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. WiMax es un protocolo parecido a Wi-Fi, pero con más cobertura y ancho de banda. También se puede encontrar otros sistemas de comunicación como LMDS (Local Multipoint Distribution Service).

2.5.2.4 WWAN (Wireless Wide Area Network, Wireless WAN)

En estas redes se encuentra tecnologías como UMTS (Universal Mobile Telecommunications System), utilizada con los teléfonos móviles de tercera

generación (3G) y sucesora de la tecnología GSM (para móviles 2G), o también la tecnología digital para móviles GPRS (General Packet Radio Service).[4]

2.6 Definición de Wi-Fi

Wi-Fi es un sistema de envío de datos sobre redes computacionales que utiliza ondas de radio en lugar de cables. Wi-Fi es una marca de la Wi-Fi Alliance (anteriormente la WECA: Wireless Ethernet Compatibility Alliance), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11g.

Existen accesorios que pueden encontrarse en varios formatos como se observa en la figura 2.2, las tarjetas PCMCIA (para portátil), PCI y USB (para ordenador de sobremesa) y esperar que muy pronto en formato SD (Secure Digital) para nuestros PDAs Palm OS.

Figura 2.2. Tipos de dispositivos Wi-Fi.

El protocolo 802.11g implementa encriptación WEP, pero no se puede mantener WEP como única estrategia de seguridad ya que no es completamente segura. Existen aplicaciones para Linux y Windows (como AiroPeek, AirSnort, AirMagnet o WEPCrack) que, escaneando el suficiente número de paquetes de información de una red Wi-Fi, son capaces de obtener las claves WEP utilizadas y permitir el acceso de intrusos a la red de datos.

2.6.1 Características:

El alcance de la señal de nuestra red Wi-Fi dependerá de:

- La potencia del Punto de Acceso.
- La potencia del accesorio o dispositivo Wi-Fi por el que se conecta.
- Los obstáculos que la señal tenga que atravesar (muros o metal).
- Cuanto más lejos (linealmente) se quiera llegar, más alto se deberá colocar el Punto de Acceso. Muchos de los actuales APs vienen preparados para poderlos colgar en la pared.
- Si se desea llegar lejos, evite también interferencias como microondas o teléfonos inalámbricos.
- Si la señal llega debilitada, utilice un amplificador de señal o si es posible, monte una nueva antena de más potencia al AP (los Puntos de Acceso de gama baja NO lo permiten) o una antena exterior al accesorio (normalmente solo para formatos PCMCIA o PCI). [5]

2.6.2 Ventajas y desventajas

Las redes inalámbricas (Wireless Network) son aquellas que se comunican por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas. La transmisión y la recepción se realizan a través de antenas.

Ventajas de las redes inalámbricas:

- Instalación simple.
- Robusta y confiable.
- Escalabilidad.
- Facilidad de uso.
- Servidor web para una administración más fácil.

Desventajas de las redes inalámbricas:

- Interferencias.
- Velocidad.
- Seguridad. [6]

2.7 Definición de Access Point

Un punto de acceso inalámbrico (WAP o AP Wireless Access Point) en redes de computadores, es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. Muchos WAP pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dan servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta cientos. Este o su antena son normalmente colocados en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena inalámbrica y existen varios tipos como se observa en la figura 2.3. [7]

Figura 2.3. Tipos de Access Point.

2.7.1 Ejemplos de antenas de puntos de acceso

Rubber Duck

El “RubberDuck”, antena dipolo, tiene un dipolo suministrado con algunos puntos de acceso Aironet de Cisco y otros dispositivos.

- Esta antena es más estética que el mástil de la versión de montaje.
- Esta antena es solo para aplicaciones en interiores y se debe montar con el fin de taladros apuntando hacia el techo.
- Esta antena es de polarización vertical pero tiene una viga inclinada hacia abajo.

Figura 2.4. Antena Rubber Duck.

Diversity omni-directional ceiling mount

La antena de techo omnidireccional diversa es una excelente compañera para un punto de acceso de apoyo. Fue diseñada para interactuar con los puntos de acceso remotos, lo que maximiza la flexibilidad de instalación. Esta antena aprovecha al máximo la funcionabilidad de la diversidad integrada a los puntos de acceso Aironet, mejorando el rendimiento y la gama.

La antena es de polarización vertical, pero tiene una viga inclinada ligeramente hacia abajo permitiendo que su patrón de cobertura, pueda cubrir las áreas por debajo del techo.

- Ideal para múltiples instalaciones.
- Más estético que El “RubberDuck”.
- Asegura una fácil instalación.

Figura 2.5. Antena Diversity omni-directional ceiling mount.

Diversity patchwall mount

Esta antena es excelente para apoyar un punto de acceso diverso. Fue diseñada para interactuar con los puntos de acceso remotos lo que maximiza la flexibilidad de instalación. Esta antena aprovecha al máximo la funcionalidad de la diversidad integrada en los puntos de acceso Aironet, mejorando el rendimiento y la gama. Proporciona un patrón de cobertura hemisférica y es ideal para montar en las paredes. Cuenta con las siguientes características:

- Cuenta con 2 antenas en un paquete para la diversidad espacial.
- Aplicaciones de exterior/interior.
- Ideal para múltiples instalaciones.
- Más estético que El “RubberDuck”.
- Asegura fácil instalación. [8]

Figura 2.6. Antena Diversity patch wall mount.

2.8 Conmutador:

La potencialidad de un conmutador es su capacidad para filtrar cierto tipo de tráfico a través de la MAC, soportar telefonía IP, permitir administración remota, monitoreo en detalle por cada puerta y medidas de seguridad que permitan rechazar tráfico malicioso.

En cuanto al rendimiento o capacidad de tráfico de un conmutador dependerá de si se trata de un conmutador de acceso (punto de entrada para conectar los computadores de los usuarios) que requiere un rendimiento bajo de distribución o departamentales (que interconectan a varios conmutadores de Acceso).

El conmutador de núcleo debe registrar un altísimo rendimiento y baja tasa de pérdida de información (1%) ya que están a cargo de intercambiar información entre todos los conmutadores de distribución o entre los edificios y departamentos de una empresa. Deberían soportar 30Gbps de tráfico total como base. [9]

2.8.1 El modelo jerárquico de 3 capas

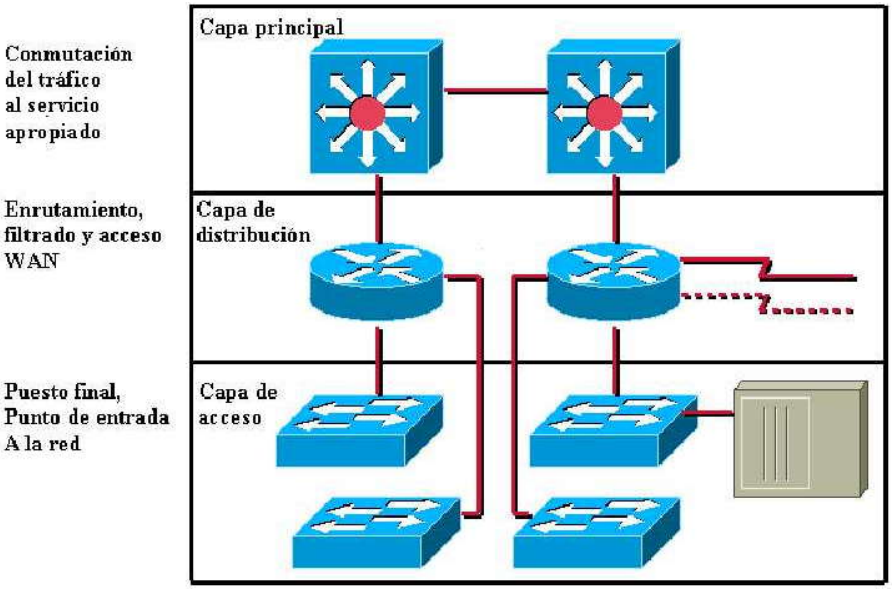


Figura 2.7. Modelo jerárquico de tres capas.

2.8.1.1 Capa de Acceso

La capa de acceso de la red es el punto en el que cada usuario se conecta a la red. Ésta es la razón por la cual la capa de acceso se denomina a veces capa de puesto de trabajo. Los usuarios, así como los recursos a los que estos necesitan acceder con más frecuencia, están disponibles a nivel local. El tráfico hacia y desde recursos locales está confinado entre los recursos, conmutadores y usuarios finales. En muchas redes no es posible proporcionar a los usuarios un acceso local a todos los servicios, como archivos de bases de datos, almacenamiento

centralizado o acceso telefónico a la web. En estos casos, el tráfico de usuarios que demandan estos servicios se desvía a la siguiente capa del modelo: la capa de distribución.

2.8.1.2 Capa de Distribución

La capa de distribución de la red (denominada a veces de grupo de trabajo) marca el punto medio entre la capa de acceso y los servicios principales de la red. La función primordial de esta capa es realizar funciones tales como enrutamiento, filtrado y acceso a WAN. En un entorno de campus, la capa de distribución abarca una gran diversidad de funciones, entre las que figuran las siguientes:

- Servir como punto de acumulación para acceder a los dispositivos de capa.
- Enrutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo.
- Segmentar la red en múltiples dominios de difusión / multidifusión.
- Traducir los diálogos entre diferentes tipos de medios, como Token Ring y Ethernet.
- Proporcionar servicios de seguridad y filtrado.

La capa de distribución puede resumirse como la capa que proporciona una conectividad basada en una determinada política, dado que determina cuándo y cómo los paquetes pueden acceder a los servicios principales de la red. La capa de distribución determina la forma más rápida para que la petición de un usuario (como un acceso al servidor de archivos) pueda ser remitida al servidor. Una vez que la capa de distribución ha elegido la ruta, envía la petición a la capa del núcleo principal. La capa principal podrá entonces traspasar rápidamente la petición al servicio apropiado.

2.8.1.3 Capa de Núcleo Principal

La capa del núcleo principal (también llamada capa backbone), se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados. Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios. Estos servicios se conocen como servicios globales o corporativos. Algunos de tales servicios pueden ser e-mail, acceso a Internet o videoconferencia.

Cuando un usuario necesita acceder a un servicio corporativo, la petición se procesa al nivel de la capa de distribución. El dispositivo de la capa de distribución envía la petición del usuario al núcleo. Este se limita a proporcionar un transporte rápido hasta el servicio corporativo solicitado. El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado al núcleo. [10]

2.9 Control inalámbrico:

LAN inalámbrica (WLAN), los controladores deben simplificar el despliegue y el funcionamiento de las redes inalámbricas, ayudan a garantizar su buen rendimiento, seguridad mejorada, y la máxima disponibilidad de la red.

Los controladores de WLAN se comunican con los puntos de acceso sobre cualquier Capa 2 o Capa 3 de infraestructura. Apoyan el sistema de funciones que incluyen:

- Aumento de la seguridad de WLAN con la política de seguimiento y detección de intrusos.
- Inteligencia de radiofrecuencia (RF) de gestión.
- Administración centralizada.

- Calidad de servicio (QoS).

- La movilidad de servicios, tales como el acceso de invitados, voz IP sobre Wi-Fi, y servicios de localización.

- En servicios de voz y datos, para el seguimiento de la ubicación, los controladores de WLAN de Cisco proporcionan el control, escalabilidad, seguridad y confiabilidad que usted necesita para construir altamente segura la empresa, a escala de redes inalámbricas. [11]

2.9.1 Características de los Equipos

Se van a presentar las diferentes características de los equipos que se necesita adquirir en la empresa para la implementación de este proyecto, como se trata de una empresa del estado, se tiene que entrar en concurso para la adquisición en el portal de compras públicas, por ese motivo se presentan algunas marcas.

2.9.1.1 Control inalámbrico

¿Qué pasaría si sus empleados pudieran trabajar en cualquier lugar: salas de conferencias, muelles de carga o incluso pasillos?

Con un controlador LAN Controller y los puntos de acceso se puede configurar una red inalámbrica que proporcione a los empleados la flexibilidad que desean y necesitan para trabajar de forma más eficaz y segura.

ESPACIO EN BLANCO
INTENCIONAL

Wireless Controller Cisco

Figura 2.8. WirelessController Cisco.

Un controlador Cisco 2100 Series Wireless LAN Controller admite:

- **Conexión inalámbrica:** Con los dispositivos inalámbricos como teléfonos IP, portátiles y teléfonos, los empleados se pueden comunicar y colaborar desde cualquier lugar.

- **Amplia cobertura:** Con un soporte de hasta seis puntos de acceso, los empleados no están fuera de alcance ni desconectados.

- **Seguridad:** La capacidad de soportar la mayoría de los estándares de seguridad significa que sus datos están siempre protegidos.

- **Integración:** Como parte de las soluciones de redes inalámbricas unificadas de Cisco, se integra perfectamente con productos de administración inalámbrica, puntos de acceso, puentes inalámbricos y supervisión de Cisco.

Características:

Cisco Wireless LAN Controllers Serie 2100 ofrecen una amplia gama de características, que incluye:

- Soporte para múltiples combinaciones de puntos de acceso y enlaces redundantes.
- Seguridad estándar, autenticación de identificación y protocolos de cifrado para obtener unos niveles de protección óptimos.

- Acceso de invitado seguro.

- Voz a través de WLAN.

- Integración con Cisco Control inalámbrico System para una configuración y monitorización de la red de área local inalámbrica completa.

- Cómodo montaje en escritorio o en rack, gracias a su pequeño tamaño [12].

Tabla 2.2.

Equipo Cisco 2106.

Modelo	Ventajas clave
Cisco 2106 Series Wireless LAN Controller 	• Admite varias combinaciones de puntos de acceso y conexiones de red. • Proporciona una configuración, administración y control de políticas de AP centralizada. • Plataforma para servicios de movilidad avanzados como acceso de invitado seguro, voz a través de WLAN, seguridad ampliada. • Integrado con Cisco Unified Wireless Network y el sistema de control inalámbrico.

[13]

Tabla 2.3

Equipo Cisco wireless Express 526.

Modelo	Ventaja clave
Cisco Wireless Express 526 Mobility Controller 	• Admite hasta 12 puntos de acceso de Wireless Express. • Proporciona una configuración, administración y control de políticas de AP centralizada. • Plataforma para servicios de movilidad avanzados como acceso de invitado seguro, voz a través de WLAN. • Solución rentable. • Cómodo montaje en escritorio o en la parte superior de los estantes. • Integrado con Cisco Smart Business Communications System y Cisco Configuration Assistant • 3Com® Wireless LAN Controller WX2200

[14]

HP WX5000 Access *Controller*

Figura 2.9. Wireless Controller HP.

Tabla 2.4

Equipo HP WX5000.

Característica	Descripción
Movilidad de arquitectura	
Red y la movilidad de los dominios	Grupos de 3Com wireless, información del usuario y los controladores de compartir la autorización a que los usuarios se desplazan, apoyo a la movilidad sin interrupciones y aplicación de la seguridad a través de la red inalámbrica.
Reenvío distribuido	Optimizar el flujo de tráfico, reducir la latencia y mejorar el rendimiento.
Topología de la independencia	Al proporcionar una capa de 2 ruta de tráfico de Capa 3, controladores inalámbricos 3Com, conmutadores y MAPs operaran como una infraestructura integrada dividida en dispositivos L2/L3 incluso en redes distribuidas remotas, lo que facilita la expansión o modificación de la WLAN,
Roaming rápido	Traspaso rápido de la información del usuario y las autorizaciones en la Red y dominio de movilidad, permite a un sistema de roaming con la integridad de sesión y una movilidad lo suficientemente robusta como para soportar tráfico de voz.
Múltiples colas por usuario	Basada en la clase de colas de tráfico en el MAP ayuda a garantizar que la voz y otras aplicaciones en tiempo real de recibir la clase de servicio y calidad de servicio que necesitan en la WLAN.
Pay-as-a-crecer escalabilidad	A medida que la red de clientes crece y mayor rendimiento se necesita, los clientes sólo para la actual Wireless LAN Access Controller MAP (o FIT AP) Actualización de licencias (LIS-WX-32 o LIS-WX-128).
Encriptación	
Encriptación de clase empresarial	WPA2, AES, TKIP y WEP a cabo en la ayuda MAPA protege y asegura a todas las comunicaciones.
Cifrado por usuario de asignación	Diferentes políticas de seguridad se aplican en un esquema por usuario o por grupo base para el control de seguridad flexible y en profundidad y de gestión.
Seguridad AAA	
Local o el servidor RADIUS de autenticación IEEE 802.1X	Control de autenticación y gestión centralizada de todos los usuarios de la red ayuda a garantizar que sólo los usuarios autorizados acceden a la red.
Apoyo virtual grupo privado	El personal de TI puede asignar políticas que controlan por usuario o por grupo de acceso de red a través de la red WLAN para una itinerancia segura y sin problemas y para mantener el tráfico de usuario separado y seguro.
Movilidad perfil	El personal de TI de forma dinámica se puede aplicar permisos de acceso basado en los atributos devueltos por el servidor AAA donde indica que MAP o puertos LAN de autenticación de un usuario o grupo puede usar.

Continua ⟶

La integración y la descarga de RADIUS AAA	Controladores de acceso inalámbrico puede asumir back-end de cifrado de clave tareas de generación y la autenticación, la reducción de la carga de procesamiento y el aumento de la escala y la eficiencia de servidores AAA RADIUS centrales, mientras que la reducción del tráfico AAA sobre la WLAN.
Usuario, MAC y VLAN "englobamiento	El personal de TI puede asignar políticas AAA a grupos de usuarios, subred o un dispositivo de cómoda, eficientes y rentable administración de WLAN.
Servidumbre de autenticación	Por la autenticación 802.1X la máquina de unión con la autenticación de usuario802.1x, sólo los usuarios de confianza y los dispositivos cliente se proporcionan acceso a la red.
Time-of-day/day-of-week/location Access	El personal de TI son capaces de controlar y restringir el acceso a la red de recursos sobre la base de la ubicación del edificio y / o sobre una base horaria, diaria o semanal.
Lugar la aplicación de políticas	El personal de TI puede agregar o anular AAA definidos por los permisos de acceso basados en la localización del usuario, proporcionando una opción de ubicación centralizada o específica la aplicación de políticas.
Seguridad y control RF	
Rogue AP detección	Programadas o bajo demanda RF exploraciones identificar puntos de acceso no autorizado y redes ad-hoc y alertar al personal de TI central, puntos de acceso dedicado continuamente que puede barrer el espacio aéreo para la protección de 24x7 en entornos que requieren mayor seguridad.
Doble banda de RF exploraciones	Los puntos de acceso de radio única pueden barrer de 2,4 GHz y 5 GHz 802.11n y canales asociados, mientras que la WLAN se mantiene en funcionamiento.
RF en tiempo real de seguimiento y control	RF analiza la fuerza de la señal medida y el uso, las herramientas de software se ajustan de forma dinámica las cargas de tráfico, la alimentación, la huella de RF o las asignaciones de canales para maximizar la cobertura con la capacidad.
El acceso controlado de puntos de control	Mantienen de forma centralizada y distribuida la configuración MAPA, elimina la necesidad de configurar individualmente cada dispositivo. Los mapas también permiten la gestión de ancho de banda y granular por usuario o de cada SSID y características de equilibrio de carga que mejora ampliamente el rendimiento de la red y la experiencia del usuario final.
Control central y administración	
Basada en la identidad de red	Proporciona todos los servicios basados en la identidad del usuario así que cosas como miembros virtuales del grupo privado, ACLs, autenticación, políticas de itinerancia y de la historia, seguimiento de la ubicación, el uso de ancho de banda y otras autorizaciones toda la estancia con los usuarios, ya que deambulan, también le dice al administrador de TI que está conectado a la de la red, donde están, donde han estado, que servicios utilizan y cuáles son los servicios que han utilizado.

Tabla 2.5

Resumen del Software

Característica	Descripción
Sistema operativo común	3Com Wireless LAN Controller WX3000 Unificado de los modelos utilizan el mismo resultado operativo de 3Com Comware software del sistema que se utiliza en la empresa 3Com, cambia como el conmutador 4200G, 4500G,4800G, 5500G y familias S7900E y ruteadores empresariales como las familias de routing de 3Com MSR.

[15].

RFS6000 Wireless LAN/Switch Controller Motorola

Figura 2.10. RFS6000 LAN/Switch.

EspecificacionesdelRFS6000

Esta plataforma de red de comunicación inalámbrica integrada, permite el envío de voz móvil y servicios de datos altamente seguros dentro y fuera de la empresa.Diseñado para empresas medianas y grandes, el modelo RFS6000 simplifica y reduce los costos asociados con las soluciones integradas dado que ofrece el mejor rendimiento, seguridad, escalabilidad y capacidad de gestión de su

clase, a la vez que permite satisfacer las necesidades de sus aplicaciones empresariales de misión crítica altamente exigentes.

Tabla 2.6

Equipo Motorola RFS6000.

Reenvío de paquetes	
Puentes Ethernet 802.1D-1999; puentes 802.11-.802.3; sistemas tagging y trunking 802.1Q VLAN; ARP proxy; redireccionamiento de paquetes	
Interconexión inalámbrica	
LAN Inalámbrica:	Admite 32 WLAN; segmentación de tráfico multi-ESS/BSSID; asignación VLAN a ESSID; asignación automática de VLANs (con autenticación RADIUS); solicitud de protocolo de ahorro de energía; roaming preferente; control de congestión con Administración de Banda Ancha; Pooling de VLAN
Puertos de acceso:	Admite de 1 a 48 puertos de acceso de funcionalidad básica; adopción automática de puertos de acceso con ACL; balanceo de carga de puertos de acceso; conversión de secuencia directa de punto de acceso a puerto de acceso.
AP Adaptable:	Admite de 1 a 48 puntos de acceso AP51X1 802.11a/b/g y AP7131 802.11a/b/g/n independientes de Motorola en modo adaptable para soluciones en sitios remotos y sucursales.
Alimentación por Ethernet:	Integrada, hasta 29,7 vatios por Puerto Ethernet, hasta un máximo de 180 vatios para funcionamiento simultáneo
Implementación de Nivel 2 o Nivel 3 de Puertos de Acceso y Puntos de Acceso AP Adaptable AP51X1 802.11a/b/g y AP7131 802.11a/b/g/n	
Movilidad de Nivel 3 (roaming entre subredes)	
Gateway de VPN sobre IPSec	Admite cifrado DES, 3DES y AES 128 y AES 256; admite funcionalidades de VPN de sitio a sitio y de cliente a sitio
Acceso seguro de invitado (Provisión de punto de acceso público)	Autenticación local basada en Web; redireccionamiento de URL para Inicio de sesión de usuario; páginas de bienvenida e inicio de sesión personalizables; compatibilidad con sistemas de facturación/autenticación externos
Compatibilidad con RADIUS (Atributos específicos de proveedor de Motorola y estándar)	VLAN basadas en usuario (estándar) Autenticación basada en MAC (estándar) Calidad de servicio basada en usuario (Motorola VSA) Autenticación basada en la ubicación (Motorola VSA) ESSID permitidos (Motorola VSA)
Compatible con NAC (control de acceso a redes) con sistemas de terceros de Microsoft y Symantec	
Calidad de servicio (QoS) inalámbrica optimizada	
Calidad de servicio (QoS) inalámbrica optimizada	Priorización y precedencia de tráfico 802.11
Calidad de servicio (QoS) inalámbrica optimizada	WMM con ahorro de energía y control de admisión; WMM U-APSD
Calidad de servicio (QoS) inalámbrica optimizada	Clasificación de paquetes de niveles 1-4; 802.1p prioridad de VLAN; DiffServ/TOS
Resistencia y redundancia del sistema	
Redundancia activa: en reposo, activa: activa y uno a muchos con puerto de acceso y equilibrio de carga MU; recuperación automática (al detectar interferencia de RF o pérdida de la cobertura RF)	
Banco de Firmware Dual soporta la funcionalidad de respaldo de imágenes en caso de contingencias	
Extensibilidad del sistema	
Ranura ExpressCard™	Disponibilidad de tarjeta EVDO/HSPA opcional para servicios de backhaul de banda ancha en el futuro
Interfaz PCI-X	
Administración	
Interfase de línea de comandos (serie, telnet, SSH); GUI segura basada en Web (SSL); SNMP v1/v2/v3; SNMP traps -40+ opciones configurables por el usuario; Syslog; cliente TFTP; protocolo seguro de tiempo de red (SNTP); archivos de configuración de switch basados en texto; DHCP (cliente/servidor/repetidor), configuración automática de switch y actualizaciones de firmware con opciones DHCP; varios roles de usuario (para acceso de switch); Syslog, MIBs (MIB-II, Etherstats, configuración y supervisión específicas del switch inalámbrico)	
Puertos de acceso y puntos de acceso:	AP300 (802.11a/b/g); Instalaciones de Nivel 2 y 3 con soporte de IP estática; Puntos de Acceso de modo AP Adaptable AP51X1 802.11a/b/g y Modo Adaptable AP7131 802.11a/b/g/n
Selección automática de canal de radiofrecuencia (ACS); administración de control de energía de transmisión (TPC); configuración de RF basada en código de país; Preparado para estándares 802.11b, 802.11g, 802.11a, y 802.11n	
Seguridad de red	
Firewall con estándar Stateful Inspection	
Listas de Control de Acceso (ACL) L2/3/4 ACL	
IDS inalámbrico:	Detección multimodo de AP intrusos, lista negra de clientes, autenticación/asociación excesiva; investigación excesiva; disociación/desautenticación excesiva; errores de descifrado; fallos excesivos de autenticación; repetición excesiva de 802.11; fallos crypto VI excesivos (repetición TKIP/CCMP)
Análisis de anomalías:	Control de Acceso a los Medios (MAC) Fuente = Dest MAC; tamaños de cuadros ilegales; MAC Fuente es multidifusión; contramedidas TKIP; direcciones totalmente cero
IPS inalámbrico vía RF Management Suite	
	802.3af" y "802.3at Draft; 1 Interfaz de Administración x 10/100 puerto OOB 1 Host x USB 2.0; 1 Ranura x ExpressCard™ (en modo USB); 1 tarjeta x Express: 1 Interfaz X PCI-X; 1 Puerto Serial (estilo RJ45)
MTBF:	>65.000 Horas
Requisitos de Energía Eléctrica	
Voltaje de entrada de AC:	90 – 264 VAC 50/60Hz
Corriente de entrada máxima de AC:	6A@115 VAC, 3A@230 VAC
Frecuencia de entrada:	47 Hz a 63 Hz
Entorno del usuario	
Temperatura de operación:	0°C a 40°C
Temperatura de almacenamiento.	-40°C a 70°C
Humedad de operación:	5% a 85% (sin condensación)
Humedad de almacenamiento:	5% a 85% (sin condensación)
Disipación de calor:	665 BTU por hora
Normativa	
Seguridad de producto:	UL / cUL 60950-1, IEC / EN60950-1
Cumplimiento de EMC:	FCC (EE.UU.), Industria Canadá, CE (Europa), VCCI (Japón), C-Tick (Australia/Nueva Zelanda)
Servicios de Movilidad para Empresas Recomendados	
Servicio al Cliente:	Service from the Start Advance Exchange Support
Número de Parte	
RFS-6010-100R0-WR:	Switch inalámbrico sin puertos
RFS-6010-10010-WR:	Switch inalámbrico de 8 puertos
RFS-6010-10030-WR:	Switch inalámbrico de 24 puertos
RFS-6010-10060-WR:	Switch inalámbrico de 48 puertos
RFS-6010-UC-08-WR:	Certificado de actualización de la Serie RFS6000 de 8 puertos

2.10 INFORME DEL DISEÑO DE LA RED

Se debe escribir un documento del diseño, que describa completamente su diseño de red. El documento debe incluir los componentes lógicos y físicos del diseño. Las secciones siguientes describen los temas que se deben incluir en un documento comprensivo del diseño.

2.10.1 SUMARIO ADMINISTRATIVO

Un documento del diseño puede tener muchas páginas, por esta razón es esencial que se incluya al principio del documento, un resumen que indique los puntos principales del mismo. El resumen debe tener una extensión no superior a una página y se debe indicar los encargados y los participantes claves del proyecto que decidirán si aceptan el diseño.

2.10.2 META DEL PROYECTO

Esta sección indica el principal objetivo del diseño de la red. La meta se orienta a lo financiero o está relacionada con los objetivos que tienen las empresas en función de su eje de negocios. Esta sección tiene el tamaño de un párrafo, frecuentemente se escribe como una sola oración. Si está bien escrita las personas que toman las decisiones al leer el informe comprenderán el propósito principal y la importancia del diseño de la red.

2.10.3 ALCANCE DEL PROYECTO

La sección del alcance del proyecto proporciona información acerca de la extensión del proyecto, incluyendo un resumen de los departamentos y redes que serán afectados por el mismo. En esta sección se especifica si es un nuevo diseño

o es la modificación de una red existente. Además se debe indicar si el diseño es de un simple segmento de red, un conjunto de redes LAN, una red de un edificio o de un Campus, un conjunto de redes WAN o redes de acceso remoto, o si es una red empresarial.

2.10.4 REQUISITOS DE DISEÑO

Mientras que la sección de la meta del proyecto es generalmente muy breve, la sección de requisitos del diseño es la oportunidad de enumerar todos los requerimientos comerciales y técnicos para el diseño de red. La sección de requisitos del diseño debe enumerar las metas en orden de la prioridad, las metas críticas deben ser indicadas.

2.10.5 OBJETIVOS COMERCIALES

Los objetivos comerciales explican el papel del diseño de red, el cual ayudará a la organización a proporcionar mejores productos y servicios a sus clientes.

Muchos diseñadores de redes tienen problemas al escribir la sección de los objetivos comerciales porque están más interesados en los objetivos técnicos. Sin embargo, es crítico que se centre el documento del diseño de red en la capacidad en la que el nuevo diseño va a ayudar a los clientes, solucionando problemas de negocio en el mundo real.

La mayoría de los negocios empiezan un proyecto de diseño de red para ayudarse a aumentar el crédito, reducir costos operacionales e ineficacias, y mejorar comunicaciones corporativas. Otras metas típicas incluyen envíos parciales del edificio con otras empresas y ampliarse en mercados mundiales. En este punto en el proceso del diseño de red, se deberá tener una comprensión de

las metas de negocio de sus clientes y poder enumerarlas en los documentos del diseño en orden de prioridad.

2.10.6 OBJETIVOS TÉCNICOS

- **Escalabilidad:** El crecimiento que puede soportar el diseño de la red.

- **Disponibilidad:** La cantidad de tiempo que una red está disponible para los usuarios, expresado a menudo como un porcentaje del tiempo de funcionamiento MTBF (mean time between failure) y MTTR (mean time to repair)**.** La documentación de la disponibilidad puede también incluir cualquier información recopilada en el costo monetario asociado a tiempo muerto de la red.

- **Calidad de la red:** Los criterios del cliente para aceptar el nivel de servicio de la red, debe analizar: throughput, precisión, eficiencia, retardo, variación del retardo (jitter) y el tiempo de respuesta. Se debe especificar los requisitos de throughput para los equipos de internet working, utilizando PPS (paquetes por segundo). Los requisitos específicos de throughput para ciertas aplicaciones deben ser especificados en la sección de aplicaciones.

- **Seguridad:** Metas generales y específicas para proteger la capacidad de la organización de dirigir los negocios sin interferencia de intrusos o daños al equipo, a datos, o a operaciones. Esta sección debe también enumerar los varios riesgos de la seguridad que el cliente identificó durante la fase del requisito-análisis del proyecto del diseño.

- **Flexibilidad:** Metas generales y específicas de calidad, problemas, configuración, seguridad, y gerencia empresarial.

- **Uso:** Se define como la facilidad para que los usuarios accedan a la red y los servicios brindados por esta. Aquí se incluyen los objetivos para simplificar tareas relacionadas con direcciones, nombres y recursos de la red.

- **Adaptabilidad:** La facilidad con la cual un diseño e implementación de la red puede adaptarse a las averías de la red, a los patrones de tráfico que cambian, al negocio adicional o a los requisitos técnicos, las nuevas prácticas de negocio y otros cambios.

- **Factibilidad:** Es información de carácter general sobre la importancia de reducir el coste que se asoció al equipo y a servicios de la red. La información específica del presupuesto se debe incluir en la sección del presupuesto de proyecto.

