



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA

INGENIERÍA EN COMPUTACIÓN
INFORME DE ACTIVIDADES

DISEÑO E IMPLEMENTACIÓN DE UNA RED INALÁMBRICA UNIFICADA
CON TECNOLOGÍA CISCO

IVÁN ALEXANDER AVILÉS DOMÍNGUEZ

CIUDAD UNIVERSITARIA JUNIO 2011

ÍNDICE

Introducción	3
Objetivo	6
1. Cisco Systems	7
1.1 Productos y Servicios	7
1.2 Organigrama	12
2. Experiencia Profesional	13
3. Proyecto de Red Inalámbrica	19
3.1 Metodología Cisco Ciclo de Vida	19
3.1.1 Preparación	19
3.1.2 Planeación	19
3.1.3 Diseño	20
3.1.4 Implementación	20
3.1.5 Operación	21
3.1.6 Optimización	21
3.2 Situación y Problemática antes del Proyecto	22
3.3 Metodología aplicada al Proyecto	23
3.3.1 Preparación del Proyecto	23
3.3.2 Planeación del proyecto	23
3.3.3 Diseño de la Red	30
3.3.4 Implementación de la Solución	37
3.3.5 Configuración de Access Point	51
3.3.6 Configuración de Servidores de Seguridad (ACS)	55
3.3.7 Wireless Control System WCS	65
4. Resultados del Proyecto	69
4.1 Operación del Proyecto	71
4.2 Optimización del Proyecto	76

Introducción

Como consultor de redes Cisco he tenido la oportunidad de participar en la gestación de diferentes proyectos, tanto en el ramo privado como gubernamental. El proyecto inicia desde que el cliente expone sus necesidades, enseguida se debe conocer su infraestructura de red (topología, tipos de aplicaciones que utilizan, cantidad de usuarios, políticas de seguridad, etc.) para poder ofrecerle una solución a su medida. El ingeniero debe estar altamente capacitado con los conocimientos técnicos y especificaciones de los equipos que conformarán la solución, la cual puede incluir servicios LAN, WLAN, WAN, Voz o Seguridad.

Cada uno de los proyectos tiene características distintas que ofrecen la oportunidad de intervenir de una manera total o solo complementar soluciones existentes. En algunas ocasiones el objetivo es sólo sustituir una red actual por una nueva que incluya algunos servicios extra sin aprovechar las nuevas funcionalidades que la tecnología posee, en este tipo de proyectos el cliente toma el control de gran parte del proyecto. Sin embargo, cuando se trata de ofrecer una solución completa, es decir en una nueva implementación es donde se tiene la oportunidad de participar en el diseño de cada uno de los elementos que formarán parte del proyecto.

Mi formación en la Facultad de Ingeniería ha sido una base sólida para analizar diversos escenarios en diseño e implementación de soluciones de redes, la capacidad de poder liderar proyectos desde el inicio hasta llegar finalmente a la documentación de cada una de las características que conformaron la solución para que la red tenga el mantenimiento adecuado y pueda ofrecer servicios de calidad.

En el ámbito de las redes inalámbricas (muchos de los cuales son los mismos que para redes cableadas), algunos de los puntos importantes para diseñar una solución son los siguientes:

-
- Tipo de tráfico utilizado
 - Cantidad de usuarios
 - Crecimientos a corto y mediano plazo
 - Políticas de seguridad
 - Características físicas del inmueble
 - Direccionamiento IP
 - Cobertura
 - Infraestructura actual

A grandes rasgos estos son algunos de los requerimientos más importantes para diseñar una red inalámbrica, los cuales se tocarán más a fondo en los capítulos siguientes.

Una vez que se tienen todos los requerimientos del cliente se debe tomar la decisión sobre el hardware (el equipamiento que se le ofrecerá). Los equipos dependerán si la red inalámbrica es interior o exterior, autónoma o unificada, si se instalará en espacios abiertos o cerrados y demás características que mencionaré más adelante.

Una vez implementada la solución se deberán realizar protocolos de pruebas para validar el correcto funcionamiento de acuerdo al diseño inicial.

Finalmente se instala la solución y se realizan pruebas con usuarios finales para comprobar su desempeño.

Una vez entregado el proyecto se entra en la fase de operación donde debe mantenerse monitoreada la red para actuar de manera oportuna en caso de falla.

La última fase del proyecto es la optimización del mismo, aquí es donde se afinan situaciones que puedan surgir repentinamente, como cambios en la configuración, nuevas características para mejorar el comportamiento de la red.

En la metodología abordaré cada uno de los puntos del Ciclo de vida de Cisco (PPDIOO) y su utilización en la solución de una red inalámbrica para el sector gubernamental.

Objetivo

El objetivo de este informe es explicar de manera detallada el diseño e implementación de un proyecto de red inalámbrica unificada capaz de ofrecer servicios de datos con equipo de última tecnología. El documento pretende ofrecer una visión real acerca del desarrollo de un proyecto de redes basado en la metodología del Ciclo de Vida de Cisco, que incluye todos los elementos involucrados para el éxito de una implementación.

1. Cisco Systems

Cisco es una empresa internacional que diseña y vende soluciones de tecnología de la información como redes de datos y voz, seguridad en redes, así como servicios profesionales de consultoría y soporte. Sus oficinas principales se encuentran en San José California y tiene más de 70, 000 empleados alrededor del mundo. Cisco reportó cerca de 40 billones de dólares de ingresos en 2010, también está ubicada en el número 16 en la lista de las empresas de tecnología más grandes del mundo.

1.1 Productos y Servicios

Actualmente el portafolio de productos y servicios de Cisco está enfocado a tres segmentos de mercado:

- Empresas y Proveedores de Servicios
- Pequeñas Empresas
- Hogar

A continuación se describe de manera general las soluciones ofrecidas por Cisco.

Empresas y Proveedores de Servicios

Borderless Networks: Sistemas de seguridad, aceleración de aplicaciones en redes WAN y sistemas de administración de redes.

Colaboración: Video IP y teléfonos, Tele presencia, Comunicaciones Unificadas, Servicios de Call Center y aplicaciones móviles.

Centros de datos y Virtualización: Computo Unificado, Switches para Centros de Datos y Almacenamiento.

IP NGN (IP NGN (Next Generation Networks): Redes Ruteadas y Switcheadas para Proveedores de Servicio Móvil, Servicios de Televisión contribuidos.

Pequeñas y Medianas Empresas

WAN y LAN:Routers y Switches.

Seguridad y Vigilancia: Cámaras IP, soluciones de seguridad en redes de datos.

Soluciones de Voz y Conferencia: Teléfonos IP, Gateways, WebEx, Servicios de Video Conferencia.

Redes Inalámbricas: WiFi Access Point, Controladores y Antenas.

Sistemas de Almacenamiento

Hogar (Usuarios Finales)

Productos de la línea Access Point Linksys

Productos de la línea Switches y Cable Modems Linksys

Cable módems de Banda Ancha

Cisco ūmi para Video Conferencia

A continuación se listan los dispositivos y el software ofrecidos por Cisco.

Hardware

- Flip cámara de bolsillo
- Cisco IP Phones (7945, 7965, 7942, 8900 series, 9900 series, 6900 series)
- Cisco LocalDirector: load-balancing appliance.
- Routers: 837, 1000 Series, 2500 Series, 7600, 12000, 3600 Series, ASR Series y CRS-1 and CRS-3
- Cisco Security Manager
- Security appliances: ASA 5500, PIX 500 series
- Unified Computing: Cisco Unified Computing System (UCS) Plataforma de Servidores Virtuales: con sistemas VMWare corriendo en hardware Cisco.
- Catalyst switches: Cisco Catalyst 2900 Series, Cisco Catalyst 3000 Series, Catalyst 4500, Cisco Catalyst 6500 Series
- Sistemas de Colabracion: Cisco TelePresence, Cisco adquirió Tandberg, líder mundial en sistemas de Telepresencia.
- VOIP: Wireless IP Phone 7920
- CLEO: Low Earth Orbit router
- Cisco Wireless LAN
- Cisco Cius: Tablet de colaboración basado en Android.
- Cisco Wide Area Application Services (WAAS)

Software

- Internetwork Operating System
- NX-OS
- Cisco Active Network Abstraction
- Cisco Fabric Manager
- Cisco AnyConnect Secure Mobility Client
- Cisco Systems VPN Client
- CiscoView
- CiscoWorks Network Management software
- Clean Access Agent, Cisco NAC Appliance
- Cisco Eos
- Packet Tracer, simulador didáctico de redes
- Cisco Network Magic Pro
- Cisco Unified Communications Manager
- Cisco IP Communicator
- Cisco Quad
- Cisco Security Manager
- Herramientas de Colaboración WebEx

Servicios de Voz

Cisco se convirtió en el mayor proveedor de Voz sobre IP para empresas y ahora está expandiéndose hacia el Mercado de usuario final con la adquisición de Scientific Atlanta y Linksys. Scientific Atlanta ofrece equipamiento para empresas proveedoras de servicios de cable, como Time Warner, Cablevisión, UPC y otras. Linksys se ha asociado con compañías como Yahoo para integrar servicio de Voz sobre IP con teléfonos inalámbricos.

Certificaciones como Carrera

Cisco Systems también patrocina una línea de Certificaciones Profesionales para las soluciones de sus productos. Existen cinco niveles de certificación: Principiantes, Asociados, Profesionales, Expertos y recientemente Arquitecto, también ocho diferentes planes en sus diferentes tecnologías: Routing y Switching, Diseño, Seguridad de Redes, Proveedor de Servicios y recientemente introdujo Operaciones de Proveedor de Servicio, Almacenamiento, Voz y Wireless.

2. Experiencia Profesional

A lo largo de mi trayectoria profesional he tenido la oportunidad de laborar en diferentes empresas tanto en México como en el extranjero, a continuación ofrezco una breve reseña de las compañías y las actividades que he desarrollado.

Mi primera opción de trabajo llegó después de asistir a una feria laboral en la Universidad. Existían algunas opciones interesantes pero poco viables por el hecho de requerir experiencia o simplemente porque no eran del ramo al cual quería dedicarme. MIGESA contaba con una mesa de información que solo ofrecía folletos donde solicitaban a gente recién egresada para laborar en las diferentes áreas de la empresa, estas eran Ingeniero de Servicio para soporte en diferentes cuentas o Ingenieros de Soporte en sitio.

Después de tres entrevistas logré ser parte de la empresa y comencé como Ingeniero de Servicio, las actividades que el puesto requería eran sencillas y no ofrecían área de crecimiento o motivación profesional ya que solo era reemplazar hardware dañado en diferentes puntos de la ciudad, donde el cliente GE Capital ofrecía sus servicios. Actividades como remplazos de impresoras, cambiar un regulador de energía o una unidad de CD dañadas eran las labores cotidianas.

Afortunadamente después de un par de semanas fui requerido para moverme a la cuenta de Fedex Kinkos donde solicitaban un Ingeniero de Soporte para cubrir las cinco sucursales. Aquí es donde realmente inicié mi desarrollo profesional al poner en práctica mis habilidades adquiridas en mi formación en la Facultad de Ingeniería. Las actividades que tuve en ese periodo de 1 año fueron diversas, por ejemplo, soporte de los sistemas operativos Windows XP, Windows 2000 Server y Mac OS. Soporte a usuarios en sitio y de forma remota, soporte a impresoras y plotters de gran escala así como la instalación y soporte de diversas aplicaciones requeridas para los usuarios. Estuve a cargo de la administración del correo electrónico corporativo (Exchange 2000), la consola de antivirus (Symantec) y el Directorio Activo.

Uno de los proyectos donde participé fue la migración de las computadoras al Dominio corporativo, la generación y aplicación de políticas de usuario.

En el ámbito de las redes, FedExKinkos contaba con cableado estructurado y se utilizaba equipo Cisco, básicamente una topología Hub and Spoke donde cada sucursal tenía un Router corriendo servicios de voz (Call Manager Express), firewall PIX para los servicios de VPN, y Swiches Catalyst para la conexión de los usuarios de voz y datos, además de teléfonos IP de diferentes modelos. Aquí tuve mi primer acercamiento con la tecnología Cisco, fui conociendo de manera muy general y pude realizar modificaciones muy sencillas en los diferentes equipos activos para la resolución de problemas y control de cambios.

Después de unos meses de actividad fui asignado para coordinar ciertas actividades con el cliente que requerían a un grupo personas para realizar mantenimientos preventivos a PC y equipo activo. Asimismo participé en la generación y verificación del cumplimiento de los niveles de servicio (SLA) firmados con el cliente. Trabajé en la generación de manuales de procedimientos de algunas soluciones como Antivirus y Directorio Activo. Al final de mi periodo en esta área me fueron asignados un par de ingenieros en el equipo de trabajo, a los cuales tenía que capacitar y después coordinar. Aquí es donde se presenta la oportunidad de tener más contacto con el cliente, tomar decisiones sobre los recursos, planear nuevos proyectos y mediar, cuando fue necesario, los derechos y obligaciones que existen en una relación cliente-proveedor.

Surgió la opción de crecimiento dentro de la empresa para ser parte del área de Networking, ya que la empresa era Gold Partner de Cisco, y pude de manera definitiva entrar a este mundo de Redes de computadoras.

Al ser este un mundo muy distinto al del soporte y de las labores que venía realizando anteriormente, el área de redes Cisco requería un trabajo más especializado, por lo tanto inicié con el autoestudio para conseguir la primera de mis certificaciones de Cisco (CCNA). Esto me ayudó bastante para poder ser asignado a diferentes proyectos.

Uno de mis primeros proyectos fue la realización de un análisis de red para Deloitte y con la finalidad de ofrecerles servicios de soporte y mantenimiento a toda la red a nivel nacional. La empresa me envió a un curso de redes inalámbricas para poder cumplir un perfil de especialización requerido por Cisco y mantener el Gold Partner, es este tiempo obtuve mi segunda certificación en diseño de redes Cisco (CCDA). A partir de aquí me encargué de prácticamente todos los proyectos de redes inalámbricas en la empresa, es decir diseño, implementación y soporte para diversos clientes. Uno de los proyectos más importantes que realicé fue en TV Azteca; diseñé e instalé la red inalámbrica para un nuevo edificio que alojaría a los directivos de Grupo Salinas. Dicho proyecto fue parte de una solución general de redes Cisco que se implementó en el campus de TV Azteca el cual incluyó Switching y Telefonía IP.

Con el éxito de esta instalación y el plan de renovar la red LAN se inicia un proyecto para migrar la red inalámbrica autónoma existente a una red unificada; nuevamente fui designado para estar al frente. Inicialmente se realizó una revisión para conocer el estado actual de la red para iniciar con la propuesta formal, dicha red estaba constituida por aproximadamente 100 equipos inalámbricos Cisco. Estos Access Point se controlarían por un par de equipos centralizados que fueros parte de dos Switches 6509, equipos alojados en la granja de servidores, (renovación de la red LAN) proyecto que estaría iniciando prácticamente al mismo tiempo.

La renovación de la red actual a una red robusta con tecnología Cisco fue último proyecto donde participé como proveedor de servicios de red para TV Azteca. La parte más importante fue el diseño del Core y la granja de Servidores, aquí use utilizó uno de los modelos de Switch capa 3 más robustos en la familia Catalyst (6509).

Para la capa de acceso se ocuparon varios modelos como 3750G y 4948 en algunos casos. Este proyecto requirió la participación de diversos grupos de trabajo por parte de TV Azteca, MIGESA y CISCO debido a la magnitud y criticidad del mismo; gente del área de Servidores, Aplicaciones, Soporte, Telecom, Project Managers y área comercial estuvieron involucrados. Por el lado de la empresa donde laboraba estuvimos involucrados cerca de 10 ingenieros en diferentes momentos del proyecto.

Cuando la migración de un proyecto de este tamaño inicia hay que tener un plan de acción para realizarla (Plan de Implementación) y plan de regreso al estado actual (Backout) en caso de que el primero falle, estos dos planes deber ser creados para cada migración. Algunas de las características que se modificaron fueron: cableado estructurado, uplinks 10 GB, movimiento de todos los nodos de red a los nuevos equipos, nuevo direccionamiento, segmentación de la red, servicios de DHCP autenticado, seguridad en cada uno de los puertos con diferentes características (IP Arp Inspection, DCHP snooping), etc. Después de varios meses de migración finalmente se pasó a la fase de operación, aquí se entregaron memorias técnicas y manuales de atención de incidentes para el personal de soporte que se encargaría de administrar la red migrada.

Finalizando este exitoso proyecto me ofrecen una posición en TV Azteca para administrar la red LAN y Wireless recién migrada. Trabajando como ingeniero Senior en el área de telecom de Azteca Servicios. Ya como empleado de TV Azteca participé en proyectos internos como la renovación de la red del AVID y la red de Azteca Novelas, algunas de mis actividades cotidianas eran la atención de incidentes (último nivel de escalación) relacionados con la red del Campus Ajusco. Aquí es cuando obtuve mi tercera certificación, ésta vez en la tecnología inalámbrica para tomar ventaja de toda la experiencia que había adquirido en mi trayectoria como consultor.

Después de un año de laborar en esta empresa se me presenta una oportunidad de regresar a la consultoría con otro partner de Cisco, DESCAR, partner con gran presencia en Latinoamérica.

En esta empresa trabajé para diferentes clientes en soluciones de Switching, Wireless, Seguridad y Voz. Algunos de los clientes son KPMG, Baker Hughes, Banamex, Pemex, Infotec, Auditoría Superior de la Federación, IMPI y Secretaría de Salud.

Los procesos de esta empresa se basaban en ITIL y estándares ISO, lo cual requería la generación de diferentes documentos durante el período de vida de un proyecto, algunos de los documentos eran Detalle de Ingeniería, Plan de Implementación, Protocolo de Pruebas y Memoria Técnica. Cada uno de estos documentos era realizado por los ingenieros del área de Implementación de la cual era parte.

Uno de los proyectos más grandes e importantes donde he trabajado fue la implementación de la red inalámbrica para la Secretaría de Salud en cada una de sus sedes en la Ciudad de México.

Esta instalación fue parte del proyecto de renovación de red de la Secretaría, que incluyó diseño e implementación de la red Wireless, LAN, WAN, Seguridad y Voz. Alrededor de 4000 usuarios conectados a la red de datos, 3000 usuarios de voz y 300 Access Point. Justo este proyecto de la red inalámbrica es el que se aborda en este trabajo. Al ser DESCAs una empresa con presencia en Latinoamérica tuve la oportunidad de viajar a Nicaragua para atender un problema urgente relacionado con el enlace WAN de Bimbo en su central de reparto de Managua. Además fui enviado a Bogotá donde se capacitó a un grupo de ingenieros de diversos lugares de América en una solución de Catching para servicios de video en Internet y Protocolos PSP ofrecida por la empresa Israelí PeerApp, la cual recién se había unido al grupo de partners de DESCAs.