2.10.7 GRUPO DE USUARIOS Y ALMACENAMIENTO DE DATOS

En esta sección se realiza una lista de la mayoría de grupos de usuarios, se incluye el tamaño, localización y principales aplicaciones, se puede utilizar la tabla 2.7 para crear un resumen de la comunidad de usuarios. Además se debe crear una lista de almacenamiento de datos (servidores y hosts) y su localización. En la tabla 2.8 se reúne la información de almacenamiento de datos.

Tabla 2.7.

Comunidad de Usuarios

Usuario nombre	Tamaño (Número de Usuarios)	Localización de los usuarios	Aplicaciones usadas por los usuarios

Tabla 2.8.

Almacenamiento de datos.

Almacenador de datos	Localización	Aplicaciones(s)	Utilizados por el grupo de usuarios

2.10.7.1 Aplicaciones de la Red

En esta sección se crea una lista de las aplicaciones NUEVAS Y EXISTENTES DE LA RED, para realizar un resumen de las aplicaciones se pueden utilizar la tabla 2.9.

Tabla 2.9.

Requisitos técnicos para las Aplicaciones de la red.

Nombre de la aplicación	Tipo de aplicación	Aplicación Nueva S/N	Crítica	Costo de la caída de la aplicación	Aceptable MTBF

Además añadir el tráfico existente de la red como se ve en la tabla 2.10

Tabla 2.10.

Características de Tráfico de las Aplicaciones de la red.

Nombre de la Aplicación	Tipo de flujo	Protocolo usado	Grupo de usuarios	Servers, Hosts	Requisitos aproximados de ancho de banda	Requisito de QoS

2.10.8 ACTUAL ESTADO DE LA RED

Esta sección describe brevemente la estructura y el funcionamiento de la red existente. Debe incluir un mapa de alto nivel de la red que identifique la localización de los dispositivos del internet working, los sistemas de almacenamiento y segmentos de la red. El mapa de alto nivel debe documentar los nombres y las direcciones de dispositivos y de segmentos importantes e indicar el tipo y las longitudes de los segmentos principales de la red. Para internet works muy grandes, se pueden necesitar dos o tres mapas de alto nivel.

Los mapas de red deben incluir el diseño lógico y los componentes físicos (por ejemplo la localización y el alcance de redes privadas virtuales (VPN's) de LAN's virtual (VLAN's), segmentos de firewall, server cluster y otros. Los mapas deben también caracterizar la topología lógica de la red interna y que componen la internet work. Los mapas de la red, deben indicar si la red es jerárquica o plana, estructurada o no estructurada, entre otros. Deben también indicar la geometría de la red (por ejemplo, estrella, anillo, bus, hub, spoke, o malla). La documentación del estado actual de la red también describe brevemente estrategia o estándar para el nombramiento de los dispositivos. Si las aplicaciones del cliente (o los planes a utilizar) tratan técnicas de sumarización se debe indicar en el documento del diseño.

Una sección importante del estado actual de la sección de la red del documento del diseño de red se debe dedicar a un análisis de la salud y del funcionamiento de la actual red.

Los informes detallados se pueden poner en el apéndice del documento del diseño para evitar abrumar al lector con demasiada información en esta etapa. Es importante que el lector pueda comprender rápidamente el diseño lógico y la sección física del diseño del documento, porque esas secciones contienen la esencia de su oferta del diseño.

2.10.8.1 Diseño Lógico

La sección del diseño lógico documenta los siguientes aspectos del diseño de red:

- La topología de la red, incluyendo uno o más dibujos que ilustran la arquitectura lógica de la actual red y la nueva red.

- Un modelo para tratar segmentos de la red y dispositivos.

- Un modelo para nombrar los dispositivos de la red.

- Una lista de los protocolos de enrutamiento, puenteo, conmutación y otros, las recomendaciones específicas de la puesta en práctica de estos protocolos.

- Se recomienda para la seguridad, incluyendo un resumen de las políticas y de los procedimientos de la seguridad. (Si el plan detallado de la seguridad fue desarrollado como parte del diseño de red, se puede anexar al informe del diseño.).

- Administración de la red de arquitecturas, procesos y productos.

- El diseño debe ser racional, en función de los objetivos de los clientes y el estado actual de la red.

2.10.8.2 Diseño Físico

En la sección de diseño físico se describe las características y las aplicaciones recomendadas para las tecnologías y los dispositivos que se seleccionaron para implementar el diseño. Puede incluir la información para la red del Campus, la red

del acceso remoto y la red WAN. Esta sección puede también incluir la información sobre cualquier servicio de los proveedores.

2.10.9 Resultados de la prueba del diseño de red

Esta sección describe el resultado de la prueba que se realizó para verificar el diseño de red. Es una de las partes más importantes del documento de diseño porque le da ocasión de probar al cliente que el diseño resolverá los requisitos de calidad, seguridad, utilidad y flexibilidad. Se puede describir cualquier sistema del prototipo o piloto que en ejecución se ponga y los componentes de prueba:

- Prueba de objetivos
- Prueba de criterios aceptados
- Prueba de herramientas
- Prueba de escritorio

2.10.10 Resultados y observaciones

En los resultados y observaciones, se debe incluir cualquier técnica de la optimización que se recomiende para que se aplique al diseño para asegurarse de que cumpla ciertos requisitos.

BIBLIOGRAFÍA CAPÍTULO 2

- [1] Definición VLAN
  http://es.kioskea.net/contents/internet/vlan.php3
- [2] DVLAN (VLAN dinámicas)
  http://www.utpl.edu.ec/eccblog/wp-content/uploads/2007/04/articulo-tecnico_asignacion-y-administracion-de-vlans-dinamicas.pdf
- [3] Redes inalámbricas
  https://belenus.unirioja.es/~secarcam/redes/lan/inalambricas.html
- [4] Tipos de redes
  https://belenus.unirioja.es/~secarcam/redes/lan/inalambricas.html
- [5]Wi-fi
  http://www.taringa.net/posts/info/2715628/Que-es-WiFi_.html
- [6] Ventajas y desventajas.
  http://www.uv.mx/iiesca/revista/documents/redes2008-2.pdf
- [7] Punto de acceso
  http://es.wikipedia.org/wiki/Punto_de_acceso_inal%C3%A1mbrico
- [8] Tipos de antennas
  Cisco – Aironet Wireless
- [9] Conmutador
  http://www.helpy.com.ar/noticiasweb/2009/mayo/19-05-2009-1.htm
- [10] **El modelo jerárquico de 3 capas**
  http://www.geocities.ws/yagniri/teg/capitulo2.html
- [11] Control inalámbrico
  http://dspace.espoch.edu.ec/bitstream/123456789/328/1/18T00409.pdf
- [12] Controlador Cisco 2100 Series Wireless LAN Controller
  http://www.cisco.com/web/LA/soluciones/comercial/products/wireless/2100_series_wireless_lan_controller/index.html
- [13] Cisco 2106 Series Wireless LAN Controller
  http://www.cisco.com/web/solutions/smb/espanol/productos/inalambrica/wireless_LAN_controller_serie_2100.html#~models

- [14] Cisco Wireless Express 526 Mobility Controller http://www.cisco.com/web/solutions/smb/espanol/productos/inalambrica/wireless_LAN_controller_serie_2100.html#~models
- [15] **HP WX5000 Access *Controller*** http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&taskId=120&prodSeriesId=4177387&prodTypeId=12883&objectID=c02504816
- [16] **RFS6000 Wireless LAN/Switch Controller Motorola** http://www.bearcomlatam.com/Equipos_en_Redes_y%20Banda_Ancha_Motorola/Motorola/SOLUCIONES%20WIRELESS%20LAN/WLAN-RFS6000.pdf

CAPÍTULO 3: Situación Actual

3.1 Descripción de la Empresa

3.1.1 Física

El edificio ALPALLANA, está dividido en diez pisos los cuales se detalla a continuación:

En la Planta Baja funciona el departamento de Sistemas, en la parte del Centro de Datos se encuentra 3 Rack's, sistema de UPS para protección de los equipos.

- En el primer Rack se encuentra el acceso de internet conectado con un Ruteador, además se encuentra un conmutador de acceso.

- El segundo es un Rack de IBM, donde se encuentran alojadas las aplicaciones de la empresa, además tiene Storage para almacenamiento de la información.

- El Tercer Rack consta de panel de puntos de red, donde se encuentra todo el cableado de fibra óptica que se dirige a todos los pisos del edificio para interconectar las tarjetas del conmutador de núcleo.

- Además se tiene una PC con sistema operativo Linux Red Hat, en el cual funcionan las listas de accesos, el servidor DHCP.

En los pisos 2, 3, se tiene conmutadores de accesos para la distribución de la comunicación en los equipos terminales.

En el piso 5, 7 y 10 se encuentran dos conmutadores de Acceso para distribuir a cada piso inferior y al que se encuentran los equipos.

En el caso de los conmutadores del piso 10, se distribuye para una oficina y una sala de reuniones. El resto de puntos están distribuidos en los pisos 8 y 9.

En los conmutadores de los pisos 5, 7 y 10 se encuentran conectados por cable UTP los AP's de los pisos 4, 6, 8, 9 y 10.

Todos los conmutadores de accesos constan de tarjetas de puertos de fibra óptica, que están conectados a las tarjetas en el Centro de Datos en el conmutador principal.

3.1.2 Lógica

La red de datos de PETROECUADOR tiene una topología en estrella, lo que permite obtener conectividad completa entre todos los dispositivos de networking. Al crearse este tipo de topología ha permitido enlazarse con todas las dependencias filiales del estado como por ejemplo PETROCOMERCIAL.

Es importante mencionar que el Edificio ALPALLANA no fue creado bajo estándares de cableado estructurado en su totalidad, sin embargo de acuerdo a las necesidades y el crecimiento acelerado, existe cableado tendido en algunos pisos del mencionado edificio.

3.2 Análisis Actual de la Empresa

3.2.1 Requisitos de Diseño

Para el mejoramiento del nivel de seguridad y movilidad de los usuarios de la red de datos del edifico ALPALLANA se determina los siguientes objetivos técnicos:

3.2.2 Objetivos Técnicos:

PETROECUADOR es una Institución que se encuentra en continuo crecimiento, por lo cual la red de datos deberá ser considerada para un crecimiento aproximadamente de cinco años de acuerdo a las necesidades presentadas en el edificio ALPALLANA.

- Ofrecer mayor movilidad a los usuarios permitiendo aprovechar toda la infraestructura inalámbrica para el óptimo funcionamiento de los sistemas informáticos.

- Aumentar el porcentaje de seguridad a nivel de usuario con la utilización de VLAN´s Dinámicas.

3.2.3 RED ACTUAL

3.2.3.1 Escalabilidad

PETROECUADOR al estar en un crecimiento continuo se ha visto en la necesidad de incrementar personal en diferentes áreas de trabajo, por lo cual la utilización acelerada y no planificada, ha ocasionado que actualmente la red de datos de la Institución no soporte la incorporación excesiva de nuevos usuarios y equipos de interconexión, también se maneja dispositivos de voz IP.

Actualmente la red LAN soporta aproximadamente 500 dispositivos como: computadoras, impresoras, teléfonos IP, servidores, mismos que están interconectados a través de conmutador de acceso y distribución dependiendo el caso.

3.2.3.2 Disponibilidad

PETROECUADOR en la actualidad no tiene una bitácora en relación al tiempo de disponibilidad por lo cual no se podrá precisar un valor exacto en este cálculo, sin embargo, de acuerdo a entrevistas realizadas al personal encargado de redes se pudo conocer que aproximadamente ha existido una suspensión de servicio de 24 horas en un año por lo cual se determina que la disponibilidad de la red actual es del 99.78%.

En lo que se refiere a la red inalámbrica, es un panorama totalmente contrario, puesto que solo existen puntos de acceso a la red inalámbrica en ciertos sectores de algunos pisos del Edificio ALPALLANA.

3.2.3.3 Calidad

Se observa en la siguiente figura varios parámetros obtenidos de diferentes herramientas de diagnóstico, como por ejemplo Whats´up Gold y PRTG, las mismas que permitiran tener una visión de la calidad de red actual que maneja PETROECUADOR en el edificio ALPALLANA.

WhatsUp Gold Premium Edition 11 es la herramienta utilizada para el análisis de tráfico y se puede observar en el manual de usuario en el Anexo D. A continuación se presentan los resultados obtenidos mediante el mismo.

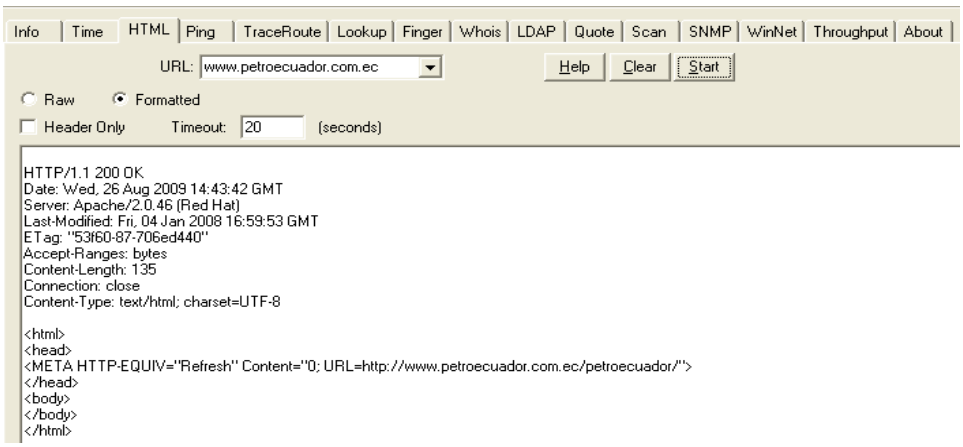


Figura 3.1. Ejemplo Real de HTML.

Como se puede observar en la Figura 3.1, al ingresar una dirección URL refleja valores de respuesta así como del encabezado de la página seleccionada.

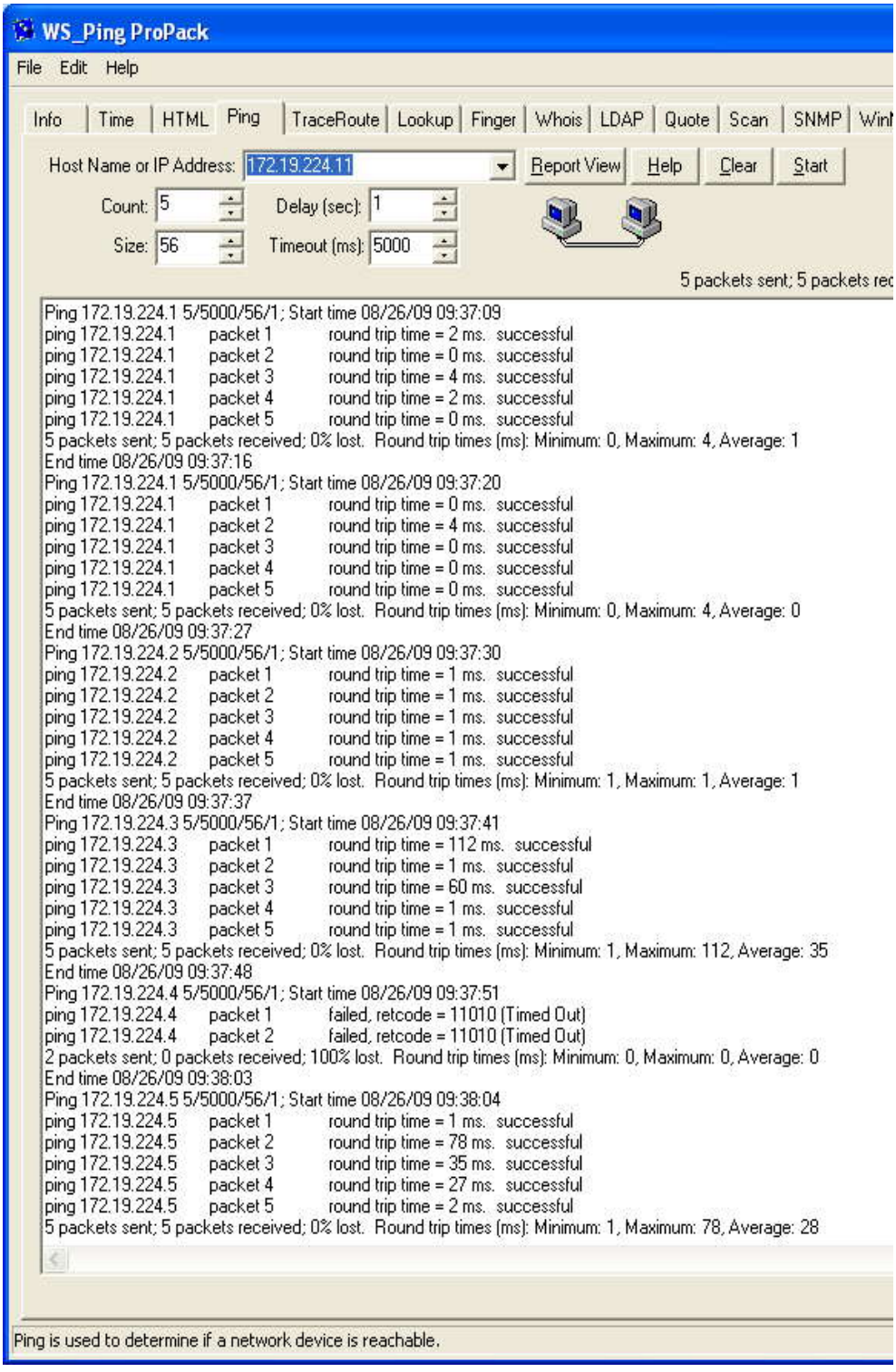


Figura 3.2. Ejemplo Real de PING.

Con el comando de diagnóstico ping se puede observar tiempos de respuestas promedio, los cuales nos permiten tener una visualización del tiempo de respuesta que existe entre 6 equipos de networking como se muestra en la figura 3.2.

Figura 3.3. Ejemplo Real de TracerRoute.

Para el análisis de la red se puede observar la Figura 3.3 en la que se visualiza el envío de 20 paquetes a varios equipos de networking.

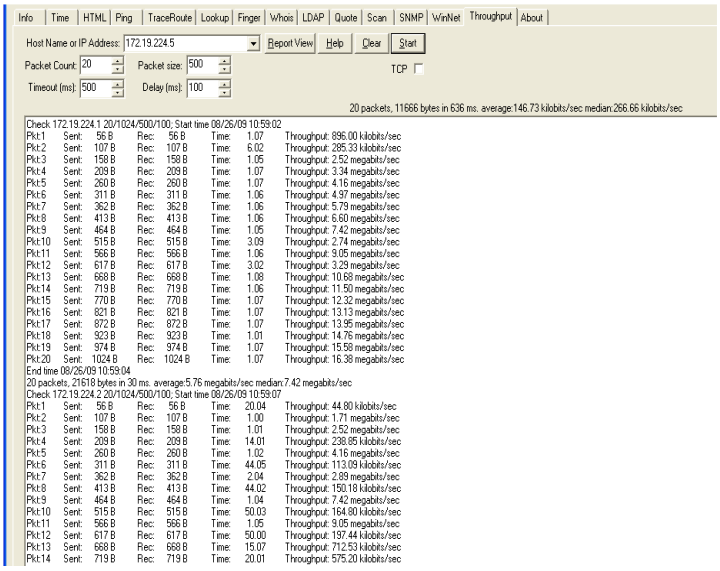


Figura 3.4. Ejemplo Real de Throughput.

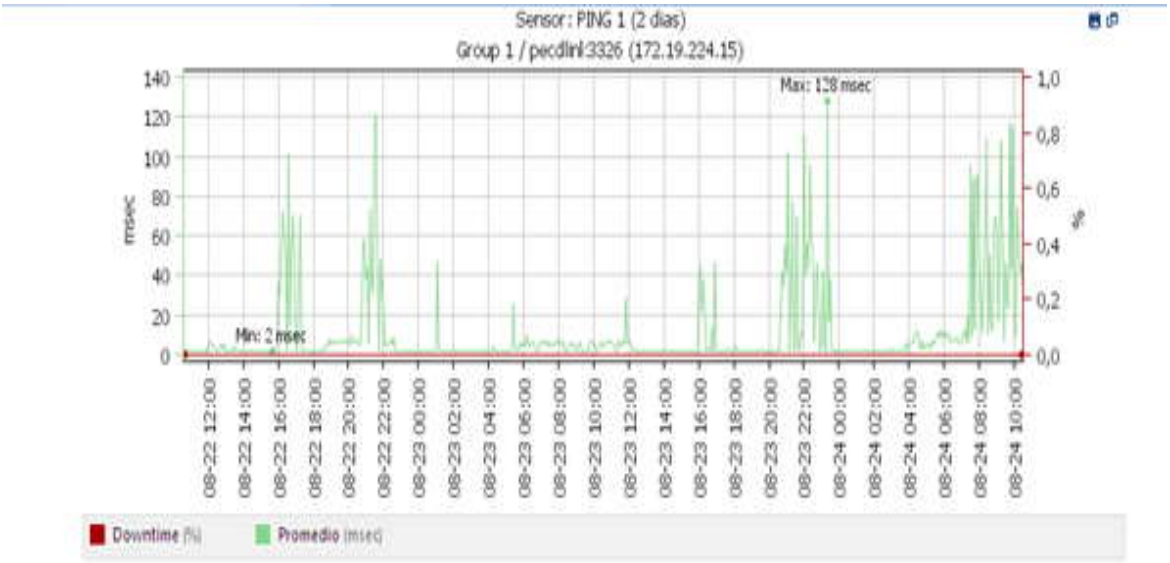
Se pueden observar en la Tabla 3.4 las mediciones realizadas del throughput (Tasa de Transferencia de Datos efectiva) de la conexión LAN de todo el edificio, se puede visualizar un análisis de una semana completa con el envío de 20 paquetes.

Tabla 3.1.

Análisis de resultados de Throughput.

		Ubicación	Dispositivo	T.min (ms)	T. max (ms)	T. Promedio (ms)	Throughput Promedio
Diario		Cuarto de Telecom.	Cisco-6500 (172.19.224.1)	1.00	5.08	1.17	8.56 Megabits/s
		2do Piso	cisco WS-C3548 (172.19.224.3)	1.03	105.09	26.70	730.11 kilobits/s
		3ro. Piso	cisco WS-C3548 (172.19.224.2)	1.02	86.05	21.72	295.00 kilobits/s
		5to Piso	cisco WS-C3548 (172.19.224.5)	1.03	143.06	25.93	341.36 kilobits/s
			cisco WS-C2950 (172.19.224.14)	2.00	13.02	2.89	2.74 Megabits/s
		7mo. Piso	cisco WS-C3548 (172.19.224.6)	1.04	213.02	52.68	277.38 kilobits/s
			cisco WS-C3560G (172.19.224.21)	1.00	4.07	1.90	5.45 Megabits/s
		10mo. Piso	cisco WS-C3524 (172.19.224.8)	1.01	34.04	4.36	2.12 Megabits/s
			cisco WS-C3560G (172.19.224.24)	1.00	6.00	4.34	3.76 Megabits/s
		Cuarto de Teleco.	Cisco-6500 (172.19.224.1)	1.00	4.02	1.43	8.23 Megabits/s
		2do Piso	cisco WS-C3548 (172.19.224.3)	1.02	161.02	18.33	361.72 kilobits/s
		3ro. Piso	cisco WS-C3548 (172.19.224.2)	1.02	78.05	16.64	470.98 kilobits/s
		5to Piso	cisco WS-C3548 (172.19.224.5)	1.03	89.06	16.89	522.25 kilobits/s
			cisco WS-C2950 (172.19.224.14)	1.09	13.02	4.21	2.34 Megabits/s
		7mo. Piso	cisco WS-C3548 (172.19.224.6)	1.08	117	24.21	381.31 kilobits/s
			cisco WS-C3560G (172.19.224.21)	1.00	8.01	1.90	4.79 Megabits/s
		10mo. Piso	cisco WS-C3524 (172.19.224.8)	1.02	38.07	6.24	396.55 kilobits/s
			cisco WS-C3560G (172.19.224.24)	1.00	8.03	2.76	2.45 Megabits/s

Para éste análisis se utilizó la herramienta PRTG con la finalidad de realizar un segundo análisis sobre la calidad de la red de datos, con lo cual se puede observar que los valores son similares.



Fecha Hora	Promedio	Downtime	Cobertura
Promedios (de 576 valores)	11 msec	0 %	100 %

1 to 50 of 576 — Cuenta de objetos

Fecha Hora	Promedio	Downtime	Cobertura
24.08.2009 10:25:00 - 10:30:00	32 msec	0 %	100 %
24.08.2009 10:20:00 - 10:25:00	45 msec	0 %	100 %
24.08.2009 10:15:00 - 10:20:00	42 msec	0 %	100 %
24.08.2009 10:10:00 - 10:15:00	54 msec	0 %	100 %
24.08.2009 10:05:00 - 10:10:00	75 msec	0 %	100 %
24.08.2009 10:00:00 - 10:05:00	9 msec	0 %	100 %
24.08.2009 9:55:00 - 10:00:00	14 msec	0 %	100 %
24.08.2009 9:50:00 - 9:55:00	114 msec	0 %	100 %
24.08.2009 9:45:00 - 9:50:00	43 msec	0 %	100 %
24.08.2009 9:40:00 - 9:45:00	117 msec	0 %	100 %
24.08.2009 9:35:00 - 9:40:00	23 msec	0 %	100 %
24.08.2009 9:30:00 - 9:35:00	26 msec	0 %	100 %
24.08.2009 9:25:00 - 9:30:00	47 msec	0 %	100 %
24.08.2009 9:20:00 - 9:25:00	7 msec	0 %	100 %
24.08.2009 9:15:00 - 9:20:00	57 msec	0 %	100 %
24.08.2009 9:10:00 - 9:15:00	108 msec	0 %	100 %
24.08.2009 9:05:00 - 9:10:00	53 msec	0 %	100 %

Figura 3.5. Tabla de resultados del PRTG.

3.2.3.4 Seguridad

PETROECUADOR posee servidores de autentificación, autorización y de no repudio, los cuales permiten definir perfiles de usuario así como usuarios-administradores y a la vez restringir los servicios de acuerdo a las funciones de los servidores públicos.

Adicionalmente, la Institución se encuentra trabajando con una parametrización en los equipos de interconexión de VLAN's estáticas, este sistema permite brindar y asignar redes a los usuarios en las distintas dependencias o departamentos del edificio ALPALLANA.

3.2.3.4.1 Configuración Actual de los Conmutadores Cisco

Cada conmutador utilizado en el edificio ALPALLANA tiene una configuración distinta a los demás, por lo cual se detallan los equipos utilizados.

Conmutador CISCO Catalyst 2950: Este modelo necesita ser configurado en cada puerto el acceso a la VLAN que pertenezca, troncalizar el puerto asignando a la misma VLAN y colocar el modo troncalizar. [1]

Conmutador CISCO Catalyst 3550: Este modelo necesita configurar en cada puerto el acceso a la VLAN que pertenezca, troncalizar el puerto asignando a la misma VLAN, el encapsulamiento del trunk se realiza para poder troncalizar este modelo.[2]

Conmutador CISCO Catalyst 3560G PoE: Este modelo de conmutador como la versión del IOS es más actualizado, no es necesario configurar mayormente, sólo se debe asignar el modo, en este caso de acceso, a la VLAN que pertenece. [3]

3.2.3.5 Administración

La administración se la realiza en cada equipo lo que ocasiona grandes inconvenientes en el cambio y en la actualización de equipos de interconexión. Existen servidores de dominio o DNS los mismos que nos permiten autentificar y autorizar el acceso a los usuarios a nivel de equipos en el dominio.

Actualmente se lleva una administración individual por cada equipo de networking lo que ha ocasionado que exista parametrización independiente de estos equipos, impidiendo la correcta administración centralizada a través de un equipo.

Adicionalmente la Institución maneja un software de monitoreo el que le permite verificar si el equipo se encuentra en estado activo, este software se denomina IPCHECK el mismo que nos permite visualizar si el equipo se encuentra en estado UP o levantado físicamente, si el equipo está en estado *down* se procede a verificar y a levantar el servicio, sin embargo para realizar esto el personal técnico se traslada del cuarto de equipos hacia la ubicación del equipo dañado.

3.3 DISEÑO LÓGICO.

La red de datos de PETROECUADOR tiene una topología en estrella, lo que permite obtener conectividad completa entre todos los dispositivos de networking. Al crearse este tipo de topología ha permitido enlazarse con todas las dependencias filiales del estado como por ejemplo PETROCOMERCIAL.

ESPACIO EN BLANCO
INTENCIONAL

Es importante mencionar que el Edificio ALPALLANA no fue creado bajo estándares de cableado estructurado en su totalidad, sin embargo de acuerdo a las necesidades y el crecimiento acelerado, existe cableado tendido en algunos pisos del mencionado edificio.

Adicionalmente debido a los niveles de seguridad implementados en el edifico ALPALLANA se maneja VLAN estáticas las mismas que a continuación se puede observar en la tabla 3.2.

Tabla 3.2.

Tablas VLAN.

VLAN	Nombre	Estado
1	default	active
2	SERVIDORES	active
4	PRESIDENCIA	active
5	GCI	active
6	PRO	active
7	AIN	active
8	GEF	active
9	GAD	active
10	SISTEMAS	active
11	CAP	active
12	IDT	active
13	GPA	active
14	ACP	active
15	Abas	active
16	ANTIGUA	active
17	VPNGYE	active

Continua ⟶

18	FILIALES	active
19	AULA	active
20	CÍRCULO	active
21	TELEFONÍA	active
22	ITT	active
23	BCE	active
24	DIS	active
25	TRA	active
26	AVQ	active
27	DYA	active
28	Vides	active
29	ENLACES	active

ESPACIO EN BLANCO
INTENCIONAL

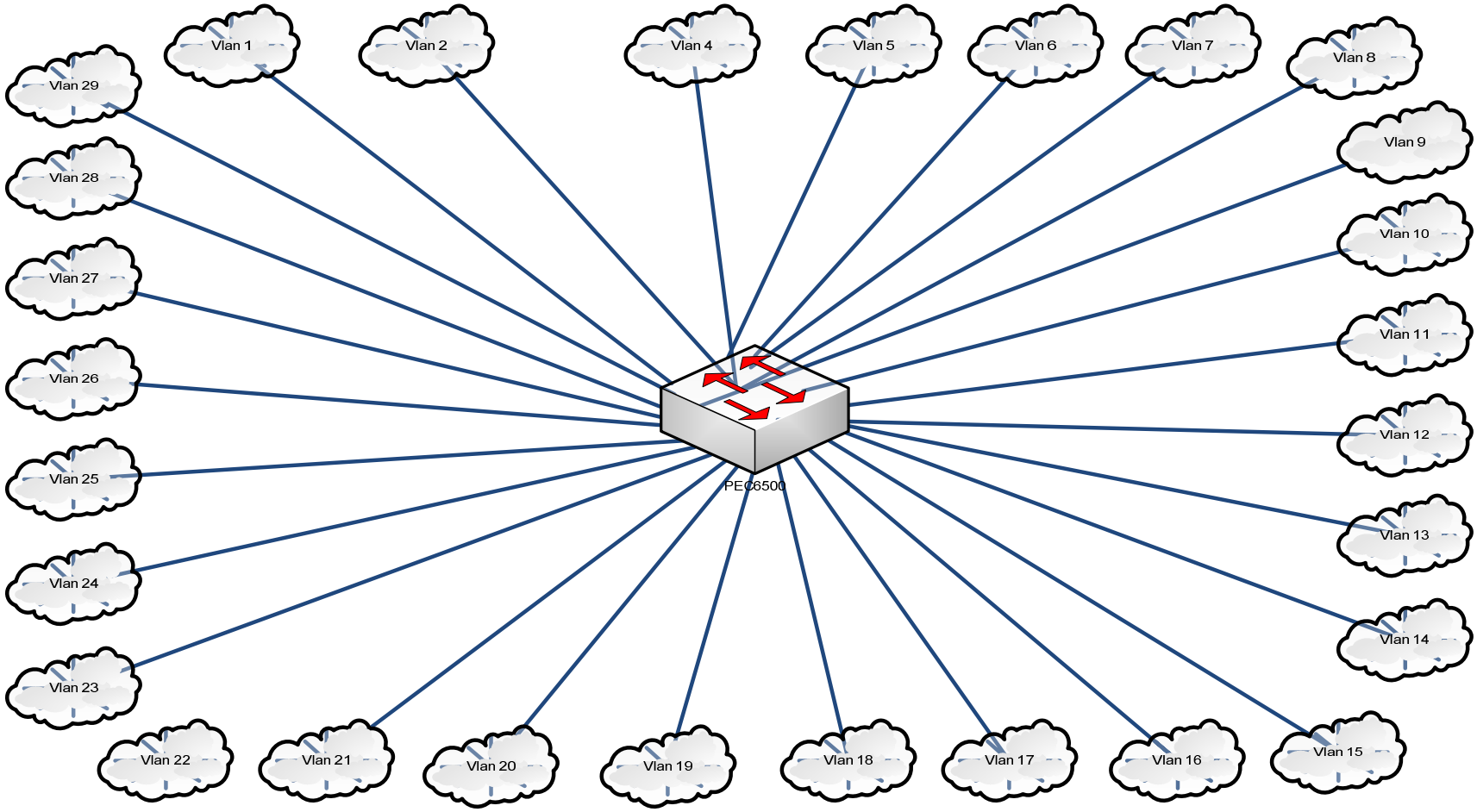


Figura 3.6. Mapa lógico Actual de la Red de datos.

Como se puede observar en la tabla 3.2 se puede encontrar cada nomenclatura de las VLAN's utilizadas, las cuales representan a las distintas dependencias de la empresa.

1. Default: Esta VLAN viene creada por defecto y se utiliza para administrar el equipo de forma remota.

2. SERVIDORES: Servidores.

4. PRESIDENCIA: Como su nombre lo indica es para brindar todos los privilegios a la plana mayor de la empresa.

5. GCI: Gerencia de Comercio Internacional.

6. PRO: Red designada con Producción.

7. AIN: Auditoría Interna.

8. GEF: Gerencia de Economía y Finanzas.

9. GAD: Gerencia Administrativa.

10. SISTEMAS: Departamento de Sistemas.

14. ACP: Administración de Contratos Petroleros.

16. ANTIGUA: Red antigua de servidores.

18. FILIALES: Las filiales de PETROECUADOR.

19. AULA: Red para los practicantes de PETROECUADOR**.**

20. CÍRCULO: Un enlace que se tiene en el círculo militar para cursos de EPR.

21. TELEFONÍA: Como su nombre lo dice aquí se trabaja en telefonía IP.

22. ITT: Ishpingo Tambococha Tiputini

23. BCE: Banco Central del Ecuador.

27. DYA: Documentación y Archivo Central.

28. VIDEO: Enlace para video conferencia.

ESPACIO EN BLANCO
INTENCIONAL

En la tabla 3.3 se muestra la relación entre conmutadores con cada VLAN en la que está configurada en ese equipo

Tabla 3.3.

Relación Conmutador VLAN.

A / B	1	4	5	6	7	8	9	10	14	16	18	19	20	21	22	23	27	28
pec3548man1	X					X	X	X		X		X	X	X				
pec3560pb2	X					X	X	X			X			X	X			X
PEC3548P2	X						X							X				
PEC3548P3	X					X	X	X	X	X	X			X				
PEC3548P5	X	X	X		X		X							X				
pec2950p5	X		X		X		X							X				
PEC3548P7	X		X	X			X							X				
pec3560Gp7	X		X											X				
PEC3524P10	X	X												X				
pec3560Gp10	X	X												X	X	X	X	X
Pec3560Gaula	X											X		X				X

A	Nombre del Equipo
B	Número de VLAN

pecxxyy	**Significado**
pec	PETROECUADOR
xx	Modelo de Conmutador
yy	Ubicación de equipo

DIAGRAMA FISICO DE RED DEL EDIFICIO ALPALLANA

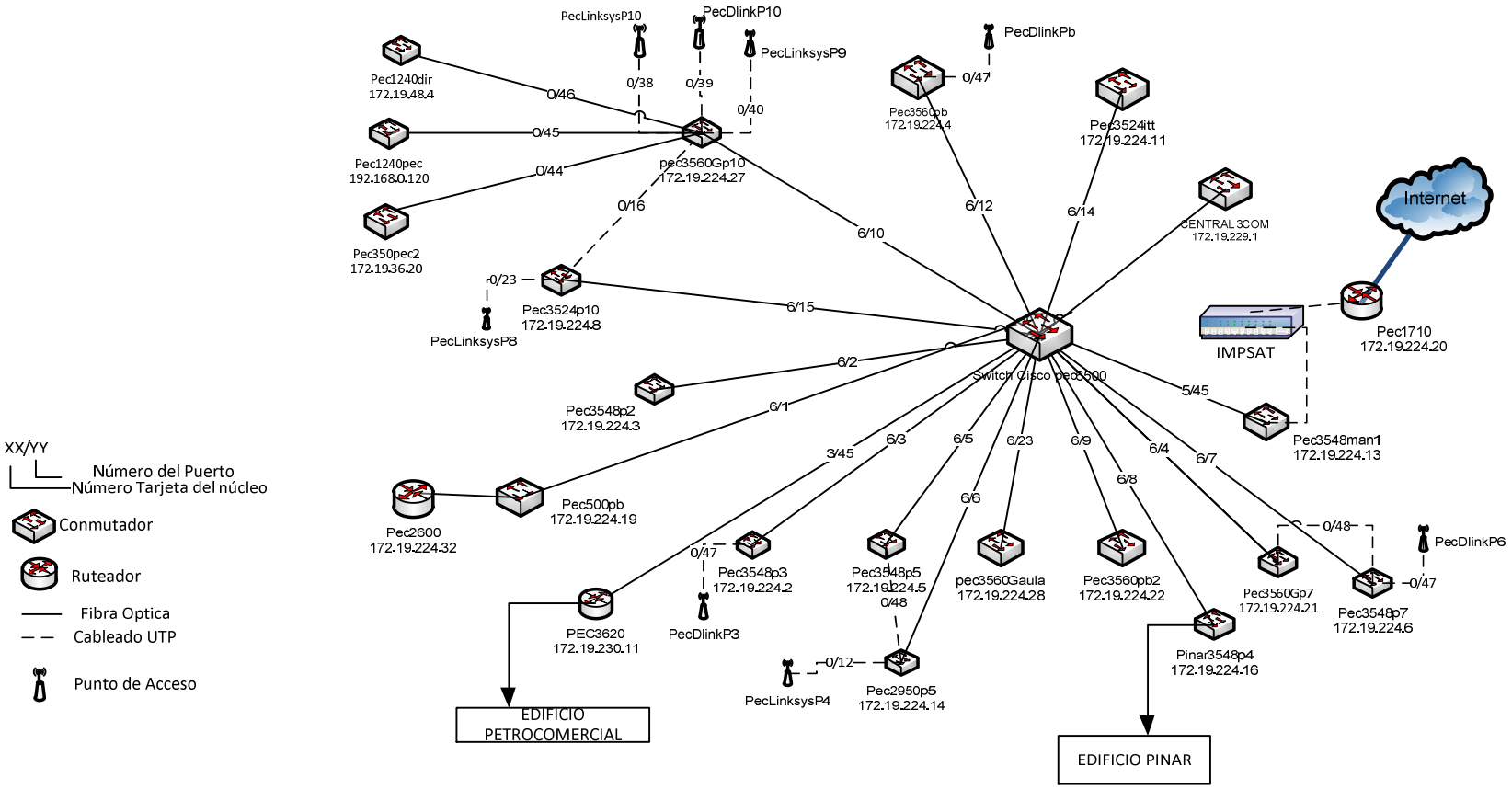


Figura 3.7. Mapa Físico Actual de la Red de Datos.

3.4 Diagrama Físico del Edificio ALPALLANA

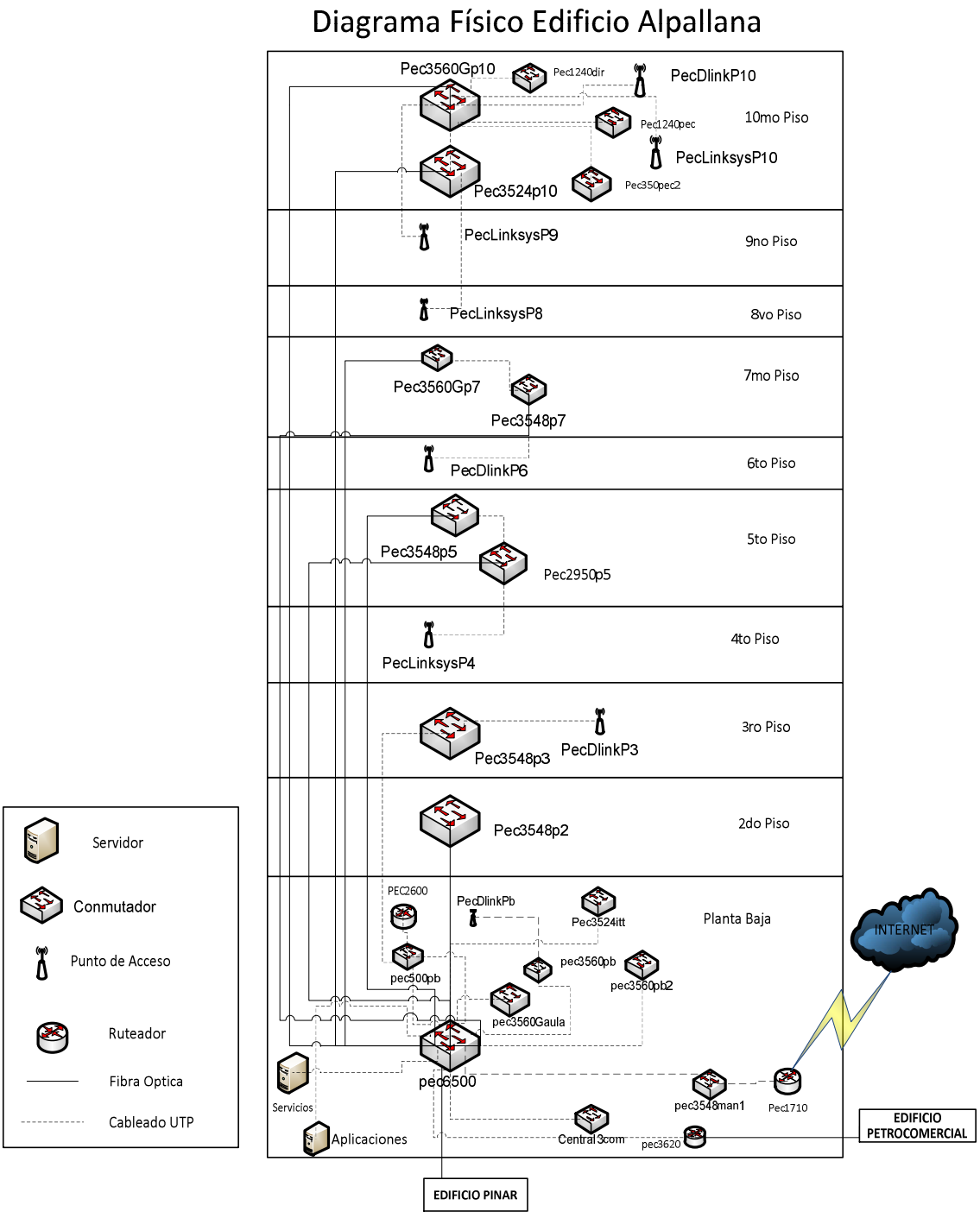


Figura 3.8. Mapa Físico Vertical del Edificio ALPALLANA.

TOPOLOGÍA DE RED FÍSICA

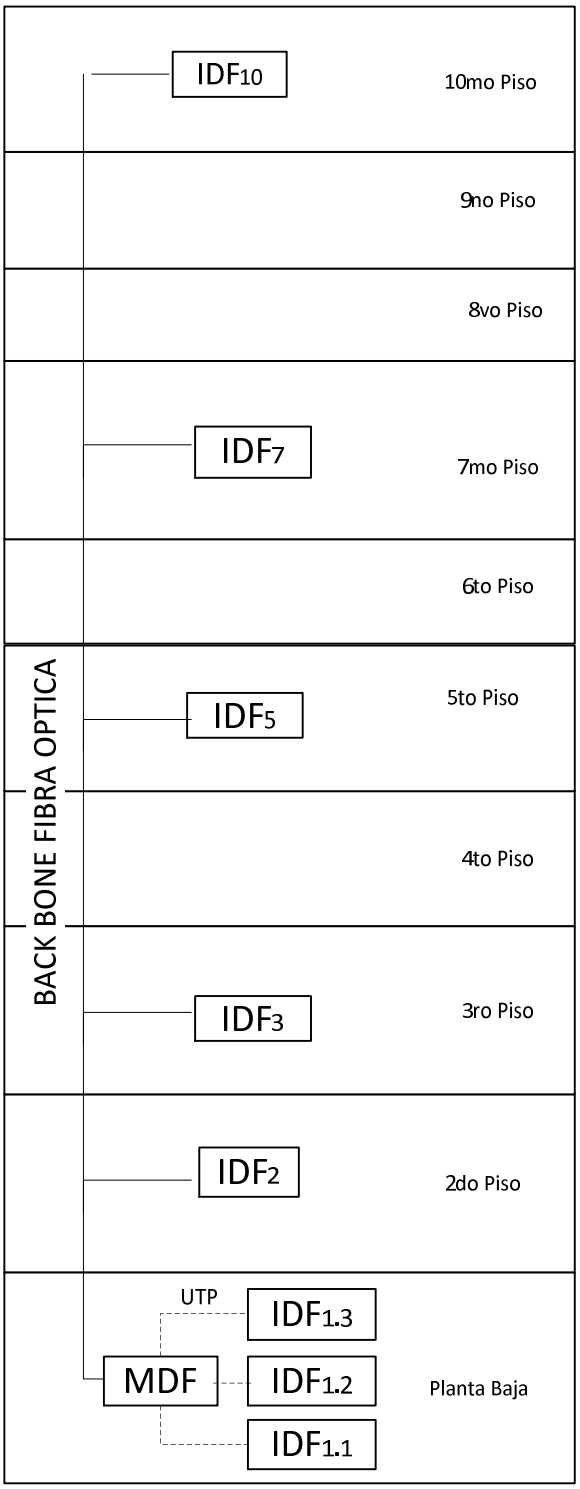


Figura 3.9. Topología de Red del Edificio ALPALLANA.

Tabla 3.4.

Relación AP.

Puntos de Acceso
PecDlinkP10
PecLinksysP10
PecLinksysP9
PecLinksysP8
PecDlinkP6
PecLinksysP4
PecDlinkP3
PecDlinkPB

pecxxyy	Significado
pec	PETROECUADOR
xx	Modelo de Conmutador
yy	Ubicación de equipo

El cableado de la red de datos de PETROECUADOR, no está diseñado 100% con normas ni estándares, por lo cual existe cableado tendido en la mayor parte del edificio, por otra parte se han realizado remodelaciones de algunos pisos y a su vez se realizó un cableado estructurado nuevo, en el Anexo E se podrán observar los planos del edificio administrativo con los puntos de red de datos actual.

Las configuraciones realizadas de los tres conmutadores se encuentran en el Anexo C.

Tabla 3.5.

DESCRIPCIÓN FÍSICA DE LA RED.

DESCRIPCIÓN FÍSICA DE LA RED DEL EDIFICIO ALPALLANA									
PISO	TOPOLOGICO		NUCLEO	ACCESO	OFICINA	AP	ROUTER	TOTAL SW	TOTAL AP
PB	MDF		PEC6500						
		IDF1.1		PEC3560PB					
							PEC3620		
				PEC3560PB2		PECDLINKPB			
		IDF1.2		PEC500PB					
				PEC3524ITT	PEC3560GAULA		PEC2600		
		IDF1.3		PEC3548MAN1			PEC1710		
		TOTAL	1	6	1	1	3	8	1
P2		IDF2		PEC3548P2					
		TOTAL		1					
P3		IDF3		PEC3548P3		PECDLINKP3			
		TOTAL		1		1		1	1
P5		IDF5		PEC3548P5					
				PEC2950P5		PECLINKSYSP4			
		TOTAL		2		1		2	1
P7		IDF7		PEC3560GP7					
				PEC3548P7		PECDLINKP6			
		TOTAL		2		1		2	1
P10		IDF10		PEC3524P10		PECLINKSYSP8			
						PECLINKSYSP9			
				PEC3560gP10	PEC1240DIR	PECLINSYSP10			
					PEC1240PEC	PECDLINKP10			
					PEC350PEC2				
		TOTAL		2	3	4		5	4

Se escogió una muestra de 11 personas del departamento de sistemas del Edificio ALPALLANA, para que respondan la encuesta que se encuentra en el Anexo F, y se obtuvieron los siguientes resultados:

Figura 3.10 Configuración Genérica.

Figura 3.11 Tiempo en Configuración de un Conmutador.

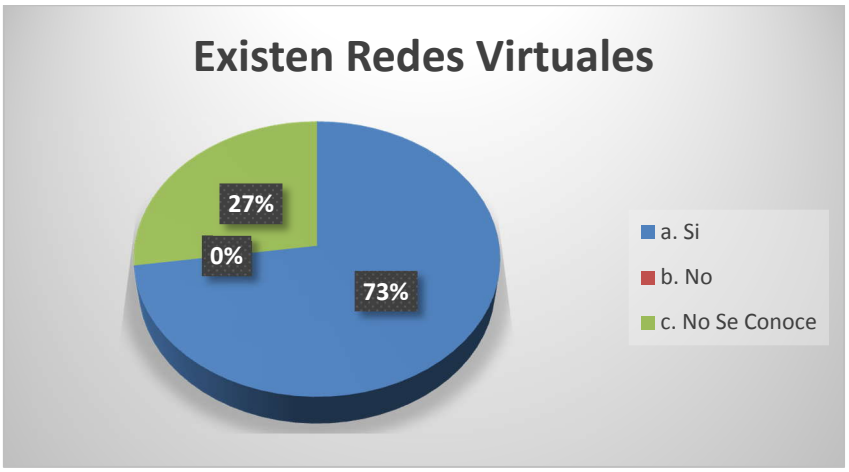


Figura 3.12 Existencia de Redes Virtuales.

Figura 3.13 Segmentación dividida por Áreas.

Figura 3.14 Existencia de Redes Virtuales para Invitados.

Se escogió una muestra de 22 personas del Edificio ALPALLANA, para que respondan la encuesta que se encuentra en el Anexo G, y se obtuvieron los siguientes resultados:

Figura 3.15 Disponibilidad de Acceso a la Red Inalámbrica.

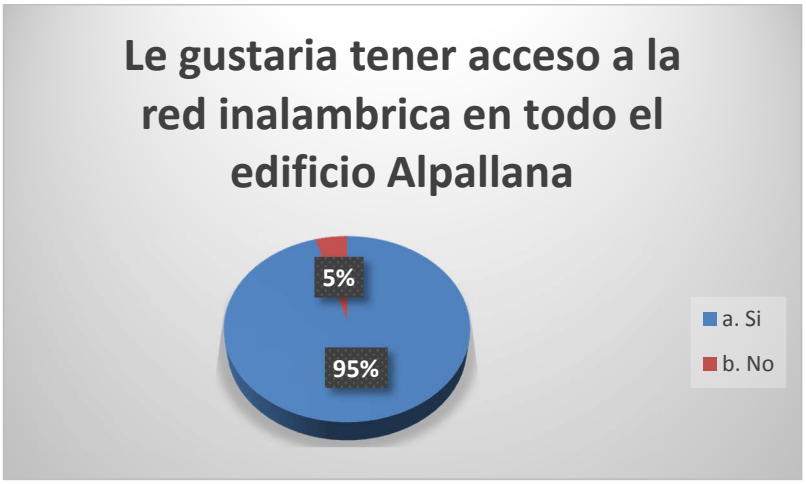


Figura 3.16 Acceso a la Red Inalámbrica.

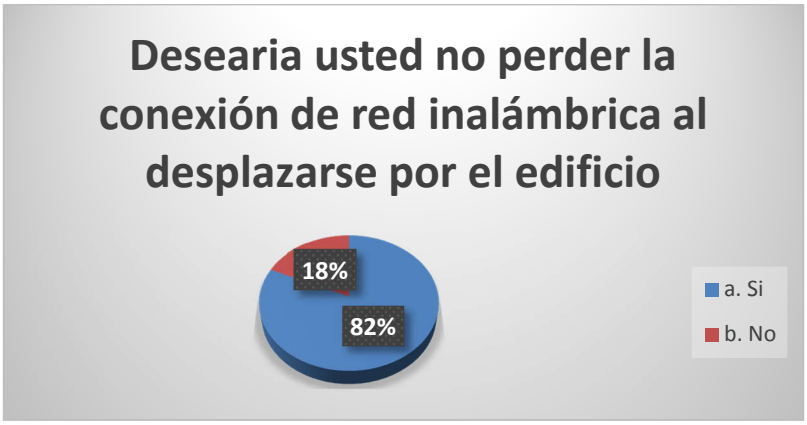


Figura 3.12 Movilidad con la Red Inalámbrica.

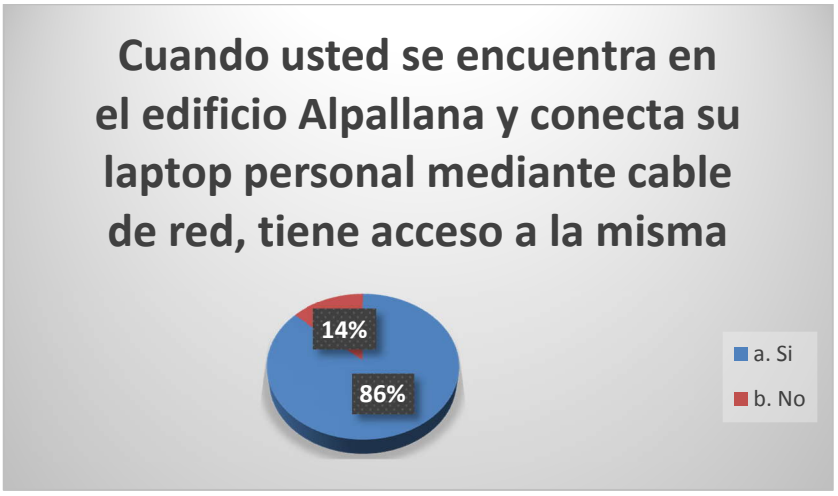


Figura 3.12 Existencia de Segmentación para Invitados.

Figura 3.12 Calidad de la Señal Inalámbrica.

El resultado de las encuestas es el siguiente:

- Que no pueden tener un conmutador preparado para cualquier emergencia, puesto que no se sabría cuál es el que se podría dañar.
- Que cualquier persona que ingrese un equipo adicional al de la empresa podría ingresar a la red de datos.
- Que no se tiene señal en todos los lugares del edificio ALPALLANA
- Que a los usuarios les gustaría conectarse a la red inalámbrica y no perder la señal si les toca movilizarse a otro sector del edificio

BIBLIOGRAFÍA CAPÍTULO 3

- [1] ConmutadorCISCO Catalyst 2950 http://www.cisco.com/en/US/products/hw/conmutadores/ps628/index.html
- [2]ConmutadorCISCO Catalyst 3550 http://www.cisco.com/en/US/products/hw/conmutadores/ps646/index.html
- [3] ConmutadorCISCO Catalyst 3560G PoE http://www.cisco.com/en/US/products/hw/conmutadores/ps5528/index.html

CAPÍTULO 4: Estudio para la Implementación de la tecnología de VLAN Dinámicas y Control inalámbrico

4.1 PROPUESTA DE SOLUCIÓN

4.1.1 Escalabilidad

La red de datos propuesta permitirá tener una escalabilidad de acuerdo a un crecimiento de 5 años, esto se debe a que los equipos de distribución utilizados son de tipo modular de acuerdo al modelo que será adquirido.

4.1.2 Disponibilidad

Con la implantación de la arquitectura de la VLAN's Dinámicas y el mejoramiento de la velocidad de transmisión de datos realizado por la creación de cableado estructurado con normas y estándares, la disponibilidad se mantendrá en un promedio de 99.98% debido a que únicamente sufrirán caídas de red por cambio de equipos de interconexión en el caso de existir este inconveniente en la parte de la red cableada.

Con la implementación de la parte inalámbrica se mejoraría la velocidad de transmisión debido a la mayor capacidad de radiación de los equipos inalámbricos, además de la disponibilidad de la señal que seguirán teniendo los usuarios en cualquier lugar del edificio ALPALLANA.

4.1.3 Seguridad

Con la implantación de la tecnología propuesta se conseguirá tener un mayor control de la red y de los equipos que se conectan a la misma, ya que se contaría con la creación de un archivo plano donde se generarán las tablas MAC y constarán todos los dispositivos. Por lo que a los equipos que no consten en ese rango de direcciones MAC se les asignaría una red de invitados, la misma que va a estar sin ningún permiso para ingresar a la red de datos de la empresa y sólo tendrán acceso a internet limitado, como se muestra en la Tabla 4.1 VLAN Propuesta y en la Tabla 4.2 Direccionamiento IP.

Tabla 4.1.

Tabla VLAN Propuesta.

VLAN	Nombre
2	SERVIDORES
4	PRESIDENCIA
5	GCI
7	AIN
8	GEF
9	GAD
10	SISTEMAS
11	CAP
13	GPA
14	ACP
17	VPNGYE
18	FILIALES
19	AULA
20	CÍRCULO
21	TELEFONÍA
22	ITT

Continua ⟶

24	DIS
25	TRA
26	AVQ
27	DYA
28	Video
29	ENLACES
30	Invitados

ESPACIO EN BLANCO
INTENCIONAL

Tabla 4.2.
Direccionamiento IP Propuesto.

VLAN	Red	Primera IP	Ultima IP	Brodcast	Mascara
10	172.19.110.0	172.19.110.1	172.19.110.254	172.19.110.255	/24
11	172.19.111.0	172.19.111.1	172.19.111.254	172.19.111.255	/24
19	172.19.112.0	172.19.112.1	172.19.112.254	172.19.112.255	/24
20	172.19.113.0	172.19.113.1	172.19.113.254	172.19.113.255	/24
21	172.19.114.0	172.19.114.1	172.19.114.254	172.19.114.255	/24
22	172.19.115.0	172.19.115.1	172.19.115.254	172.19.115.255	/24
24	172.19.116.0	172.19.116.1	172.19.116.254	172.19.116.255	/24
2	172.19.117.0	172.19.117.1	172.19.117.126	172.19.117.127	/25
	172.19.117.128	172.19.117.129	172.19.117.254	172.19.117.255	/25
5	172.19.118.0	172.19.118.1	172.19.118.62	172.19.118.63	/26
8	172.19.118.64	172.19.118.65	172.19.118.64	172.19.118.65	/26
9	172.19.118.128	172.19.118.129	172.19.118.190	172.19.118.191	/26
13	172.19.118.192	172.19.118.193	172.19.118.254	172.19.118.255	/26
14	172.19.119.0	172.19.119.1	172.19.119.62	172.19.119.63	/26
17	172.19.119.64	172.19.119.65	172.19.119.126	172.19.119.127	/27
4	172.19.119.128	172.19.119.129	172.19.119.158	172.19.119.159	/28
7	172.19.119.160	172.19.119.161	172.19.119.174	172.19.119.175	/28
25	172.19.119.176	172.19.119.177	172.19.119.190	172.19.119.191	/28
26	172.19.119.192	172.19.119.193	172.19.119.206	172.19.119.207	/28
27	172.19.119.208	172.19.119.209	172.19.119.222	172.19.119.223	/28
28	172.19.119.224	172.19.119.225	172.19.119.238	172.19.119.239	/28
29	172.19.119.240	172.19.119.241	172.19.119.242	172.19.119.243	/30
18	172.19.119.244	172.19.119.245	172.19.119.246	172.19.119.247	/30
30	192.168.1.0	192.168.1.1	192.168.1.254	192.168.1.255	/24

4.2 Diagrama Lógico

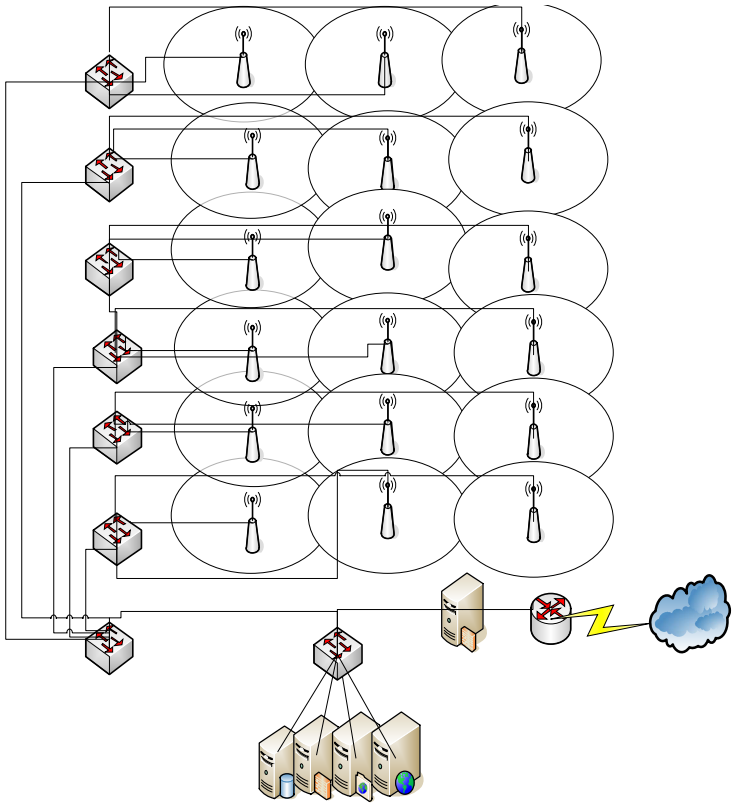


Figura 4.1. Mapa Estructural del Edificio ALPALLANA.

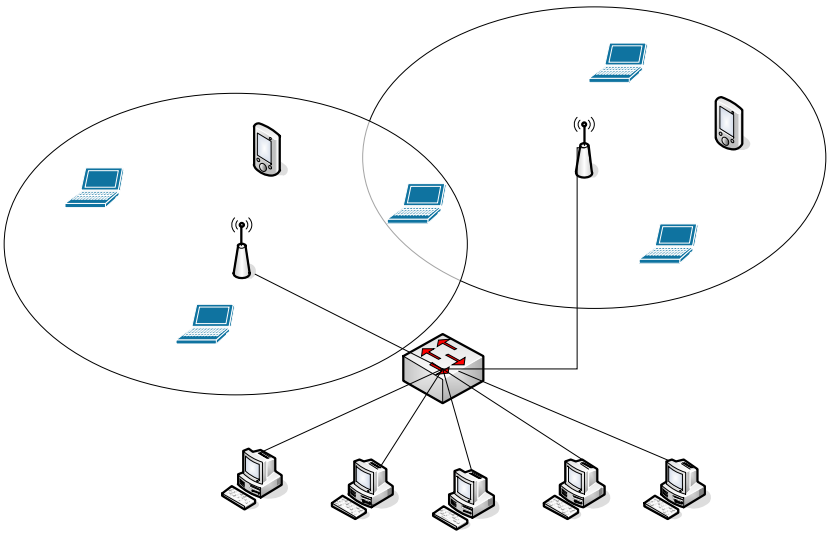


Figura 4.2. Diagrama Lógico Propuesto del Edificio ALPALLANA.