Finalmente se presenta la oportunidad de trabajar en Estados Unidos representando a CISCO por medio de la empresa ComputerNet en Carolina del Norte, empresa en la que laboro hasta la fecha. Obtuve mi primera certificación a nivel profesional de Cisco (CCVP) misma que avala tus conocimientos en soluciones unificadas de voz. He trabajado con BB&T, uno de los bancos más importantes en la zona Este del país donde realicé soporte y ingeniería para la red de voz que está conformada por cerca de 10 mil teléfonos alojados en 5 Clusters divididos en 2 Centros de Datos (Wilson y Charlotte). El trabajo realizado con este cliente fue probar cada una de las nuevas soluciones requeridas en un laboratorio de redes, ya que no debería existir impacto alguno al momento de implementar la solución en producción.

Debido a la criticidad de su operación, debían crearse documentos para justificar cada una de las modificaciones a realizarse, las cuales era avaladas por el grupo de ingeniera de BB&T antes de su implementación.

Actualmente me encuentro trabajando en un proyecto con otro banco (Wells Fargo-Wachovia), el objetivo es renovar la red de voz actual. Este proyecto está contemplado para finalizarse en 2 años. Se deben consolidar cerca de 20 Cluster que corren Call Manager Version 4.x en plataforma Windows y versión 6.x en plataforma Linux en 5 súper Clusters con equipos MCS 7845 con versión 7.1 que corre sobre Linux.

Se implementó un área de configuración en las oficinas del cliente donde se simula la red actual y la red nueva, aquí se lleva a cabo el proceso y las migraciones de cada uno de los sitios. Para dicha simulación se instalaron servidores virtuales, utilizando VmWare VSphere 4, donde se replica de manera exacta la red actual del cliente. Se utilizan diferentes herramientas de voz para obtener la Base de Datos actual (SQL) y se manipula para poder instalarla en los nuevos equipos que utilizan Informix. Se realiza una depuración de la información obsoleta, como Extensiones, Calling Search Spaces, Particiones, Traslaciones, Interfaces analógicas y digitales, etc. También trabajo en la creación de templates de configuración de los Gateways (MGCP, H.323) de voz para su registro en los nuevos servidores y participo en la migraciones que tenemos los jueves y viernes donde se mueven en promedio 2000 usuarios en una red de voz que tiene cerca de 30 mil extensiones en todo el país.

En este proyecto estamos involucrados aproximadamente 20 personas que representamos a Cisco y otros 20 del lado de Wells Fargo. Hasta la fecha este ha sido el proyecto más interesante en el que he participado. Afortunadamente he tenido oportunidad de trabajar con diferentes clientes y en diferentes lugares, lo cual genera una visión mucha más amplia y me siento orgulloso de seguir aportando mis habilidades y conocimientos adquiridos en la Facultad de Ingeniería así como la experiencia y la continua auto capacitación.

3. Proyecto de red inalámbrica

3.1 Metodología Cisco Ciclo de Vida

Todos los proyectos en que he trabajado en mi experiencia como Consultor de Redes son basados en el Ciclo de Vida de Cisco, llamado PPDIOO, Preparación, Planeación, Diseño, Implementación, Operación y Optimización, el cual ofrece una serie de recomendaciones que deben ser aplicadas en todo proyecto para este resulte exitoso.

A continuación se citan de manera general cada uno de los puntos que conforman el Ciclo de Vida.

3.1.1 Preparación

El éxito de un proyecto inicia con la preparación; una visión amplia, los requerimientos y tecnologías necesarias para soportar una solución que sea competitiva. En la fase de preparación una compañía determina un caso de negocio partiendo de las necesidades y del Retorno de Inversión (ROI) al adoptar una nueva tecnología. Se debe tener especial cuidado en las necesidades futuras y en el desarrollo de una estrategia tecnológica y una arquitectura de alto nivel que cubra todas las necesidades de negocio.

3.1.2 Planeación

Una implementación exitosa depende de una evaluación precisa de la red actual, la disposición general de los involucrados en apoyar la solución. En la fase de planeación, una empresa comprueba si tiene recursos suficientes para gestionar un proyecto de implementación de la tecnología desde el inicio hasta el fin. Para evaluar y mejorar la seguridad de la red, una compañía realiza pruebas de su red para que esté preparada para problemas como detección de intrusos y la vulnerabilidad a las redes externas.

La empresa desarrolla un plan detallado del proyecto para identificar los recursos, las posibles dificultades, las responsabilidades individuales y las tareas críticas necesarias para entregar el proyecto final a tiempo y dentro del presupuesto acordado.

3.1.3 Diseño

El desarrollo de un diseño detallado es fundamental para reducir los riesgos, retrasos y el costo total de instalación. Utilizar un diseño de acuerdo con los objetivos de negocio y los requisitos técnicos puede mejorar el rendimiento de la red, mientras se garantiza la alta disponibilidad, confiabilidad, seguridad y escalabilidad. Las operaciones del día a día y los procesos de gestión de red deben ser anticipados, y cuando sea necesario, se crean aplicaciones personalizadas para integrar nuevos sistemas en la infraestructura existente. La fase de diseño también puede guiar y acelerar la ejecución exitosa con un plan de configuración, protocolos de pruebas y validación de servicios.

3.1.4 Implementación

Una red es esencial para cualquier organización exitosa, esta debe prestar servicios esenciales sin interrupción. En la fase de implementación, una empresa trabaja para integrar los dispositivos y las nuevas capacidades de acuerdo al diseño sin comprometer la disponibilidad de la red o el rendimiento. Después de identificar y resolver problemas potenciales, la empresa intenta acelerar el retorno de inversión con una migración eficiente esto incluye la instalación, configuración, integración, pruebas y la puesta en marcha de la solución. Una vez que la operación es validada, una organización puede empezar a expandir y mejorar las habilidades al personal de TI para aumentar aún más la productividad y reducir el tiempo de inactividad del sistema.

3.1.5 Operación

El funcionamiento de la red representa una porción significativa del presupuesto de TI, así que es importante poder reducir los gastos operativos y al mismo tiempo mejorar el rendimiento. A lo largo de la fase de operación, una compañía monitorea de forma proactiva la salud de la red para mejorar la calidad del servicio, mitigar las interrupciones y mantener una alta disponibilidad, confiabilidad y seguridad.

Proporcionar un marco eficiente y herramientas operativas para responder a los problemas, una empresa puede evitar el costoso tiempo improductivo y la interrupción del negocio. La participación de personal experto permite a una organización dar cabida a las actualizaciones, adiciones y cambios de manera confiable.

3.1.6 Optimización

Un buen negocio no deja de buscar una ventaja competitiva. Esa es la razón por la que la mejora continua es uno de los pilares del ciclo de vida de la red. En la fase de optimización, una empresa está continuamente buscando maneras de alcanzar la excelencia operativa a través de un mejor desempeño, ampliación de los servicios y las evaluaciones periódicas de la red. Toda organización busca optimizar su red y se prepara para adaptarse a las nuevas necesidades de negocio, es aquí donde el Ciclo de Vida comienza de nuevo en busca de una mejora continua.

3.2 Situación y Problemática antes del Proyecto

Las necesidades de actuales del cliente requerían no sólo contar con el equipo de trabajo y las diversas aplicaciones, sino también con una infraestructura robusta que coadyuvara al mejoramiento continuo de sus procesos a fin de cumplir los objetivos que como unidad de negocio se han trazado.

Una de las necesidades más importantes fue poder contar con una infraestructura de red que les permita ingresar a los distintos servicios y recursos de red con la capacidad de ofrecer movilidad y comunicación integral sin importar el sitio o edificio donde se encuentren físicamente, todo esto sin comprometer la seguridad de la información.

Actualmente el cliente no cuenta con una red inalámbrica que le ofrezca tales características, por lo tanto se diseñará una solución que cumpla con las necesidades principales, así como la posibilidad de poder ser escalable, redundante y segura con el afán de que el cliente dirija sus esfuerzos en mejorar sus necesidades principales de negocio con la total confianza de que cuenta con una solución de red robusta acorde a sus requerimientos.

Se requiere conectar 17 sitios en el D.F. y área metropolitana con una red unificada que sea capaz de ofrecer redundancia de al menos 25% de los Access Point (AP) y que tenga la capacidad de ofrecer Roaming y Movilidad sin importar el sitio donde el usuario se mueva. Asimismo ofrecer encriptación y autenticación centralizada para los usuarios de la empresa y acceso a Internet a Invitados bajo demanda. Finalmente tener una herramienta de administración con la capacidad de configurar, resolver los problemas y visualizar el comportamiento de toda la red inalámbrica instalada.

3.3 Metodología aplicada al Proyecto

3.3.1 Preparación del Proyecto

La solución adecuada para los requerimientos del cliente fue una red unificada capaz de centralizar la administración y operación. La red minimiza la cantidad de miembros del departamento de soporte y sobretodo la capacidad de responder a cualquier problemática del usuario, considerando que se implementaron 17 sitios.

Es aquí donde el Retorno de Inversión fue determinante al compararse contra el costo de una red autónoma que necesitaría varias personas que soportaran y operaran la red de todos los sitios. La solución unificada requirió de un solo recurso de soporte capacitado ubicado físicamente donde se instalaron los Controladores y que se apoyaría en personal de soporte de sistemas locales en caso de ser necesaria una intervención física en algún Access Point.

En la preparación del proyecto trabajé de manera conjunta con el staff de redes del cliente, debido a que la red contaría con diversos sitios, los cuales serían centralizados en cuanto al control pero no respecto al diseño lógico, fue necesario establecer los lineamientos y así conocer la factibilidad y alcance del proyecto con miras al éxito del mismo.

3.3.2 Planeación del proyecto

El paso número uno, el cual es vital para la buena implementación de cualquier solución inalámbrica es la realización de un estudio/análisis de los sitios (Site Survey) el cual nos ofrece los resultados de los que surgirá el diseño de la solución. Este estudio arroja la cantidad de Access Point utilizada, ubicación exacta de los mismos y el tipo de antenas requeridas.

El equipo necesario para realizar un Site Survey es el siguiente:

- Equipo Laptop
- Cisco Aironet Site Survey Utility: Este software determina la cantidad de SSID en el ambiente RF y las interferencias existentes
- Cisco Aironet Wireless Adapter a/b/g: Tarjeta inalámbrica necesaria para ejecutar la herramienta anterior.
- Mapas físicos y electrónicos: Físicos para marcar la ubicación de AP y electrónicos para ser usados por la herramienta de Site Survey.
- InterpretAir WLAN Site Survey (o algún otro software similar)

Los objetivos de un Site Survey son los siguientes:

- Determinar las características de propagación de la señal RF
- Medición de la pérdida de la señal en sitio
- Conocer las aéreas que se debe cubrir
- Requerimientos de potencia de la señal en índice Señal a Ruido (SNR)
- Fuentes de interferencia

El proceso es recorrer cada espacio donde el cliente requiere cobertura e ir capturando datos con las herramientas con el afán de obtener las posiciones más adecuadas de los equipos, se toma lectura de las interferencias internas y externas existentes en cada inmueble, es decir otros Access Point de terceros y equipos que funcionan en la banda 2.4GHz como hornos de microondas y teléfonos inalámbricos.

La realización correcta de este estudio es esencial para un diseño de acuerdo a las necesidades y condiciones físicas de los inmuebles, no se debe olvidar que las ondas de RF son susceptibles a diferentes efectos que degradan y/o absorben la señal y debe tenerse especial cuidado en la posición de los Access Point, en gran parte de esto depende la estabilidad de la red.

Una mala práctica es colocar los equipos al tanteo o incluso en el mismo lugar donde estaban los anteriores AP (en caso que existan AP en alguno de los sitios). Por lo tanto es importante hacer los recorridos de manera correcta y poder interpretar los resultados para plasmarlos en el diseño.

A continuación se indica de manera detallada el procedimiento completo que se debe llevar a cabo para la realización del recorrido.

1. Se debe instalar el software Cisco Site Survey Utility
2. Se debe configurar la tarjeta Cisco a/b/g con los drivers correctos
3. Se configura un Access Point (en este caso el AP estará en modo autónomo, el cual tiene un comportamiento en cuanto al servicio ofrecido igual a un AP LWAPP, el cual necesita el Controlador para realizar este estudio) con un SSID cualquiera, sin autenticación (no tiene acceso a recurso alguno), también se requiere un DHCP pool en el AP para la laptop que se usará en el recorrido.
4. Se instala la aplicación InterpreterAir o alguna similar, aquí se carga el mapa electrónico. Para configurar los parámetros solicitados del mapa se debe contar con la mediada (en metros) de la oficina, también es posible elegir si la oficina cuenta con cubículos, puertas, cristales y materiales que puedan obstruir la señal.

Este punto es importante porque los valores plasmados en el mapa deben ser los más cercanos a la realidad lo cual garantizará resultados verídicos.

5. Una vez que el mapa está completamente configurado se debe conectar la laptop al SSID configurado en el AP, una vez garantizada la comunicación y observando en estado de la conexión en la herramienta de Cisco se procede a iniciar el recorrido.

5. Una buena práctica es iniciar en un esquina de la oficina, se elige una zona abierta donde colocar el AP en el techo con las antenas perpendiculares al mismo; como se muestra en la figura.

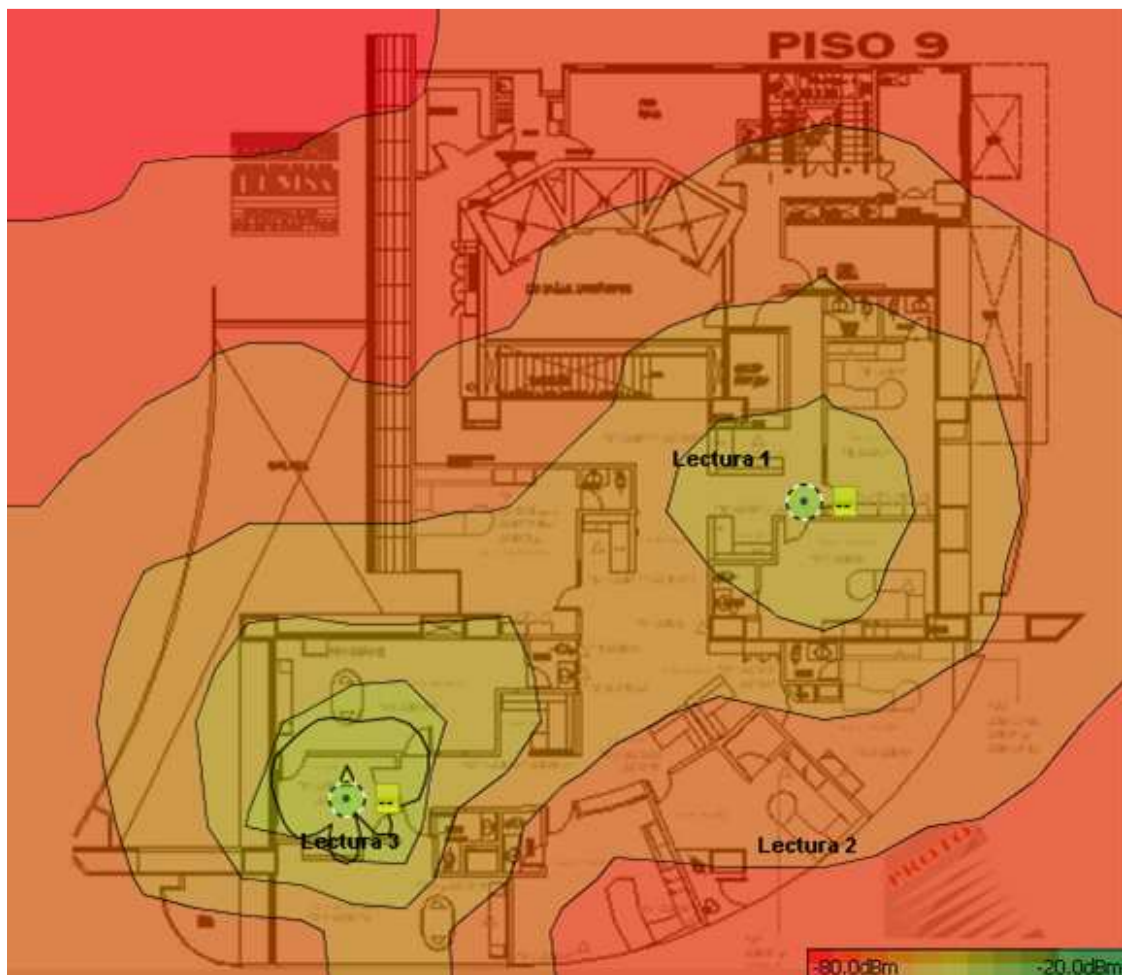
Imagen 3.3.2.1 Posición correcta en techo



6. Se realiza el recorrido en sentido opuesto al AP hasta que la señal recibida nos indique -75 dB, este parámetro es recomendado por Cisco como el límite donde puede ser garantizada una buena cobertura y por lo tanto una correcta transmisión de los datos. Una vez determinado este punto se realiza un recorrido en circular para delimitar la zona donde se colocará el siguiente AP. Justo este límite se coloca el siguiente Access Point y se procede a una lectura idéntica a la inicial, de tal manera que puedan irse cubriendo todos los espacios del lugar.

A continuación se muestra un mapa de cobertura de uno de los pisos donde existían dos Access Point los cuales fueron sustituidos y donde se realizaron modificaciones con la nueva la implementación, en el se pueden ver anotaciones, pero lo más importante es darse cuenta de la distancia cubierta la cual está basada en ciertos parámetros ya establecidos (algo como un código de colores) el cual nos indica el nivel de la señal en decibels dBm. A su vez la herramienta arroja datos con valores en cada punto (dB, índice de Señal-Ruido, etc.).

Imagen 3.3.2.2 Mapa de Cobertura



Como resultado de este Site Survey se obtuvo la cantidad de Access Point requeridos para la solución, es decir el total de equipos que cubren correctamente las zonas de todos los inmuebles de interés. Hay que señalar que normalmente se considera un porcentaje del 3 al 5 % de Access Point en caso de adiciones que el cliente solicita de manera inmediata.

NOTA: Los Access Point que se usan para el Site Survey deben ser exactamente iguales a los que se implementarán, incluso las antenas. Esto porque cada AP tiene características distintas y las antenas diferentes patrones de radiación.

Finalizando con el punto anterior, Cisco recomienda cierto modelo de Access Point y tipo de Antenas para diferentes implementaciones, interior, exterior, almacenes, oficinas, espacios abiertos, etc. sin embargo el conocimiento de la teoría y la experiencia ayudan a realizar una mejor elección.