4.3 Diagrama Físico

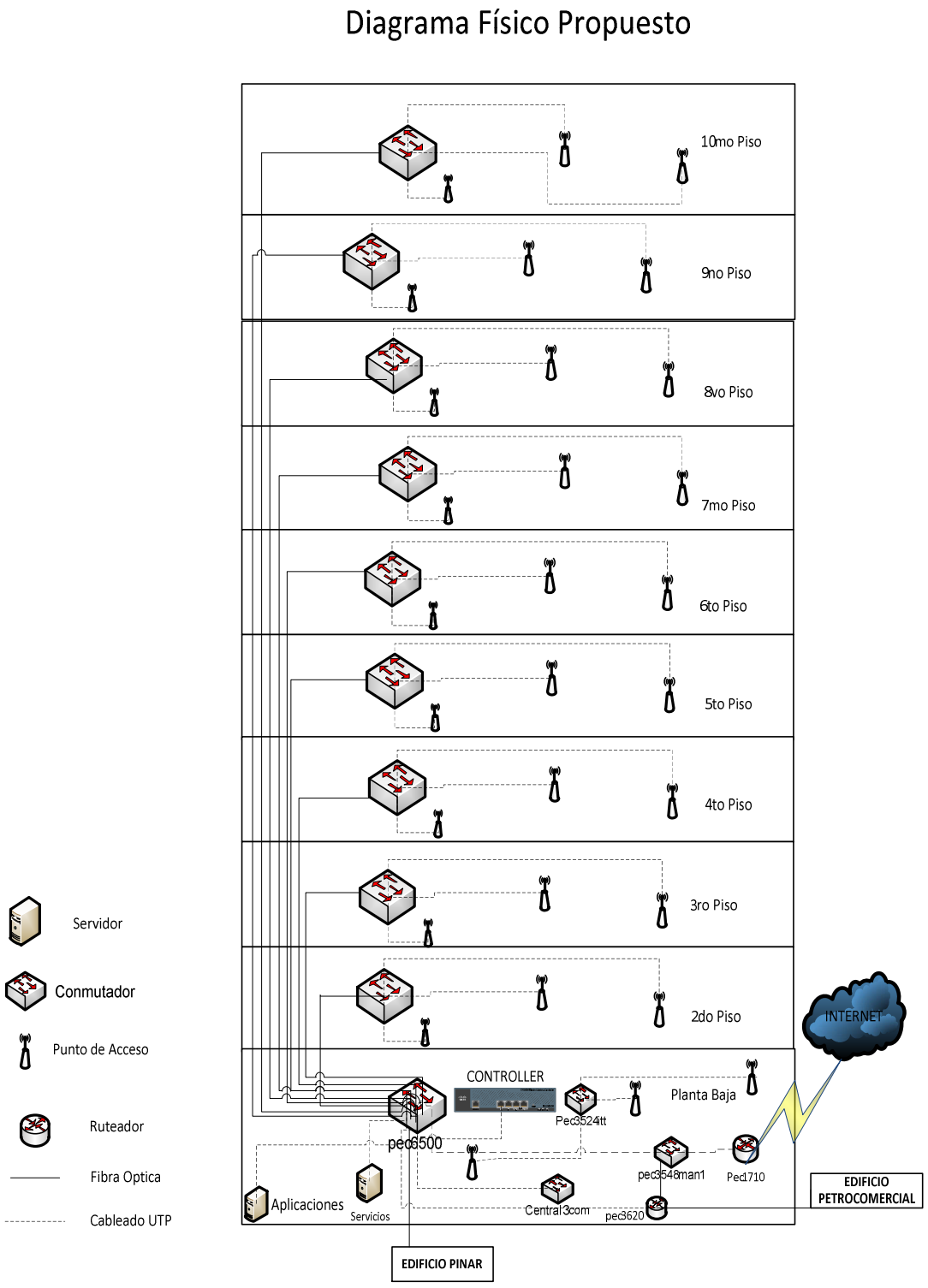


Figura 4.3. Diagrama Físico Propuesto del Edificio ALPALLANA.

Los planos donde se detalla la estructuración del diagrama físico de los puntos de acceso se encuentran en el Anexo E.

4.4 Configuración de los equipos Cisco para el funcionamiento de la tecnología DVLAN

Para el funcionamiento de las VLAN dinámicas es necesario configurar los conmutador de acceso y el conmutador central para habilitar las opciones del servidor de VMPS.

Servidor VMPS

Para configurar el servidor VMPS, se requiere ejecutar los siguientes comandos en el modo privilegiado del conmutador central:

- Especificar el método para descargar el archivo de configuración:
  - ✓ Set vmpsdownloadmethodtftp

- Configurar la dirección IP del servidor TFTP:
  - ✓ Set vmpsdownloadserver [dirección IP]

- Habilitar el servidor VMPS:
  - ✓ Set vmpsstateenable

- Verificar configuración:
  - ✓ Show vmps

Clientes VMPS

Para configurar un cliente VMPS ingrese al modo de configuración global del conmutador y ejecute los siguientes comandos:

- Configurar la dirección IP del servidor VMPS:
  Switch (config) #vmps server [dirección IP del servidor VMPS]

- Verificar la configuración a través del comando:
  Switch #Show vmps

Configuración de los puertos del conmutador que van a trabajar con asignación dinámica de VLAN's, con los siguientes comandos:

- Ingresar al modo de configuración de la interface:

Switch(config) #interface FastEthernet 0/1

- Cambiar el tipo de asignación de VLAN:

Switch(config-if) #switchport Access mode dynamic

- Habilitar STP (Spanning Tree Protocol)
  Switch(config-if) # spantreeportfast enable

4.5 Equipos Requeridos en Propuesta de Solución

Mediante conversaciones con el personal técnico del área, se consideró la opción de que todas las filiales de PETROECUADOR se unirían en un solo edificio administrativo, permitiendo una administración centralizada, así como un correcto desempeño, funcionalidad y administración de VLAN dinámicas, se deberá adquirir:

a. Conmutador Central

- ✓ Mínimo 20000 direcciones MAC, especificar máximo
- ✓ Soporte VMPS Server

- ✓ Módulo de 24 puertos Giga bit Ethernet
- ✓ Se necesita manejar de forma centralizada la creación, eliminación y edición de VLAN`s
- ✓ Cisco IOS® Software Release 12.2(18)SXF4

b. Para Administrar las Wireless se necesita adquirir:

- o Control inalámbrico Administrable compatible con el Conmutador Central.

- o El sistema Operativo del Control inalámbrico

4.6 ANÁLISIS ECONÓMICO

A continuación se podrá observar la información relacionada a los costos de algunos equipos a invertir en la implementación de la solución de VLAN´s dinámicas, el análisis está realizado con valores de fecha actual del mercado ecuatoriano.

COSTOS EN EQUIPAMIENTO

Para la implementación de la solución propuesta es necesaria la adquisición de varios equipos de interconexión, la información económica relacionada con los equipos fue obtenida a través de contacto personal, telefónico y correos electrónicos con algunas empresas, que de acuerdo a la nueva ley de Contratación Pública están debidamente registradas en el Ministerio de Industria y Competitividad.

La proforma de las herramientas adquiridas se puede observar en los anexos A y B.

Tabla 4.3.

Costo de hardware.

EQUIPO	CANTIDAD	VALOR UNITARIO	VALOR TOTAL	VIDA ÚTIL AÑOS
CONMUTADOR CENTRAL MODULAR	1	$ 152902	$ 152902	**5**
CONMUTADORDISTRIBUCIÓN	10	$ 15833	$ 158330	**5**
ACCESS POINT	30	$ 100	$ 3000	**5**
WIRELESS LAN CONTROLLER	1	$ 7917.25	$ 7917.25	**5**
			$ 322149.25	

Se ha considerado una vida útil de 5 años de acuerdo a la **Ley Orgánica de Administración Financiera y Control** "**LOAFIC"** por la cual se rigen las entidades públicas.

COSTO EN SOFTWARE

Se deberá adquirir un software que permita la administración centralizada a través de un solo equipo y software, por lo cual a continuación se detalla el software a adquirir.

Tabla 4.4.

Costo de software.

SOFTWARE	# LICENCIAS	VALOR UNITARIO	VALOR TOTAL
CONTROL INALÁMBRICOLER SYSTEM	1	$ 2197.25	$ 2197.25
			$ 2197.25

COSTO DE GESTIÓN, DISEÑO E IMPLEMENTACIÓN

Tabla 4.5.

Costo de gestión, Diseño e Implementación.

DESCIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
INGENIERO DE PROYECTOS	1	$ 4000	$ 4000
TÉCNICO ESPECIALISTA	4	$ 1500	$ 6000
			$ 10000

COSTO TOTAL

Tabla 4.6.

Costo Total.

DESCRIPCIÓN	VALOR TOTAL
HARDWARE	$ 322149.25
SOFTWARE	$ 2197.25
GESTION, DISEÑO E IMPLEMENTACIÓN	$ 10000.00
	$ 334,346.50

El Costo puede variar al año de implementación tomando en cuenta un 5% de inflación anual

4.7 Configuración de puntos de acceso

Establecimiento de AP prioridad de conmutación por error

Cuando un controlador falla, el controlador de copia de seguridad configurado para el punto de acceso, de repente recibe un número de peticiones y se une a las peticiones. Esto puede causar que el controlador llegue a un punto de saturación y rechace algunos de los puntos de acceso.

Mediante la asignación de prioridad a un punto de acceso, que tienen cierto control sobre los puntos de acceso que son rechazados.

En una situación de conmutación por error, cuando el controlador de seguridad está saturado, los puntos de mayor prioridad de acceso pueden unirse al controlador de seguridad por los puntos de menor prioridad de acceso.

Para configurar los ajustes de prioridad para los puntos de acceso, primero debe activarse la función de Prioridad AP, para permitir la función de prioridad de AP, siga estos pasos:

Paso1 Elija **Configure** >**Controllers**.

Paso2 Haga clic en la dirección IP del controlador correspondiente.

Paso3 En el menú lateral izquierdo, seleccione **System**>**General**.

Paso4 De la prioridad de conmutación por error de AP en el menú desplegable, seleccione **Enable**.

Configuración de las credenciales mundial de puntos de acceso

Los puntos de acceso autónomos por defecto permiten contraseña.

Esta contraseña permite a los usuarios iniciar en el modo sin privilegios y ejecutar comandos ***show*** y ***debug***, planteando una amenaza a la seguridad. La contraseña por defecto permitirá ser cambiada para evitar accesos no autorizados y permitir a los usuarios para ejecutar comandos de configuración del puerto de consola del punto de acceso.

En el WCS y el software del controlador de versiones anteriores a la 5.0, se puede establecer, en el punto de acceso que permite la contraseña, solo para puntos de acceso que están conectados al controlador. En la versión de software WCS y el controlador 5.0, se puede configurar un nombre de usuario global y contraseña, permite para todos los puntos de acceso, ya que heredan unirse a un controlador. Esto incluye todos los puntos de acceso que están unidos al controlador y que cualquiera pueda unirse en el futuro. Cuando se le añade un punto de acceso, también puede optar por aceptar esta iniciativa mundial, nombre de usuario y contraseña o anular sobre una base por punto de acceso y asignar un nombre de usuario, contraseña y activar contraseña. También en el controlador de software versión 5.0, después de que un punto de acceso se une al controlador, el punto de acceso permite a

los puertos de consola de seguridad, y se le pedirá su nombre de usuario y contraseña cada vez que inicie sesión en el punto de acceso al puerto de consola. Al iniciar una sesión, usted está en el modo sin privilegios, y se debe introducir **enable password** para poder utilizar el modo privilegiado.

Estos controladores de software versión 5.0, se caracterizan porque son compatibles con todos los puntos de acceso que se han convertido de modo ligero, excepto la serie 1100. Puntos de acceso VxWorks no son compatibles.

Las credenciales mundiales que se configuran en el controlador se conservan a través del controlador y punto de acceso que se reinicia. Se sobrescribe solo si el punto de acceso se une a un nuevo controlador que está configurado con un nombre de usuario y contraseña global. Si el nuevo controlador no está configurado con las credenciales de nivel mundial, el punto de acceso conserva el nombre de usuario y contraseña global configurada para el primer controlador.

Es necesario un seguimiento cuidadoso de las credenciales utilizadas por los puntos de acceso. De lo contrario, podría no ser capaz de entrar en un puerto de consola del punto de acceso. Si es necesario, puede borrar la configuración del punto de acceso para devolver el nombre de usuario y la contraseña del punto de acceso a la configuración predeterminada.

Siga estos pasos para establecer un nombre de usuario y contraseña global:

Paso 1 Elija **Configure**>**Controllers** o **Configure**>**Access Point.**

Paso 2 Elija una dirección IP de un controlador con versión de software 5.0 o posterior, o escoja un punto de acceso que esté asociado con el software versión 5.0 o posterior.

Paso 3 Seleccione **System**> AP **UserName Password** en el menú lateral

izquierdo (véase en la figura 4.4). Con su respectivo nombre de usuario y contraseña que esté establecido.

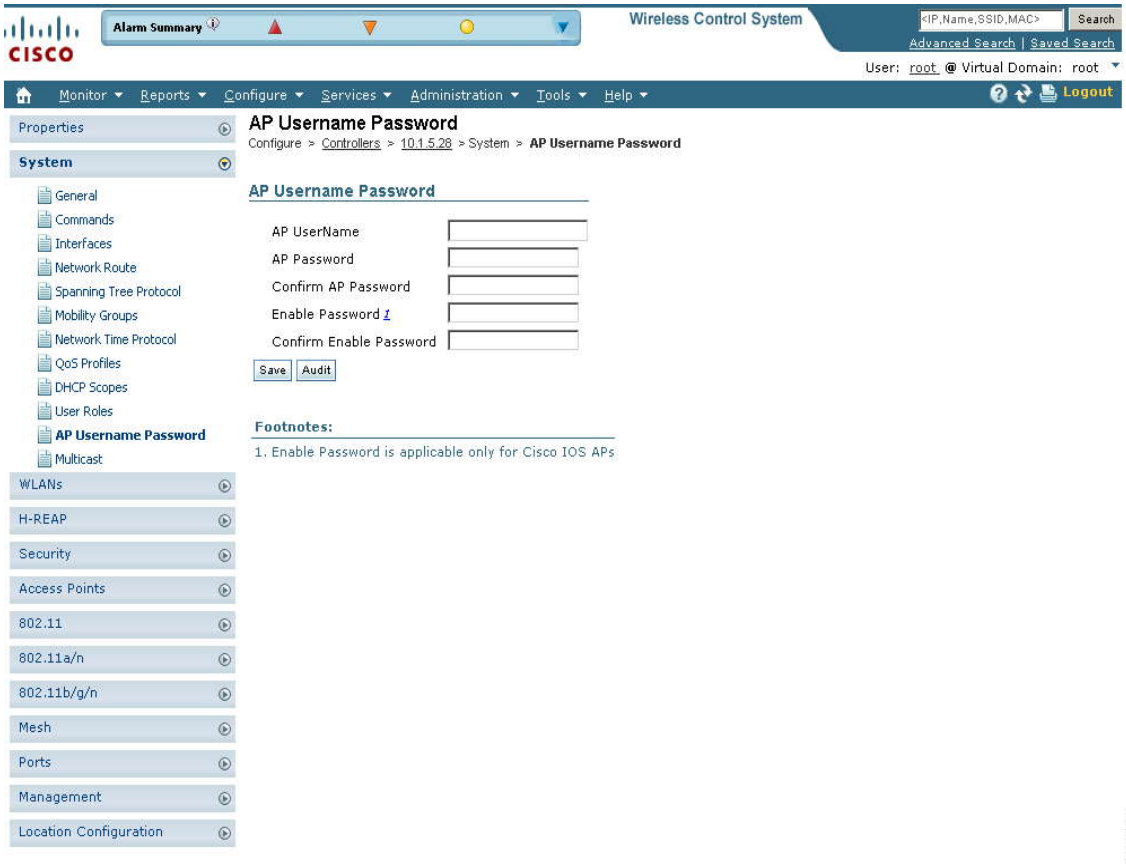


Figura 4.4 Ventana APUsernamePassword.

Paso 4 En el campo *Nombre de AP*, introduzca el nombre que va a ser heredado por todos los puntos de acceso que unen a los controladores.

Paso 5 En el campo *Contraseña AP*, introduzca la contraseña que va a ser heredada por todos los puntos de acceso que unen a los controladores. Volver a entrar en el campo *Confirmar contraseña AP*.

Paso 6 Para los puntos de acceso autónomos Cisco, también debe escribir y confirmar una contraseña de activación.

En el AP se habilita el campo *Contraseña*, introduzca la contraseña de activación que se heredan todos los puntos de acceso que unen a los controladores. Volver a entrar en el campo donde se confirmar la contraseña y actívela.

Paso 7 Haga clic en **Save**.

Configuración de Ethernet Bridging y etiquetado de VLAN Ethernet

Puente Ethernet se utiliza en dos escenarios de red:

1. Punto a punto y punto a multipunto, puente entre mapas (paquetes sin etiqueta). Una típica aplicación de trunking podría superar el tráfico entre edificios en un campus (véase figura 4.5).

No es necesario configurar el etiquetado VLAN para utilizar puente Ethernet para punto a punto y punto a multipunto.

ESPACIO EN BLANCO
INTENCIONAL

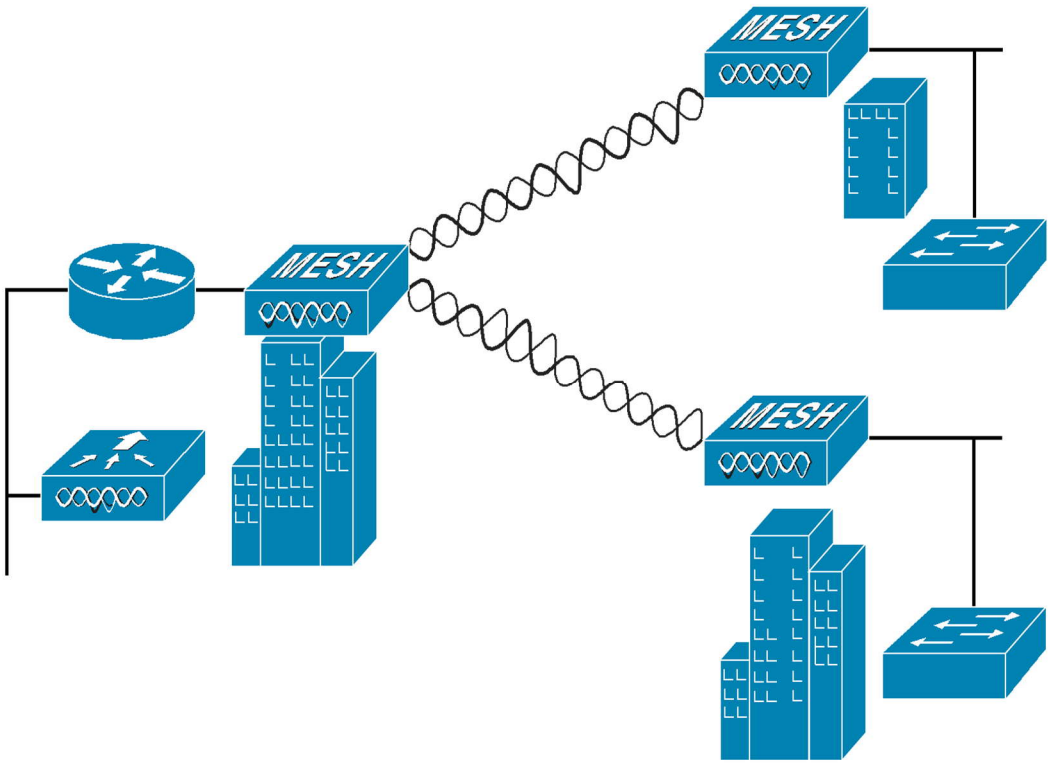


Figura 4.5 Puente Punto a punto y punto-a-multipunto.

2. Etiquetado VLAN Ethernet permite el tráfico de aplicaciones específicas para segmentos dentro de una malla inalámbrica y remitido (puente) a una LAN alámbrica (modo de acceso) o un puente a otro inalámbrico de malla de red (modo de troncalizado).

Una aplicación típica de la seguridad de acceso público a través de Ethernet etiquetado VLAN, es la colocación de cámaras de video de vigilancia en varios lugares al aire libre dentro de la ciudad. Cada una de estas cámaras de video tiene un cable de conexión con un mapa. El video se transmite a través de la red de retorno inalámbrica a un puesto de mando central en una red cableada (véase figura 4.6).

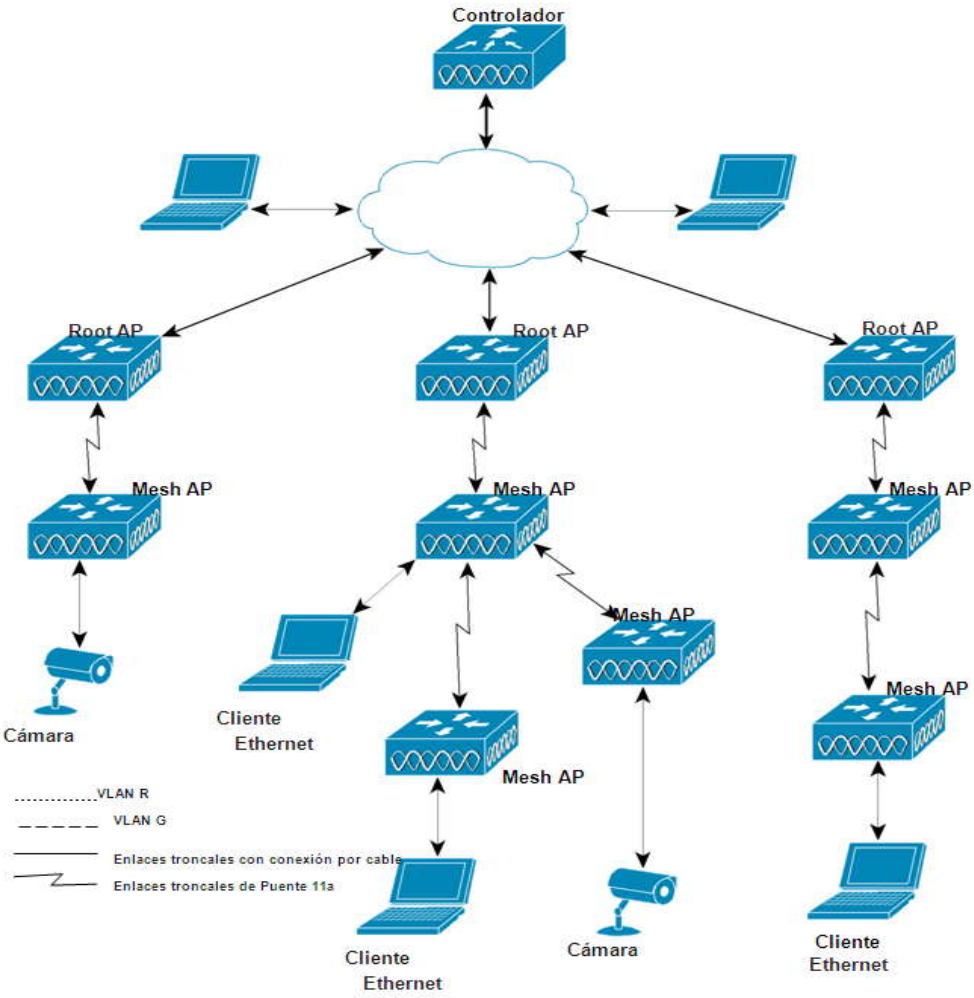


Figura 4.6. Etiquetado de VLAN Ethernet.

Directrices Ethernet VLAN Tagging

• Por razones de seguridad, el puerto Ethernet de un punto de acceso de malla (RAP y MAP) está desactivado por defecto. Se habilita mediante la configuración de Ethernet Bridging en el puerto de malla de punto de acceso.

• Se debe habilitar el puente Ethernet en todos los puntos de acceso en la red de malla para permitir Ethernet VLAN Tagging para operar.

• Debe establecer el modo de VLAN como no-VLAN transparente (parámetro de malla mundial).

VLAN transparente está activada por defecto. Para establecer la no-VLAN transparente, debe desmarcar la opción VLAN transparente en la Malla Global de la ventana de parámetros.

• Configuración de VLAN en un punto de acceso de malla, solo se aplica si todos los puntos de acceso de enlace ascendente de la malla son capaces de soportar esa VLAN.

- Mesh AP
- Controller
- VLAN R
- VLAN G
- Wired trunk links
- 11a bridge trunk links
- Ethernet
- client
- Ethernet
- Camera client
- Camera
- Ethernet
- client
- Root AP Root AP Root AP
- Mesh AP Mesh AP
- Mesh AP
- Mesh AP
- Mesh AP

Configuración de Ethernet Bridging y etiquetado VLAN Ethernet

Si los puntos de enlace ascendente de acceso no son capaces de soportar la VLAN, entonces la configuración se guarda en lugar que aplica.

El etiquetado de VLAN solo se puede configurar en las interfaces Ethernet.

- En 152X puntos de la malla de acceso, se hace uso de tres de los cuatro puertos secundarios interfaces Ethernet: puerto0-PoE, 1 puerto PoE a cable, y el puerto 3 - fibra. No se puede configurar el puerto 2 - cable como Interfaz secundaria Ethernet.

- En el etiquetado VLAN Ethernet, puerto 0-PoE en el RAP se conecta al puerto del tronco del interruptor de la red cableada. Puerto 1-PoE en el mapa conecta dispositivos externos tales como videocámaras.

• Interfaces de Backhaul (802.11a radios) actúan como principales interfaces Ethernet. Viajes de regreso funcionan como troncos en la red y llevan todo el tráfico de VLAN entre la red inalámbrica y por cable.
No se requiere para configurar la interfaz principal de Ethernet.

• Debe configurar el puerto del conmutador en la red que está conectada a la RAP (puerto 0-PoEin) para que acepte paquetes etiquetados por su puerto de enlace troncal. El PAR envía todos los paquetes recibidos de la red de malla etiquetada a la red cableada.

• No es necesaria dentro de la red de malla la configuración para apoyar el etiquetado VLAN en la red de retorno 802.11a interfaz Ethernet.

- Esto incluye el RAP puerto de enlace ascendente Ethernet. La configuración necesaria se realiza automáticamente utilizando un mecanismo de registro.

- Cualquier cambio de configuración de un enlace Ethernet 802.11 actuando como un backhaul se ignora, y uno de los resultados de advertencia. Cuando el enlace Ethernet ya no funciona como una red de retorno, la modificación y la configuración se aplican.

• No se pueden configurar las VLAN's en el puerto del módem-02-cable de un punto de acceso 152X. Configurar VLAN en los puertos 0 (PoE-in), 1 (PoE-out), y 3 (de fibra).

• Si un puente entre dos mapas, se introduce la distancia (de malla) entre los dos puntos de acceso que están tendiendo un puente. (No se emplea a las aplicaciones en las que se reenvíe el tráfico conectado a la MAP para el PAR en el modo de acceso).

• Cada sector admite hasta 16 VLAN's, por lo tanto, el número acumulado de las VLAN con el apoyo del RAP (MAP) no puede exceder de 16.

• Los puertos de Ethernet en los puntos de acceso funcionan como de costumbre, el acceso o los puertos troncales en un despliegue de marcado Ethernet.

- **Modo normal**: En este modo, la interfaz Ethernet VLAN es transparente por defecto y no acepta o envía paquetes etiquetados. Tramas etiquetadas de los clientes. Las tramas sin etiquetase remiten a la VLAN nativa en el puerto de enlace troncal RAP.

- **Modo de acceso**: En este modo solo los paquetes sin etiquetar son aceptados. Debe etiquetar todos los paquetes con una VLAN configurada por el usuario llamado access-VLAN. De este modo para entrar en vigor, la VLAN debe ser *no-VLAN* transparente.

Utilice esta opción para aplicaciones en las que se recoge información de los dispositivos conectados al MAPA como cámaras o computadoras y remitido a la RAP. El PAR se aplica etiquetas y reenvía el tráfico a un conmutador en la red cableada.

- **Modo troncal:** Este modo requiere que el usuario configure una VLAN nativa, una VLAN permite listas (no por defecto). En este modo, paquetes con etiqueta y sin etiqueta son aceptados. Usted puede aceptar paquetes sin etiquetas y con etiquetas con la VLAN nativa especificada por el usuario. Puede aceptar etiquetado de paquetes si están etiquetados con una VLAN en la lista de permitidos VLAN. De este modo la VLAN debe ser *no-VLAN* transparente.

Utilizando esta opción para aplicaciones de transición como el reenvío de tráfico entre los dos mapas de residente en edificios separados dentro de un campus.

- El puerto del conmutador conectado a la RAP debe estar troncalizado.
- El puerto de trunk en el conmutador y el puerto RAP troncalizado deben coincidir.
- Una configuración de VLAN en un puerto Ethernet MAPA no puede funcionar como una VLAN de administración.
- El PAR siempre debe conectarse a la VLAN nativa (ID 1) en un switch.
- Interfaz principal del PAR Ethernet por defecto es la VLAN nativa de 1.

Habilitación de Ethernet Bridging y VLAN Tagging.

Se procede a estos pasos para habilitar Ethernet Bridging y etiquetado VLAN en un RAP o MAP.

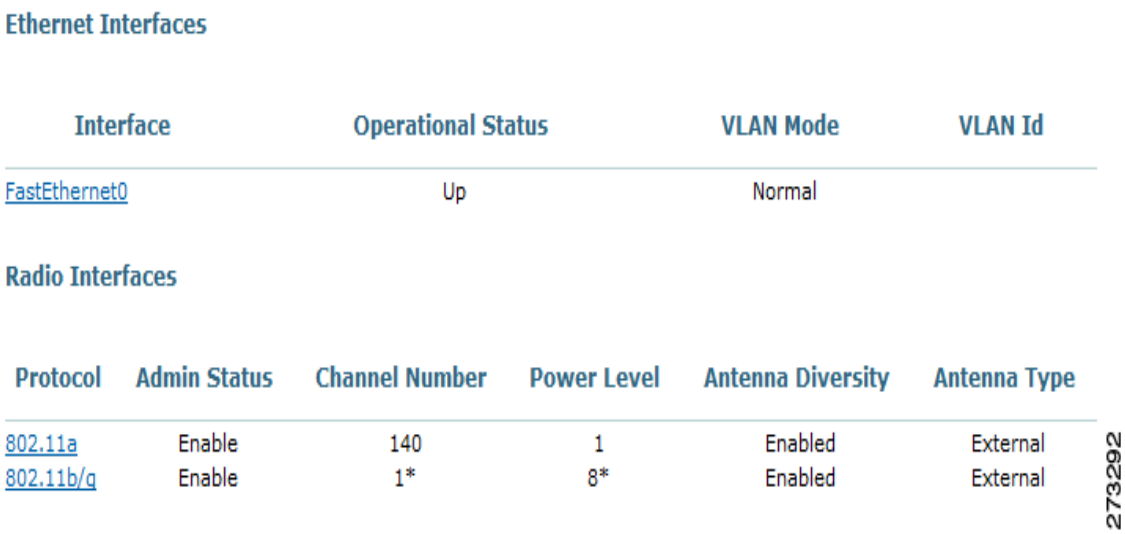
Paso 1 Elija **Configure**>**Access Point**.

Paso 2 Haga clic en el nombre del punto de acceso de malla para el Ethernet puente que desea habilitar. Aparece una configuración ventana del punto de acceso.

Paso 3 En la sección de información de enlace, seleccione la tasa de retorno adecuado de la velocidad de datos desplegable del menú. El valor por defecto es de 24 Mbps para la interfaz de red de retorno 802.11a.

Paso4 En la sección de información de enlace, seleccione **Enable** en el menú desplegable del Ethernet Bridging.

Paso5 Haga clic en el enlace de interfaz Ethernet correspondiente (por ejemplo, FastEthernet o gigabitEthernet1) (véase la figura 4.7).



Ethernet Interfaces

Interface	Operational Status	VLAN Mode	VLAN Id
FastEthernet0	Up	Normal	

Radio Interfaces

Protocol	Admin Status	Channel Number	Power Level	Antenna Diversity	Antenna Type
802.11a	Enable	140	1	Enabled	External
802.11b/g	Enable	1*	8*	Enabled	External

273292

Figure 4.7 Configuración >Punto de acceso> ventana AP Nombre.

Paso 6 Haga clic en AccessPoint>EthernetInterfaceWindow

Figure 4.8 AccessPoint>EthernetInterfaceWindow.

Las opciones de configuración pueden variar para cada uno de los modos de la VLAN (el acceso normal y el tronco).

a. Si va a configurar un MAPA y los puertos RAP normal y eligió FastEthernet0, elija modo Normal de la VLAN en el menú desplegable. En este modo, la interfaz Ethernet VLAN transparente por defecto, no acepta o envía etiquetado de paquetes. Tramas etiquetadas de los clientes se dejan caer. Las tramas sin etiqueta son enviadas a la VLAN nativa en el puerto de enlace troncal RAP.

b. Si está configurando un puerto de acceso MAPA y eligió gigabitEthernet1 (puerto PoE de 1 out).

1. Elija **Access** de la VLAN en el menú desplegable.

2. Introduzca una ID de VLAN. El ID de VLAN puede ser cualquier valor entre 1 y 4095.

3. Haga clic en **Save**.

VLAN ID 1 no está reservada para la VLAN por defecto.

c. Si va a configurar una RAP o puerto troncal MAPA y eligió gigabitEthernet0 (o FastEthernet0), (Puerto 0-PoE).

1. Elija **Trunk** de la lista desplegable de VLAN del menú.

2. Introduzca un ID de VLAN nativa para el tráfico entrante. La VLAN ID nativa puede ser cualquier valor entre1 y 4095. No asigna ningún valor a una VLAN de usuario (el acceso).

3. Introduzca un ID de VLAN troncalizada para el tráfico saliente y haga clic en **Add**.

Si el reenvío de paquetes sin etiquetas, no cambia el ID de la VLAN troncalizada de valor de cero (por ejemplo, como puente MAP-a-MAP, el medio ambiente del campus).

En el reenvío de paquetes etiquetados, introduzca un ID de VLAN (1 a 4095) que no esté ya asignado (por ejemplo, como RAP para cambiar la red de cable).

Para eliminar una VLAN de la lista, haga clic en **Delete**.

4. Haga clic en **Save**.

Nota Por lo menos un punto de acceso de mallas se debe establecer RootAp en la red de malla.

Configuración de puntos de acceso

Elija **Configure**>**Access Point** para ver un resumen de todos los puntos de acceso en la base de datos de Cisco WCS.

La información de resumen incluye lo siguiente:

• Ethernet MAC

• Dirección IP

• Radio

• Mapa de Ubicación

• Tipo de AP

• Controlador

• Estado de la operación

• Alarma de estado

• Auditoría de Estado

Nota Si se ciernen sobre el valor de estado de auditoría, el tiempo de la última auditoría se muestra.

Paso 1 Haga clic en el enlace situado bajo Nombre de AP para ver información detallada acerca de que el nombre de punto de acceso (véase en la figura 4.9).

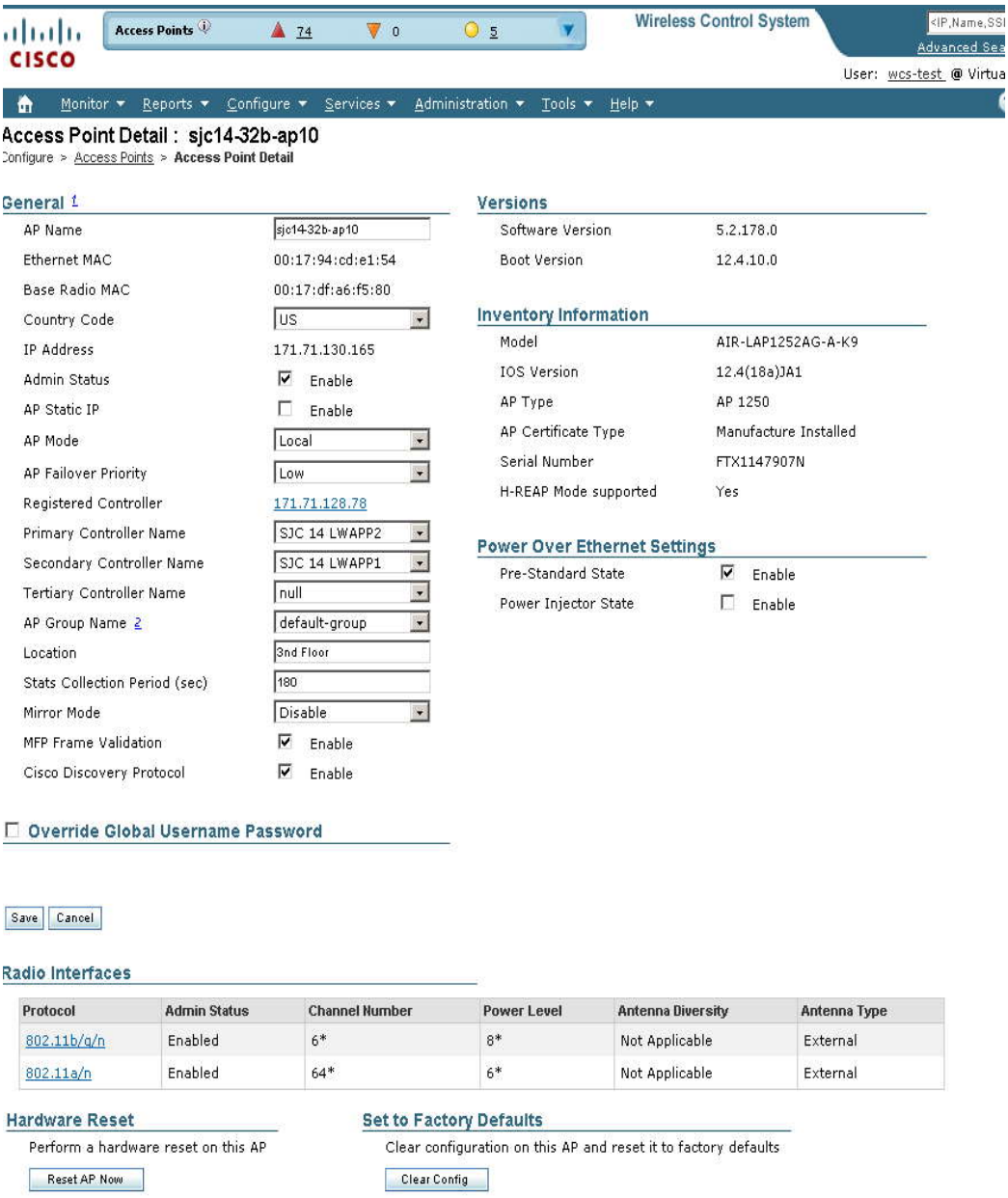


Figure 4.9 Información a detalle del punto de acceso

El software del sistema operativo detecta automáticamente y se añade un punto de acceso a la WCS Cisco base de datos, ya que se asocia con los controladores existentes en la base de datos de Cisco WCS.

Tenga en cuenta los parámetros del punto de acceso puede variar según el tipo de punto de acceso.

Algunos de los parámetros de la ventana se rellenan automáticamente.

• La parte general se muestra en el MAC Ethernet, la dirección MAC de Radio

Base, la dirección IP y el estado.

• La parte de las versiones de la ventana muestra la versión de software y de
• La parte de la información de inventario muestra el modelo, tipo AP, tipo de certificado, número de serie, y obtener el apoyo de modo.
• La parte de Radio Interfaces proporciona el estado actual de las radios 802.11a / n y 802.11b/g/n como el estado de administración, número de canal, potencia, modo de antena de diversidad de antenas y el tipo de antena.

El cambio de los parámetros del punto de acceso hace que el punto de acceso se desactive temporalmente y algunos clientes podrían perder la conectividad.

Paso 2 Introduzca el nombre asignado al punto de acceso.

Paso 3 Use el menú desplegable para elegir un código de país para establecer el apoyo de múltiples países. Los puntos de acceso están diseñados para su uso en muchos países con distintos requisitos reglamentarios. Se puede configurar un código de país para asegurar que el punto de acceso cumple con las regulaciones de su país:

• Puede configurar hasta 20 países por controlador.

• Debido a que solo un Auto-RF del motor y una lista de canales disponibles existentes, la configuración de múltiples países, los límites de los canales disponibles para Auto-RF en los canales comunes. Un canal común, que es legal en el país y configurado.

• Al configurar los puntos de acceso para varios países, los canales de Auto-RF se limitan a la mayor potencia disponible en todos los países que está configurado el nivel. Un punto de acceso puede establecer superar estas limitaciones (o de forma manual puede ajustar los niveles por encima de esos límites), pero con Auto-RF no se selecciona automáticamente un canal no común o elevar el nivel de poder más allá que en todos los países.

Paso 4 Si desea habilitar el punto de acceso para fines administrativos, marque la casilla de verificación **Enable**.

Paso 5 Si hace clic en **Enable** en la casilla de verificación la IP estática del AP, una dirección IP estática siempre se le asigna al punto de acceso en lugar de obtener una dirección IP de forma dinámica en el arranque.

Paso 6 Seleccione la función del punto de acceso desde el menú desplegable. No es necesario reiniciar después de que el modo es cambiado, excepto cuando el modo en el monitor. Que se le notifique el reinicio al hacer clic en **Save**. Los modos disponibles son los siguientes:

• **Local**: Esta es la operación normal del punto de acceso y la opción por defecto del modo AP. Con este modo, los clientes de datos son atendidos mientras que los canales configurados son analizados en busca de ruido. El punto de acceso se va de canal de 50 ms. que completa un ciclo a través de cada canal para el período especificado en la configuración RF Auto.

• **H-REAP**: Elija H-REAP desde el modo de AP en el menú desplegable para permitir REAP híbrido para un máximo de seis puntos de acceso. Los puntos de acceso H-REAP del cliente puede cambiar el tráfico de datos a nivel local y realizar la autenticación del cliente a nivel local cuando su conexión con el controlador se ha perdido.

• **Monitor**: Este es el modo de recepción de radio y sólo permite que el punto de acceso configurado analice todos los canales cada 12 segundos. Solo los paquetes que se envían de autenticación en el aire con un punto de acceso configurado de esta manera. A modo de punto de acceso de monitor detecta, pero no puede conectarse a un **rogue** sospechoso como un cliente para prepararse para el envío de paquetes RLDP.

Puede ampliar el modo de monitor de etiquetas para incluir cálculo de la ubicación, permitiendo el seguimiento de monitor de modo optimizado (TOMM). Cuando es activado, puede especificar los cuatro canales en la banda de 2,4 GHz (802.11b / g de radio) de un punto de acceso utilizado para controlar las etiquetas. Esto le permite concentrarse en las exploraciones del canal, solo los canales de las etiquetas que se encuentran tradicionalmente (como los canales 1, 6 y 11) en su red. Para permitir que TOMM, también deberá realizar ediciones adicionales en la radio 802.11b / g del punto de acceso.

Para configurar los puntos de acceso de Cisco WIPS adaptable, seleccione **Monitor**. Elija **Enhanced WIPS Engine Enabled**y seleccione **WIPS** desde el modo de monitorización desplegable del menú.

Antes de poder habilitar un punto de acceso que esté en el modo WIPS, debe deshabilitar los radios del punto de acceso. Si no desactiva el punto de acceso inalámbrico, aparecerá un mensaje de error. Después de que han permitido que el punto de acceso WIPS, volverá a habilitar las radios.

• **Detector de Rogue**: En este modo, el punto de acceso inalámbrico está apagado y el punto de acceso detecta el tráfico solamente por cable. Los controladores que operan en este modo de monitorear los puntos de acceso no autorizados. El controlador envía todos los puntos de acceso no autorizado y al cliente las listas de direcciones MAC para el detector. La lista de direcciones MAC se compara con lo que los puntos de acceso WLC espera. Si las

direcciones MAC concuerdan, se puede determinar qué puntos de acceso están conectados a la red cableada.

•**Sniffer**: Funcionamiento en modo sniffer captura el punto de acceso y envía todos los paquetes sobre un determinado canal a una máquina remota que se ejecuta Airopeek. Estos paquetes contienen información como marca de tiempo, intensidad de la señal, tamaño del paquete y así sucesivamente. Esta función solo puede activarse si se ejecuta Airopeek, que es un software analizador de red de terceros que soporta la decodificación de los datos paquetes.

• **Puente-Puente:** Es un modo especial donde funciona un punto de acceso autónomo como una red inalámbrica cliente y se conecta a un punto de acceso ligero. El puente y sus clientes de cable se enumeran como cliente WCS en si el modo de AP está en el puente y el punto de acceso es el puente capaz.

Paso 7 Desactive los radios de punto de acceso.

Paso 8 Dé prioridad de conmutación por error de AP en el menú desplegable, seleccione Bajo, Medio, Alto o críticos para indicar el acceso prioritario a punto de conmutación por error. La prioridad predeterminada es baja.

Paso 9 En el campo controlador primario, secundario y superior, se puede definir el orden en que los controladores se accede.

Paso 10 El nombre del grupo AP desplegable muestra todos los nombres de punto de acceso de grupo que se han definido mediante WLAN>AP Grupo de VLAN, puede especificar si este punto de acceso está ligado a ningún grupo.

En un punto de acceso con el nombre del grupo de 31 caracteres para las versiones anteriores de WLC 4.2.132.0 y 5.0.159.0.

Paso 11 Introduzca una descripción de la ubicación física donde se encuentra el punto de acceso.

Paso 12 En el período del parámetro de Estadísticas de la colección, entre la hora en la que el punto de acceso envía estadísticas a 0,11 al controlador. El rango válido es de 0 a 65535 segundos. El valor 0 significa que las estadísticas no deben ser enviadas.

Paso 13 Seleccione **Enable** para el modo de espejo, si desea duplicar (a otro puerto) todo el tráfico de origen se termina en un único dispositivo cliente o punto de acceso. Modo de espejo es útil en el diagnóstico específico de problemas en la red pero solo debe ser activada en un puerto no utilizado desde cualquier conexión a este puerto hasta que deje de responder.

Paso 14 Usted puede configurar en un controlador de impresora multifunción. Cuando lo haga, la gestión de la protección del marco y validación están habilitadas por defecto para cada punto de acceso que se unió, y es la autenticación automática de punto de acceso desactiva. Después de MFP es habilitado en un controlador, puede desactivar y volver a habilitar para cada WLAN y puntos de acceso.

Si hace clic para activar MFP marco de validación, tres funciones principales se realizan:

• **Gestión marco de protección:** Cuando la protección está activada la gestión de marco, el punto de acceso protege a los marcos de gestión que transmite mediante la adición de una integridad de los mensajes de información de verificación elemento (MICIE) para cada fotograma. Cualquier intento de copiar, modificar, reproducir o invalida el marco del MICEC, causando los puntos de acceso de recepción que se han configurado para detectar paquetes MFP al informe de la discrepancia.

• **Gestión marco de la validación**: Cuando la validación de la gestión de cuadro está activada, el punto de acceso valida todos los marcos de gestión que recibe de otros puntos de acceso en la red. Cuando el originador está configurado para transmitir tramas MFP, el punto de acceso se asegura de que la MICIE está presente y coincide con el contenido del marco de gestión. Caso de recibir una trama que no contiene una MICIE válida, los informes de la discrepancia con el sistema de gestión de red. Con el fin de este informe de discrepancia, el punto de acceso debe estar configurado para transmitir tramas MFP. Del mismo modo, para el marcas de tiempo para funcionar correctamente, todos los controladores de red debe ser **Transfer Protocol** (NTP) sincronizadas.

Paso 15 Haga clic en **Cisco Discovery Protocol** si desea activarla. CDP es una búsqueda de protocolos de dispositivos que se ejecutan en todos los equipos de Cisco-manufacturados, tales como ruteadores, puentes y servidores de comunicación. Cada dispositivo envía periódicamente mensajes a una dirección de multidifusión y escucha los mensajes que otros envían con el fin de aprender acerca de los dispositivos vecinos. Cuando se inicia el dispositivo, se envía un paquete CDP y especifica si el dispositivo es de alimentación en línea habilitado para que la potencia solicitada pueda ser suministrada.

El cambio de los parámetros del punto de acceso desactiva temporalmente un punto de acceso y podría resultar en la pérdida de la conectividad a algunos clientes.

Paso 16 Seleccione **enable rogue detection**.

La detección Rogue se desactiva automáticamente en los puntos de acceso **OfficeExtend** porque los puntos de acceso que se despliegan en un ambiente en el hogar, probablemente detecten un gran número de falsos dispositivos.

Paso 17 Marque **Encryption** para habilitar la encriptación.

Activar o desactivar la funcionalidad de cifrado hace que el punto de acceso reinicie el sistema, que a su vez hace que los clientes pierdan conectividad.

DTLS cifrado de datos se activa automáticamente los puntos de acceso para mantenerla seguridad de OfficeExtend. Solo está disponible si el punto de acceso está conectado a 5,500 controladores de la serie con una licencia más.

Paso 18 Si la detección de puntos está activada, el punto de acceso inalámbrico está apagado y el punto de acceso escucha por cable solo el tráfico. Los controladores que operan en este modo de monitorear los puntos de acceso no autorizados. El controlador envía todos los puntos de acceso no autorizados y al cliente la dirección MAC de la lista para el detector, y el detector de **rogué** remite esta información a la WLC. La lista de direcciones MAC se compara con lo que los puntos de acceso WLC espera. Si las direcciones MAC concuerdan, se puede determinar que los puntos de acceso están conectados en la red cableada.

Paso 19 Seleccione la casilla de verificación **SSH Access**.

Paso 20 Seleccione la casilla **Telnet Access**.

Un punto de acceso OfficeExtend puede ser conectado directamente a la WAN, que podría permitir el acceso externo si la contraseña por defecto es utilizada por el punto de acceso. Por lo tanto, Telnet y SSH se desactivan del acceso de forma automática de los puntos de acceso OfficeExtend.

Paso 21 Si desea reemplazar las credenciales de este punto de acceso, compruebe el **Override Global Username Password**. Puede introducir un nuevo suplicante nombre de usuario AP, contraseña AP y activar contraseña que se desea asignar a este punto de acceso.

Sobre el sistema>**AP Username Password page**, puede establecer las credenciales de acceso global para todos los puntos a la herencia que se unen a un controlador. Estas credenciales establecidas aparecen en la parte inferior derecha de la ventana de la ficha Parámetros de AP.

La información que usted introduce es conservada a través de controlador y reinicia el punto de acceso y si el acceso punto se une a un nuevo controlador.

Paso 22 Verifique **Enable Link Latency**, habilite para permitir que la latencia de enlace para este punto de acceso o desactivar evita que el punto de acceso desde el envío del tiempo de ida y vuelta al controlador después de cada respuesta de eco sea recibido.

Paso 23 Ahora se puede manipular el poder a través de la configuración de inyección WCS sin tener que ir directamente a los controladores. En el Power Over Ethernet sección de Configuración, seleccione la casilla de verificación para activar pre-estándar o inyector de energía del estado.

Configuración de puntos de acceso Pre-estándar que se elija, si el punto de acceso es impulsado por un alto poder del conmutador, de lo contrario, está con discapacidad. Si el poder estatal inyector está marcado, las opciones de alimentación del inyector aparecen. Los valores posibles son instalar o reemplazar. Si decide anular, puede introducir una dirección MAC o dejarlo vacío, así que es suministrada por WLC.

Para determinar en qué fuente de energía está funcionando WCS, vaya a **Monitor**>**Access Points**, haga clic en **Edit**, **View**y elija mover estado de PoE en el cuadro vista de la información. Después de hacer clic en **Submit**, el estado de POE aparece en la última columna. Si el dispositivo es alimentado por un inyector, el estado POE aparece como No aplicable.

Paso24 Verifique la casilla de verificación **Enable**, para permitir a las siguientes configuraciones H -REAP:

AjustesH-REAP no se pueden cambiar cuando el punto de acceso está activado.

• **OfficeExtend AP**: El valor predeterminado es Activado.

Al desactivar la casilla de verificación simplemente desactiva el modo OfficeExtend de este punto de acceso. No deshacer todos los ajustes de configuración del punto de acceso, pero pone en el punto de acceso a riesgo ya que se convierte de forma remota desplegado.

Si desea borrar la configuración del punto de acceso y volver a la configuración por defecto de fábrica, haga clic en **Clear Config** en la parte inferior del punto de datos de acceso a la página. Si desea borrar solo personal SSID del punto de acceso, haga clic en **Reset Personal SSID** en la parte inferior del punto de acceso detalles de la página.

Cuando se selecciona **Enabled** para el AP OfficeExtend, un mensaje de advertencia proporciona la siguiente información:

- Los cambios de configuración que automáticamente produce. Cifrado y latencia del enlace están habilitadas.

La detección de puntos, acceso SSH, Telnet y accesos discapacitados.

- Un recordatorio para configurar al menos un controlador primario, secundario y terciario (incluyendo el nombre y la dirección IP).

Normalmente, un punto de acceso busca primero el controlador primario a unirse. Después de eso, el controlador trata el secundario y luego el controlador terciario. Si ninguno de estos controladores está configurado, el

punto de acceso cambia a un modo de descubrimiento por defecto en un intento de unir cualquiera que sea el controlador que se puede encontrar.

Un punto de acceso OfficeExtend solo busca un controlador primario, secundario o terciario a unirse. No busca más por un controlador configurado. Debido a esto, es importante configurar al menos un nombre principal, el controlador secundario o terciario y Dirección IP.

Una advertencia que permite el cifrado hace que el punto de acceso reinicie el sistema y así los clientes pierdan conectividad.

• **Menor latencia controlador de Ingreso**. Cuando está activado, el punto de acceso pasa de un orden de prioridad de búsqueda (primario, secundario, terciario y control) a la búsqueda controlada con las mejores latencias de medición (por lo menos latencia). El controlador con la menor latencia ofrece el mejor rendimiento.

El único punto de acceso lleva a cabo esta búsqueda, una vez cuando inicialmente se une al controlador. Hace que no vuelva a calcular el controlador primario, secundario y terciario, medidas de latencia, una vez se unieron para ver si las medidas han cambiado.

• Habilitar VLAN: Cuando se selecciona, entre los nativos de identificador de VLAN.

Paso 25 Seleccione la función del punto de acceso de malla en la función del menú desplegable. El valor predeterminado es MAP.

Un punto de acceso en una red de malla funciona como un punto de acceso de root (RAP) o el punto de acceso de malla (MAP).

Paso 26 Introduzca el nombre del grupo del puente a la que pertenece el punto de acceso. El nombre puede tener hasta 10 personajes.
Grupos del puente se utilizan para agrupar lógicamente los puntos de acceso de malla.

Para obtener los puntos de acceso de malla de comunicación, deben tener el nombre de puente de un mismo grupo.

Para configuraciones en las que distintos sectores se requiere, asegúrese de que cada uno de sus RAP y mapas asociados han separado los nombres de grupos del puente.

El tipo de parámetro aparece si el punto de acceso de malla es un punto de acceso interior y exterior y el parámetro de red de retorno de interfaz muestra el punto de acceso inalámbrico que está siendo utilizado como el retorno del punto de acceso.

Paso 27 Seleccione el tipo de datos para la interfaz de red de retorno en el menú desplegable. Las tasas de los datos disponibles son dictadas por la interfaz de red de retorno. La tasa de morosidad es de 18 Mbps.

Este tipo de datos son compartidos entre los puntos de malla de acceso y se fija para toda la red de malla.

No cambie la tasa de datos para una solución de redes de malla desplegada.

Paso 28 Seleccione **Enable** en el puente Ethernet en el menú desplegable para habilitar puente Ethernet para la malla punto de acceso.

Paso 29 Haga clic en **Save** para guardar la configuración.

Paso 30 Vuelva a activar la radio del punto de acceso.

Paso 31 Si usted necesita restaurar este punto de acceso, haga clic en **Reset AP Now**.

Paso 32 Haga clic **Reset Personal SSID** para restablecer el acceso OfficeExtend SSID personal punto de la fábrica.

Paso 33 Si es necesario eliminar la configuración del punto de acceso y restablecer todos los valores por defecto de fábrica, haga clic en **Clear Config**

Descarga de imágenes

Desde la página seleccione un comando en el menú desplegable en la ventana **Configure**> acceder a la ventana de puntos, puede seleccionar Descargar AP Imagen autónoma. WCS comprueba que no más de diez puntos de acceso son seleccionados para su descarga. Una advertencia adecuada es cuando aparece si se descarga en otro progreso. La imagen debe ser compatible con todos los puntos de acceso seleccionados antes de la descarga de imágenes.

La descarga de imágenes comienza inmediatamente y no puede ser programada para un tiempo futuro. Descarga de una imagen de pantalla de estado se muestra y se actualizan periódicamente.

Importación de configuración del punto de acceso.

Desde la página seleccione un comando en el menú desplegable en la ventana **Configure**>**Access Point**, puede descargar las configuraciones de puesta en marcha de puntos de acceso que se guardan en la base de datos utilizando a la Importación, e lAPWCS comando de configuración. La configuración más reciente se mantiene en la base de datos WCS. Usted no

puede descargar una sola configuración de múltiples puntos de acceso con esta función.

Selección de la antena 11n

WCS proporciona la capacidad de activar o desactivar el uso de antenas específicas. Todas las antenas están habilitadas por defecto.

Por lo menos un transmisor y una antena receptora deben estar habilitados. No se puede deshabilitar la transmisión de todos o todas las antenas de recepción, a la vez.

Si elige **Configure>Access Point** y seleccione un elemento 802.11n de la columna de radio.

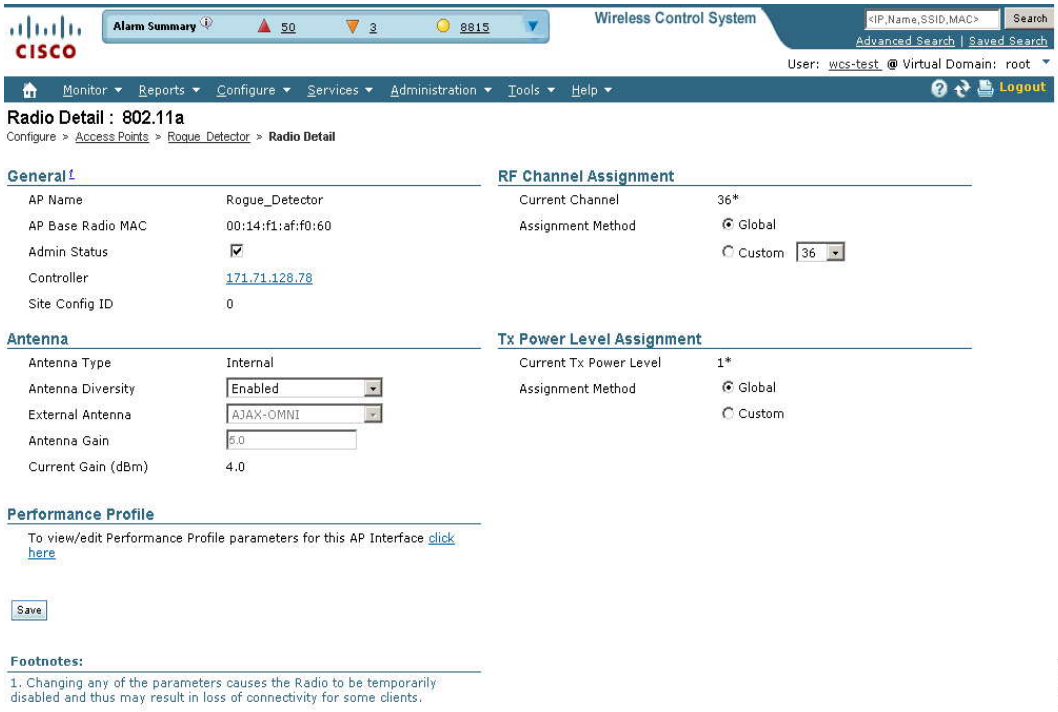


Figure 4.10 Punto de acceso >802.11a/n.

Los siguientes parámetrospantalla11n, pueden ser modificados:

El cambio de cualquiera de los parámetros, hace que el radio se desactive temporalmente y por lo tanto puede resultar en la pérdida de conectividad para algunos clientes.

General

• AP Name: El nombre del operador definido de punto de acceso.

• AP Base Radio MAC: Dirección MAC de la radio base del punto de acceso.

• Admin Status: Check de administración de la caja para el estado de la administración del punto de acceso.

• Controller: La dirección IP del controlador. Haga clic en la dirección IP del controlador para obtener más detalles.

• Site Config ID: Número de identificación.

Antena

• Antenna Type: Indica una antena externa o interna.

• Antenna Diversity: Seleccione Right, Left o Enable.

Para antena externa, seleccione una de las siguientes:

- Enabled: Seleccione esta opción para permitir a la diversidad tanto en los conectores izquierdos y derechos del Access Point.

- Left: Utilice esta opción si el punto de acceso tiene antenas desmontables y se instala una alta ganancia de la antena en el conector de la izquierda del punto de acceso.

- Right: Si el punto de acceso tiene antenas desmontables y se instala una alta ganancia de antena en el conector de la derecha del punto de acceso.

Para antenas internas, seleccionar una de las siguientes:

- Enabled: Seleccione esta opción para permitir a la diversidad tanto en el lado A y lado B.

- Side A: Utilice esta configuración para permitir la diversidad en el lado A (frente a la antena) solamente.

- Side B: Utilice esta configuración para permitir la diversidad en el lado B (antena trasera) solamente.

- External Antenna: Seleccione la antena externa u otra en el menú desplegable.

- Antenna Gain: Escriba la ganancia de la antena deseada en el cuadro de texto.

La ganancia máxima de los dBi de la antena, para antenas direccionales y el promedio de ganancia en dBi de antenas omnidireccionales conectado al adaptador de red inalámbrica. La ganancia está en múltiplos de 0,5 dBm. Un valor entero 4 significa 4 x 0,5 = 2 dBm de ganancia.

Tabla4.7

Nombre de Antena, Ganancia y Descripción.

Nombre de Antena	Ganancia(dB)	Descripción
AIR-ANT1000	0.00	Antena integrada
CUSH-S5157WP	3.00	5.15-5.87GHzdiversidad de banda ancha, panel de antena (lado ganancia y atenuación de la espalda).
KODIAK-DIRECTIONAL	8.00	Integrado Kodiak antena direccional.
KODIAK-OMNI	5.00	Kodiak antena omnidireccional.
AIR-ANT1728	5.20	Omni montaje en el techo la antena
AIR-ANT1729	6.00	Parche de pared de antena
AIR-ANT2012	6.50	Diversidad parche de pared de antena
AIR-	10.00	Yagi maestro o de la pared soporte de la antena
AIR-ANT5959	2.00	Omni diversidad montaje en el techo la antena.
AJAX-OMNI	5.00	Ajax integrado antena omnidireccional
AIR-	3.50	Omni antena dipolo
AIR-	3.50	antena dipolo blanco
AIR-	3.50	3.5dB5 gris, no la articulación de la antena dipolo.
AIR-	2.20	2.2 antena dipolo blanco
AIR-		
AIR-	2.20	2.2dBigris, no la articulación de la antena dipolo
AIR-	4.50	Omni diversidad de antenas
AIR-	6.00	Omni antena
AIR-ANT3549	9.00	parche de pared de antena
AIR-ANT4941	2.20	Omni antena dipolo
AIR-ANT2506	0.00	Omni masa soporte de la antena.
AIR-ANT3213	5.20	Omni diversidad de antenas pilar
CUSH-	3.00	Integrado 2.4/5GHz hemisférica patrón
CUSH-	6.00	Montaje en el techo de 6 dBi omni.
AIR-	7.00	Soporte de pared diversidad parche antena
AIR-ANT5175V	7.50	Omni antena para Wireless Bridge
AIR-	9.50	Soporte de pared parche antena
AIR-	9.50	Sector de la antena para Wireless Bridge
AIR-ANT2455V	5.50	Omni antena para Wireless Bridge
CUSH-S54717P	17.00	Parche de antenas de puente inalámbrico
CUSH-	14.00	Parche de antenas de puente inalámbrico
CUSH-S2406BP	8.00	Omni antena para Wireless Bridge
AIR-ANT1100	2.20	por defecto de antena para AP1100

La Tabla 4.8 muestra los valores por defecto de algunos de los atributos de un punto de acceso cuando se agrega a la WCS, por primera vez:

Tabla 4.8

Atributos del Access Point.