*Para este proyecto se consideraron 300 Access Point.

NOTA: En algunos casos la cantidad de Access Point no solo la determina el nivel de cobertura requerida, también la cantidad de usuarios promedio que estarán conectados a la red inalámbrica (considerar un máximo de 25 por AP, si solo transmiten datos). En este proyecto la cantidad de usuarios no era considerable debido a que la red inalámbrica sería nueva y no se tendrían demasiados usuarios conectados.

Después se elige el modelo de Controlador a usar, gran parte de la decisión es con base en el número de Access Point; otros puntos a considerar serían la escalabilidad prevista, si se cuenta con algún Controlador actualmente, si se requiere redundancia, etc.

Para este proyecto se utilizó un modelo de Controlador Appliance 4400 en su modelo más robusto, el modelo instalado es AIR-WLC4404-100-K9, donde 04 significa que tiene cuatro puertos de distribución (Fibra Óptica) para comunicarse a la infraestructura donde se conectarán los AP, esta infraestructura son los Switches.

A su vez se debe elegir un licencia que puede soportar hasta 100 AP, en este caso se propusieron 4 Controladores con licencias de 100 cada uno, es decir un soporte de hasta 400, lo cual nos deja una holgura de 100 AP (un Controlador completo) el cual actuará como BackUp de cualquier de los 300 AP existentes, lo cual cumple con el requerimiento inicial del cliente el cual fue ofrecer al menos 25% de redundancia.

Como parte de la planeación de proyecto se debe poner especial cuidado en la seguridad requerida por el cliente, esta es basada en políticas bien establecidas que se deben seguir al pie de la letra por toda la unidad de negocio.

Se definió en conjunto con el personal involucrado del área de seguridad informática del cliente, se revisó la infraestructura con la que contaban, por ejemplo un Directorio Activo de Microsoft, Entidad Certificadora, herramientas de control de acceso, etc.

Otro punto que se consideró fueron los sistemas operativos y sobre todo las versiones y modelos de las tarjetas que se conectan a la red inalámbrica, esto es de suma importancia, porque el hecho de no definirlo correctamente puede dejar fuera de conexión a bastantes equipos, lo cual no es conveniente para ninguna de las partes involucradas.

Es este caso se configuraron WPA y WPA2 con PSK, que son sólo métodos de encriptación, no de autenticación, ya que el cliente no cuenta con la para soportar esta solución (Directorio Activo, Entidad Certificadora, etc.), sin embargo esta opción está planeada para una segunda fase. Este tipo de encriptación no es tan fácilmente vulnerable como WEP, además se sugirió la utilización de autenticación física de Mac Address, para esta opción se utiliza el equipo mencionado en los conceptos generales llamado Cisco Secure Access Control Server (ACS) donde residen todas las Mac Address de las tarjetas inalámbricas que los equipos que requieren acceso.

Finalmente se recomendó agregar una herramienta de Administración, Resolución de problemas (troubleshooting) y configuración que integre el control de los Controladores, valga la redundancia.

En la realización del Site Survey, el cual es medular en la fase de planeación del proyecto trabajé de maneras diversas debido a la magnitud del proyecto. En los sitios marcados por el cliente como críticos fui quien realizó el estudio de manera íntegra. Algunos otros sitios de regular magnitud fui apoyado por ingenieros compañeros de la empresa, resultados que al final tuve que validar.

Finalmente se tomó ventaja de ciertos sitios que ya contaban con estudios previos por compañeros del área de preventa quienes hicieron algunos estudios previos para cumplir con los requerimientos del RFP (Request For Proposal). De esta manera se logro completar esta fase y contar con toda la información para diseñar la solución.

3.3.3 Diseño de la Red

Como se mencionó en la Planeación, con el Site Survey se define completamente la cantidad de AP necesarios, así como el modelo basado en las Best Practices de Cisco y los conocimientos teóricos del ingeniero. Los 300 AP ubican físicamente en cada unos de los puntos indicados en los mapas del Site Survey, los cuales también definieron la cantidad de AP por sitio (esos resultados no se incluyen). Para esta solución se eligieron equipos AIR-LAP1242AG. LAP indica que son modo Lightweight (LWAPP) los cuales permiten dividir las funciones del Access Point entre procesos locales en los AP y el Controlador, haciendo a través de un túnel UDP encriptado entre AP y Controlador.

Debido a las nuevas característica de la red switchheada se definirán segmentos de red (VLANs) y la opción viable para el funcionamiento de los Controladores es hacerlo en Capa 3 del modelo OSI.

Se definió de qué manera se conectaría los Controladores a la red Cableada, el cual será el punto de conexión hacia todos los servicios de red corporativos.

Se partió de la primicia donde el cliente contaba con un Centro de Datos donde residen los equipos que son el Core de la red (Datos, Voz y Seguridad)

Este sitio central conecta a cada una de la oficinas remotas a través de enlaces dedicados L2L (LAN-to-LAN) hacía los SW de Core, equipos robustos que ofrecen redundancia, ruteo, calidad de servicio, alto procesamiento de información, etc. Es aquí donde se colocó el Controlador 1 con 100% de utilización (cantidad de AP).

El Controlador 2 se colocará en este mismo sitio pero sin utilización real, es decir será el respaldo (BackUp) para poder aceptar hasta 100 AP de cualquiera de las ubicaciones esto en caso de que falle uno de los tres Controladores restantes.

Por cuestiones de criticidad en uno de los sitios, lugar donde labora el responsable de la dependencia, se decide colocar el Controlador 3, para tener un equipo local que envíe la menos información posible a través de su enlace L2L y evitar problemas de congestión e incluso que la infraestructura siga funcionando aún si el enlace esta caído. Por esta razón se coloca un Controlador en este sitio.

El Site Survey arrojó resultados donde un sitio debería tener 45 AP para poder cubrir todas sus zonas del inmueble, por tal razón en este sitio se propuso instalar el Controlador 4, ya que tendría utilización de casi 50% con AP locales.

La conexión de los Controladores con los SW de Core se realizó a través de fibra óptica multimodo, los conectores necesarios para son LC-LC esto porque los Controladores soportan solo interfaces SFP (Small Form-Factor Pluggable).

Cada puerto de distribución es capaz de soportar 25 Access Point por lo tanto se deben utilizar los 4 puertos, se consideró el numero de SFPs y fibras para la conexión.

A continuación se muestran las imágenes de los elementos mencionados:

Imagen 3.3.3.1 Controlador 4404



Imagen 3.3.3.2 SFP



Imagen 3.3.3.3 Jumper de Fibra

Fibra LC-LC



En el diseño se debe considerar cuántos SIDD se configuran para cumplir con las necesidades del cliente.

Al ser una red que solo soportaría datos y requería poder conectarse con el mismo perfil configurado en las laptops dondequiera que el usuario estuviera, es decir que los usuarios pudieran moverse de un edificio a otro por alguna junta, entrenamiento o reubicación y deberían poder seguir utilizando los servicios de red sin modificación o configuración extra.

Se decidió configurar tres diferentes SSID, uno para las áreas gerenciales, otro para los usuarios internos por debajo de un nivel gerencial y un tercero para invitados (llámense consultores, proveedores o clientes).

El segmento de red (VLAN) gerencial se configuró con una calidad de servicio (QoS Silver) que garantizará la transmisión aun cuando existiera una saturación en la red.

El acceso a los usuarios por debajo del nivel gerencial (les llamé Usuarios Generales), no tendrían configurada calidad de servicio en su VLAN.

Los usuarios Invitados serían capaces de conectarse a Internet, sin poder ingresar a ningún servicio de red corporativo, esto se limitó con listas de acceso (ACLs).

Como resultado de las charlas con el cliente y de la revisión de los Sistemas Operativos y la infraestructura se decidió configurar seguridad WPA y WPA2 con TKIP o AES. También se configuró autenticación física de las Mac Address de las tarjetas inalámbricas, tal autenticación se hizo en los Servidores de Cisco Secure Access Control Server (ACS). Este diseño incluye a los dos SSIDs corporativos.

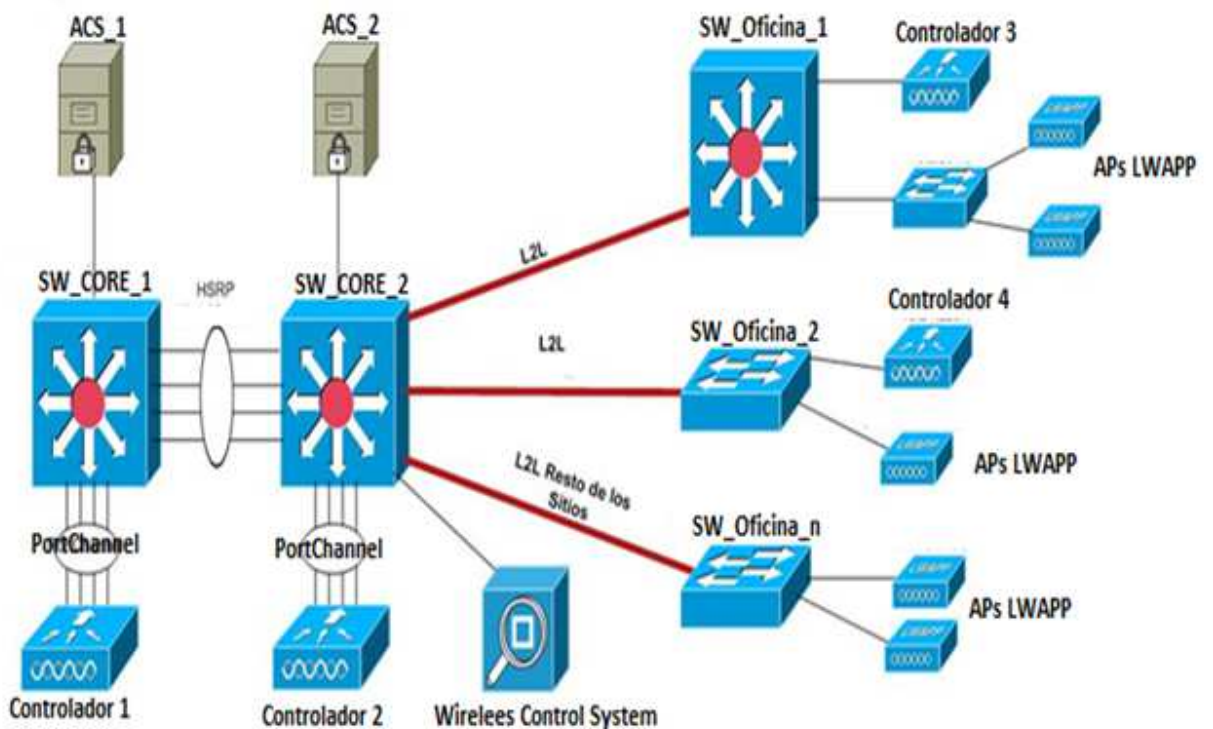
Los Servidores ACS se implementaron de manera redundante, es decir que replican su Base de Datos del primario al secundario. Para el acceso a la red de Invitados se realizará una autenticación vía Web donde el usuario necesita ingresar usuario y contraseña correctos, datos que son generados por el administrador de la red. Estos accesos también son verificados contra en Servidor ACS.

Los Servidores ACS son modelo CSACSE-1113-K9, los cuales se conectarán directo a los equipos de Core, los Switches más robustos de la solución que residen en el centro de datos, así que la redundancia en comunicación está garantizada y también el servicio de autenticación de usuarios inalámbricos con los dos ACS.

Una herramienta importante para el mantenimiento y la resolución de problemas de la red inalámbrica es una aplicación llamada Wireless Control System (WCS), la cual se encarga de centralizar a los Controladores en un solo punto de configuración, administración y control de la red. Se propone un Servidor IBM para montar la aplicación y las licencias necesarias para soportar los 300 APs.

El siguiente paso es diseñar la topología de red para definir la interconexión con la red cableada, punto vital e importante para un buen funcionamiento de la red. La figura muestra la topología de la solución.

Imagen 3.3.3.4 Diagrama de la Solución Inalámbrica



Se tienen los siguientes elementos:

Switches de Core: Son los encargados de ofrecer redundancia, alto rendimiento y procesamiento de datos, así como y el ruteo de toda la red. Se conectaron a través de un puerto llamado EtherChannel que ofrece mayor ancho de banda para el intercambio y comparten una IP virtual para la alta disponibilidad con el protocolo HSRP.

ACS: Los encargados de la seguridad de la red conectados a los equipos de Core configurados para replicar la Base de Datos de un equipo al otro.

Wireless LAN Controller WLC: Conectados por fibra óptica a los equipos de Core, en el caso de los Controlador 1 y 2. Controlador 3 y 4 se conectará n también vía fibra en el Core del sitio remoto.

Access Point: Los Access Point estarán conectados a los Switches de acceso a través de un puerto TRUNK, el cual dejará pasar todas las redes configuradas para los SSIDs.

Wireless Control System (WCS): Se conectará en los equipos de Core del sitio central.

Las conexiones entre cada sitio remoto hacia el sitio central se harán mediante un enlace dedicado L2L (LAN-to-LAN) de entre 6 y 8 Mbps.

El diseño de la red fue relativamente sencillo, esto debido a que la red de datos sería también implementada por la misma empresa, el diseño inalámbrico fue realizado 100% por mí. Las consideraciones que se tomaron fue el direccionamiento utilizado, las políticas de seguridad aplicadas en el firewall, el sistema operativo de las computadoras que se conectan a la red inalámbrica y los parámetros de calidad de servicio requeridos por la red .

El diseño de la solución se basó en la criticidad de los sitios, la cantidad de usuarios que se conectarían y los requerimientos de equipo del cliente. Al ser una implementación en un organismo gubernamental cabe señalar que la cantidad de equipo destinado por sitio, algunas veces, se mide con base en el presupuesto de cada área en más que en el presupuesto de toda la dependencia.

3.3.4 Implementación de la Solución

En la implementación se deben tomar en cuenta y configurar todos los puntos incluidos en la Planeación y el Diseño. La lógica de configuración es la siguiente:

- Controladores
- Access Point
- ACS
- WCS
- Conexión de todos los elementos
- Revisión de la solución
- Protocolos de pruebas

Para los Controladores se configuran los puntos siguientes:

- Nombre, IP Management, IP AP Manager y accesos para su administración
- Interfaces
- SSIDs (redes para la conexión de los usuarios)
- Seguridad (Encriptación y Autenticación)
- Puertos de distribución para la conexión a los switches
- Redundancia

Cuando el Controlador es instalado por primera vez o después de un Reset Factory Default (borrado de toda la configuración existente), se inicia con un Startup Wizard (un asistente de configuración) para poder comenzar con la misma.

Los pasos son los siguientes:

1. Asegurarse que el nombre del Controlador no sea mayor a 32 caracteres.
2. Agregar el usuario y contraseña del Administrador, cada uno de máximo 24 caracteres.
3. Configurar la interface del Service Port (la cual se utiliza cuando la red se ha caído y no es posible administrarla a través la interface de Management). Se tiene la opción de DHCP o estático, se recomienda que sea estático.
4. Enseguida se debe configurar la IP de Management, con máscara y default Gateway, de manera opcional se puede configurar la VLAN a la cual esta asignada.
5. Se debe configurar el numero de Puertos de Distribución, es esta instalación se utilizaron los 4 para poder soportar la carga máxima de Access Point.
6. De manera opcional se puede configurar el DHCP Pool, es decir el grupo de direcciones IP que usaran los clientes que se conecten a la red. En este caso la configuración de DHCP se hizo en los Switches.
7. Configurar si el Controlador trabajara en Capa 2 o 3 del modelo OSI, en este caso se configuró como Capa 3.
8. Se debe configurar un IP virtual que será usada de manera interna por los Controladores para fines de seguridad y movilidad, en este caso se configuró la IP 1.1.1.1.

-
9. Configurar el Cisco WLAN Solution Mobility Group (RF group), este nombre el común a todos los Controladores y es usado para negociar los parámetros de movilidad y ambiente RF con los demás Controladores involucrados.
 10. Configurar el primero SSID que se usará para la red, en este caso se configuró el perfil "VIP" para las áreas gerenciales y direcciones.
 11. Configurar si lo clientes al conectarse a la red inalámbrica soportarán direcciones IP estáticas o solo dinámicas, se recomienda que solo sean dinámicas (DCHP), opción configurada en esta solución.
 12. Finalmente, de manera opcional, se configura el Servidor Radius para la autenticación. Esta configuración se hizo vía Web, ya que presenta todas las opciones requeridas.
 13. El siguiente paso es habilitar los radios que serán usados en la red, es decir 802.11a, b y/o g. En este caso se configuraron b y g.
 14. Finalmente se configura la opción de Radio Resource Management, RRM (auto RF). Esta opción ayuda a que el Controlador coordine y negocie en ambiente RF (canales y potencias) dentro de la red instalada.

Una vez que se tienen estos parámetros se debe realizar la conexión de los Puertos de Distribución hacia los Switches para lograr la comunicación:

La configuración es la siguiente:

```
interface GigabitEthernet1/15
description MXLIE01S01WLC01
switchport trunk native vlan 220
switchport mode trunk
channel-group 1 mode on
```

A continuación se explica el efecto de cada comando:

interface GigabitEthernet1/15

(puerto físico donde se conecta uno de los Puertos de Distribución)

description MXLIE01S01WLC01

(se usa como etiqueta para identificar el equipo conectado)

switchport trunk native vlan 220

(se indica a qué VLAN pertenece la IP de management)

switchport mode trunk

(se configura el puerto del Switch para que acepte el paso de todas las VLAN -SSIDs)

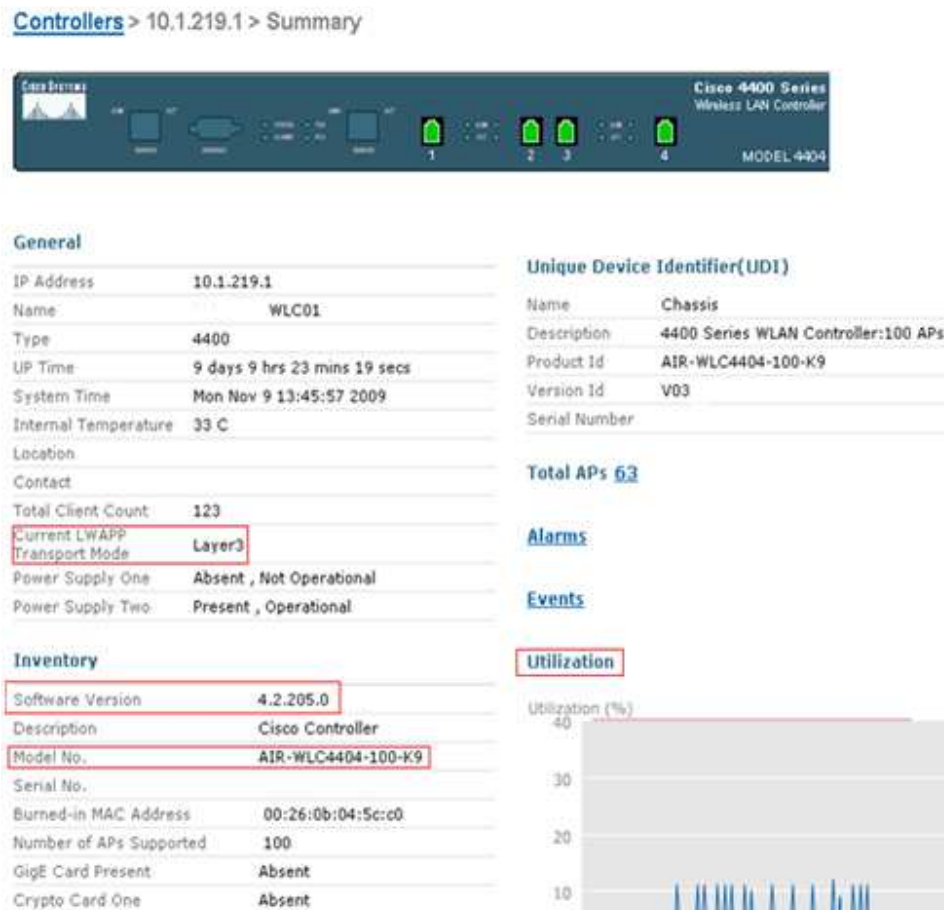
channel-group 1 mode on

(se agrega el puerto a una interface Virtual)

De esta manera se configuraron los cuatro puertos en cada Switch para soportar LAG (Link Aggregation).