Tipo de AP	Tipo de	Antenas de apoyo
AP1200	802.11ª	KODIAC-OMNI,KODIAK-DIRECTIONAL,AIR-ANT5135D-R, AIR-ANT5145V-R,AIR-ANT5160V-R,AIR-ANT5170V-R,
	802.11b/g	AIR-ANT4941,AIR-ANT1728,AIR-ANT2012,AIR-ANT1729, AIR-ANT2410Y-R,AIR-ANT5959,AIR-ANT3549, AIR-ANT2506,AIR-ANT3213,AIR-ANT2460,AIR-ANT2465, AIR-ANT2485
AP1240	802.11ª	AIR-ANT5135D-R,AIR-ANT5145V-R,AIR-ANT5160V-R, AIR-ANT5170V-R,AIR-ANT5195V-R
	802.11b/g	AIR-ANT4941,AIR-ANT1728,AIR-ANT2012,AIR-ANT1729, AIR-ANT2410Y-R,AIR-ANT5959,AIR-ANT3549, AIR-ANT2506,AIR-ANT3213,AIR-ANT2460,AIR-ANT2465, AIR-ANT2485
AP1131	802.11ª	AJAX-OMNI
	802.11b/g	AJAX-OMNI
AP1100	802.11b/g (onlyb/g)	AIR-ANT1100
AP1310	802.11ª	AIR-ANT5135D-R,AIR-ANT5145V-R,AIR-ANT5160V-R, AIR-ANT5170V-R,AIR-ANT5195V-R
	802.11b/g	BR1310,AIR-ANT4941,AIR-ANT1728,AIR-ANT2012, AIR-ANT1729,AIR-ANT2410Y-R,AIR-ANT5959, AIR-ANT3549,AIR-ANT2506,AIR-ANT2506,AIR-
Tipo de AP	**Tipo de**	**Antenas de apoyo**
AP1250	802.11ª	AIR-ANT5135D-R,AIR-ANT5145V-R,AIR-ANT5160V-R, AIR-ANT5170V-R,AIR-ANT5195V-R
	802.11b/g	AIR-ANT2460,AIR-ANT2465,AIR-ANT2485,AIR-ANT4941, AIR-ANT1728,AIR-ANT2012,AIR-ANT1729, AIR-ANT2410Y-R,AIR-ANT5959,AIR-ANT3549, AIR-ANT2506,AIR-ANT3213
AP1000	802.11ª	AIR-ANT1000,AIR-ANT5135D-R,AIR-ANT5145V-R, AIR-ANT5160V-R,AIR-ANT5170V-R,AIR-ANT5195V-R, CUSH-S5157WP,CUSH-S24516DBP
	802.11b/g	AIR-ANT1000,AIR-ANT4941,AIR-ANT1728,AIR-ANT2012, AIR-ANT1729,AIR-ANT5959,AIR-ANT2506,AIR-ANT3213, AIR-ANT2460,AIR-ANT2465,AIR-ANT2485, CUSH-

Continua ⟶

AP1030	802.11ª	AIR-ANT1000,AIR-ANT5135D-R,AIR-ANT5145V-R, AIR-ANT5160V-R,AIR-ANT5170V-R,AIR-ANT5195V-R, CUSH-S5157WP,CUSH-S24516DBP
	802.11b/g	AIR-ANT1000,AIR-ANT4941,AIR-ANT1728,AIR-ANT2012, AIR-ANT1729,AIR-ANT5959,AIR-ANT2506,AIR-ANT3213, AIR-ANT2460,AIR-ANT2465,AIR-ANT2485, CUSH-
AP1500	802.11ª	AIR-ANT5175V,AIR-ANT58G10SSA,CUSH-S54717P, CUSH-S49014WP
	802.11b/g	AIR-ANT2455V,CUSH-S2406BP
AP1505	802.11ª	AIR-ANT5175V,AIR-ANT58G10SSA,CUSH-S54717P, CUSH-S49014WP
	802.11b/g	AIR-ANT2455V,CUSH-S2406BP

WLAN Override

Los siguientes parámetros802.11a WLAN override aparece:

- WLAN Override: Seleccione Activar o desactivar desde el menú desplegable.

Cuando se habilita la anulación WLAN, el sistema operativo muestra una tabla con todas las corrientes de solución inalámbrica Cisco WLAN. En la tabla, seleccione WLAN para permitir la operación WLAN y desactive la opción WLAN para no permitir la operación de WLAN para este 802.11a Radio Cisco.

La anulación WLAN no se aplica a los puntos de acceso compatibles con la función WLAN 512.

Perfil de rendimiento

Haga clic en URL para ver o editar los parámetros de rendimiento para este perfil de interfaz del punto de acceso.

• ClientLink: Para activar o desactivar el enlace de cliente para las radios del punto de acceso por interfaz. Esta característica admite para el legado

(Orthogonal Frequency-Division Multiplexing) las tasas de OFDM. La interfaz debe ser compatible con ClientLink, y las tasas de OFDM deben estar activadas. Además, dos o más antenas debe ser habilitada para la transmisión, y las tres antenas deben estar habilitadas para la recepción.

El número máximo de clientes admitidos es de 15. Si la configuración de la antena restringe la operación a una sola antena de transmisión o las tasas de OFDM son discapacitados, ClientLink no se puede utilizar.

RF Canal Asignación

Asignación de canales de visualización con los siguientes parámetros de RF 802.11:

- Current Channel: Número de Canal del punto de acceso.
- Assignment Method: Seleccione uno de los siguientes:

    - Global: Utilice esta opción si el canal de su punto de acceso se establece a nivel mundial por el controlador.
    - Custom:Use esta opción si el canal del punto de acceso se establece a nivel local. Seleccione un canal de la lista desplegable.

- Channel width: Seleccione el ancho del canal en el menú desplegable. Las selecciones incluyen 20, por encima de 40, y por debajo de 40.

La asignación de canales de RF soporta 802.11n 40 MHz en la banda de 5 GHz de 40 MHz, la canalización permite radios para lograr mayores tasas de datos instantáneos.

Si se selecciona un ancho de banda más grande reduce los canales no solapados que podría reducir el rendimiento de la red global para las implementaciones de algunos.

Tx Power asignación de nivel

- Current Tx Power Level: Indica el nivel de transmisión de energía actual.

- Assignment Method: Seleccione uno de los siguientes:

    - Global: Utilice esta opción si el nivel de su punto de acceso de alimentación está en el mundo por el controlador.

    - Custom: Use esta opción si el nivel de su punto de acceso es el poder establecido localmente. Elija un nivel de potencia de la lista desplegable.

Selección de la antena11n

WCS proporciona la capacidad de activar o desactivar el uso de antenas específicas. Todas las antenas están habilitadas por defecto.

Por lo menos un transmisor y una antena receptora deben estar habilitados. No se puede deshabilitar la transmisión de todos o todas las antenas de recepción, a la vez.

Los siguientes parámetros de selección de la antena parece 11n:

- Transmit Antenna: Haga clic en la casilla de verificación al lado de la antena A o B para hacerlo posible.

- Receive Antenna: Haga clic en la casilla de verificación al lado de la antena A, B, o C para hacerlo posible.

Configuración de radios de punto de acceso para el seguimiento optimizado de modo de monitor

Para optimizar el cálculo de seguimiento y ubicación de las etiquetas, puede activar el monitor de seguimiento en modo optimizado (TOMM) en un máximo de cuatro canales en la banda 2,4 GHz (802.11b / g de radio) de un punto de acceso. Esto le permite enfocar el canal de exploraciones solo en aquellos canales en los que las etiquetas suelen ser programadas para operar (como los canales 1, 6 y 11).

Después de habilitar el modo de monitorización a nivel de punto de acceso, debe habilitar y asignar turismo y se escoge monitoreo de canales de la radio 802.11b / g del punto de acceso.

Siga los siguientes pasos para configurar, activar turismo y asignar los canales de supervisión en el punto de acceso inalámbrico.

Paso 1 Después de activar el modo monitor en el nivel de punto de acceso, seleccione **Configure**>**Access Point**.

Paso 2 En la ventana de Puntos de Acceso, elija el **802.11 b / g radio** conexión del punto de acceso apropiado.

Paso 3 En la parte general, **Admin Status**desmarcando la casilla de verificación. Esto desactiva la radio.

Paso 4 Marque la casilla **TOMM**. Esta casilla de verificación solo aparece para Monitor AP Mode. Los menús desplegables para cada uno de la pantalla de cuatro canales configurables.

Paso 5 Seleccione los cuatro canales en los que desea el punto de acceso para controlar las etiquetas.

Puede configurar menos de cuatro canales para el monitoreo. Para eliminar un canal de control, seleccione **NONE** en el canal en el menú desplegable.

Paso 6 Haga clic en **Save**. La selección de canales se guarda.

Paso 7 En la ventana de parámetros de radio, vuelva a activar la radio, marcando la casilla de **Admin Status** de administración.

Paso 8 Haga clic en **Save**. El punto de acceso está configurado como un **Admin Status** y se escoge.

El modo de AP se muestra como Monitor / turismo y se escoge en **Monitor**>ventana **Access Point**.

Programación de estado del radio

Para programar un cambio de estado de la radio (activar o desactivar), siga estos pasos:

Paso 1 Elija **Configure**>**Access Point**.

Paso 2 Seleccione la casilla de verificación del punto de acceso aplicable (s).

Paso 3 En la página Seleccione un comando en el menú desplegable, seleccione **Schedule Radio Status**.

Paso 4 Haga clic en **Go**.

Paso 5 Seleccione **Enable** o **Disable** en el estatus del menú desplegable.

Paso 6 Usa **Hours** y **Minutes** en elmenú desplegable para determinar la hora programada.

Paso 7 Haga clic en el ícono de calendario para seleccionar la fecha prevista para el cambio de estado.

Paso 8 Si la tarea programada es recurrente, elija **Daily** o **Weekly**, según sea el caso. Si la tarea programada es un evento único, elija **No Recurrence**.

Paso 9 Seleccione **Save** para confirmar la tarea programada.

Viendo las tareas programadas

Para ver la actualidad de las tareas programadas del estado de la radio, siga estos pasos:

Paso 1 Elija **Configure**>**Access Point**.

Paso 2 Seleccione la casilla de verificación del punto de acceso aplicable.

Paso 3 En la página seleccione un comando en el menú desplegable, seleccione

View Scheduled Radio Task(s).

Paso 4 Haga clic en **Go**.

ESPACIO EN BLANCO
INTENCIONAL

La tarea programada de información incluye:

- Scheduled Task(s): Seleccione la tarea para ver sus puntos de acceso y el radio del punto de acceso.
- Scheduled Radio adminStatus: Indica el cambio de estado (Activar o Desactivar).
- Schedule Time: Indica el tiempo de la tarea de programación que se produce.
- Execution status: Indica si la tarea está programada.
- Recurrence: Indica diario o semanal, si la tarea programada es recurrente.
- Next Execution: Indica la hora y la fecha en que ocurrió la siguiente tarea.
- Last Execution: Indica la hora y la fecha en que ocurrió la última tarea.
- Haga clic Unschedule: Desprogramar para cancelar la tarea programada. Haga clic en **OK** para confirmar la cancelación.

Visualización de los detalles de malla Enlace

Puede acceder a los detalles de malla enlace de varias maneras:

• Malla de tabulación en la página principal de WCS.
• Monitor: Puntos de acceso y haga clic en **Mesh Links**y luego en el enlace **Details.**

• Después de importar un archivo KML de Google Earth, haga clic en el enlace **APMesh**.

Las estadísticas actuales se muestran en la parte superior de la página seguido de diagramas de ciertas estadísticas.

• SNR Graph: SNR: Gráficos arriba y hacia abajo se combinan en un mismo gráfico. Cada conjunto de datos es representado por diferentes colores.

• Link Metrics Graph: El enlace ajustado a métricas y no ajustados se combina en un solo gráfico. Cada conjunto de datos está representado por diferentes colores.

• Packet Error Rate Graph.

• Link Events: La web de los últimos cinco eventos para el enlace se muestran.

• Mesh Worst SNR Links.

• AP Uptime: Estas estadísticas ayudan a determinar si un punto de acceso se reinicie con frecuencia.

• LWAPP Join Taken Time: Estas estadísticas determinan el tiempo que tarda un punto de acceso a unirse.

• Location Links: le permite navegar con el mapa WCS o la ubicación en Google Earth.**[1]**

4.7 Configuración de Controladores y Conmutadores

Adición de controladores

Usted puede agregar controladores de uno en uno o en grupos. Siga estos pasos para agregar los controladores.

Paso 1 Elija **Configure**>**Controllers**.

Paso 2 En el cuadro seleccione un comando en el menú desplegable, seleccione **Add Controllers** y haga clic **Go**. El complemento de la Ventana del controlador (vea la Figura 4.11).

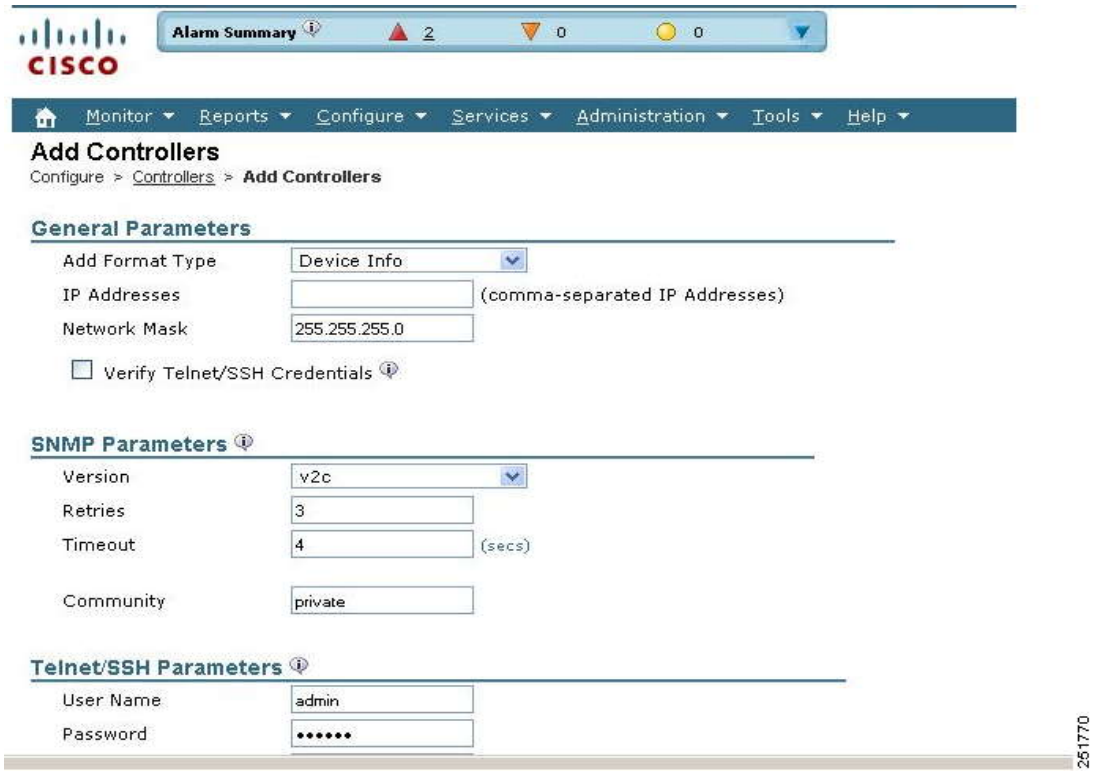


Figura 4.11 Ventana Agregar controlador

Paso 3 Seleccione uno de los siguientes:

Si desea agregar un controlador utilice comas para separar varios controladores, deje el formato agregar del tipo de menú en la información del dispositivo.

Si desea agregar varios controladores mediante la importación de un archivo CSV, seleccione archivo del tipo de formato, agregar en el menú desplegable. El archivo CSV permite generar el archivo de importación propia y agregar los dispositivos que desee.

Cuando un controlador es eliminado del sistema, los puntos de acceso asociados no se eliminan automáticamente y por lo tanto permanecen en el sistema. Estos puntos de acceso deben ser disociados a quitar manualmente.

Si desea agregar un controlador a través de un enlace WCS GRE utilice IPsec o una menor relación con el MTU de varios fragmentos, es posible que necesite ajustar Max Var Binds Per PDU. Si es demasiado alto, el controlador puede dejar de ser agregado a la WCS. Para ajustar la configuración Max Var Binds Per PDU, siga los siguientes pasos:

1) Deje WCS.
2) Vaya a la ubicación del archivo Snmp Parameters. propiedades abierto del servidor que ejecuta WCS.
3) Editar Max Var Binds Per PDU a 50 o inferior.
4) Reinicie WCS.

Paso 4 Si elige la información del dispositivo, escriba la dirección IP del controlador que desee agregar. Si desea agregar varios controladores, utilice una coma entre la cadena de direcciones IP.

Si un límite de bytes parcial se usa y la dirección IP parece ser transmitida (sin tener en cuenta los límites de parcial bytes), existe una limitación en la

adición de los controladores en WCS. Por ejemplo,10.0.2.255/23 no se puede añadir, pero puede 10.0.2.254/23.

Si elige Archivo, haga clic en **Buscar** para encontrar la ubicación del archivo CSV que desee importar, la Tabla 4.9 nos da un claro ejemplo de la información que a encontrar en el archivo CSV.

Tabla 4.9.

Ejemplos de Archivos CSV

Dirección IP	Versio nsnmp	Comunidad snmp	Máscara de red
172.19.35.	v2	public	255.255.255.0
172.19.35.	v2	public	255.255.255.0
172.19.35.	v2	private	255.255.255.0
172.19.35.	v2	private	255.255.255.0

Los siguientes ejemplos de archivos CSV son:

Los archivos CSV pueden contener los siguientes campos:

- ip_address
- network_mask
- snmp_version
- snmpv2_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout

172.19.35.53 v2 public 255.255.255.0
172.19.35.54 v2 public 255.255.255.0
172.19.35.55 v2 private 255.255.255.0
172.19.35.56 v2 private 255.255.255.0

- telnet_user_name
- telnet_password
- telnet_retries
- telnet_timeout

Paso 5 Haga clic en **Verify Telnet/SSH Credentials** casilla de verificación si desea este controlador para verificar credenciales Telnet / SSH. Es posible que desee dejar esta opción sin marcar (o desactivado), debido al tiempo considerable que toma para el descubrimiento de los dispositivos.

Paso 6 Use la versión en el menú desplegable para elegir v1, v2c, o v3.

Paso 7 En el parámetro de reintentos, introduzca el número de veces que se intenta descubrir el controlador.

Paso 8 Proporcionar la sesión del cliente del valor de tiempo de espera en segundos. Esto determina la cantidad máxima de tiempo que permite a un cliente antes de que se vea obligado a volver a autenticar.

Paso 9 En el parámetro de la Comunidad, entre tanto públicos como privados (parav1 y v2 solo).

Paso 10 Seleccione **None**, HMAC-SHA, o HMAC-MD5 (para v3) para el tipo de autorización.

Paso 11 Introduzca la contraseña de autorización (para v3).

Paso 12 Introduzca **None**, DES CBC, CFB-o AES de 128 (para v3) para el tipo de privacidad.

Paso 13 Introduzca la contraseña de privacidad (para v3).

Paso 14 Introduzca la información de las credenciales de Telnet para el controlador. Si elige la opción **File** y añadió varios controladores, la información se aplicará a todos los controladores especificados. Si ha agregado controladores de un archivo CSV, la información de nombre de usuario y contraseña se obtiene a partir del archivo CSV.

El nombre de usuario Telnet / SSH debe tener privilegios suficientes para ejecutar comandos en plantillas CLI.

El nombre de usuario y contraseña por defecto es ***admin***.

Paso 15 Introduzca los reintentos y los valores de tiempo de espera. El número predeterminado de reintentos es 3 y vuelva a intentar el tiempo de espera predeterminado es de 1minuto.

Paso 16 Haga clic en **OK**.

El descubrimiento de plantillas de controladores

Cuando se solicite WCS puede buscar plantillas asociadas a un controlador y observar los resultados.

Paso 1 Elija **Configure**>**Controller**.

Paso 2 Elija un controlador que desee, haga clic en la casilla de verificación delante de la columna de dirección IP.

Paso 3 En la página seleccione un comando en el menú desplegable, seleccione **Discover Templates from Controller** y haga clic en **Go**.

Un mensaje de advertencia confirma que el descubrimiento renueva la plantilla de configuración del controlador en primer lugar.

Una vez ya aplicada al controlador la página de resultados muestra el nombre de la plantilla, el número y tipo de plantilla.

Configuración IGMP Snooping

WCS proporciona una opción para configurar IGMP snooping y los valores de tiempo de espera en el controlador. Puntos de acceso deben suscribirse al grupo LWAPP multidifusión con IGMP.

Siga estos pasos para configurar IGMP snooping.

Paso 1 Elija **Configure**>**Controllers**.

Paso 2 Elija un controlador deseado.

Paso 3 Elija**System**> **Multicast**en el menú lateral izquierdo.

Paso 4 El soporte Ethernet Multicast desplegable por defecto estará desactivo. Si opta por Unicast, el controlador unicasts tiene todos los paquetes multicast para todos los puntos de acceso asociados al controlador. Este método no es el más eficiente, pero puede ser necesario para las redes que no admiten la multidifusión. Si usted elige Multicast, el controlador envía los paquetes de multidifusión a un grupo de LWAPP multicast. Este método reduce la sobrecarga en el procesador de control y cambia el trabajo de replicación de paquetes a la red.

Paso 5 Si elige Multicast, debe introducir una dirección de grupo.

Paso 6 Seleccione **Enable** en el modo de Movilidad Multicast en el menú desplegable para cambiar el estado IGMP snooping o para ajustar el tiempo de espera de IGMP.

Cuando IGMP snooping está activada, el controlador reúne informes de IGMP los clientes y luego envía cada punto

de acceso a una lista de los clientes de escuchar a un grupo multicast. El punto de acceso reenvía los paquetes multicast solo a los clientes.

Paso 7 Cuando el tiempo de espera, el controlador envía una consulta a todas las redes WLAN. Aquellos clientes que están escuchando en el grupo multicast envían un paquete al controlador.

Paso 8 Si se activa el modo de Movilidad Multicast, debe introducir un Grupo de Movilidad de direcciones de multidifusión. Cisco Discovery Protocol (CDP) es un protocolo de detección de dispositivos que se ejecuta en todos los equipos fabricados Cisco.

Un dispositivo activado con CDP envía actualizaciones periódicas de interfaz a una dirección de multidifusión de darse a conocer a los dispositivos vecinos.

Configuración de los temporizadores AP

Algunas de estas configuraciones avanzadas para el modo de temporizador HREAP y local están disponibles para el controlador de WCS.

Siga estos pasos para configurar los temporizadores avanzados y reducir el tiempo de detección de fallos.

Paso 1 Elija **Configure** >**Controllers**.

Paso 2 Elija el controlador que desea establecer la configuración del temporizador.

Paso 3 En el menú lateral izquierdo, seleccione **System**>**AP Timers**. La ventana aparece como AP temporizadores.

Esta opción solo está disponible para los controladores con la versión 6.0 o posterior.

Paso 4 Haga clic en **Local Mode** o **H-REAP**.

Paso 5 Para reducir el tiempo de detección de fallos, puede configurar el intervalo de latidos rápidos del corazón (entre el controlador y el punto de acceso) con un tiempo de espera menor. Cuando el temporizador expira latidos rápidos del corazón (en todos los intervalos de latidos del corazón), el punto de acceso determina si los paquetes de datos se han recibido del controlador en el último intervalo. Si no hay paquetes que se han recibido, el punto de acceso envía un eco rápido de petición al controlador. A continuación, puede introducir un valor entre 1 y 10 segundos.

El controlador de serie 5500 acepta un punto de acceso rápido, valor del temporizador de pulso (modo local o HREAP) en el rango de 10 a 15.

Paso 6 Haga clic en **Save**.

Configuración del controlador de WLAN

Puesto que los controladores pueden soportar 512 configuraciones de WLAN, WCS proporciona una forma eficaz para activar o desactivar varias WLAN a una hora determinada para un controlador determinado.

Siga estos pasos para ver un resumen de las redes de acceso local inalámbrico (WLAN) que ha configurado en la red.

Paso 1 Elija **Configure** >**Controllers**.

Paso 2 Haga clic en la dirección IP del controlador correspondiente.

Paso 3 En el menú, seleccione **WLAN> WLAN Configuration**.

La configuración WLAN en resumen aparece la ventana (ver Figura 4.12). Esta ventana de configuración WLAN contiene los valores encontrados

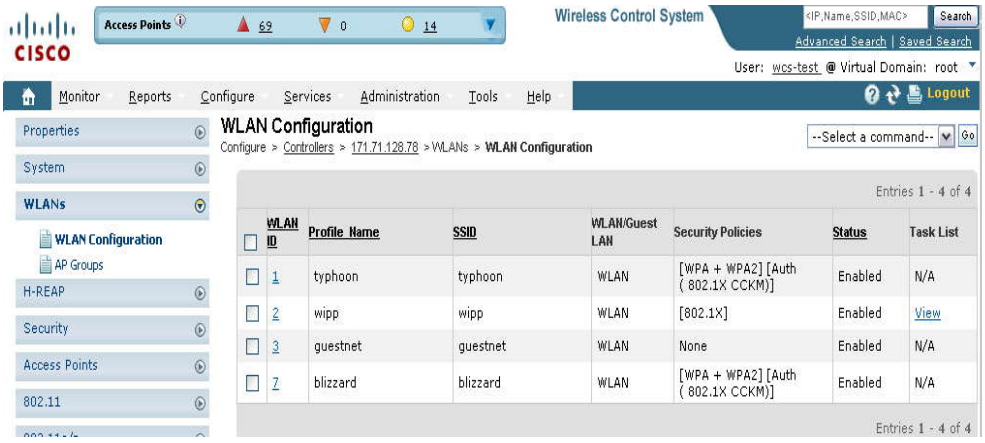


Figura 4.12 Ventana de la configuración WLAN.

Tabla4.10.

Resumen de WLAN.

Parámetro	Descripción
Checkbox	Para su eliminación. Haga clic en **Delete WLAN's** .Seleccionar un comando desplegable del menú.
WLANID	Número de identificación de la WLAN. Nombre de perfil definido por el usuario, el nombre de perfil especificado como la creación de la plantilla de WLAN. Nombre de perfil es el nombre de la WLAN.
ProfileName	Identificador de conjunto que se está emitiendo por WLAN / LAN Invitado, específica si se trata de una WLAN o LAN de invitados.
SSID	Identificador de conjunto que se está emitiendo por WLAN / LAN Invitado, específica si se trata de una WLAN o LAN de invitados.
WLAN/GuestLA	Especifica si es una WLAN o un invitado LAN
SecurityPolicies	Políticas de seguridad habilitado en la WLAN
Status	Es activado o desactivado.
Task List	Si una tarea está programada en **Configure**> **Scheduled**

Ver los detalles de WLAN

Utilice las pestañas (General, Seguridad, QoS, y Avanzado) para ver o editar los parámetros de la WLAN (véase la Figura 4.13).

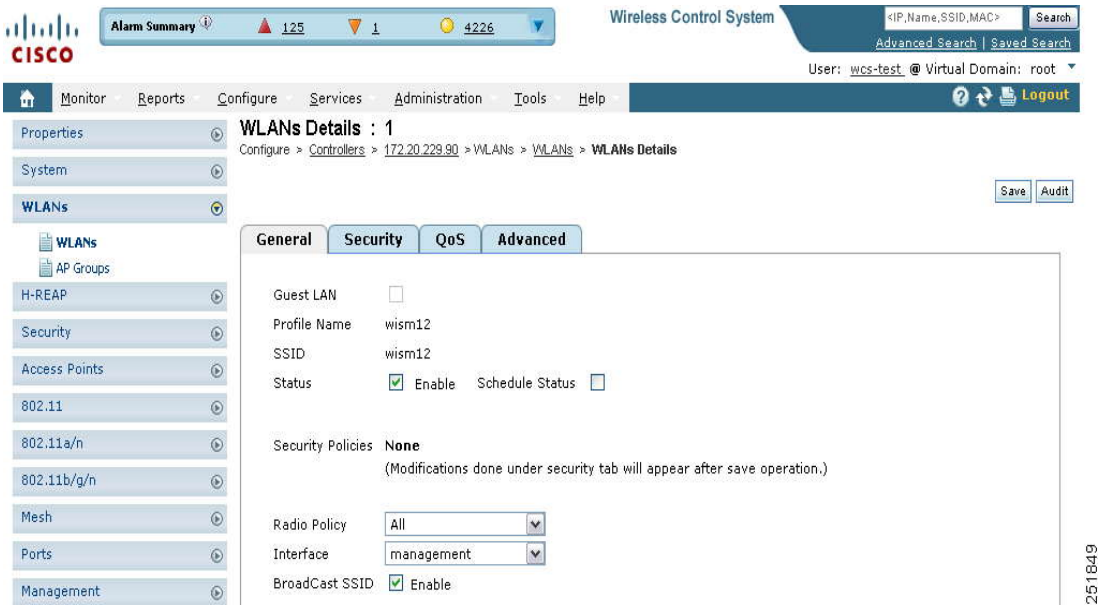


Figura4.13 Ventana detalles de WLAN

GeneralTab

La ficha General incluye la siguiente información:

Dependiendo de la plantilla de WLAN utilizados para este controlador, estos parámetros pueden ser o no ser disponible.

- **Guest LAN**: Indica si es o no es una LAN de visitante WLAN.
- **Profile Name**
- **SSID**
- **Status:** Seleccione la casilla de verificación **Enable** para activar esta WLAN.

Para configurar la hora de inicio del estado de la WLAN debe estar activada, seleccione **Schedule Status**. Seleccione las horas y minutos en los menús desplegables. Haga clic en el ícono de calendario para seleccionar la fecha de aplicación.

- Horario de estado.

- Políticas de seguridad: Identifica el conjunto de las políticas de seguridad mediante la ficha de seguridad (incluye políticas de seguridad, como ninguno, 802.1X, WEP estática, WEP 802.1X estática, WPA + WPA2, y CKIP).

Cambios en las políticas de seguridad aparecen en esta sección después de que se guarda la página.

- Política de Radio: Seleccione en el menú desplegable, solo 802.11a, 802.11g, 802.11b / g sólo 802.11a / g.

- Interface: Seleccione en el menú desplegable.

- SSID Broadcast: Haga clic en la casilla de verificación para habilitar.

- La interfaz de salida: Seleccione el nombre de la interfaz de la aplicación. Este WLAN proporciona una ruta del controlador de tráfico por cable a cada uno de los clientes invitados.

Si solo tiene un controlador en la configuración, elija **Management** del egreso de interfaz del menú desplegable.

- Interfaz de entrada: Seleccione la aplicación de VLAN en el menú desplegable. Esta interfaz proporciona un camino entre los clientes invitados por cable y el controlador a través del interruptor de la capa de acceso 2.

Security Tab

La ficha de seguridad incluye tres fichas adicionales: nivel 2, nivel 3, y los servidores de AAA.

La capa 2 de Seguridad

Uso de la Capa 2, seguridad en el menú desplegable para elegir entre: 802.1x, WEP estática, Cranite, Static WEP-802.1x, WPA1+WPA2, and CKIP.Estos parámetros se describen en la Tabla 4.11.

Tabla 4.11.

Capa 2 Opciones de seguridad.

Parámetros	Descripción
None	Ninguno, No. Nivel 2 de seguridad seleccionado
802.1x	802.11Encriptacion de datos: • Type—WEP • Key Size—40,104, or128bits.

Continua ⟶

ESPACIO EN BLANCO INTENCIONAL

Static WEP	802,11 Cifrado de datos: • Type • Key Size—notset, 40,104, or128 bits. • Key Index—1 to4. • Encryption Key • EncryptionKeyFormat—ASCIIor HEX. • AllowedSharedKeyAuthentication: Seleccionela casilla de verificación para activar.
Cranite	Para configurar Cranite, la WLAN debe utilizar el FIPS140-2compatible para Cranite inalámbrica de pared Software Suite, que utiliza el cifrado AES y túneles VPN paracifrar y verificar todas las tramas de datos realizado por el Cisco Wireless LAN Solution.
Static WEP-802.1X	Parámetros de encriptación estática: • Type • Key Size—notset, 40,104, or128 bits. • Key Index—1 to4. • Encryption Key • EncryptionKeyFormat—ASCIIor HEX.
	802.1Xparametros: • 802.11Data Encryption • Type • Key Size—40,104, or128bits.

Continua ⟶

ESPACIO EN BLANCO INTENCIONAL

Parámetro	Descripción
WPA+WPA2	WPA + WPA2 Use esta opción para habilitar WPA, WPA2, o ambas cosas. WPA permite a Wi-Fi Protected Access con TKIP-MIC de cifrado de datos o AES. Cuando WPA + WPA2 está seleccionada, puede utilizar Cisco Centralizado de administración de claves (CCKM), autenticación de administración de claves, que permite intercambio rápido cuando un cliente se desplaza de un punto de acceso a otro. Cuando WPA + WPA2 es seleccionado como el nivel 2 por política de seguridad y Pre-Shared Key está activada, ni CCKM o 802.1X puede activarse; si bien, CCKM y 802.1X puede activarse al mismo tiempo. WPA + WPA2 parámetros: • WPA1: Seleccione la casilla de verificación para activar. • WPA2: Seleccione la casilla de verificación para activar. Autenticación de administración de claves • 802.1X Seleccione la casilla de verificación para activar. • CCKM-Seleccione la casilla de verificación para activar. • PSK-Seleccione la casilla de verificación para activar.
CKIP	**CKIP** Protocolo de Integridad de Clave Cisco. Un punto acceso de Cisco anuncia apoyo a CKIP en faro y sonda de paquetes de respuesta. CKIP se puede configurar solo cuando Aironet IE está habilitada en la WAN. **Nota:** no es compatible con el punto acceso 10xx. Parámetros CKIP: • 802,11 cifrado de datos o Tipo. o Tamaño de la clave (no se define), 40, 104 o 128 bits. o de clave-1 a 4. o La clave de cifrado. o La clave de cifrado de formato ASCII oHEX.

La capa 3 (Seguridad)

Utilice la Capa 3 o de Seguridad en el menú desplegable para elegir entre **None** (ninguno), **VPN Pass Through, e IPsec** (Internet Protocol Security). Los parámetros de la ventana cambiarán de acuerdo con la selección que realice.

Según el tipo de WLAN en la capa de 3 los parámetros pueden o pueden no estar disponibles.

Si elige pasar a través de VPN, debe introducir la dirección de Gateway de VPN.

IPsec es un conjunto de protocolos para asegurar las comunicaciones IP mediante la autenticación y/o cifrando de cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves criptográficas.

- Web Policy: Seleccione de la casilla de verificación para especificar políticas tales como la autenticación de paso o redirección de web condicional. Esta sección también le permite a los usuarios invitados el login de páginas de vista personalizada.

Si elige pasar la entrada de correo electrónico. Marque esta casilla de verificación si desea que a los usuarios se les pida para las direcciones de su correo electrónico cuando se intenten conectar con el de la red.

Para permitir que los usuarios invitados puedan ver las páginas personalizadas de inicio de sesión, siga estos pasos:

Paso 1 Desactive **Global WebAuth Configuration** de la casilla de verificación.

Paso 2 Seleccione **Web Auth Type**en el menú desplegable de nivel de seguridad>Capa 3 (**Layer 3 tab**).

- Default Internal: El usuario invitado recibe la página de inicio por defecto.
- Customized WebAuth: Páginas personalizadas de inicio de sesión se puede descargar de**Upload/Download** comandos de la página.
    - Seleccionar **Web Auth Login Page**, **Web Auth Login Failure Page**, or **Web Auth Logout Page** desde los menús desplegables.
    - Seleccione **None** de cualquiera de los menús desplegables, si no desea observar una página personalizada de esa opción.
- External: Al usuario invitado se le redirige a una página de acceso externo. Introduzca la URL de la página de inicio de sesión en el campo de autenticación web externos campo URL.

Si selecciona **external**, puede seleccionar hasta tres RADIUS y servidores de seguridad LDAP >página AAA.

AAA Servidores

Seleccione los servidores RADIUS y LDAP para anular el uso de servidores de forma predeterminada en la WLAN actual.

- RADIUS Servers: El uso de los menús desplegables para seleccionar la autenticación de servidores y de contabilidad.

Con esta selección, el servidor RADIUS por defecto especificado para la WLAN sustituye el servidor RADIUS que está configurado para la red. Si los tres servidores RADIUS configurados para una WLAN en particular, un servidor tienen la máxima prioridad y así sucesivamente.

- LDAP Servers: Si no hay servidores LDAP, son elegidos entre los menús desplegables, utiliza WCS por defecto para el servidor LDAP de la base de datos.

- Local EAP Authorization: Permite a los usuarios y a los clientes inalámbricos se autentiquen a nivel local. Es diseñado para uso en oficinas remotas que desea mantener la conectividad inalámbrica a los clientes cuando el sistema de **back-end** se interrumpe o no.

  Seleccione la casilla de verificación para activar si usted tiene un perfil EAP configurado. Seleccione el perfil del menú desplegable.

- Allow AAA Override: Cuando está activado, si un cliente tiene en conflicto AAA y un controlador de WLAN tiene los parámetros de autenticación, la autenticación del cliente se lleva a cabo por el servidor AAA.

Como parte de esta autenticación, el sistema operativo mueve los clientes de la WLAN de Cisco por defecto, la solución a una VLAN devueltos por el servidor AAA y predefinidas en el interfaz de configuración de control (solo cuando se configura para el filtrado de MAC, 802.1X, WPA o la operación).

En todos los casos, el sistema operativo también utiliza QoS y ACL proporcionada por el servidor AAA, ya que siempre están predefinidos en la configuración de la interfaz del controlador. (Este cambio de VLAN por la AAA se conoce también como anular redes de identidad.)

Cuando **AAA override** está desactivada, todos los valores predeterminados de autenticación del cliente con el parámetro de la configuración de la autenticación del controlador y la autenticación se realiza solamente por el servidor AAA si el controlador de WLAN no contiene parámetros de autenticación de cliente específico.

QoS Tab

- Calidad de Servicio (QoS): En el menú desplegable, seleccione Platino (voz), oro (video), plata (Mejor esfuerzo), o de bronce (de fondo).
    - Los servicios tales como VoIP se debe establecer en oro. No discriminar servicios como mensajería de texto se puede establecer en bronce.
- Parámetros de WMM
    - Política de WMM: Elija movilidad reducida, piscina (para permitir a los clientes a comunicarse con la WLAN),o necesario (para que sea obligatorio para los clientes que se han habilitado para las comunicaciones WMM).
    - 7920 AP CAC: Seleccione la casilla de verificación para habilitar el soporte de teléfonos Cisco 7920.
    - 7920 Cliente CAC: Seleccione la casilla de verificación para habilitar el soporte WLAN para las versiones anteriores del software en los teléfonos 7920. El límite de CAC se encuentra en el punto de acceso para las nuevas versiones de software.

Advanced Tab

• H-REAP Local de conmutación: Seleccione la casilla de verificación para conmutación local híbridos REAP. Cuando está activado, el punto de acceso H-REAP maneja la autenticación del cliente y los interruptores de paquetes del cliente a nivel local.

Conmutación H-REAP local solo se aplica a puntos de acceso Cisco 1130/1240/1250 series. No son compatibles con L2TP, PPTP, CRANITE, y autenticaciones de fortaleza. No se aplica para WLAN ID 9-16.

- Session Timeout (en segundos): Establece el tiempo máximo de una sesión de cliente que puede continuar antere-autenticación.

- Aironet IE: Seleccione la casilla de verificación para habilitar el soporte para **Aironet information elements (IEs)** de este WLAN.

    - Si del navegador Internet Explorer está activada, el punto de acceso Aironet IE envía un 0x85 (que contiene el nombre del punto, la carga, el número de clientes asociados, y así sucesivamente) en el faro dalas respuestas de esta WLAN, el controlador envía Aironet IEs 0x85 y 0x95 (que contiene la dirección IP de administración del controlador y la dirección IP del punto de acceso) en la respuesta si recibe Aironet IE 0x85 en la solicitud de la asociación.

- IPv6: Seleccione la casilla de verificación para habilitar el IPv6.

La capa 3, la capa de seguridad debe ser establecida en **None** para que IPv6 esté habilitado.

- Diagnóstico de canal: Haga clic para activar los diagnósticos. Cuando está activado, los clientes pueden conectarse a esta WLAN con fines de diagnóstico.

Los resultados de las pruebas de diagnóstico se almacenan en la tabla de SNMP, y las encuestas de WCS se almacenan en estas tablas para observar los resultados.

- Anulación de interfaz de ACL: Seleccione una lista de control de acceso definidos (ACL) en el menú desplegable.

La selección de una ACL es opcional y el valor predeterminado es Ninguno

- Bloqueo Peer to Peer: En el menú desplegable, selecciona Disable, Drop, o Forward-Up Stream.

    - Esta opción permite al usuario configurar el bloqueo peer-to-peer para los clientes individuales en lugar de modo universal para todos los clientes WLAN.

    - Cliente de exclusión: Seleccione la casilla de verificación para permitir la exclusión automática de clientes. Si está habilitada, establezca el tiempo de espera en segundos para las máquinas de clientes con discapacidad.

    - Las máquinas cliente están excluidos por la dirección MAC y su estado puede ser observado.

    - Un entorno de tiempo de espera de 0 indica que el control administrativo es necesario para volver a habilitar al cliente.

Al cierre de sesión no está activado, el cliente sigue siendo excluido y no el tiempo de espera (de estado excluidos). Esto no implica que la función de exclusión esté desactivada.

- Media Session Snooping: Haga clic para activar Snooping IGMP. Esta característica permite al punto de acceso detectar el establecimiento, la terminación, el fracaso de las llamadas de voz, luego informar al controlador y al WCS. Se puede activar o desactivar para cada WLAN.

Cuando **media session snooping** está habilitado, los radios del punto de acceso WLAN anuncian para **Session Initiation Protocol (SIP)** los paquetes de voz. Cualquier paquete destinado o procedente de puertos número 5060 se consideran para una inspección adicional. El punto de acceso accede a las pistas ya sea Wi-Fi Multimedia (WMM) y los clientes no son establecimiento de llamada WMM, en una llamada activa, o en el proceso de terminar una llamada y luego notificar al controlador de eventos llamada importante.

- NAC Support: Compruebe la casilla de verificación de NAC Support para activarla. Errores SIP se descubren para generar trampas que aparecen en la solución de problemas del cliente y las pantallas de alarmas. El controlador puede integrarse con el aparato en modo de NAC fuera de banda, donde el aparato permanece en la Ruta NAC de datos solo hasta que los clientes han sido analizados y limpiados. Fuera de la banda de modo *reducirla carga de tráfico* en el aparato y permite procesamiento centralizado NAC.

- Período DTIM (en intervalos de beacon): Para 802.11a / n y 802.11b/g/n, especifique la frecuencia de la DTIM paquete enviado en el medio inalámbrico. Este período se puede configurar para cada WLAN (con excepción de invitados WLAN) en todos los controladores de la versión 6.0 y anteriores.

- DHCP

  - DHCP Server: Seleccione la casilla de verificación para anular el servidor DHCP y escriba la dirección IP del servidor DHCP.

Para algunas configuraciones de WLAN, este ajuste es necesario.

  - DHCP Addr. Assignment: Si marca la casilla de verificación, los clientes conectados a esta WLAN obtendrán una dirección IP desde el servidor DHCP por defecto.

- Gestión del marco de protección (MFP)

  - MFP Signature Generation: Si la casilla está marcada, permite la generación de firmas para 802,11 marcos de gestión transmitida por un punto de acceso asociado con esta WLAN. Con generación de la firma, los cambios en los marcos de gestión transmitida por un intruso se detectan y son reportados.

  - MFP de Protección al Cliente: En el menú desplegable, **Optional**, **Disabled** o **Required** para las distintas configuraciones de WLAN.

  - MFP Version: muestra la versión del marco de gestión de protección. El lado del cliente MFP está disponible solo para aquellas WLAN configuradas para soportar clientes CCXv5 (o posterior). Además, WPA1 primero se debe configurar.

Adición de una WLAN

Para agregar una red WLAN, siga estos pasos:

Paso 1 Elija **Configure>Controllers.**

Paso 2 Haga clic en la dirección IP del controlador adecuado.

Paso 3 En el menú lateral izquierdo, seleccione **WLAN>WLAN Configuration**.

Paso 4 En la página seleccione dentro del menú desplegable, seleccione **Add a WLAN.**

Paso 5 Haga clic en **Go** Para abrir los datos WLAN: Añadir de la ventana de plantilla (ver Figura 4.14).

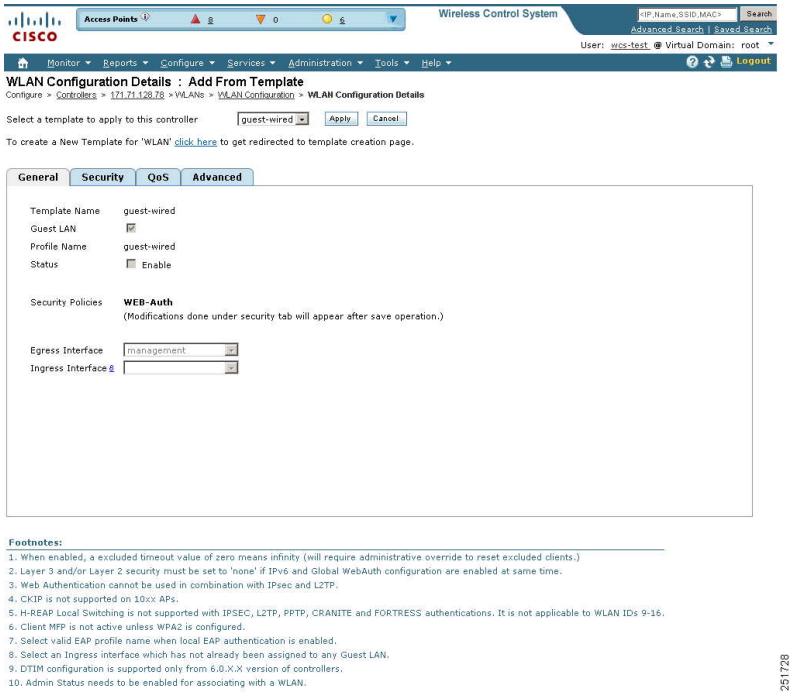


Figura 4.14 Detalles de WLAN: Agregar desde ventana de la plantilla

Paso 6 Elija una plantilla de la lista, seleccione una plantilla para aplicar a este controlador en el menú desplegable.

Paso 7 Haga clic en **Apply**.

Para crear una nueva plantilla para redes WLAN, utilice el vínculo, haga clic aquí en esta ventana GUI o elegir**Configure** > **Controller Template Launch Pad**> **WLANs** > **WLAN.**

Eliminación de una WLAN

Para eliminar una WLAN, siga estos pasos:

Paso 1 Elija **Configure**>**Controllers.**

Paso 2 Haga clic en la dirección IP del controlador adecuado.

Paso 3 En el menú lateral izquierdo, seleccione **WLAN**>**WLAN Configuration.**

Paso 4 Seleccione las casillas de verificación de las redes WLAN que desea eliminar.

Paso 5 En el cuadro Seleccione un comando en el menú desplegable, seleccione Suprimir una WLAN.

Paso 6 Haga clic en **Go**.

Paso 7 Haga clic en **OK** para confirmar la eliminación.

Horarios de la gestión de WLAN Estado

WCS le permite cambiar el estado de más de una WLAN a la vez en un controlador determinado. Usted puede seleccionar varias redes WLAN y seleccionar la fecha y hora para que el cambio de estado, para tomar su lugar. Para programar múltiples redes WLAN para un cambio de estado, siga estos pasos:

Paso 1 Elija **Configure**>**Controllers**.

Paso 2 Haga clic en la dirección IP del controlador adecuado.

Paso 3 En el menú lateral izquierdo, seleccione **WLAN**>**WLAN Configuration.**

Paso 4 Seleccione las casillas de verificación de la WLAN que desea programar para un cambio de estado.

Paso 5 En el cuadro seleccione un comando en el menú desplegable, seleccione **Schedule Status**para abrir la Ventana de Lista WLAN de detalles de tareas (ver Figura 4.15).

ESPACIO EN BLANCO INTENCIONAL

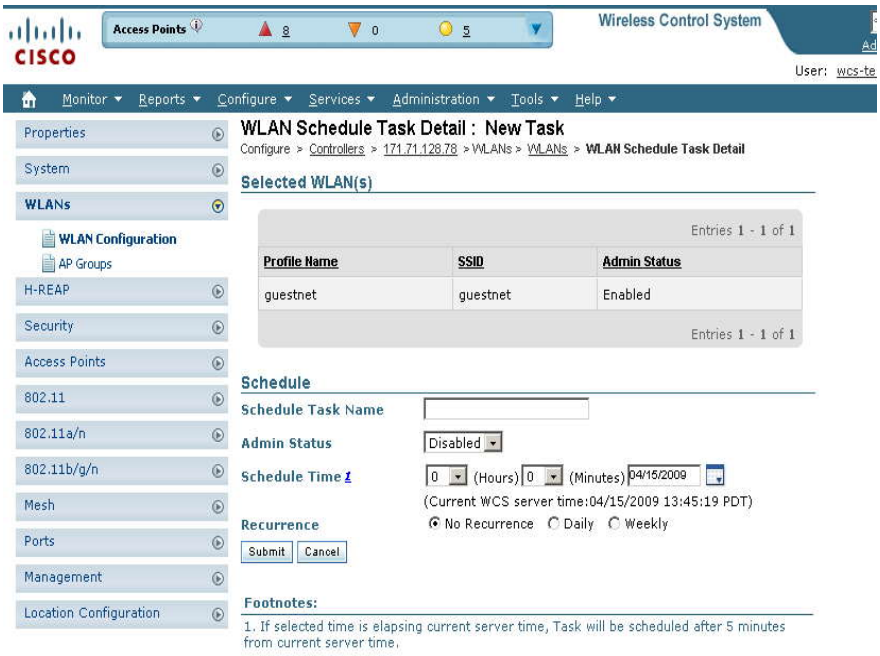


Figura 4.15 Ventana de detalle de la programación de tareas WLAN

El seleccionado WLAN listadas en la parte superior de la ventana.

Paso 6 Escriba un nombre para tarea programada para identificar a este programa de cambio de estado.

Paso 7 Seleccione el nuevo Estatus (activado o desactivado) en el menú desplegable.

Paso 8 Seleccione el tiempo de programación con las horas y los minutos los menús desplegables.

Paso 9 Haga clic en el ícono de calendario para elegir una fecha de programación o introduzca la fecha en el cuadro de texto (DD / MM / AAAA).

Paso 10 Seleccione el botón de repetición de radio, adecuado para determinar la frecuencia del cambio de estado, la recurrencia o no.

Paso 11 Haga clic en **Submit** para iniciar el programa de cambio de estado.

Viendo WLAN Configuración de resultados de la tarea programada

Para ver y administrar todas las tareas programadas de WLAN en WCS, siga estos pasos:

Paso 1 Seleccione **Configure > Scheduled Configuration Tasks**.

Paso 2 En la barra lateral izquierda, seleccione **WLAN Configuration** para abrir la ventana de configuración de WLAN lista de tareas.

Paso 3 Marque la casilla de **scheduled task** si desea ver los resultados de la tarea.

Paso 4 En la página seleccione un comando en el menú desplegable, haga clic en **View History**. La configuración de WLAN.

Para tarea programada, se abre nueva ventana de resultados y muestra la siguiente información:

- Status: Indica el estado de resultado de la tarea.
- Templates Applied: Indica el número de plantillas que aplica esta tarea. Haga clic en el número de plantilla aplicada para ver detalles de la plantilla.
- Template Failed: Indica el número de plantillas que esta tarea ha fallado. Haga clic en número de error de plantillas para ver los registros de error para esta tarea.
- Task Execution Time: Indica la fecha y hora de la ejecución de la tarea.

Anclas de movilidad

Anclajes de movilidad son uno o más controladores que se define como anclas para la WLAN. Clientes (802.11 estaciones móviles, tales como un ordenador portátil) van siempre unidas a una de las anclas.

Esta característica se puede utilizar para restringir una WLAN a una subred única, independientemente del punto de entrada del cliente en la red. De esta manera, los usuarios pueden acceder a un público o invitado WLAN a través de una empresa pero que todavía está restringida a una subred específica.

El invitado WLAN también puede ser usado para proporcionar equilibrio de carga geográfica porque las redes WLAN pueden representar una sección particular de un edificio (por ejemplo, un vestíbulo, restaurante, y así sucesivamente).

Cuando un cliente se asocia primero a un controlador de un grupo de movilidad que se ha pre-configurado como la movilidad de anclaje para una red WLAN, el cliente asocia al controlador local, una sesión local se crea para el cliente. Los clientes pueden estar anclados únicamente a los controladores de anclaje pre-configurados de la WLAN. Para una determinada WLAN, debe configurar el mismo conjunto de controladores de anclaje en todos los controladores en el grupo de movilidad.

Cuando un cliente se asocia primero a un controlador de un grupo de movilidad que no se ha configurado como un anclaje de la movilidad para una red WLAN, el cliente asocia con el controlador local, una sesión local se ha creado para el cliente, y el controlador se anunció a los controladores de otros en el grupo de la misma movilidad. Si el anuncio no ha sido respondido, los contactos con una controladora de los controladores configurados de anclaje para el WLAN y crea una sesión de extranjeros para el cliente en el conmutador local.

Paquetes encapsulados y entregados reciben desde el cliente a la red cableada. Paquetes a los clientes son recibidos por el ancla de control y remitirá al interventor extranjero a través de un túnel de la movilidad con EitherIP. La política exterior del controlador desencapsula los paquetes y los reenvía al cliente.

Un controlador de la serie 2000 no puede ser designado como un ancla para una red WLAN. Sin embargo, una WLAN creada en 2000 una serie de controladores puede tener un controlador de la serie 4100 o un controlador de serie 4400 como ancla.

De la Capa 3 L2TP las políticas de seguridad no están disponibles para las redes WLAN configurada con una movilidad de anclaje.

Para ver el estado en tiempo real de los anclajes de la movilidad de una WLAN específica, siga estos pasos:

Paso 1 Elija **Configure**>**Controllers**.

Paso 2 Haga clic en la dirección IP del controlador adecuado.

Paso 3 En el menú, seleccione **WLAN**> **WLAN Configuration**.

Paso 4 Haga clic en un identificador de WLAN para ver los parámetros de una WLAN específica.

Paso 5 Seleccione la ficha **Advanced**.

Paso 6 Haga clic en el enlace **Mobility Anchors**. La Tabla 4.12 describe los parámetros que se muestran.

Tabla 4.12.

Anclas de Movilidad

Parámetro	Descripción
MobilityAnchor	Dirección IP del ancla
Status	Estado del ancla, Por ejemplo, accesible o inaccesible.

Configuración AAA de los parámetros generales

La Seguridad> AAA> La ventana general permite configurar las entradas de base de datos local en un controlador. Siga estos pasos para configurar las entradas de la base de datos local.

Paso 1 Elija **Configure**>**Controllers**.

Paso 2 Haga clic en la dirección IP del controlador correspondiente.

Paso 3 En el menú lateral izquierdo, seleccione **Security > AAA > General**.

Paso 4 Introduzca el número máximo de entradas permitidas de la base de datos. El rango válido es de 512 a 2048. Esta cantidad entrará en vigor el próximo reinicio. La corriente máxima muestra el valor máximo eficaz actualmente fijado en el controlador.

Descripción del parámetro

Dirección IP de movilidad de **Anchor**. Estado actual de anclaje. Por ejemplo, puede llegar a fuera de cobertura.

Configuración de los usuarios de Red Local

Puede almacenar las credenciales (usuario y contraseña) de todos los usuarios de la red local. Estas credenciales se utilizan para autenticar a los usuarios. Por ejemplo, locales EAP puede utilizar la base de datos de usuarios locales como base de datos de **backend** para recuperar las credenciales del usuario. Debe crear un usuario de red local y definir una contraseña al iniciar la sesión como un cliente de autenticación web.

Paso 1 Elija **Configure**>**Controllers**.

Paso 2 En el menú lateral izquierdo elija **Security** > **AAA** >**Local Net Users**.

Paso 3 Si se mantiene la importación de archivos mientras esté activado, deberá introducir una ruta de archivo o haga clic en el botón **Browse** para navegar a la ruta del archivo. Luego continúe con el Paso 11. Si se deshabilita la primera fila en el archivo es el encabezado. Los datos de la cabecera no son leídos por el WCS de Cisco. La cabecera puede estar en blanco o llena. La WCS Cisco lee los datos a partir de la segunda fila.

Paso 4 Introduzca un nombre de usuario y password (contraseña). Es obligatorio llenar el nombre de usuario y password (contraseña) en todas las filas.

Paso 5 Introduzca un perfil. La columna de perfil si se deja en blanco (o lleno con cualquier perfil) significa que un cliente en cualquier perfil puede utilizar esta cuenta.

Paso 6 Introduzca una descripción del perfil.

Paso 7 Utilice el menú desplegable para elegir el SSID que aplica el usuario local o elegir cualquier opción SSID.

Paso 8 Introduzca una descripción definida por el usuario de esta interfaz. Ir a Paso 11.

Paso 9 Si desea reemplazar el parámetro de plantilla existente, haga clic en **enable** para activar este parámetro.

Paso 10 Haga clic en **Save**.

Configuración de las nuevas solicitudes de enlace LDAP

WCS ahora admite la configuración de LDAP para ambos un enlace anónimo o autenticado. Un enlace es un socket de apertura que realiza una búsqueda. Siga estos pasos para configurar las solicitud desde enlace LDAP.

Paso 1 Elija **Configure**>**Controllers**.

Paso 2 En la barra lateral izquierda del menú seleccione **Security** > **AAA** > **Local Net Users**.

Paso 3 En el tipo de enlace en el menú desplegable, seleccione autenticado o anónimo. Si usted elige autenticado, deberá introducir un nombre de usuario y contraseña.

Paso 4 En el campo de usuario del servidor de Base DN, escriba el nombre completo del sub-árbol en el servidor LDAP que contiene una lista de todos los usuarios.

Paso 5 En el servidor de campo de atributos de usuario, escriba el atributo que contiene el nombre de usuario en el servidor LDAP.

Paso 6 En el campo servidor tipo de usuario, introduzca el atributo **Object Type** que identifica al usuario.

Paso 7 En el campo tiempo de espera de retransmisión, introduzca el número de segundos entre las retransmisiones. El rango válido es de 2 a 30 segundos, y el valor por defecto es de 2 segundos.

Paso 8 Seleccione la casilla de comprobación de estado de administración si desea que el servidor LDAP tenga privilegios de administrador.

Paso 9 Haga clic en **Save**.

Gestionar usuarios en orden de autenticación

Puede controlar el orden en que los servidores de autenticación se utilizan para autenticar a un controlador de gestión de usuarios.

Paso 1 Elija **Configure**>**Controllers**.

Paso 2 Haga clic en una dirección IP.

Paso 3 En el menú lateral izquierdo, seleccione **Management** >**Authentication Priority**.

Paso 4 La base de datos local busca en primer lugar. Elige mediante RADIUS o TACACS + para la siguiente búsqueda. Si no quieren que la base de datos local busque en primer lugar, elige una segunda. Si la autenticación está utilizando la base de datos local falla, el controlador utiliza el siguiente tipo de servidor.

Paso 5 Haga clic en **Save**.

Configuración del puente 802.3

El controlador es compatible con el puente 802.3 y aplicaciones que los utilizan, como lo que normalmente se utiliza para cajas registradoras y servidores de caja registradora. Sin embargo, para que estas aplicaciones funcionen con el controlador, el 802.3 se ha de puentear en el controlador.

La prima 802.3 permite que el controlador del puente no IP para aplicaciones de marcos no se esté ejecutando sobre IP. Solo que esta prima 802.3 formato de trama se soporta actualmente.

Puede configurar 802.3 puente con WCS versión 4.1 o posterior. Siga estos pasos:

Paso 1 Haga clic en **Configure**>**Controllers**.

Paso 2 Haga clic **System**>**General**para acceder a la página General.

Paso 3 En el puente 802,3, en el menú desplegable, seleccione **Enable** para habilitar el puente 802,3 en el controlador o **Disable** para desactivar esta función. El valor predeterminado es **Disable**.

Paso 4 Haga clic en **Save** para confirmar los cambios.

Establecimiento de AP prioridad de conmutación por error

Por orden de prioridad asignado a un punto de acceso, que tienen cierto control sobre lo que los puntos de acceso son rechazados. En una situación de conmutación por error cuando el controlador de seguridad está sobrecargado, los puntos de acceso de mayor prioridad se unen a la copia de seguridad del controlador y separa los puntos de menor prioridad de acceso.

Para configurar los ajustes de prioridad para los puntos de acceso, primero debe activar la función de Prioridad AP. Para permitir que la función de Prioridad de AP, siga estos pasos:

Paso 1 Elija **Configure**>**Controllers**.

Paso 2 Haga clic en la dirección IP del controlador correspondiente.

Paso 3 En el menú lateral izquierdo, seleccione **System**>**General**.

Paso 4 De la prioridad del conmutación por error AP desplegable, seleccione **Enable**.

Para configurar la prioridad de un punto de acceso, siga estos pasos:

Paso 1 Elija **Configure**>**Access Points ><AP Name>**.

Paso 2 De la prioridad del AP en el menú desplegable, seleccione la prioridad de aplicación Low, Medium, High, Critical (bajo, medio, alto, Crítica).

Tenga en cuenta que el valor por defecto es baja.

Solicitudes de descubrimiento de Primer Envío

El punto de acceso tiene una lista de controladores de copia de seguridad y periódicamente envía peticiones principales del descubrimiento a cada entrada en la lista.

Paso 1 Elija **Configure**>**Controllers**.

Paso 2 Haga clic en la dirección IP del controlador correspondiente.

Paso 3 En el menú lateral izquierdo, seleccione **System**>**General**.

Paso 4 Haga clic en **AP Primary Discovery Timeout** para el tiempo de espera. Cuando se configura el temporizador de la petición del descubrimiento principal especifica la cantidad de tiempo que un controlador tiene que responder a la solicitud de descubrimiento del punto de acceso antes de que el punto de acceso asuma que el controlador no se puede unir y espera una respuesta desde el controlador de descubrimiento siguiente de la lista. Introduzca un valor entre 30 y 3600 segundos.

Paso 5 Haga clic en **Save**.

Haciendo ping a un dispositivo de red desde un controlador

Siga estos pasos para hacer ping a los dispositivos de red de un controlador.

Paso 1 Haga clic en **Configure**>**Controllers**. Para ir a la página de todos los controladores.

Paso 2 Haga clic en la dirección IP deseada **IP Address**> página **Controller Properties**.

Paso 3 En la barra lateral, seleccione **System > Commands** > para observar la dirección IP>**Controller Commands**.

Paso 4 Seleccione **Ping From Controller**de la Administración del menú desplegable y haga clic en **Go**.

Paso 5 En el cuadro escriba una dirección IP (xxxx) de ventana del ping, escriba la dirección IP del dispositivo de red que desea que el controlador de ping y haga clic en **OK**.

WCS muestra la ventana de resultados Ping, que muestra los paquetes que han sido enviados y recibidos. Reinicie y haga ping al dispositivo de red o haga clic

en **Close** para detener al hacer ping al dispositivo de red y salir de la ventana resultados de ping.

Load-Based CAC para controladores

Basados en la carga CAC que incorpora un esquema de medición que toma en cuenta el ancho de banda consumido por todos los tipos de tráfico de sí mismo, desde puntos de acceso **co-channel**, y por **la co-located** interferencia del canal.

Basados en la carga CAC también abarca el consumo de ancho de banda adicional resultante de PHY y el deterioro del canal.

De la carga basada en CAC, el punto de acceso periódicamente toma las medidas y las actualizaciones de la utilización del canal de RF, la interferencia de canales y las llamadas adicionales que el punto de acceso puede admitir. El punto de acceso admite una nueva llamada si el canal tiene suficiente ancho de banda no utilizado para apoyar a esa llamada. De esta manera, basados en la carga CAC evita la sobre-suscripción del canal y calidad de servicio se mantiene en todas las condiciones de la carga WLAN y la interferencia.

Para habilitar la carga basada en CAC de un controlador mediante el interfaz web de WCS, siga estos pasos:

Paso 1 Haga clic en **Configure**>**Controllers**.

Paso 2 Haga clic en el enlace de la dirección IP del controlador.

Paso 3 Haga clic en **Voice Parameters** en 802.11a / n o 802.11b/g/n. El 802.11a / n (o 802.11b/g/n) Voz página Parámetros (vea la Figura 4.16).