A partir de este punto es posible conectar una computadora a la red e ingresar vía WEB al Controlador y continuar con la configuración como se muestra en la siguiente imagen.

Imagen 3.3.4.1 Página principal de Controlador



En esta imagen se muestran parámetros generales de la configuración, algunos de los más importantes a resaltar son:

Versión de Software: 4.2.205.0

Modo LWAPP: Layer 3 (capa 3)

Modelo de Controlador: AIR-WLC4004-100-K9

Utilización: Porcentaje actual de utilización de los recursos del Controlador

El siguiente paso es la configuración de los SSIDs (WLAN). Continuando con la configuración vía Web (la cual es más amigable y directa que la configuración por CLI (Command Line Interface)).

La configuración de los SSID involucra interfaces que deben ser creadas en los Switches y que serán mapeadas (relacionadas) con los SSID (WLAN).

Se debe configurar un SSID por cada WLAN, en este caso se configuraron 3 WLANs.

A continuación se muestra una imagen de la configuración de las WLAN:

En la imagen puede verse el nombre de las interfaces, la VLAN a la cual pertenecen, la dirección IP. Esta interfaces deben ser alcanzadas en la red LAN, es decir debe de haber conectividad garantizada desde la red cableada para que asegurar que la red inalámbrica funcionara de manera correcta al mapear el SSID (WLAN) a la interface (VLAN).

A continuación se muestra la manera de configurar una VLAN en capa 2 y Capa 3 en un Switch L3.

```
config terminal
vlan 223
name INVITADOS
exit
```

```
config terminal
Interface VLAN 223
ip address 10.1.223.1 mask 255.255.255.0
no shut
exit
```

Los pasos de configuración de la interfaces son los siguientes:

1. Agregar una interface
2. Escribir el nombre de la interface (normalmente se recomienda usar el mismo que se le asignara a la WLAN)
3. Escribir el identificador de la VLAN (VLAN ID), es el mismo ID con el cual se configura la VLAN en el Switch
4. Se escribe la dirección IP, Mascara y Default Gateway

Una vez creadas tantas interfaces como sean necesarias se procede a configurar las WLAN en el Controlador; en este proyecto se configuraron tres WLANs lo cual implica tres VLAN en los Switches para cada uno de los Sitios donde se conectó el Controlador.

Imagen 3.3.4.2 Interfaces del Controlador

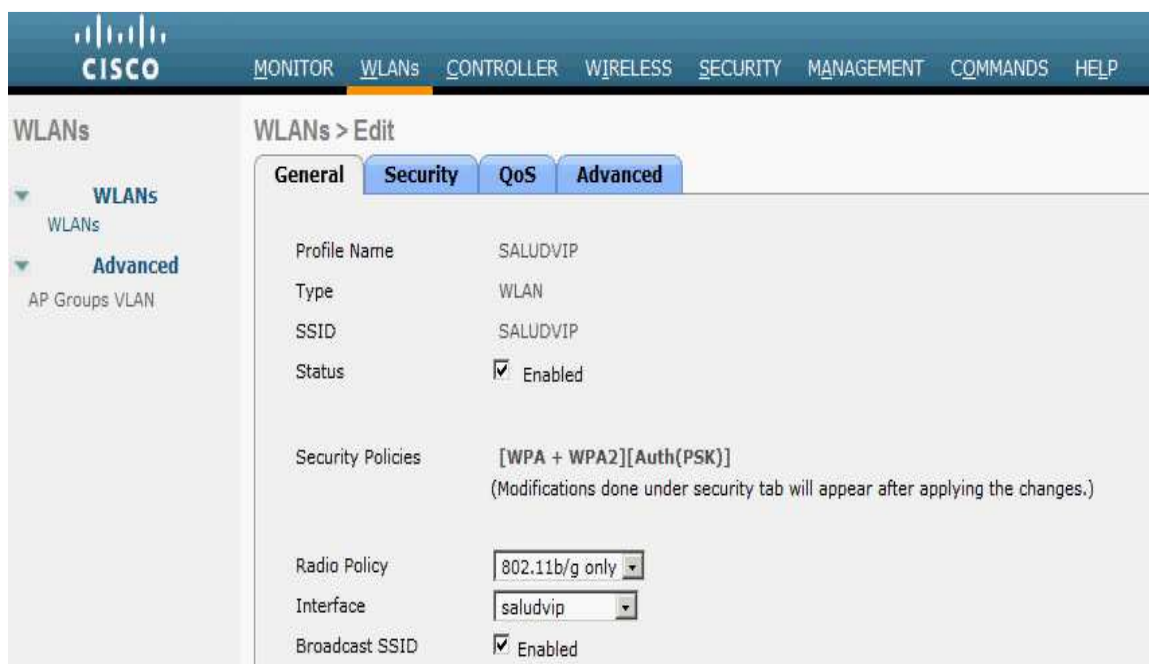
Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	untagged	10.1.219.2	Static	Enabled
management	untagged	10.1.219.1	Static	Not Supported
saludinvitados	223	10.1.223.1	Dynamic	Disabled
saludvip	221	10.1.221.1	Dynamic	Disabled
saludwlan	222	10.1.222.1	Dynamic	Disabled
service-port	N/A	192.168.0.1	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported
wlan2	431	10.1.225.3	Dynamic	Disabled

La configuración de las WLAN debe seguir el siguiente orden:

- i. Crear una nueva WLAN
- ii. Escribir el nombre de la misma
- iii. Escribir el nombre del SSID
- iv. Elegir el tipo de seguridad que se desea, para este proyecto se decidió configurar WPA TKIP y WPA2 AES. En este punto se configura el PSK (PreShareKey) la llave preestablecida.

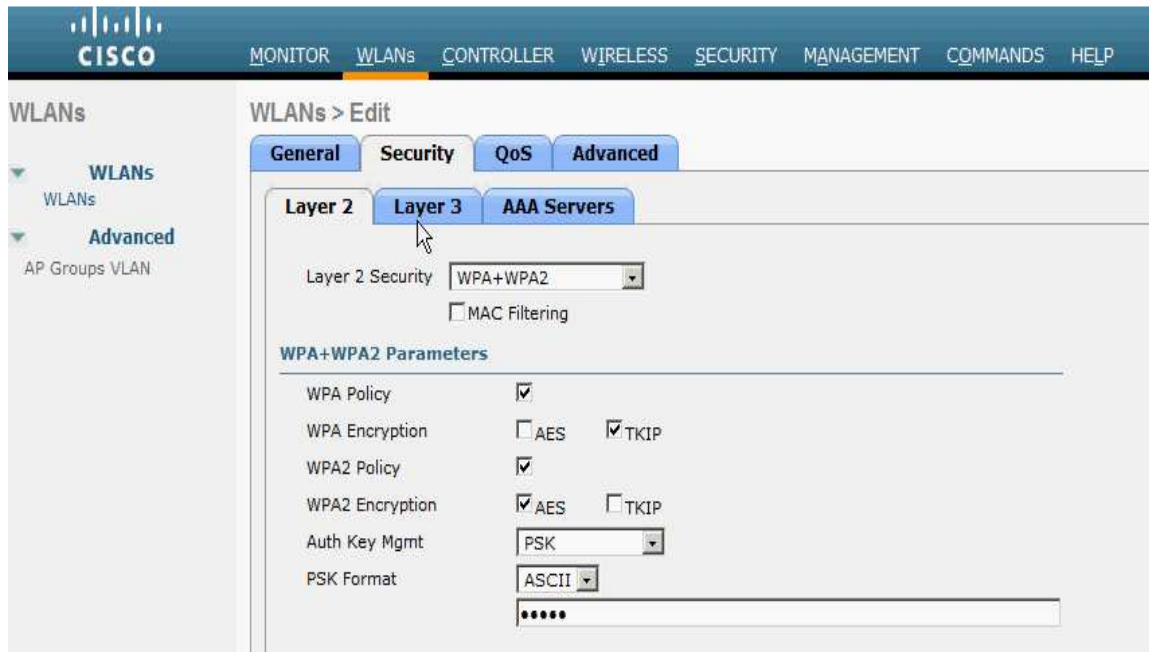
A continuación se muestra la imagen de una interface configurada:

Imagen 3.3.4.3 Configuración de WLANs



La siguiente imagen muestra los parámetros de seguridad de las WLAN:

Imagen 3.3.4.4 Configuración de parámetros de seguridad de capa 2



En esta imagen se puede observar que la opción de Security está siendo configurada en Layer 2 (capa 2), de la misma manera se debe configurar cada WLAN corporativa.

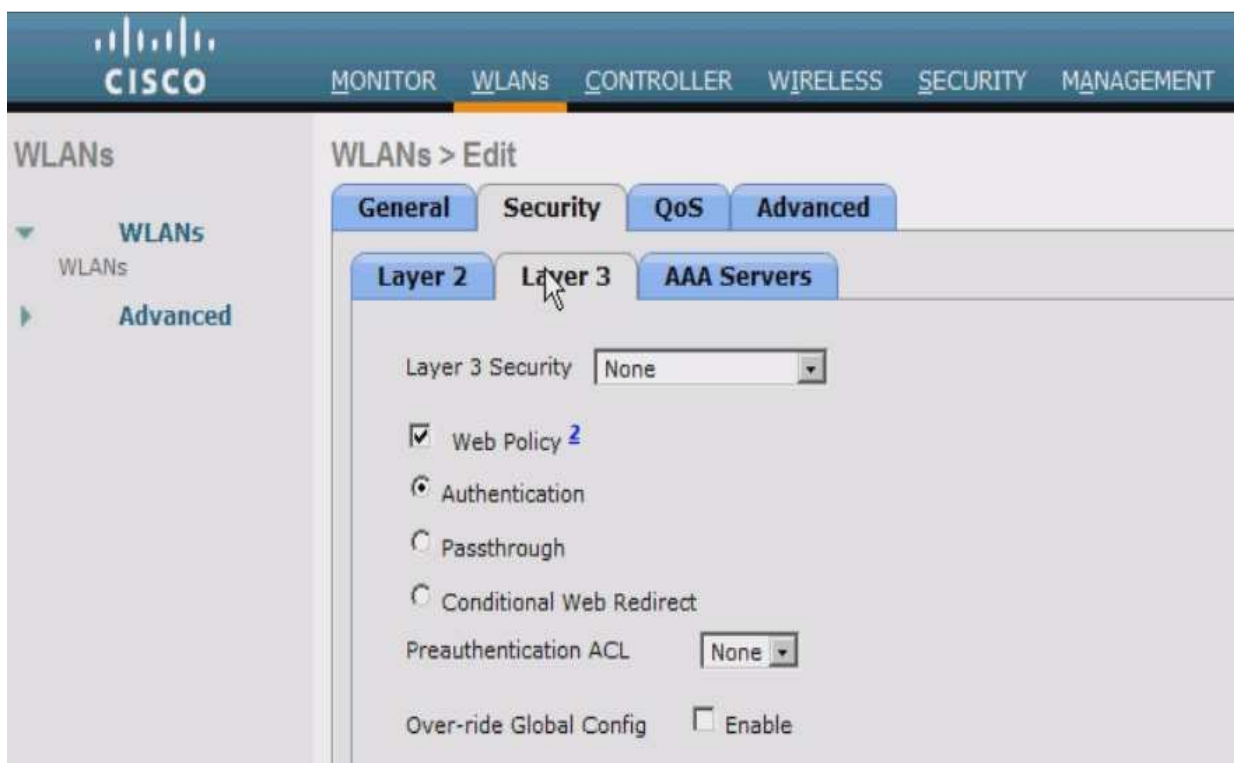
En el caso del acceso para Invitados (Guest), como ya se mencionó, se debe considerar una autenticación vía Web la cual incluye requiere el ingreso de un usuario y contraseña que serán administrados de manera local en el ACS (Access Control Server).

Una WLAN de Invitados es donde los usuarios no tienen acceso a la red corporativa debido a que normalmente son usuarios externos, proveedores o personal con que trabajo provisionalmente en la dependencia. La configuración de la seguridad se debe hacer en Layer 3 (capa 3) como se muestra en la siguiente imagen. Se puede observar que la configuración se hace bajo la opción Layer 3, sin embargo en la opción precisa de Layer 3 se elige la opción NONE.

Enseguida se elige la opción de Web Policy, para que los usuarios sean re direccionados a una página web donde se ingresa Username y Password.

En las redes de Invitados, el usuario se conecta de manera “automática” al SSID, hasta este punto está asociado a la red y el usuario cuenta con una dirección IP, en ese momento no hay comunicación a ningún punto de la red excepto al DNS. El usuario debe abrir un Explorer o cualquier browser donde se solicitan las credenciales de acceso. Para evitar la comunicación de una red de Invitados con la red corporativa se debe configurar lista de acceso, la cuales sirven para filtrar ciertas redes (y puertos) origen hacia ciertas redes (y puertos) destino para asegurar segmentos de la red corporativa.

Imagen 3.3.4.5 Configuración de parámetros de seguridad de capa 3



A continuación se muestran los comandos de configuración de las listas de acceso para la red de Invitados.

```
ip access-list extended INVITADOS
permit udp any any eq bootps
permit ip 10.8.223.0 0.0.0.255 host 204.153.24.1
permit ip 10.8.223.0 0.0.0.255 host 148.207.38.1
permit ip 10.8.223.0 0.0.0.255 host 207.249.5.10
deny ip 10.8.223.0 0.0.0.255 10.0.0.0 0.255.255.255
permit ip 10.8.223.0 0.0.0.255 any
```

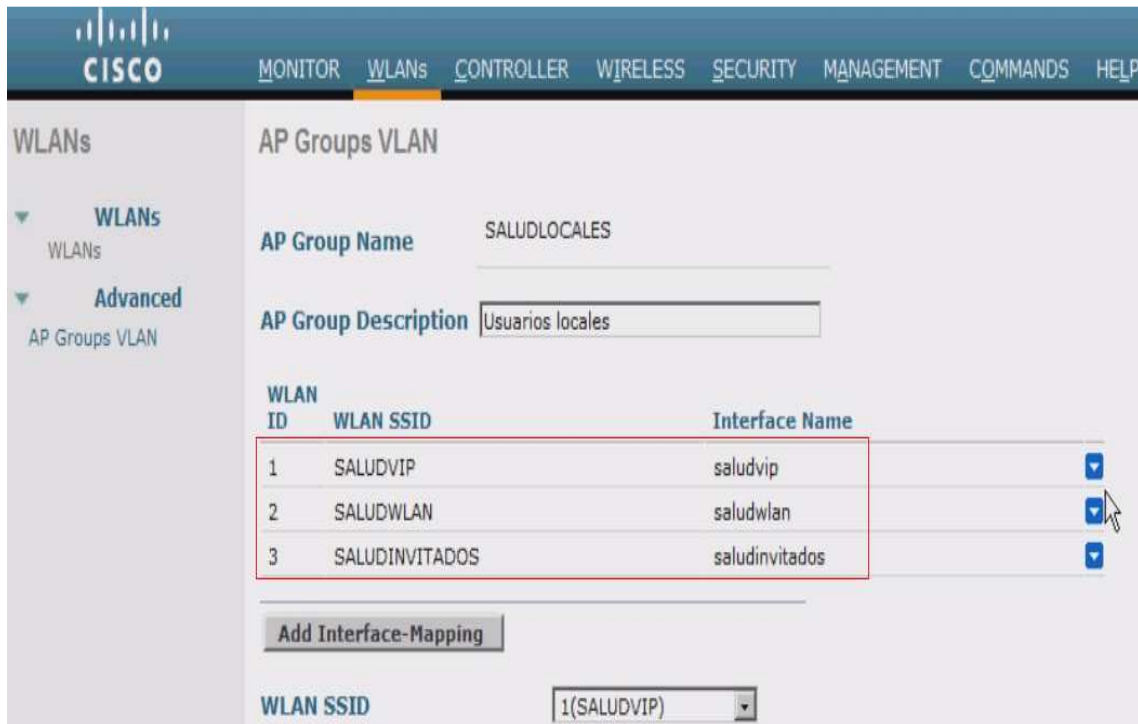
```
interface Vlan223
ip address 10.9.223.254 255.255.255.0
ip access-group INVITADOS in
```

La manera de configurar la lista de acceso es elegir un nombre, saber qué redes se deben filtrar, en este caso se permiten la red de Invitados hacia los DNS y el DHCP server y después se niega la comunicación a toda la red corporativa. Finalmente se aplica la lista de acceso a la interface VLAN.

Otro de los parámetros de configuración para la red de Invitados debe ser el Servidor Radius (ACS) donde se configuran las credenciales la cual se mencionara de manera detallada más adelante. A continuación se debe configurar una característica donde los SSID estarán disponibles de manera local cuando los Controladores están ubicados en un sitio remoto, mapear el SSID con la interface y después agruparlos para poder manipularlos en los Access Point que nos convenga (donde se desean publicar los SSID).

Esta característica se llama AP Groups y se muestra la configuración en la imagen, básicamente sólo se elige el nombre del Grupo y cada SSID se va asociando con la interface (VLAN) correspondiente.