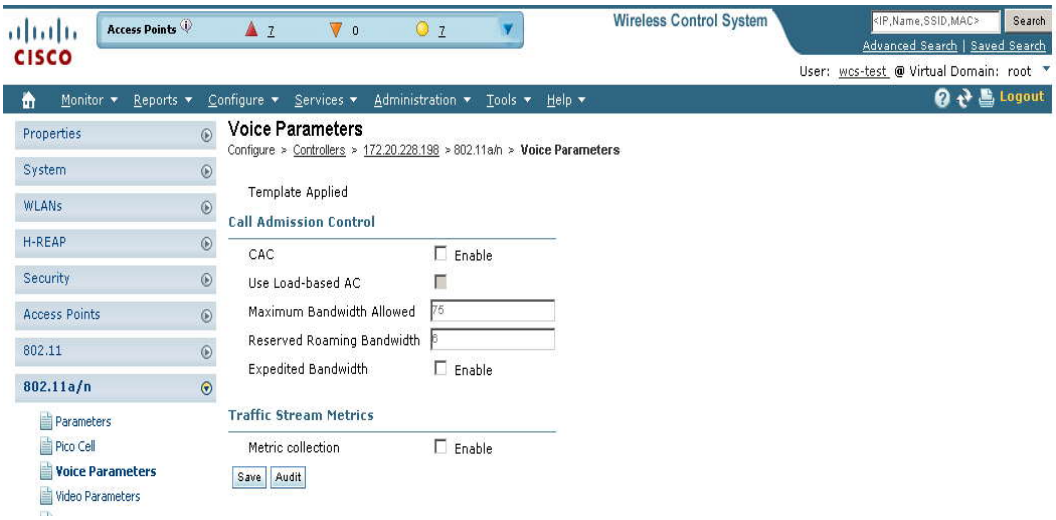


Figura 4.16. 802.11a/n Página de parámetros de voz

Paso 4 Haga clic en la casilla de verificación para permitir que el ancho de banda CAC. Para que los usuarios finales experimenten una calidad de sonido aceptable durante una llamada telefónica de VoIP, los paquetes deben ser entregados a partir de un extremo a otro con baja latencia y la baja pérdida de paquetes. Para mantener la calidad de servicio en diferentes cargas de la red, el control de llamadas de admisión (CAC) se requiere. CAC en un punto de acceso le permite mantener el control de QoS en la red que está experimentando la congestión y mantiene el número máximo permitido de llamadas a una cantidad aceptable.

Paso 5 Determine si desea habilitar la carga basada en CAC de banda de radio. Si lo hace, incorpora una medición de esquema que considera el ancho de banda consumido por todos los tipos de tráfico de sí mismo, de **co-channel** de puntos de acceso y por **co-located** interferencia del canal.

Paso 6 Introduzca el porcentaje de ancho de banda máximo permitido.

Paso 7 Introduzca el porcentaje de **roaming** ancho de banda reservado.

Paso 8 Haga clic en la casilla de verificación si desea habilitar el ancho de banda acelerado como una extensión de la CAC en caso de llamadas de

emergencia. Usted debe tener un ancho de banda de IE acelerado que es Cisco Compatible Extensions (versión 5) compatible con lo que la solicitud TSPEC se da una mayor prioridad.

Paso 9 Haga clic en la casilla de verificación si desea habilitar la recolección de métricas. Métricas de tráfico corriente son una serie de estadísticas acerca de VoIP en su red LAN inalámbrica y le informa sobre la calidad de servicio de la LAN inalámbrica. El punto de acceso para recoger los valores de medición, las mediciones de tráfico de flujo deben estar habilitadas. Cuando esto está activado, el controlador comienza a recopilar datos estadísticos cada 90 segundos para las interfaces de 802.11b/g/n desde todos los puntos de acceso asociados. Si usted está usando VoIP o video, active esta función.

Paso 10 Haga clic en **Save.**

Configuración de un controlador Umbral RRM (para 802.11a/n o 802.11b/g/n)

Siga estos pasos para configurar:

Paso 1 Elija **Configure**>**Controllers**.

Paso 2 Haga clic en la dirección IP del controlador apropiado para abrir la página de propiedades del controlador.

Paso 3 En el menú lateral izquierdo, **802.11a/n** > **RRM DCA. 802.11a/n RRM DCA**.

Paso 4 Realice los cambios necesarios a los umbrales de nivel de cobertura, los umbrales de carga y los umbrales para las trampas.

Paso 5 Haga clic en **Save**.

Configurar SNMPv3

Al configurar un controlador, puede agregar ajustes SNMPv3 o cambiar la configuración (y de cualquier otros ajustes), establecido desde el controlador agregado previamente. (Si SNMPv3está activado en la red interruptor Ethernet, utilice el conmutador Ethernet de CLI o la interfaz de usuario que cambia para incluir a todos los OID y el uso de la opción de contexto para crear un grupo para cada VLAN.) Siga estos pasos para establecer la configuración de SNMPv3.

Paso 1 Elija **Configure**>**Controllers**.

Paso 2 Haga clic en la dirección IP del controlador de la aplicación o seleccione **Add Controller** de la selección de un comando en el menú desplegable y haga clic en **Go**.

Paso 3 De la ventana en la parte de los parámetros de SNMP, seleccione la **v3** (versión 3) del menú desplegable.

Paso 4 Usted puede cambiar los reintentos y los valores de tiempo de espera que se establecieron para este controlador, si lo desea.

Paso 5 En el tipo de privacidad en el menú desplegable, seleccione entre **None, CBC-DES,** o **CFB-AES-128**.

AES se refiere a Advanced Encryption algoritmo estándar establecido por el Instituto Nacional de Estándares y Tecnología (NIST). Es más seguro que los antiguos algoritmos DES.

CFB (Comentarios cifrados) se refiere al método AES, utiliza para cifrar los paquetes y 128 se refiere a la longitud de la clave (128 bits).

Paso 6 Las contraseñas utilizadas para obtener las claves de encriptación de algoritmos de 128, debe contener un mínimo de12 caracteres. Escriba una clave de protección que se ajuste a este criterio.

Paso 7 Haga clic en **OK**.

Configurar el acceso con conexión de cable Invitado

El acceso por cable Invitado permite a los usuarios invitados a conectarse a la red el acceso de invitados de un cable Ethernet conexión designado y configurado para el acceso de invitados. Con conexión de cable, puertos del acceso de invitados podrían estar disponibles en una oficina de invitado o puertos específicos en una sala de conferencias.

El acceso por cable de huéspedes puede ser configurado en una configuración autónoma o en una configuración de doble controlador, el empleo de un ancla y un controlador de extranjeros. Esta última configuración se utiliza para aislar aún más por cable el tráfico de acceso a invitados pero no es necesario para el despliegue de acceso de invitados con cable.

Con conexión de puertos de cable el acceso de invitados inicialmente terminar en un conmutador de capa 2 o el puerto de conmutador que se ha configurado con interfaces VLAN para el tráfico de conexión por cable a los huéspedes.

El tráfico de invitados con conexión de cable troncal, el interruptor de acceso a un controlador inalámbrico LAN. Este controlador está configurado con una interfaz que se asigna a un cable de acceso a invitados de VLAN en el acceso interruptor.

Si hay dos controladores en uso, el controlador (extranjeros) que recibe el tráfico de invitados con cable del conmutador reenvía el tráfico de invitados

conectado a un controlador de anclaje que también está configurado para los clientes del cable de acceso. Después del éxito del tráfico de clientes conectados al controlador de anclaje, uno bidireccional Ethernet sobre IP (EoIP) del túnel se establece entre los controladores de extranjeros y de anclaje para manejar este tráfico.

Si bien el acceso por cable de invitado es administrado por las anclas y los extranjeros cuando los controladores son dos desplegados, la movilidad no es compatible con cable clientes de acceso a invitados. En este caso, DHCP y web de autenticación para el cliente son manejados por el controlador de anclaje.

Puede especificar cuánto ancho de banda un usuario invitado por cable se le asigna en la red mediante la configuración y la asignación de un papel y el contrato de ancho de banda. Para más detalles sobre la configuración de estas características, se refieren a la "**Creating Guest User Accounts**".

Para crear interfaces dinámicas de acceso inalámbrico de usuario invitado, haga clic en **Configure**>**Controllers** y después dela elección de una dirección IP determinada, elija **System** > **Interfaces** (vea Figura 4.17). Dos interfaces deben crearse: una para la entrada y una para la salida. La interfaz de entrada proporciona un camino entre los clientes invitados por cable y el controlador a través de un interruptor de acceso de nivel 2. La interfaz de salida proporciona una vía de salida del controlador para el tráfico de clientes invitados.

ESPACIO EN BLANCO INTENCIONAL

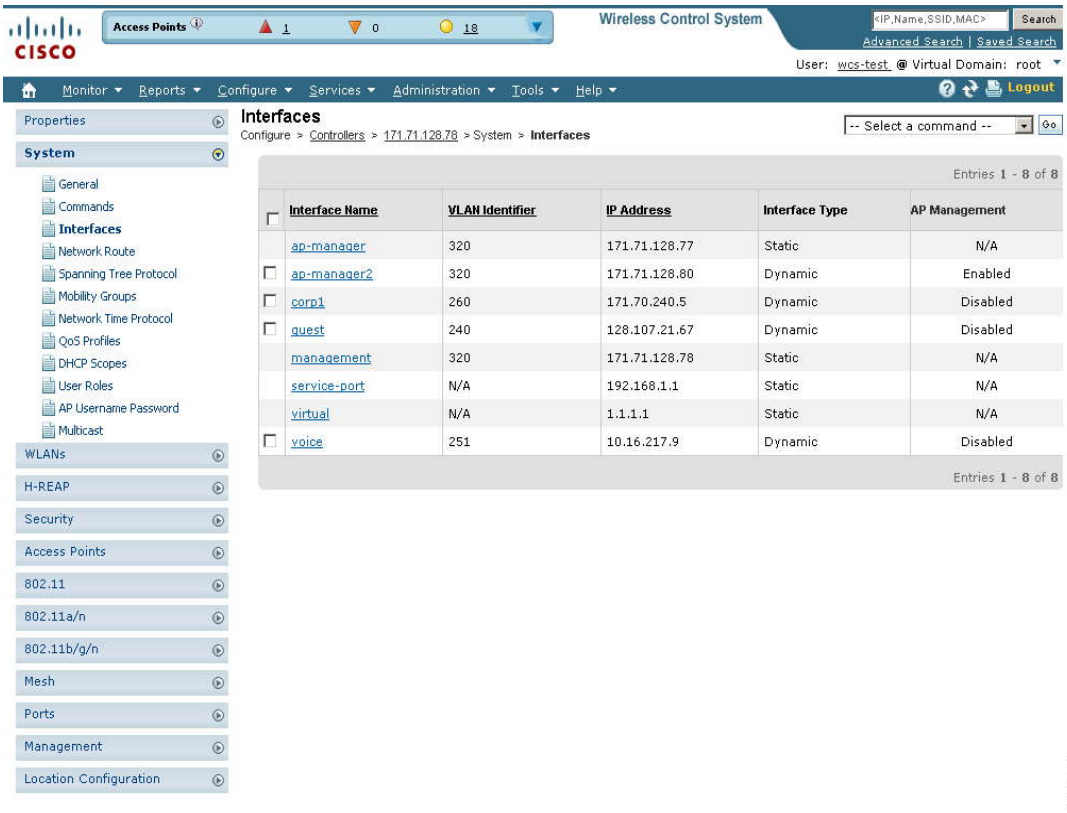


Figura 4.17 Ventana de resumen de interfaces.

Creación de una interfaz de entrada

Siga estos pasos para crear una interfaz de entrada.

Paso 1 Elija **Add Interface.** Seleccione un comando en el menú desplegable y haga clic en **Go**.

Paso 2 Haga clic en el nombre de la interfaz. Los detalles Interfaces: Nueva ventana de configuración (vea la Figura 4.18).

ESPACIO EN BLANCO INTENCIONAL

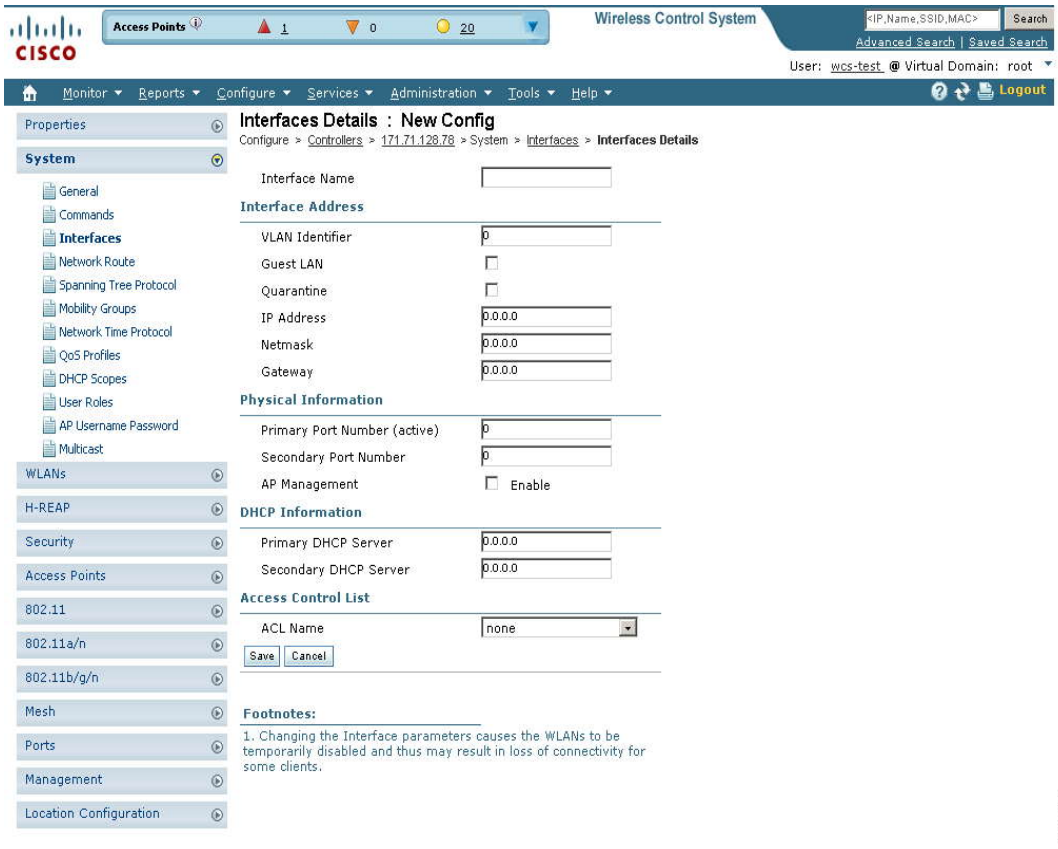


Figura 4.18 Detalles de interface: Ventana nueva configuración.

Paso 3 En la interfaz **Name field**, escriba un nombre para esta interfaz, como **guestinterface**.

Paso 4 Introduzca un identificador de VLAN para la nueva interfaz.

Paso 5 Compruebe la casilla de **Guest LAN**.

Paso 6 Introduzca el número de puerto de primario y secundario.

Paso 7 Haga clic en **Save**.

ESPACIO EN BLANCO INTENCIONAL

Creación de una interfaz de salida

Siga estos pasos para crear una interfaz de salida:

Paso 1 Elija **Add Interface**. Seleccione el comando en el menú desplegable y haga clic en **Go**.

Paso 2 Haga clic en un nombre de interfaz. Los detalles Interfaces: aparece nueva configuración.

Paso 3 En el campo *Nombre de interfaz*, escriba un nombre para esta interfaz, como **quarantine**.

Paso 4 En el campo de identificador de VLAN, introduzca un valor distinto de cero para la identificación de acceso VLAN, como por ejemplo 10.

Paso 5 Seleccione la casilla de verificación de "**quarantine**" e introduzca un valor distinto de cero para el ID de la VLAN de "**quarantine**", tales como 110.

Puede tener el apoyo **NAC-support** en la red WLAN o invitado, ficha de plantilla WLAN avanzada para interfaces con activado de cuarentena.

Paso 6 Introduzca la dirección IP, máscara de red y puerta de enlace predeterminada.

Paso 7 Introduzca los números de puerto primario y secundario.

Paso 8 Proporcionar una dirección IP para el servidor DHCP primario y secundario.

Paso 9 Configurar los campos restantes de esta interfaz y haga clic en **Save**.

Ahora está listo para crear una LAN por cable para el acceso de invitados.

Creación de una LAN por cable para el acceso de invitados

Siga estos pasos para configurar y habilitar la conexión por cable de usuario invitado en la red:

Paso 1 Para configurar una LAN por cable para el acceso de invitados de usuario, haga clic en redes **WLAN**>*Configuración WLAN* de la barra lateral izquierdadel menú.

Paso 2 Seleccione **Add a WLAN** de la lista. Seleccione un comando en el menú desplegable y haga clic en **Go**. **WLAN**>**Add**.

Desde la ventana de plantilla (ver Figura 4.19).

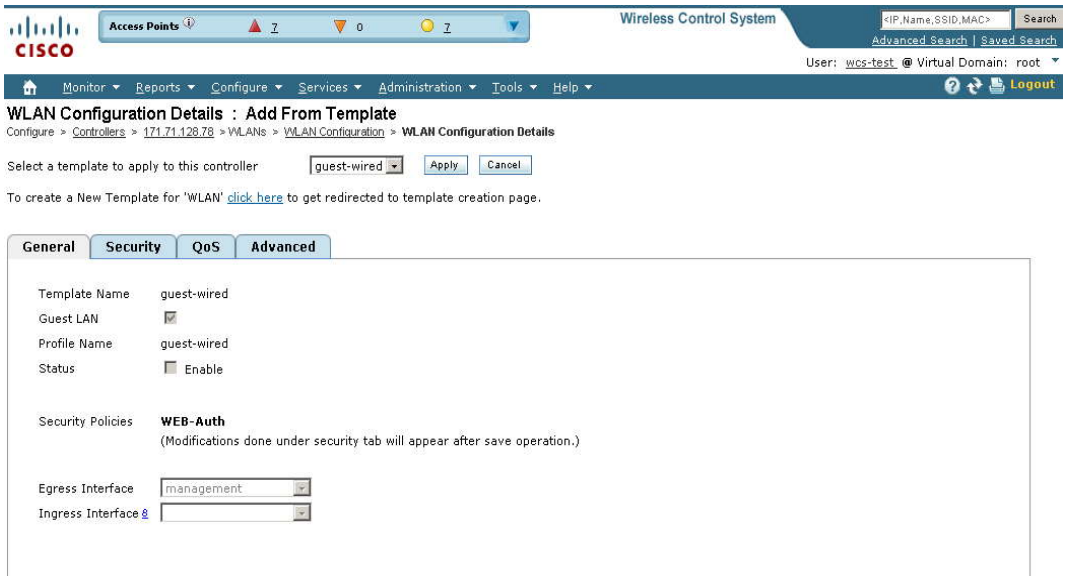


Figura 4.19 WLAN>Agregar desde una plantilla.

Paso 3 Si usted tiene una plantilla establecida que desea aplicar a este controlador, elija la plantilla de *nombre cliente LAN* en el menú desplegable. De lo contrario, haga clic en el vínculo **click here** para crear una nueva plantilla.

Asegúrese de que las identificaciones de WLAN estén en el partido de la misma red antes de reenviar la plantilla de WLAN.

Paso 4 En la ficha general de Nueva plantilla, escriba un nombre en el campo **Template Name** que identifica a la red LAN de invitados.

No utilice espacios en el nombre introducido.

Paso 5 Active la casilla de Invitado LAN.

Paso 6 Introduzca el nombre del perfil.

Paso 7 Seleccione la casilla de verificación **Enable** para el parámetro de estado.

Paso 8 En **Template Name** del menú desplegable, seleccione el nombre de la interfaz deseada.

Paso 9 De la interfaz de salida en el menú desplegable, seleccione la interfaz de salida.

Si tiene solo un controlador en la configuración, elija la gestión del egreso de interfaz de menú desplegable.

Paso 10 En la interfaz de entrada en el menú desplegable, seleccione la interfaz de entrada que creó.

Paso 11 Haga clic en **Security > Layer 3** para modificar la política de seguridad por defecto (autenticación web) o asignar a determinados autenticaciones web (login, logout, la falta de inicio de sesión) y la fuente de las páginas del servidor.

a. Para cambiar la política de seguridad de pasarela, revisar la casilla de verificación **Web Policy** a través de la opción. Esta opción permite a los usuarios acceder a la red sin tener que introducir un nombre de usuario o contraseña.

Una entrada de correo electrónico donde la casilla de verificación aparece. Marque esta casilla de verificación si desea que a los usuarios se les envíen la pregunta por su e-mail cuando se trata de conectarse a la red.

b. Para especificar una ventana de autenticación web, desactive la Casilla de configuración global **WebAuth**.

1. Cuando el tipo de autenticación Web en el menú desplegable aparece, elija una de las siguientes opciones para definir la página de acceso web para los usuarios invitados que estén conectados a la inalámbrica:

Interna: muestra la web, por defecto la página de acceso para el controlador. Este es el valor por defecto.

Muestra de inicio de sesión personalizado de web, la falta de inicio de sesión y cerrar la sesión de las páginas. Cuando la opción personalizada se selecciona, tres menús separados desplegables para el acceso, la falta de inicio de sesión, y cerrar la sesión de selección de página aparecen.

No es necesario definir una página personalizada para las tres de las opciones. Seleccione **None** en el desplegable correspondiente del menú si no desea que aparezca una página personalizada para esa opción.

Estas páginas de inicio de sesión opcional, la falta de inicio de sesión y cerrar la sesión se descargan en el controlador como **webauth.tar** archivos.

Paso 12 Si ha seleccionado externo como el tipo de autenticación Web en el paso 11, haga clic en **Security** > **AAA Servers** y seleccionar hasta tres RADIUS y LDAP utilizando los menús desplegables.

Paso 13 Haga clic en **Save**.

Paso 14 Repita el proceso si un segundo (ancla) del controlador se está utilizando en la red.

BIBLIOGRAFÍA CAPÍTULO 4

- [1] Chapter 9 CiscoWirelessControlSystemConfigurationGuide http://www.cisco.com/web/ES/publicaciones/07-01-Cisco-red-autodefensiva.pdf
- [2]Chapter 10 CiscoWirelessControlSystemConfigurationGuide http://www.cisco.com/web/ES/publicaciones/07-01-Cisco-red-autodefensiva.pdf

- Catalyst 6500 Series Conmutador Software Configuration Guide—Release 8.7. Disponible en: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/vmps.pdf

CAPÍTULO 5: Conclusiones y Recomendaciones

5.1 Conclusiones:

- En la etapa de levantamiento de la infraestructura física y lógica de la red de datos, se observa la inexistencia de puntos de acceso inalámbrico en los diferentes pisos del edificio, lo que no permite disponer de un servicio inalámbrico seguro, ágil y permanente.

- Los problemas técnicos identificados en la red de datos del edificio ALPALLANA, permite considerar como una alternativa viable, la implementación de segmentación dinámica de redes basadas en el estudio presentado

- La asignación de las DVLAN's ayudará a tener conmutadores configurados genéricamente, lo cual agilita los tiempos de cambio de equipos en el caso que se dañe, o se de baja al equipo.

- La utilización del protocolo SNMP, en conmutadores administrables, será un factor clave para poder solventar oportunamente los problemas de configuraciones en forma remota

- Los costos establecidos a la fecha en este proyecto, son los adecuados y acorde a la propuesta de solución presentada.

- Al usar el Wireless Control junto a las DVLAN's se adquirirá un control más específico para los usuarios que utilicen equipos portátiles, porque tendrá el mismo manejo que los equipos fijos por medio de la MAC.

- Mediante la creación de un segmento de red para invitados, se controlará de mejor manera, a los usuarios que conecten maquinas cuyas MAC no se encuentren registradas, de esta forma, solo tendrán acceso a Internet y no a la información de la empresa.

5.2 Recomendaciones:

- Mantener Actualizada la información de las configuraciones e inventarios de los equipos que son integrantes de las redes de datos.

- Mantener actualizado los diagramas de las topologías físicas y del cableado estructurado en cada uno de los pisos.

- Utilizar equipos de la marca Cisco en la implementación del proyecto, esto facilitara el acoplamiento entre todos los dispositivos

- Conservar todos los conmutadores que se encuentran funcionando actualmente en el Edificio, ayudara a rebajar costos.

DICCIONARIO DE TÉRMINOS

Ad-Hoc: (Punto a Punto).
Modo de conexión en una red wireless que define que nuestro equipo (PDA, ordenador portátil o de escritorio) se conectará directamente a otro equipo, en vez de hacerlo a un Punto de Acceso.

CAC: (**Call Admission Control)** Control de admisión de llamada

CCX: (Cisco Compatible Extensions) Extensiones compatibles CISCO.

CDP: (Cisco Discovery Protocol) protocolo de descubrimiento de Cisco.
Es un protocolo de red propietario de nivel 2, desarrollado por Cisco Systems y usado en la mayoría de sus equipos.

CIISCP: Colegio de Ingenieros, Informática Sistemas y Computación de Pichincha.

CLI: (**Command Line Interface)** Interfaz de Línea de Comandos.
Es un método que permite a las personas dar instrucciones a algún programa informático por medio de una línea de texto simple.

CSV: (comma-separated values).
Son un tipo de documento en formato abierto sencillo para representar datos en forma de tabla, en las que las columnas se separan por comas (o punto y coma en donde la coma es el separador decimal y las filas por saltos de línea.

DHCP: Servicio de configuración que permite a una máquina de obtener su dirección IP por vía remota

Dirección IP: (IP Address) Es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora).

Dirección MAC: (MAC address - Media Access Control address).
Es un identificador hexadecimal de 48 bits que se corresponde de forma única con una tarjeta o interfaz de red).

DN:(**Directory Number)** Número de directorio.

Domótica: El término domótica proviene de la unión de las palabras domus (que significa casa en latín) y tica (de automática, palabra en griego, 'que funciona por sí sola'). Se entiende por domótica al conjunto de sistemas capaces de automatizar una vivienda, y que pueden estar integrados por medio de redes interiores y exteriores de comunicación, cableadas o inalámbricas.

DTIM: (**Delivery Traffic Indication Message**).
Es una indicación del tráfico de mensajes que informa a los clientes sobre la presencia de buffer y/o datos del multicanal en el punto de acceso. Se genera dentro de la almenara periódica a una frecuencia especificada por el DTIM.

EAP: (Extensible Authentication Protocol).
Es una autenticación framework usada habitualmente en redes WLAN Point-to-Point Protocol.
EPR: Empresa por Resultado.
ETSI: **Escuela Técnica Superior de Ingenieros.**

Globbing: Es el proceso de expansión de un nombre de archivo específico que contiene un carácter en un conjunto de nombres de archivo que existen en el almacenamiento en un ordenador, servidor o red.

GRE: (**Generic Routing Encapsulation)** Encapsulamiento de ruteo genérico.

GPRS: (General Packet Radio Service) servicio general de paquetes vía radio.
Es una extensión del Sistema Global para Comunicaciones Móviles (*Global*

System for Mobile Communications o GSM) para la transmisión de datos no conmutada (o por paquetes).

HiperLAN: (High Performance Radio LAN).
Es un estándar global para anchos de banda inalámbricos LAN que operan con un rango de datos de 54 Mbps en la frecuencia de banda de 5 GHz.

HTML: (*HyperText Markup Language*) Lenguaje de Marcado de Hipertexto.
Es el lenguaje de marcado predominante para la elaboración de páginas web.

KML (Keyhole **M**arkup **L**anguage**).** Es un lenguaje de marcado basado en XML para representar datos geográficos en tres dimensiones.

L2TP: (*Layer 2 Tunneling Protocol).* Utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado.

LDAP: (**L**ightweight **D**irectory **A**ccess **P**rotocol) Protocolo Ligero de Acceso a Directorios.

LOAFIC: Ley Orgánica de Administración Financiera y Control.

LWAPP: (Lightweight Access Point Protocol) Protocolo Ligero para Puntos de Acceso. Es un protocolo de red utilizado para la gestión centralizada de varios puntos de acceso en una red inalámbrica WLAN.

MAP: (Manufacturing Automation Protocol).
No es un protocolo, sino una pila de protocolos basada en el modelo de referencia de interconexión de sistemas abiertos OSI de ISO.

Máscara de subred: (Subnetaddress).
Es un código numérico que forma parte de la dirección IP.

MFP: (Management Frame Protection) Protección para gestión de Frame.

MTBF: (*Mean Time Between Failure)*.
Es la media aritmética (promedio) del tiempo entre fallos de un sistema.

MTTR: (Mean Time To Repair).
Es la media aritmética (promedio) del tiempo entre reparaciones de un sistema.

MTU: (*Maximum Transfer Unit*).
Es un término que expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un Protocolo de Internet - IP.

NAC: (Network Admission Control) Control de Admisión de red.

NIST: (*National Institute of Standards and Technology)* Instituto Nacional de Normas y Tecnología.
Es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos

NTP: (**Network Time Protocol).**
Es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través de ruteo de paquetes en redes con latencia variable.

OFDM: (*Orthogonal Frequency Division Multiplexing)* modulación por división ortogonal de frecuencia.
Es una modulación que consiste en enviar la información modulando en QAM o en PSK un conjunto de portadoras de diferente frecuencia.
PCI: **(Peripheral Component Interconnect) Interconexión de Componentes Periféricos.**

Consiste en un bus de ordenador estándar para conectar dispositivos periféricos directamente a su placa base.

PCMCIA: (Personal Computer Memory Card International Association).

Es una asociación Internacional centrada en el desarrollo de tarjetas de memoria para ordenadores personales que permiten añadir al ordenador nuevas funciones.

PHY: (Physical) Físico.

PING: (uniform resource locator) **Localizador uniforme de recursos.**

Es una utilidad diagnóstica[1] en redes de computadoras que comprueba el estado de la conexión del host local con uno o varios equipos remotos de una red TCP/IP.

POE: (Power over Ethernet**)** alimentación a través de Ethernet.

Es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar.

Puerta de enlace: (Gateway).

Es la dirección IP que sirve de punto de acceso a otra red.

QoS: (Quality of Services) Calidad de Servicio.

SD: **(*Secure Digital*) bus universal en serie.**

Es un formato de tarjeta de memoria inventado por Panasonic.

RAP: (Roof-top Access Point) Punto de Acceso de azotea.

RF: (Radius Frequency) Radio Frecuencia.

Radio Frecuencia también denominado espectro de radio frecuencia o RF, se aplica a la porción menos energética del espectro electromagnético, situada entre unos 3 Hz y unos 300 GHz.

RLDP: (Rogue Location Detection Protocol) Protocolo de detección de ubicación de rogue.

Servidores DNS: (DNS server).
Es un sistema para asignar nombres a equipos y servicios de red para localizar equipos y servicios con nombres sencillos.

SIP: (**Session Initiation Protocol**) Protocolo de Inicio de Sesiones.
Es un protocolo desarrollado por el grupo de trabajo MMUSIC del IETF con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones.

SNMP: (Simple Network Management Protocol) Protocolo Simple de Administración de Red. Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

SSH: (Secure Shell) intérprete de órdenes segura.
Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

SSI: (Service Set IDentifier). Es un nombre incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red.

SSID: (Service Set Identification).
Es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red.

Tagging: Etiquetando.

Throughput: Se llama throughput al volumen de trabajo o de información que fluye a través de un sistema. Así también se le llama al volumen de información que fluye en las redes de datos.

TOMM: (Tracking Optimized Monitor Mode) Modo Monitor Optimizador de Seguimiento.

URL: (*uniform resource locator*) **localizador uniforme de recursos.**

Es una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización

USB: (*Universal Serial Bus*)bus universal en serie.

Es un puerto que sirve para conectar periféricos a un ordenador.

VMPS: (**VLAN Management Policy Server).**

Es un método para asignar puertos de un conmutadora redes virtuales específicas de acuerdo a la dirección MAC.

VPN: (*Virtual Private Network*).

Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

WECA: (Wireless Ethernet Compatibility Alliance).

Es una empresa creada en 1999 con el fin de fomentar la compatibilidad entre tecnologías Ethernet inalámbricas bajo la norma 802.11 del IEEE. WECA cambió de nombre en 2003, pasando a denominarse **Wi-Fi Alliance**.

WEP: (Wired Equivalent Privacy).

Es el tipo de encriptación que soporta la tecnología Wi-Fi. Su codificación puede ir de 64 bits hasta 128 bits.

WIPS: (Wireless Intrusion Prevention Service) Servicio de Prevención de Intrusos Wireless.

WLC: (Wireless LAN Controller**)** Controlador LAN Wireless

WLAN: (Wireless Local Area Network) **red de área local inalámbrica.**
WMM: (Windows Movie Maker).
Es un software de edición de video creado por Microsoft.

WPA: (*Wi-Fi Protected Access*) Acceso Protegido Wi-Fi. Es un sistema para proteger las redes inalámbricas (Wi-Fi

WPAN:(Wireless Personal Area Network) Red Inalámbrica de Área Personal.