Imagen 3.3.4.6 Configuración de Grupos



Otro punto importante en la configuración de una solución inalámbrica unificada que se conforma por más de un Controlador es la Alta Disponibilidad.

La característica más importante es configurar idénticamente los Controladores que participaran en la Alta Disponibilidad, esto para asegurar que todos los parámetros utilizados para que la red inalámbrica funcione correctamente se mantengan sin importar a que Controlador los AP están asociados. Una vez que se tiene la certeza que la configuración es la misma y que se han realizado las pruebas de conexión en cada uno de los Controladores que participarán en la Alta Disponibilidad se debe configurar de la siguiente manera. Cada AP puede configurarse de manera independiente con hasta tres Controladores como se muestra en la imagen. Se elige la opción Wireless, después el Access Point y finalmente la opción High Availability de interés donde escribe el nombre y dirección IP de los Controladores en el orden deseado, hasta tres.

NOTA: Esta configuración se realiza después de haber agregado los Access Point a algún Controlador, tal proceso se indica en el apartado Configuración de Access Point.

Imagen 3.3.4.7 Configuración de redundancia de controladores

The screenshot shows the Cisco Wireless Management interface for the configuration of AP2-INS-P4. The 'High Availability' tab is active, displaying a table of three controllers. The table has columns for 'Name' and 'Management IP Address'. Below the table, the 'AP Failover Priority' is set to 'Low'.

	Name	Management IP Address
Primary Controller	MXINF501WLC01	10.1.219.1
Secondary Controller	MXINF501WLC02	10.1.220.1
Tertiary Controller	MXBUEN01WLC01	10.1.221.1

AP Failover Priority: Low

El interacción de los AP entre sí requieren de algún tipo de control sobre la asignación de potencia de cobertura así como las asignación de los canales, se debe recordar que solo se permiten tres canales de no traslape, es decir que no generarán interferencia entre ellos para que la salud de la red inalámbrica se mantendrá estable. Otro punto que se garantiza con esta configuración es el Roaming.

Los parámetros que controlan estas características son Default Mobility Domain y RF Group Name, los cuales son configurados en la opción Controller, como se muestra en la siguiente imagen:

Imagen 3.3.4.8 Configuración de Mobility Domain

The screenshot shows the Cisco Controller configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The left sidebar lists various configuration categories: General, Inventory, Interfaces, Multicast, Network Routes, Internal DHCP Server, Mobility Management (highlighted), Ports, NTP, CDP, and Advanced. The main content area is titled 'General' and contains the following configuration items:

Name	MXINFS01WLC01
802.3x Flow Control Mode	Disabled
LAG Mode on next reboot	Enabled (LAG Mode is currently enabled)
Broadcast Forwarding	Disabled
AP Multicast Mode	Unicast
AP Fallback	Enabled
Apple Talk Bridging	Disabled
Fast SSID change	Disabled
Default Mobility Domain Name	WLANSALUD
RF Group Name	WLANSALUD
User Idle Timeout (seconds)	300
ARP Timeout (seconds)	300

3.3.5 Configuración de Access Point

Hasta este punto la configuración se ha concentrado en los Controladores, los cuales son la parte más importante de la solución, no solo porque son el Core de la red inalámbrica si no porque después de finalizar con este proceso la configuración de los AP es directa y sencilla, solo se deben considerar algunos detalles previos a la asignación de los AP al controlador asignado.

Los pasos para agregar los AP a un controlador son los siguientes:

- Considerar uno de los siguientes puntos para indicarle a los AP como localizar el Controlador. (Vía DNS, Configuración de la dirección IP del Controlador en cada AP, vía DHCP con la opción 43 o a través de la herramienta Upgrade Tool).

Para esta solución, lo cual recomiendo totalmente debido a que no se depende de alguna herramienta extra, se usó la opción 43 en el DHCP. A continuación se muestra la configuración del DHCP en el Switch de Core de cada sitio donde se conectaron los Access Point.

```
ip dhcp pool SALUD_ACCESS_POINT
network 10.9.218.0 255.255.255.0
default-router 10.9.218.254
option 60 ascii "VCI string of the AP"
option 43 hex f110.0a01.db01.0a01.dc01.0a02.dc01.0a18.dc01
```

El parámetro a resaltar en la configuración del DHCP es el valor en hexadecimal de los cuanto Controladores involucrados con un prefijo, los cuales serán usados por cada AP que reciba su dirección IP de este DHCP Pool y pueda realizar petición de Agregación a cualquiera de los Controladores que estén disponibles.

- Una vez que el AP contacta al Controlador, se intercambia un certificado que autentica cada uno de los AP para garantizar que ningún otro equipo no permitido pueda agregarse como AP valido en la red inalámbrica.
- En el siguiente paso el Controlador revisa la versión de los AP, en caso de ser distinta a la del Controlador, se envía una actualización.
- Agregados los AP aparecerán con el valor REG que indica un correcto registro al Controlador.

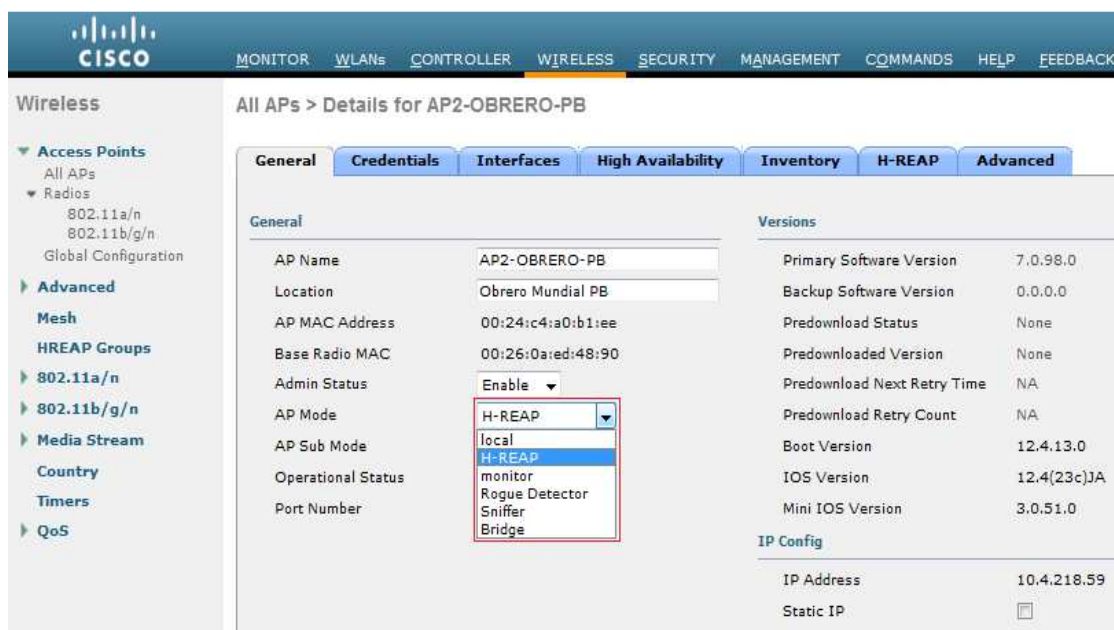
A continuación se muestra la imagen con los AP agregados satisfactoriamente:

Imagen 3.3.5.1 Verificación de APs asociados

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status
AP2-OBRERO-PB	AIR-LAP1242AG-N-K9	00:24:c4:a0:b1:ee	30 d, 18 h 35 m 58 s	Enabled	REG
AP1-ABRAHAMGLZ-P1	AIR-LAP1242AG-N-K9	00:24:c4:a0:d2:82	25 d, 01 h 44 m 08 s	Enabled	REG
AP1-ABRAHAMGLZ-P2	AIR-LAP1242AG-N-K9	00:24:c4:a0:d6:a0	25 d, 01 h 44 m 08 s	Enabled	REG
AP-EQUEGLZMTZ-P1	AIR-LAP1242AG-N-K9	00:24:c4:a0:d3:fc	38 d, 14 h 54 m 59 s	Enabled	REG
AP4-GCAMPA-P3	AIR-LAP1242AG-N-K9	00:24:c4:a0:d3:8a	17 d, 03 h 51 m 36 s	Enabled	REG
AP1-INS-P10	AIR-LAP1242AG-N-K9	00:24:c4:a0:b5:cc	79 d, 16 h 14 m 32 s	Enabled	REG
AP2-INS-P10	AIR-LAP1242AG-N-K9	00:24:c4:a0:b0:a6	79 d, 16 h 52 m 19 s	Enabled	REG
AP4-INS-P4	AIR-LAP1242AG-N-K9	00:24:c4:a0:a7:d4	78 d, 15 h 58 m 49 s	Enabled	REG
AP2-INS-P4	AIR-LAP1242AG-N-K9	00:24:c4:a0:ba:6c	78 d, 16 h 18 m 04 s	Enabled	REG
AP1-JVASCONCELOS-P4	AIR-LAP1242AG-N-K9	00:24:c4:a0:d6:6e	54 d, 09 h 03 m 30 s	Enabled	REG
AP1-INS-P4	AIR-LAP1242AG-N-K9	00:24:c4:a0:b7:7a	78 d, 14 h 41 m 25 s	Enabled	REG

- A partir de aquí se personalizan con el nombre, dirección IP (en caso de quererla cambiar o configurarla de manera estática) y alta disponibilidad (como se mencionó anteriormente).
- La opción importante que debe ser configurada en cada AP es el Modo H-Reap, el cual indica que el AP está conectado en sitio remoto y se comunica con el Controlador a través del enlace L2L. Al elegir cualquier modo de operación del AP este deberá ser reiniciado para que el valor sea tomado en cuenta. A continuación se muestra la imagen donde se configura dicha opción.

Imagen 3.3.5.2 Conversión a H-REAP



- Después que el AP Mode se cambia a H-REAP se debe configurar en la opción H-REAP el mapeo de las VLAN (SSID) que serán publicados en los AP que se conectan de manera remota. De esta manera se asegura que cada AP pueda usar las interfaces configuradas, a continuación se muestra la imagen donde se configura tal opción:

Imagen 3.3.5.3 Mapeo de VLANs

The screenshot shows the Cisco Wireless Controller interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, and SECURITY. The left sidebar shows the configuration tree under 'Wireless', with 'Access Points' expanded to show 'AP1-ABRAHAMGLZ-P1'. The main content area is titled 'All APs > AP1-ABRAHAMGLZ-P1 > VLAN Mappings'. It displays the AP Name as 'AP1-ABRAHAMGLZ-P1' and the Base Radio MAC as '00:26:0a:ee:4d:90'. Below this is a table of VLAN mappings:

WLAN Id	SSID	VLAN ID
1	WLANVIP	221
2	WLANGRAL	222
3	WLANINVITADOS	223

Below the table, there is a section for 'Centrally switched Wlans' with a table header:

WLAN Id	SSID	VLAN ID
---------	------	---------

3.3.6 Configuración de Servidores de Seguridad (ACS)

Como se ya se mencionó en la Planeación del Proyecto el Servidor Cisco Secure Access Control Server (ACS) ofrece una base de datos local con usuarios y contraseñas que serán usadas para validar a los clientes que hacen uso de la red de Invitados. Para poder dar de alta los valores necesarios en los Controladores para que sean capaces de invocar los servicios del ACS se deben realizar la configuración de los Servidores de manera inicial.

Para esta solución se consideraron dos ACS para ofrecer redundancia en caso de la perdida de servicio del primario donde se realizan las configuraciones de los equipos y los usuarios y el cual replica dicha configuración al Servidor secundario.

El servidor ACS está basado en Linux y ofrece conexión vía Consola para configurar los parámetros mínimos para poder accederlo vía Web y poder configurar todas las características necesarias.

Los pasos para configurar dichos parámetros son los siguientes:

- Conectarse vía consola con un cliente como Microsoft Hyperterminal o Secure CRT con los siguientes valores en el puerto Serial
 - Baud = 115200
 - Databits = 8
 - Parity = N
 - Stops = 1
 - Flow control = None
- Una vez conectado al Servidor se deberán ingresar las Credenciales por Default que solicita el equipo:
 - Usuario: Administrator
 - Password: setup
- Al ingresar las credenciales, el Servidor solicita de manera individual los siguientes parámetros, los cuales son mandatorio para su configuración inicial:
 - Nombre del equipo
 - DNS domain
- Cuenta (usuario y contraseña) para administrar el equipo
- Dirección IP (dinámica o estática), en este caso se configuran estáticas, mascara y default Gateway (para que estos valores sean validos se debe conectar el equipo a la red).
- Se configura horario y fecha
- Finalmente se salva la configuración y el equipo se reinicia de manera automática

- A partir de este punto se podrá ingresar al equipos vía Web siguiendo el siguiente formato:
- `http://ipaddress:2002`
- A continuación se muestra la página de inicio cuando de ingresa al ACS:

Imagen 3.3.6.1 Página principal del ACS



Cisco Secure ACS v4.2

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

X Log Off



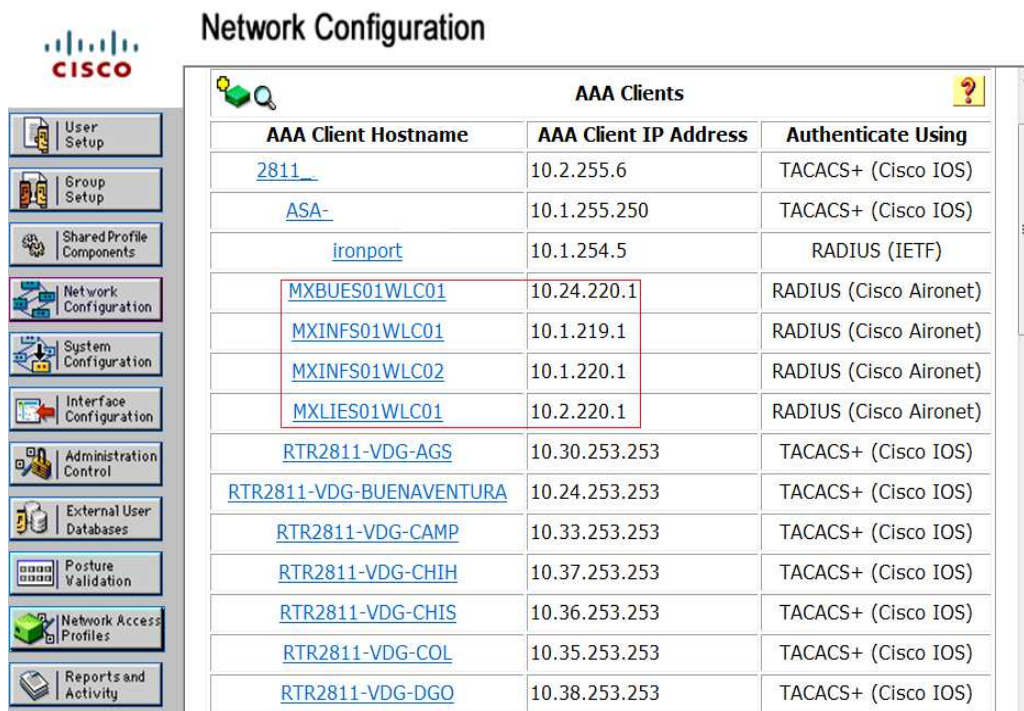
Select "Log Off" to end the administration session.

CiscoSecure ACS v4.2 offers support for multiple AAA Clients and features. It also supports several methods of authorization, authentication, and accounting, including several one-time-password cards. For more information on upgrades, please visit <http://www.cisco.com>.

CiscoSecure ACS
 Release 4.2(0) Build 124
 Copyright ©2008 Cisco Systems, Inc.
 Copyright ©1991-1992 RSA Data Security, Inc. MD5 Message-Digest Algorithm. All rights reserved.
 Copyright ©1989, 1993 The Regents of the University of California. All rights reserved.
 Copyright ©1986 University of Toronto. All rights reserved.
 Copyright ©1985-2000 Microsoft Visual C++ Version 6.0. All rights reserved.
 Copyright ©1997-2000 InstallShield Software Corporation. All rights reserved.
 All other trademarks, service marks, registered trademarks, or registered service marks mentioned herein are the property of their respective owners. Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and may cause significant and irreparable damage to anyone who suffers any such unauthorized copying.

Los primero que debe configurarse son los equipos que utilizarán los servicios de los ACS, en este caso se configuraron los Controladores, quienes invocarán al ACS para la validar a los usuarios que ingresen a la red.

Imagen 3.3.6.2 Configuración de Controladores



The screenshot shows the Cisco ACS Network Configuration interface. On the left is a navigation pane with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, and Reports and Activity. The main window displays the 'AAA Clients' table.

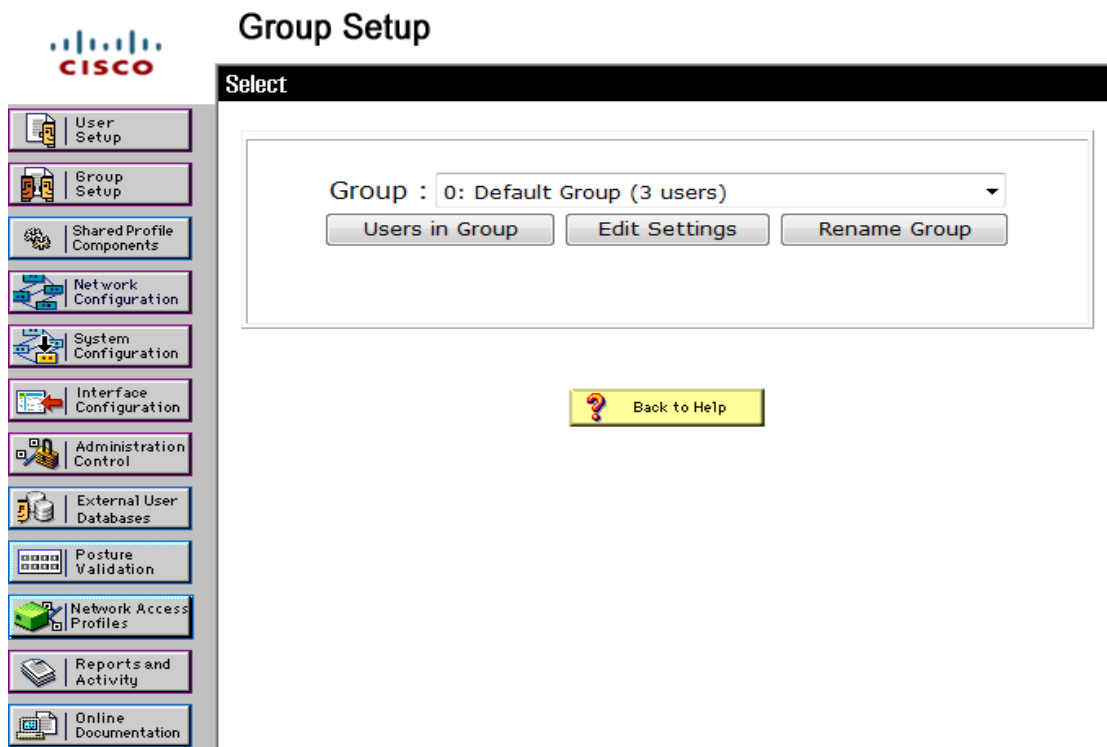
AAA Client Hostname	AAA Client IP Address	Authenticate Using
2811	10.2.255.6	TACACS+ (Cisco IOS)
ASA-	10.1.255.250	TACACS+ (Cisco IOS)
ironport	10.1.254.5	RADIUS (IETF)
MXBUES01WLC01	10.24.220.1	RADIUS (Cisco Aironet)
MXINFS01WLC01	10.1.219.1	RADIUS (Cisco Aironet)
MXINFS01WLC02	10.1.220.1	RADIUS (Cisco Aironet)
MXLIES01WLC01	10.2.220.1	RADIUS (Cisco Aironet)
RTR2811-VDG-AGS	10.30.253.253	TACACS+ (Cisco IOS)
RTR2811-VDG-BUENAVENTURA	10.24.253.253	TACACS+ (Cisco IOS)
RTR2811-VDG-CAMP	10.33.253.253	TACACS+ (Cisco IOS)
RTR2811-VDG-CHIH	10.37.253.253	TACACS+ (Cisco IOS)
RTR2811-VDG-CHIS	10.36.253.253	TACACS+ (Cisco IOS)
RTR2811-VDG-COL	10.35.253.253	TACACS+ (Cisco IOS)
RTR2811-VDG-DGO	10.38.253.253	TACACS+ (Cisco IOS)

A continuación se deben crear grupos, los cuales incluyen usuarios mismos que se brindaran a los clientes que requieran conectarse a la red. Los grupos sirven para llevar un mejor control en la administración de los usuarios, además de configurar niveles de privilegio en que a su vez son heredados a cada uno de los miembros del grupo.

En este caso se configuró un grupo por cada unidad, y 5 usuarios por cada grupo, mismos que son entregados a los responsables.

A continuación se muestra el Default Group (Grupo) donde se podrá editar el nombre por uno que describa el sitio de la dependencia.

Imagen 3.3.6.3 Configuración de Grupos



A partir de este punto se inicia la configuración del equipo. Se configuran los parámetros de replicación para soportar Alta disponibilidad en caso de la falla del ACS Primario, la imagen siguiente muestra las opciones que se eligieron como replicación en este proyecto:

La opción para ingresar a esta configuración es System Configuración > ACS Internal Database Replication.

Imagen 3.3.6.4 Configuración de componentes de Replicación

System Configuration

CAUTION: Replication will **overwrite** the selected components on the replicated clients.

CiscoSecure ACS services will be halted momentarily during replication.

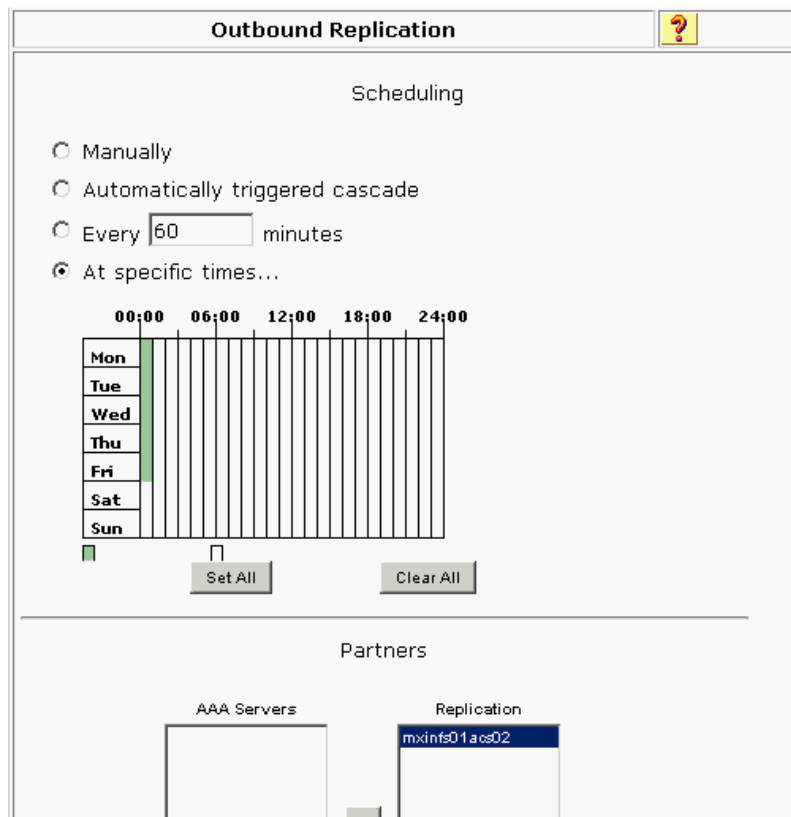
NOTE: Please disable Anti-Virus from accessing the CSDB folder present in ACS install directory for replication to work properly.

Replication Components		
Component	Send	Receive
User and Group Database	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Group Database only	<input type="checkbox"/>	<input type="checkbox"/>
Network Configuration Device tables	<input type="checkbox"/>	<input type="checkbox"/>
Distribution Table	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Interface Configuration	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Interface Security Settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Password validation settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
EAP-FAST master keys and policies	<input type="checkbox"/>	<input type="checkbox"/>
Network Access Profiles	<input type="checkbox"/>	<input type="checkbox"/>
Logging Configuration(Enable/Disable Settings)	<input type="checkbox"/>	<input type="checkbox"/>

También se debe configurar la manera en cómo se realizará la replicación, se recomienda que se programe en horarios de no operación de la red, es decir por la madrugada, como se configuró en este proyecto. La replicación será del Servidor primario al secundario todos los días a la 00:00 hrs. Tal como lo indica la siguiente imagen:

La opción para ingresar a esta configuración es System Configuration>ACS System Backup Setup

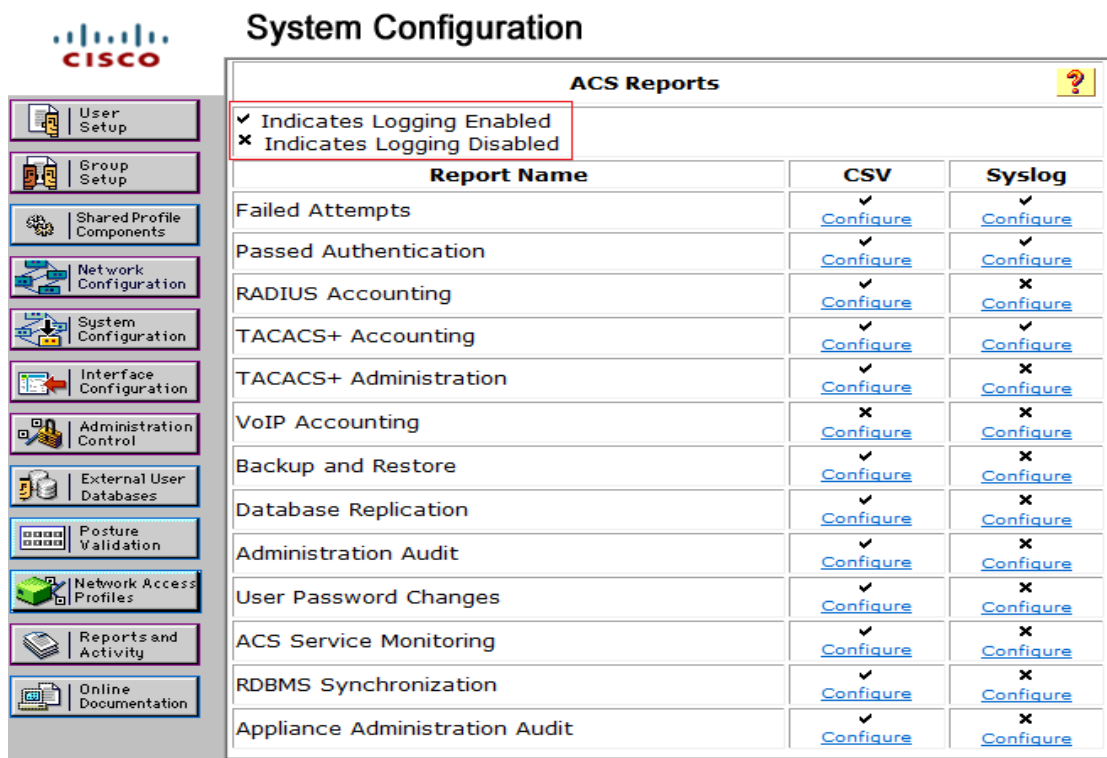
Imagen 3.3.6.5 Configuración de la Replicación



El siguiente punto a configurar son las opciones de Logging, este punto es muy importante ya que nos ofrece un detalle de las actividades registradas por el Servidor, con las cuales se puede saber si los usuarios se autentificaron o no, la razón por la cual se tienen intentos satisfactorios y fallidos en la conexión, poder registrar la actividad que realizó un usuario en caso de realizar un cambio indebido, indicadores del funcionamiento del equipo, etc.

La opción para ingresar a esta configuración es System Configuration> Logging

Imagen 3.3.6.6 Configuración de Reportes



The screenshot shows the Cisco System Configuration interface. On the left is a sidebar with navigation options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled "System Configuration" and "ACS Reports". It features a table with columns for "Report Name", "CSV", and "Syslog". The table lists various reports and their logging status for CSV and Syslog. A red box highlights the "Indicates Logging Enabled" and "Indicates Logging Disabled" options at the top of the table.

Report Name	CSV	Syslog
Failed Attempts	✓ Configure	✓ Configure
Passed Authentication	✓ Configure	✓ Configure
RADIUS Accounting	✓ Configure	✗ Configure
TACACS+ Accounting	✓ Configure	✓ Configure
TACACS+ Administration	✓ Configure	✗ Configure
VoIP Accounting	✗ Configure	✗ Configure
Backup and Restore	✓ Configure	✗ Configure
Database Replication	✓ Configure	✗ Configure
Administration Audit	✓ Configure	✗ Configure
User Password Changes	✓ Configure	✗ Configure
ACS Service Monitoring	✓ Configure	✗ Configure
RDBMS Synchronization	✓ Configure	✗ Configure
Appliance Administration Audit	✓ Configure	✗ Configure

Una manera de tomar ventaja de la replicación de los ACS cuando se trabaja con más de un Servidor es configurar totalmente el Servidor primario (lo cual implica dar de alta el Servidor secundario y su configuración) y el Servidor secundario solo con parámetros básicos (agregando al Servidor primario para aceptar las actualizaciones) y correr una replicación de manera manual para inyectar la configuración del Servidor primario al secundario. Con esto no solo se ahorra tiempo, también se asegura que la configuración en ambos Servidores sea idéntica y garantice la Alta Disponibilidad cuando sea requerida.

A continuación se debe realizar la configuración de los ACS dentro de los Controladores. De esta manera los Controladores invocarán los servicios de los ACS cuando se requiera autenticar a los usuarios.

La manera de configurarlo es la siguiente:

En la opción de Security> Tacacs en los Controladores se darán de alta los ACS con la dirección IP y un llave que debe coincidir con la llave que se configuro en los ACS cuando se dieron de alta los Controladores (dicha llave es para realizar la encriptacion y asegurar los datos).

La siguiente imagen muestra la configuración de un ACS:

Imagen 3.3.6.7 Configuración de ACS Server en Controlador

The screenshot shows the Cisco configuration interface for a controller. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The 'SECURITY' tab is active. On the left, a navigation tree shows 'Security' expanded to 'TACACS+' > 'Authentication'. The main content area is titled 'TACACS+ Authentication Servers > Edit' and displays the following configuration parameters:

Server Index	1
Server Address	10.1.220.10
Shared Secret Format	ASCII
Shared Secret	•••
Confirm Shared Secret	•••
Port Number	49
Server Status	Enabled
Server Timeout	5 seconds

Una vez configurados ambos ACS se deberá ingresar al SSID (WLAN) para indicar el uso de ambos equipos para la autenticación. Aquí es donde se configura la Alta Disponibilidad de los Servidores, la WLAN intentará contactar al Server 1 como primera opción, después de un TimeOut (5 segundos) si no se obtiene respuesta intentará contactar al Server 2. Cumpliendo así con la configuración de seguridad necesaria para el acceso inalámbrico.

Imagen 3.3.6.8 Configuración de Alta Disponibilidad

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The left sidebar shows 'WLANs' with sub-items 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > Edit' and has tabs for 'General', 'Security', 'QoS', and 'Advanced'. Under the 'Advanced' tab, there are sub-tabs for 'Layer 2', 'Layer 3', and 'AAA Servers'. The 'AAA Servers' sub-tab is active, displaying the following configuration:

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

	Authentication Servers	Accounting Servers
	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
Server 1	IP:10.1.220.10, Port:1812	None
Server 2	IP:10.1.220.20, Port:1812	None
Server 3	None	None

Local EAP Authentication

Local EAP Authentication Enabled

Authentication priority order for web-auth user

3.3.7 Wireless Control System WCS

Como ya se ha mencionado este Servidor es utilizado para centralizar la administración y configuración de los Controladores, con la ayuda de esta herramienta se minimiza el trabajo del administrador cuando se debe agregar alguna nueva configuración en la red inalámbrica, también ayuda a eliminar la posibilidad de errores cuando se debe configurar el mismo parámetro en cada Controlador. La herramienta es parte importante en la optimización de la red, ofreciendo reportes calendarizados que indican el comportamiento de la red. Este punto se enfatizará en la última parte de este informe, en la fase de Optimización.

El Wireless Control System es un software que se debe instalar en un Servidor con las siguientes características:

- Microsoft Windows 2004 Server, Red Hat Linux AS/ES v4 o VMWare ESX Server 3.0.1.
- Intel® CPU; 3.06 GHz, 2-GB RAM, 50-GB HDD

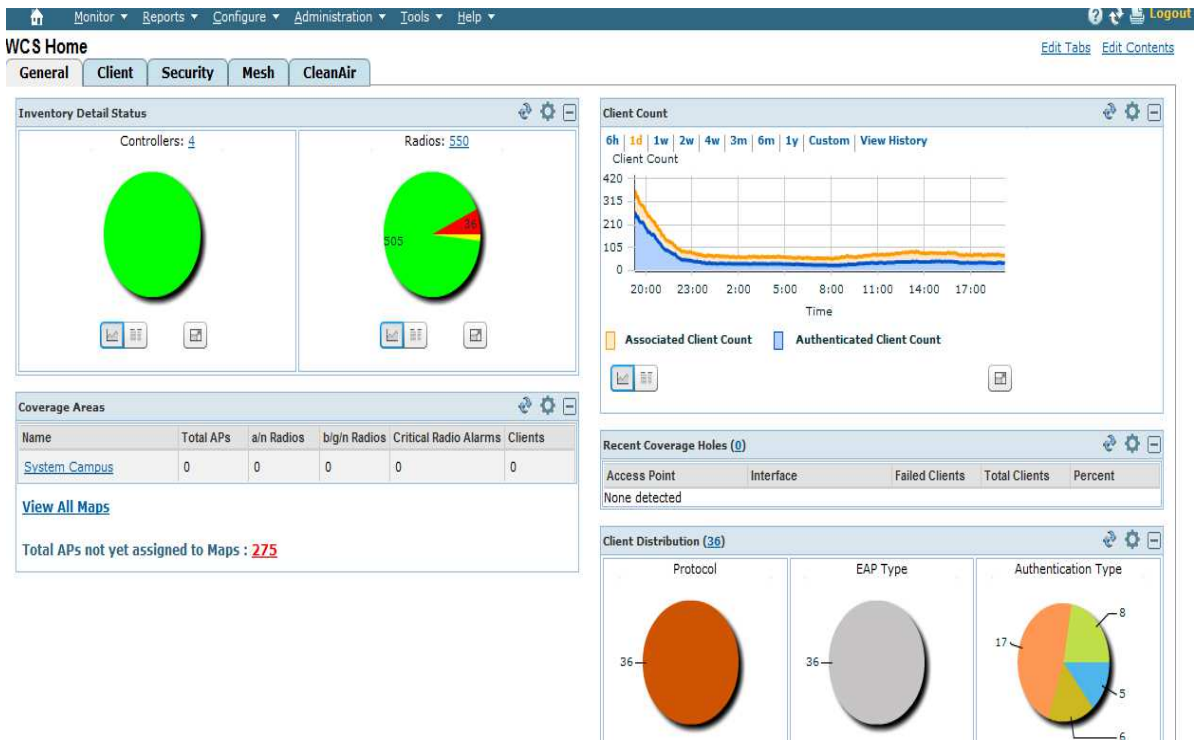
NOTA: Estos valores son mínimos para soportar hasta 500 Access Point en modo LWAPP.

Además de esto se deben adquirir las licencias para la cantidad de AP que se requieran. En este caso tenemos 300 AP, por lo tanto se solicitaron 3 licencias de 100 AP.

Una vez instalado el Sistema Operativo (en este caso fue Windows 2003 Server), se realiza la instalación del software de manera muy sencilla. Una vez que el Servidor tiene conectividad se puede ingresar a la aplicación vía web para iniciar la configuración del mismo.

Se debe agregar la dirección IP de cada uno de los Controladores, teniendo conectividad se deben poder administrar vía el WCS. A continuación se muestra la imagen.

Imagen 3.3.7.1 Menú Principal Administración WCS



Existen diversos reportes que pueden ser ejecutados para poder determinar el comportamiento de la red. Algunos de los cuales son los siguientes:

- Calidad de la señal
- Riesgos de seguridad den las interfaces
- Cantidad de usuarios conectados

Imagen 3.3.7.2 Reportes Disponibles

A continuación se muestra la imagen donde aparecen los Controladores dados de alta en el WCS.

Imagen 3.3.7.3 Verificación de Controladores en WCS

IP Address	Controller Name	Type	Location	Software Version	Mobility Group Name	Reachability Status
10.1.219.1	MXINFS01WLC01	4400	INFOTEC	7.0.98.0	WLANSALUD	Reachable
10.1.220.1	MXINFS01WLC02	4400	INFOTEC	7.0.98.0	WLANSALUD	Reachable
10.2.220.1	MXLIES01WLC01	4400	LIEJA	7.0.98.0	WLANSALUD	Reachable
10.24.220.1	MXBUES01WLC01	4400	BUENAVENTURA	7.0.98.0	WLANSALUD	Reachable

La implementación del proyecto se puede dividir en dos partes principales; la configuración de los equipos y la instalación física de los mismos. Ambos puntos son igualmente importantes. La configuración fue realizada por mí en su totalidad, para esto se contó con los equipos en el laboratorio de la empresa, donde se prepara y prueba la solución previa al envío a las instalaciones del cliente. Al ser una solución centralizada la parte medular son los Controladores y los ACS. Una vez terminada se procede a agregar solo algunos Access Point y realizar pruebas diversas. Existe una manera de que los Access Point se agreguen al Controlador una vez conectados a la red del cliente cumpliendo algunos requerimientos y configurando ciertas características de seguridad para el DHCP y los Switches, de tal manera que la cantidad de Access Point utilizados no deben ser configurados uno a uno, lo cual minimiza considerablemente el tiempo de configuración.

La siguiente tarea es la instalación de los Access Point en los lugares propuestos después del Site Survey. Estos lugares son marcados en los planos facilitados por el cliente. Un grupo de gente se dedicó a colocarlos al techo, colocar las antenas y conectarlos a la red (previa instalación de los nodos). Una vez instalados realicé una recorrido por los inmuebles para corroborar la colocación correcta y la posición de las antenas, ya que esto es crítico para tener una buena propagación de la señal. Los servidores son enviados a tres de ubicaciones distintas, uno de ellos el Centro de Datos y los restantes sitios donde se requería un servicio que no dependiera de la comunicación a través del enlace entre la oficina y el Centro de Datos. Una vez allí son colocados en el rack por la gente encargada y se le indica al equipo de cableado que puertos y tipo de fibras serán utilizadas para la conexión a la red. Una vez conectados a la red y encendidos es posible ingresar de manera remota y verificar si los Access Point están siendo agregados de manera correcta.

4. Resultados del Proyecto

Siempre que se finaliza una implementación es necesario validar la misma antes de que entre en operación. Es común que no se realicen las pruebas adecuadas sobre cada una de las características configuradas y esto puede generar fallas o deficiencias en el comportamiento de la red.

El siguiente programa de pruebas es una lista de ciertas características importantes que deben ser comprobadas. Cada prueba debe ser presenciada por el cliente y los resultados deben ser anotados en la tabla. Si el cliente identifica pruebas adicionales que se requieran durante la ejecución del protocolo de pruebas, éstas deben ser revisadas y autorizadas por los Project Managers de ambas partes y generar el control de cambios correspondiente. Los resultados de este proyecto están basados en el éxito de los siguientes protocolos de pruebas.

Tabla 4.0.1 Protocolo de Pruebas del Controlador

Prueba No.	Descripción de la Prueba	Resultado Pasó/Falló	
<i>Wireless Lan Controller</i>			
1	Los Access Points asignados al sitio deben aparecer en el WLC	Pasó <input checked="" type="checkbox"/>	Falló <input type="checkbox"/>
2	Las tres WLAN deben ser emitidas en cualquier ubicación del edificio, por medio de una laptop	Pasó <input checked="" type="checkbox"/>	Falló <input type="checkbox"/>
3	Se recibirá una IP del segmento local del sitio	Pasó <input checked="" type="checkbox"/>	Falló <input type="checkbox"/>
4	Soporta Autenticación y Encriptación para las WLANs	Pasó <input checked="" type="checkbox"/>	Falló <input type="checkbox"/>
5	Soporta red de Invitados con autenticación Radius	Pasó <input checked="" type="checkbox"/>	Falló <input type="checkbox"/>
6	El Wireless Lan Cotroller aparecerá en el Wireless Control System como Reachable	Pasó <input checked="" type="checkbox"/>	Falló <input type="checkbox"/>
7	Se debe tener acceso a internet desde cualquier WLAN	Pasó <input checked="" type="checkbox"/>	Falló <input type="checkbox"/>
8	Al generar un nuevo usuario de Invitados, se debe lograr la conexión satisfactoria a la red	Pasó <input checked="" type="checkbox"/>	Falló <input type="checkbox"/>

El éxito de estas pruebas ofrece fundamentos necesarios para que el cliente acepte el correcto funcionamiento de la solución y pueda llevarse a un proceso de cierre e iniciar con la puesta en operación.

Tabla 4.0.2 Protocolo de Pruebas ACS

Prueba No.	Descripción de la Prueba	Resultado Pasó/Falló	
Cisco Secure Access Control Server (ACS)			
1	El equipo es administrado vía WEB	Pasó <input checked="" type="checkbox"/>	Falló <input type="checkbox"/>
2	Se pueden dar de alta usuarios para la red de invitados	Pasó <input checked="" type="checkbox"/>	Falló <input type="checkbox"/>
3	El equipo registra el log de intentos exitosos y fallidos en la red de Invitados	Pasó <input checked="" type="checkbox"/>	Falló <input type="checkbox"/>
4	Se ingresa vía telnet a un SW del sitio y se debe autenticar vía Tacacs	Pasó <input checked="" type="checkbox"/>	Falló <input type="checkbox"/>
5	Al crear un usuario nuevo en el ACS primario y replicará en el ACS secundario de acuerdo al horario configurado o de manera manual	Pasó <input checked="" type="checkbox"/>	Falló <input type="checkbox"/>
6	Se deben ver los Logs de la replicación del ACS primario al secundario	Pasó <input checked="" type="checkbox"/>	Falló <input type="checkbox"/>

Una vez migrado cada sitio y con los protocolos de prueba exitosos el equipo de soporte local del cliente se dispone a configurar las computadoras y conectarlos a la red. Una vez asociadas y autenticadas se realizan pruebas de correo, internet, aplicaciones locales, servicios de impresión, recursos compartidos y finalmente se verifica el Roaming entre los diferentes Access Point.

Otro punto a considerar en los resultados del proyecto es la información obtenida en el Site Survey, aunque este es parte de la planeación, dichos resultados son vitales para la continuación del proyecto y por ende para el éxito del mismo. Dichos resultados en el Capítulo 3.3.2.

Para fines de este reporte los siguientes dos puntos 4.1 y 4.2 (Operación y Optimización) son considerados dentro de los resultados proyecto. Sin embargo en el modelo del Ciclo de Vida del Proyecto se clasifican de manera distinta.

4.1 Operación del Proyecto

Al inicio de la operación de una solución recién instalada es necesario entrenar al personal que administrará la red. Es importante tener un control sobre los procesos de operación, la metodología a seguir para la atención de un problema, la manera de realizar el troubleshooting (análisis y resolución del problema).

Se debe mantener un monitoreo constante del comportamiento de la red, realizar reportes, analizar la frecuencia y el tipo de fallas, realizar una memoria técnica que pueda servir como referencia inmediata para cualquiera que este administrando los recursos de la red con la finalidad de poder acceder a toda la información y actuar correctamente ante cualquier eventualidad.

A continuación se indican el contenido mínimo que debe incluir una memoria técnica la cual es primordial para la operación de la red.

- Diagramas de interconexión: Muestran la manera en cómo están conectados los equipos y cómo interactúan con el resto de los componentes de la red. Aquí se puede observar el flujo de los datos y ayuda a identificar en qué punto existe un problema cuando se presenta una falla en la red.
- Ubicación de los equipos: Es importante saber donde está instalado cada uno de los equipos que conforman la solución, esto facilita al administrador la resolución de problemas como fallas de conexión, fallas eléctricas, fallas de hardware, etc. Se deberá incluir el diagrama de los racks donde están montados los equipos.

-
- Descripción de la instalación física: Aquí se debe especificar el procedimiento para montar los equipos en un rack, tipo de tornillos, rieles, etc.

 - Identificación y seriales de los equipos: Se deben especificar los nombres, modelos y números de series de cada uno de los equipos involucrados en la solución.

 - Asignación de tarjetas y puertos: Cada puerto de la solución inalámbrica tiene un propósito particular y debe ser identificado detalladamente para atender cualquier falla existente.

 - Configuraciones: Se deben incluir las configuraciones de todos los equipos involucrados, en este proyecto se incluyeron las configuración de los Controladores, ACS y WCS. Tener las configuraciones es de suma importancia porque que son el respaldo en caso de falla catastrófica de alguno equipo, esto facilitará y minimizará el tiempo de respuesta a cualquier eventualidad.

 - Usuarios y Contraseñas: Se deben incluir todos los accesos a cada unos de los equipos. Cualquier persona autorizada a esta información deberá contar con toda la información para ingresar a los equipos.

 - Interfaces: Se deben incluir la interfaces todas las interfaces (VLANs en capa 3) involucradas en la solución, esto monitorear y poder identificar una falla de manera oportuna. En este caso se identifican los SSID existentes.

 - Protocolos: Se deben mencionar y detallar de manera general los protocolos utilizados en la solución, esto para poder obtener documentación más explícita en caso de ser requerida.

-
- Configuración de DHCP: Se debe indicar la manera en que están configurados los Pools de DHCP en cada uno de los Switches (los cuales fueron usados para proveer direccionamiento a la solución inalámbrica).
 - Políticas de nombres y direccionamiento IP: Finalmente se deben incluir los nombre y direcciones de cada uno de los equipos, estos valores son necesarios para realizar un monitoreo de la red y para identificar en diagramas físicos y lógicos.

En este reporte no se incluye de manera detalla la memoria técnica hecha para este proyecto debido a que sería un documento muy extenso y estaría fuera del objetivo que este reporte tiene.

Para este proyecto se asignó a un administrador de la red inalámbrica y este ingeniero fue entrenado para poder manipular cada uno de los equipos involucrados en la solución y la manera de atender los problemas más comunes que pueden presentarse.

A continuación se presenta una lista de algunos de los problemas más tipos en una solución inalámbrica y la manera de resolverlo.

Problemática: Los usuarios no pueden conectarse a la red

Resolución: Revisar el Controlador y los AP instalados en el área donde se encuentra el usuarios esta activos. Solicitar la Mac Address de la tarjeta inalámbrica y ejecutar una búsqueda en el WLC, esto arrojará una serie de Logs que indicarán el comportamiento del cliente. Si no aparece en los Logs, se deberá verificar si está siendo correctamente configurado el perfil inalámbrico en la computadora.

Problemática: Las redes inalámbricas no son visibles en la computadora del usuario.

Resolución: Revisar si los AP están activos, revisar si los AP correspondientes están publicando los SSID. Verificar si la tarjeta inalámbrica esta activa. Buscar alertas acerca de hoyos de cobertura dentro de las áreas de interés.

Problemática: Los usuarios invitados no pueden conectarse

Resolución: Revisar los Logs en el ACS y verificar las alertas. Verificar que se estén ingresando las credenciales de manera correcta.

Problemática: Se perdió conectividad con un Controlador

Resolución: Verificar la interface Etherchannel creada en el Switch correspondiente, verificar las interfaces físicas que conforman el Etherchannel (recorrir a la memoria técnica para identificar las conexiones). Verificar el cableado. Conectarse al controlador por consola o por la interface Out of Band y verificar si el sistema operativo está funcionando correctamente.

Estos son algunos de los problemas que pueden presentarse en la operación de la red inalámbrica y la manera de trabajar en su resolución.

A grandes rasgos se puede definir la operación de la red como la etapa donde se realiza el monitoreo de la red, se obtienen reportes estadísticos que incluyen cantidad de usuarios y periodos de conexión, ancho de banda utilizados, registro de fallas, control de cambios, alta y baja de usuarios, etc.

Se realizan controles de cambio para cada evento con la finalidad de tener documentada y actualizada la configuración de la red. Finalmente se entrega un directorio al cliente con la información de las personas involucradas al proyecto para que en caso de una falla sea reportada.

Como parte del servicio de Soporte a la solución del cliente se debe de entregar el proceso de escalamiento de fallas.

A continuación se indica el proceso correspondiente:

- Todo usuario cuenta con el número del Help Desk donde se abrirá un ticket indicando los síntomas y el impacto de la falla.
- Los ingenieros de Help Desk atenderán el problema haciendo un análisis de inicial, sin contactar aun al administrador de la red.
- Si el problema persiste se avisa al administrador acerca de la falla y se procede a una resolución más exhaustiva (debido a que el administrador tiene acceso total a los equipos).
- Si el problema persiste se recurre al soporte técnico de la empresa que instaló la solución con la cual se tiene una póliza de mantenimiento. El ingeniero deberá involucrase de manera completa en la resolución de problema.
- Si el problema persiste después del trabajo hecho por todos los niveles de escalamiento anteriores, se procede a levantar un caso con el fabricante (Cisco), quien cuenta con un centro de atención especializada e internamente maneja diversos niveles de escalamiento.

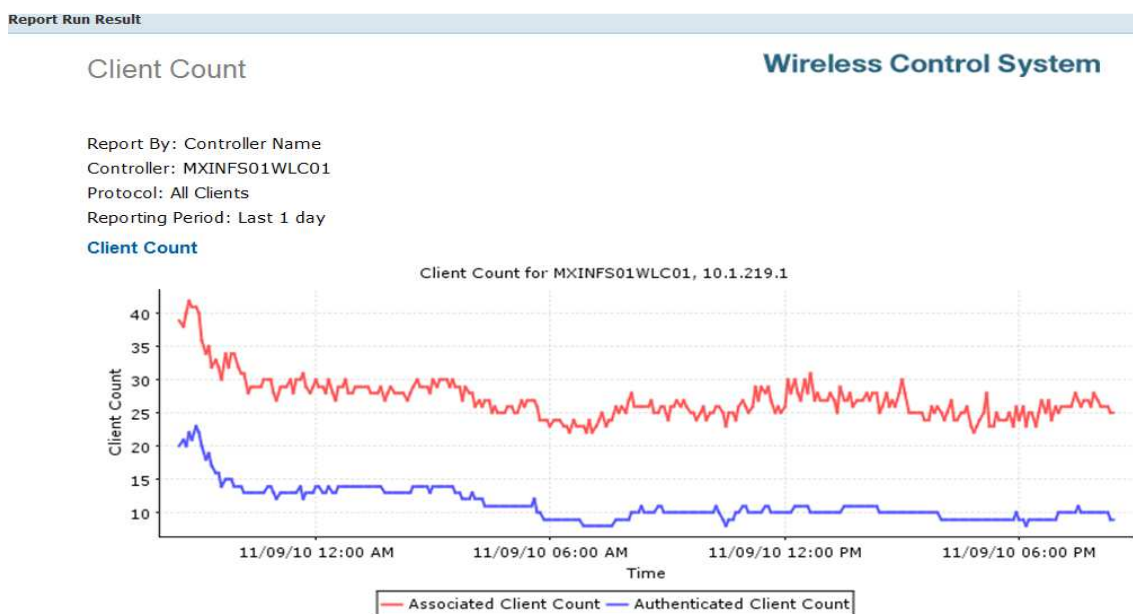
4.2 Optimización del Proyecto

En la fase de optimización es donde se busca una mejora continua de los procesos de atención a fallas, niveles de escalamiento, se mantiene un continuo monitoreo y realización de niveles de servicio para validar el comportamiento de la red inalámbrica.

Para esto se crearon reportes calendarizados donde puede observarse el comportamiento de la red. Gran parte de la optimización dependerá del nivel de reportes y la interpretación que se haga en el Wireless Control System.

A continuación se muestra un reporte donde se indican los clientes que están asociados y autenticados en un edificio de la dependencia.

Imagen 4.2.1 Reporte de clientes asociados



Este reporte ayuda a saber qué número de usuarios están intentando conectarse a la red y no lo logran (Associated Clients), se puede determinar a través de la Mac Address de la tarjetas de red si los usuarios son parte de la red corporativa, de esta manera se puede verificar de manera puntual cual que problemática presenta el usuario. También existe la posibilidad de que sean intentos fallidos que podrían ataques a la red.

A continuación se muestra el reporte de los hoyos de cobertura que se presentan en un edificio.

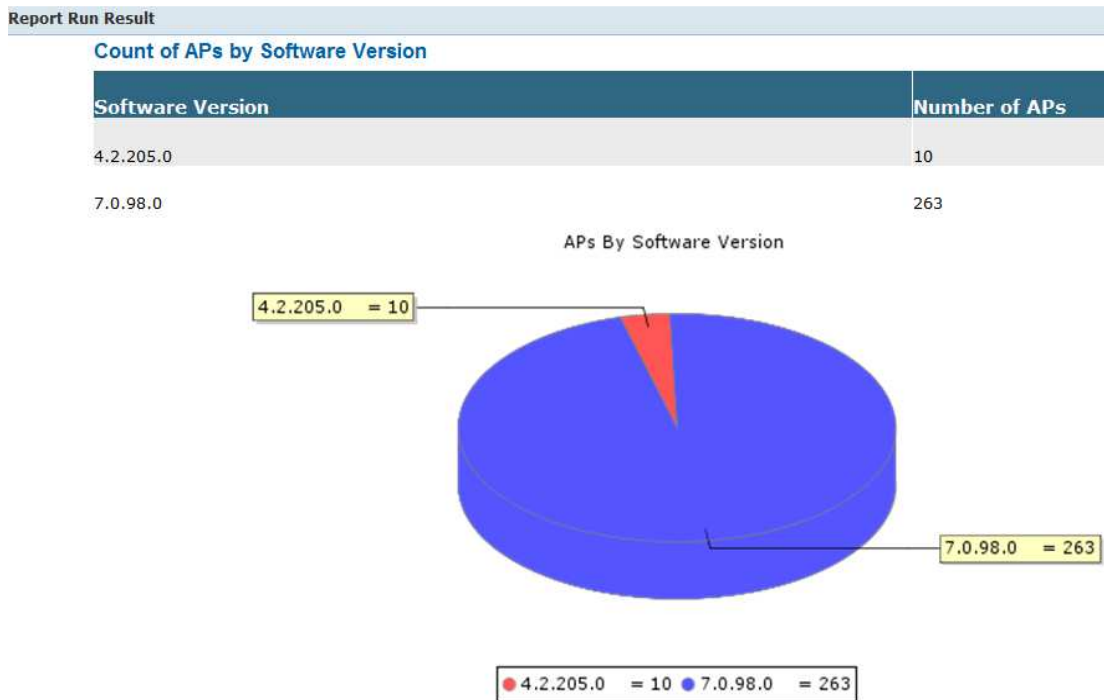
Imagen 4.2.2 Reporte de hoyos de cobertura

Report Run Result						
Coverage Hole				Wireless Control System		
Report By: AP By Controller						
Controller: 10.1.220.1 -> All Access Points						
Reporting Period: Last 2 days						
Coverage Holes in the Network						
Time	State	AP Name	Radio Type	Failed Clients	Total Clients	Worst Client RSSI
09/10/2010 15:25:01 CDT	Clear	AP1-REF450-PB	802.11b/g	0	0	0
09/10/2010 15:15:58 CDT	Active	AP1-REF450-PB	802.11b/g	4	6	-90
09/10/2010 15:11:26 CDT	Clear	AP1-REF450-PB	802.11b/g	0	0	0
09/10/2010 15:09:55 CDT	Active	AP1-REF450-PB	802.11b/g	3	6	-88
09/10/2010 15:05:23 CDT	Clear	AP1-REF450-PB	802.11b/g	0	0	0
09/10/2010 15:03:53 CDT	Active	AP1-REF450-PB	802.11b/g	3	6	-90
09/10/2010 15:00:51 CDT	Clear	AP1-REF450-PB	802.11b/g	0	0	0
09/10/2010 14:57:50 CDT	Active	AP1-REF450-PB	802.11b/g	4	7	-90

Aquí se puede observar que el mismo AP está presentando Hoyos de cobertura lo cual genera que varios usuarios hayan fallado en su intento de conexión. Esto se puede deber a que se abrió un espacio nuevo en la una oficina donde no se tenía contemplada la red. Este tipo de reportes indican de manera puntual que AP está teniendo la falla y se puede acudir directamente a esta zona para realizar una revisión exhaustiva y las pruebas correspondientes.

Se pueden ejecutar reportes de inventario para saber la cantidad de AP existentes y las versiones de sistema operativo actuales, con el fin de mantenerlos actualizados y llevar un control de los mismos. El reporte se muestra a continuación:

Imagen 4.2.3 Reporte de Access Point



También parte de los reportes de Inventario ofrecen información de cada AP (Nombre, MAC Address, Dirección IP, Modelo y Controlador al cual está asociado). El reporte se muestra a continuación:

Imagen 4.2.4 Inventario de Access Point por ubicación

AP Name	Ethernet MAC Address	IP Address	Model	Map Location	Controller Name
AP1-GCAMP-A-P2	00:24:c4:a0:b5:a2	10.17.218.45	AIR-LAP1242AG-N-K9	Root Area	MXINFS01WLC02
AP1-GCAMP-A-P3	00:24:c4:a0:b5:1c	10.17.218.56	AIR-LAP1242AG-N-K9	Root Area	MXINFS01WLC02
AP1-GCAMP-A-P4	00:24:c4:a0:b1:1a	10.17.218.35	AIR-LAP1242AG-N-K9	Root Area	MXINFS01WLC02
AP1-GCAMP-A-PB	00:24:c4:a0:a7:90	10.17.218.58	AIR-LAP1242AG-N-K9	Root Area	MXINFS01WLC02
AP1-GDL-P1	00:24:c4:a0:d6:50	10.7.218.55	AIR-LAP1242AG-N-K9	Root Area	MXLIES01WLC01
AP1-GDL-P2	00:24:c4:a0:d3:14	10.7.218.51	AIR-LAP1242AG-N-K9	Root Area	MXLIES01WLC01
AP1-GDL-P3	00:24:c4:a0:b4:4c	10.7.218.46	AIR-LAP1242AG-N-K9	Root Area	MXLIES01WLC01
AP1-GDL-P4	00:24:c4:a0:b8:98	10.7.218.44	AIR-LAP1242AG-N-K9	Root Area	MXLIES01WLC01
AP1-GDL-P5	00:24:c4:a0:a9:06	10.7.218.58	AIR-LAP1242AG-N-K9	Root Area	MXLIES01WLC01
AP1-GDL-P6	00:24:c4:a0:b5:b2	10.7.218.43	AIR-LAP1242AG-N-K9	Root Area	MXLIES01WLC01

El WCS puede ser personalizado para poder asignar nivel de alertas a los eventos que se presentan, esto es de mucha ayuda debido que se pueden clasificar las características que requieren ser monitoreadas. A continuación se muestra la imagen con algunas de las alertas detectadas por el equipo.

Imagen 4.2.5 Alertas

The screenshot shows the WCS Home interface with a navigation menu at the top (Monitor, Reports, Configure, Administration, Tools, Help) and tabs for General, Client, Security, Mesh, and CleanAir. The Security tab is active, displaying several alert panels:

- AP Threats/Attacks:** A table showing counts for AP Impersonation (67) and Denial of Service (10).
- Attacks Detected:** A table listing various attack types like Assoc flood, Bcast deauth, Auth flood, etc., with counts for Last Hour, 24 Hours, and Total Active.
- Recent Malicious Rogue AP Alarms (3):** A table listing MAC addresses, SSIDs (e.g., Red Septien, IDS-SSA), states (Contained Pending), and dates/times.
- Most Recent Security Alarms (815):** A table showing failure objects, dates/times, and messages related to authentication failures and signature attacks.

Las alertas existentes pueden ser visibles para el administrador cuando está conectado al WCS. Muchas de estas alertas pueden ser críticas y por lo tanto requerir una atención inmediata.

Imagen 4.2.6 Configuración de Severidad

Severity Configuration
Administration > Settings > Severity Configuration

Severity level changes will only apply to the newly generated alarms. Existing alarms will remain unchanged.

<input type="checkbox"/>	Alarm Condition	Alarm Category	Configured Severity
<input type="checkbox"/>	A reboot scheduled on the controller "{0}" has been canceled.	Controller	
<input type="checkbox"/>	A reboot scheduled on the controller "{0}" has been failed.	Controller	
<input type="checkbox"/>	AP Authorization Failure	Access Points	
<input type="checkbox"/>	AP Detected Duplicate IP	Security	
<input type="checkbox"/>	AP IP fallback	Access Points	
<input type="checkbox"/>	AP associated with controller	Access Points	
<input type="checkbox"/>	AP attempted to join Controller with licensed AP count exceeded	Controllers	
<input type="checkbox"/>	AP big nav DOS attack	Security	
<input type="checkbox"/>	AP contained as rogue	Access Points	

Esta herramienta ofrece la opción de enviar notificaciones vía correo a los responsables de la red con el fin de atender de manera inmediata los problemas críticos que se presenten. A continuación se muestra la opción donde se puede realizar tal configuración:

Imagen 4.2.7 Configuración de notificaciones

The screenshot shows the 'Notification Receiver' configuration page. The navigation menu includes: Home, Monitor, Reports, Configure, Administration, Tools, and Help. The left sidebar lists various configuration options, with 'Notification Receivers' highlighted. The main content area is titled 'Notification Receiver' and shows the breadcrumb path: Administration > Settings > Notification Receivers > Notification Receiver. The configuration fields are: IP Address (empty), Name (empty), Receiver Type (radio buttons for Northbound and Guest Access, with Northbound selected), Port Number (162) (UDP), and Community (public). Below these fields is a 'Criteria' section with a 'Category' dropdown and a list of checkboxes for various notification categories: All, Access Points, Clients, Coverage Hole, Context Aware Notifications, Mobility Service, Rogue AP, Security, Adhoc Rogue, Controllers, SE Detected Interference, Mesh Links, Performance, RRM, and WCS.


Otra característica importante es la optimización de un proyecto es mantener actualizados los equipos, esto para gozar de nuevos features para la red y mantenerla estable. Optimizar los recursos de los equipos (CPU y Memoria).

También se deben mantener actualizados los drivers de las tarjetas de red de los usuarios. Este punto es primordial, ya que se puede tener una excelente infraestructura de red pero los usuarios no cumplen con los requerimientos necesarios. Esto puede generar una mala percepción acerca de la confiabilidad de las redes inalámbricas.

Para mantener esta actualización existe un programa de investigación llevada a cabo por Cisco donde se indica el driver y la versión que debe tener cada tipo de tarjeta inalámbrica existente en el mercado

A continuación se muestra un ejemplo de un modelo de tarjeta Atheros donde se describe la versión y la verificación de compatibilidad con la infraestructura Cisco.

Imagen 4.2.8 Compatibilidad con los productos Cisco

	Atheros Communications, Inc. <i>Membership Level: Solution Developer</i>		
		Partnerspace URL: N/A Primary Contact Louis Isbitz louis.isbitz@atheros.com	
AR5BHB95			
Product Description	AR5BHB95. Product Models: HB95		
Product URLs	http://www.atheros.com		
	Version 7.7.0.305	Verified Compatible Cisco Products <u>Cisco Compatible eXtensions (Device)</u> • CCX Version 5	Date Tested N/A

Para finalizar con el proceso de Optimización se entrega al cliente una serie de recomendaciones para el mantenimiento de los equipos, estas incluyen:

- Fechas y actividades para un mantenimiento preventivo de los equipos, es decir una limpieza física para evitar que se dañen con el polvo y demás partículas que se acumulan en los circuitos.
- Como manipular los equipos en caso de movimiento físico o remplazo de alguna parte dañada.
- Recomendaciones para la actualización de sistemas operativos y nuevos parches.
- Realización de manuales de operación para que cualquier ingeniero que asuma la responsabilidad de la operación tome el control total de manera rápida y eficiente.

Conclusión

Las redes inalámbricas han tenido un crecimiento considerable en los últimos años, actualmente se están presentando como una opción importante para diversas unidades de negocio debido a las ventajas que ofrecen respecto a las redes cableadas. Este auge ha impulsado a los fabricantes y organismos internacionales involucrados a continuar con el desarrollo de esta tecnología.

El ámbito laboral exige que los egresados ofrezcan un valor agregado a su trabajo, es decir no solo conocimiento técnico. Las mejores oportunidades de trabajo requieren que el ingeniero tenga la capacidad de interactuar con grupos de profesionistas de distintas áreas, ser proactivo y anticiparse a los problemas, tener actitud positiva para mantener un aprendizaje continuo, ser responsable y respetuoso del trabajo de los demás así como tener la capacidad de tomar decisiones importantes. La UNAM y la Facultad de Ingeniería en su conjunto ofrecen un perfil integral de Ingeniero, el cual además de una excelente preparación teórica es complementada con habilidades sociales y humanas capaz de posicionarnos como la mejor opción en competencia laboral

En estos años de experiencia laboral he tenido la oportunidad de trabajar en empresas importantes donde he podido desarrollarme de manera importante e ir creciendo técnica y personalmente. La posibilidad de participar en diversos proyectos de redes, todos ellos con tecnología Cisco combinado con la empatía que como Consultor se debe mantener con el Cliente me han enriquecido como Ingeniero y como ser humano.

La implementación de esta red inalámbrica es uno de los proyectos más grandes e interesantes en los que he participado, en esta solución tuve la posibilidad de ser el líder técnico desde su fase de Preparación hasta la Optimización del mismo, tuve oportunidad de poner en práctica cada una de mis habilidades y obtener los resultados esperados. La responsabilidad de estar al frente de un proyecto de esta magnitud ha sido el premio al esfuerzo y trabajo arduo que he realizado desde mi egreso de la Facultad.

Los conocimientos adicionales que he adquirido con el estudio de las certificaciones de Cisco son cruciales para poder desarrollar un proyecto de esta magnitud. Las certificaciones le han dado un valor muy importante a mi trabajo desde que inicié como Ingeniero de redes, sin el conocimiento adquirido en ellas sería muy complicado ser contemplado para liderar proyectos importantes, sin embargo la formación que tuve en la Facultad me ha dado la habilidad de poder entender la información técnica de la tecnología Cisco (autoestudio) y obtener las certificaciones, así como abordar y resolver cada uno de los desafíos que se presentan en la vida laboral del ingeniero.

Bibliografía

CCNP Cisco Certification Guide

Clare Goug

Cisco Press; 3 edition (December 12, 2003)

ISBN-10: 1587201046

CCNA Wireless Official Exam Certification Guide

Brandon James Carroll

Cisco Press; 1 edition (November 2, 2008)

ISBN-10: 1587202115

CCNA Routing & Switching Official Exam Certification Guide

Wendell Odom

Cisco Press; 2 edition (September 9, 2007)

ISBN-10: 9781587201813

Deploying Cisco 440X Series Wireless LAN Controllers

<http://www.Cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html>

Fecha última de consulta: 20 Mayo 2011

Configuration Guide for Cisco Secure ACS 4.1

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/configuration/guide/cfg41.html

Fecha última de consulta: 20 Mayo 2011

Cisco Aironet Antennas and Accessories Reference Guide

http://www.Cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html

Fecha última de consulta: 20 Mayo 2011

http://en.wikipedia.org/wiki/OSI_model

Fecha última de consulta: 20 Mayo 2011

Glosario

Access Point

Es un dispositivo que permite la comunicación de diversos dispositivos sin la necesidad de un cable que los una lógicamente. Los Access Point se conectan a una red cableada a través de la cual se convierten en el punto de acceso a todos los recursos de red, mismos que ofrecen a través de ondas de radio frecuencia.

ACS (Access Control System)

Servidor que ofrece servicios de autenticación, autorización y contabilización para usuarios y equipos de red como Routers, Switches, Access Point, etc., con la finalidad de mantener un robusto sistema de seguridad en las redes de datos. Ese equipo es del fabricante Cisco y corre en existe en plataforma Linux y Windows Server.

Broadcast Domain

Se entiende como una segmentación lógica de una red de computadoras en la cual todos los nodos son alcanzables entre sí a nivel de capa 2 del modelo OSI.

CCNA

Cisco Certified Network Associate, es una certificación de segundo nivel de Cisco que valida la habilidad de instalar, configurar, operar y resolver problemas de redes de datos.

CCDA

Cisco Certified Design Associate, certificación de Cisco de segundo nivel que valida el diseño de redes de datos.

CCVP

Cisco Certified Voice Professional, es una certificación de Cisco de nivel tres que cubre todos los aspectos de redes y aplicaciones de Telefonía IP. Esta comprendida por 5 exámenes.

Collision Domain

Es un segmento de red compartido donde existen colisiones cuando más de un dispositivo intenta enviar un paquete en la red al mismo tiempo, un ejemplo de esto son los Hub. Cada puerto de un Switch es conocido como Collision Domain. En otras palabras un Switch (Capa 2) divide los Collision Domains mientras que un Router (Capa 3) divide Broadcast Domains.

DNS

Domain Name System es un sistema jerárquico de nombres para computadoras, servicios o cualquier recurso de red conectado a Internet o a una red privada, su principal función es transformar un nombre de una computadora o sitio web a una dirección IP capaz de ser reconocida y ubicada en la red mundial o local.

DHCP (Dynamic Host Configuration Protocol)

Dynamic Host Configuration Protocol es un protocolo de red encargado de asignar una dirección IP (identificador único y necesario para que una equipo pueda comunicarse en una red) a equipos así como otros valores necesarios para su comunicación. La manera de funcionar inicia cuando el cliente (equipo) envía una petición de Broadcast, un Servidor de DHCP (previamente configurado) recibe dicha petición y la responde con la información preconfigurada en dicho Servidor, esta información es dirección IP, mascara de subred, puerta de enlace (Default Gateway) y DNS.

Firewall

Barrera creada por dispositivos basada en un conjunto de reglas de seguridad que permiten mitigar accesos no autorizados a diferentes recursos de voz y datos con la finalidad de mitigar u ofrecer el paso al tráfico de red.

Granja de Servidores

Conjunto de servidores con capacidades mas allá de las computadoras comunes que alojan información crítica para la empresas ofreciendo redundancia en datos y energía los cuales están conectados al Core de la red datos. Algunas de las aplicaciones comunes son, Correo electrónico, DNS, DHCP, Antivirus, etc.

H-REAP

Hybrid Remote Edge Access Point, solución de Cisco que permite que los Access Point alojados en oficinas remotas puedan ofrecer servicios de red a través de una red (WAN) sin la necesidad de instalar un dispositivo controlador de manera local.

Mobility Domain

Dominio al que pertenecen los dispositivos inalámbricos que ofrece la capacidad de moverse de un Access Point de manera segura y sin perder comunicación. Esta característica es ofrecida por los Controladores Inalámbricos.

RFP

Request For Proposal, es un conjunto de requerimientos solicitados en la invitación de una empresa con la finalidad de tomar la mejor decisión en el desarrollo de un proyecto. Este documento estructurado ofrece el análisis de factibilidad, riesgos y procesos a seguir. Son utilizados en las licitaciones.

Roaming

Es la capacidad que tiene un dispositivo inalámbrico de poder cambiar su asociación de un Access Point a otro sin perder la comunicación con la red.

SFP

Small Form-Factor Pluggable es una interface Gigabit que se conecta a un Puerto Ethernet para unir dos dispositivos, se usa fibra óptica como medio físico de conexión.

Site Survey

Es una inspección realizada para obtener la información necesaria para poder diseñar o estimar las tareas a seguir en una actividad. Incluye ubicación y orientación precisa así como análisis de obstáculos.

Trunk

Es una conexión lógica que ofrece un acceso compartido a diversos dispositivos pertenecientes a diferentes segmentos lógico capaces de converger en es un punto.

Un trunk permite identificación de la VLAN para poder comunicar a usuarios pertenecientes al mismo Broadcast Domain pero conectados en Switches separados a través de un enlace. Este enlace lógico es conocido con Trunk y es capaz de identificar el VLANID para mantener la comunicación entre equipos.

La IEEE creó un estándar para marcar paquetes e identificar la VLAN a la que pertenecen. El protocolo es 802.11Q y es el encargado de que un Trunk funcione, es decir un puerto configurado como Trunk deberá ser marcado con este tipo de encapsulamiento. Los puertos configurados como Trunk son capaces de permitir el paso de todas las VLANs configuradas en los Swtiches. Existe una característica llamada VLAN Nativa y esto simplemente se entiende como una VLAN sin marcar, es decir no es identificada. Por default, los Switches Cisco están configurados en la VLAN 1 y está es la nativa.

VLAN (Virtual LANs)

VLAN = Broadcast Domain. Una VLAN es una división lógica de los puertos en un Switch a la que se asocia un identificador ID, esto permite asignar puertos a cierto segmento de red, los miembros de esta VLAN serán capaces de comunicarse entre ellos mientras que para lograr la comunicación entre puertos asignados a diferentes VLAN deberá existir un dispositivo Capa 3. Esta comunicación existe sin importar la ubicación física de los dispositivos.

WCS

Wireless Control System, es una herramienta de red capaz de administrar, operar Controladores Wireless, a través de un Servidor central que corre en Windows Server. Dicha herramienta es capaz de generar alertas basadas en reglas preconfiguradas con la finalidad de mantener la red inalámbrica monitoreada.

WLAN

Wireless LAN se entiende como una VLAN en el ámbito inalámbrico, dicha VLAN está asociada con el SSID que los Access Point publican el cual las tarjetas de red inalámbricas son capaces de detectar.

WLC

Wireless LAN Controller, equipo de red Cisco el cual es el centro de operación de una red unificada, es capaz de ofrecer configuración, servicios de roaming, análisis de interferencias y administración de los Access Point.

Anexo

Las redes inalámbricas son aquellas capaces de transmitir información sin que existan cables de por medio, la comunicación se hace mediante ondas de radio frecuencia. Transmisión y recepción de datos son realizadas a través de Access Point (AP). Algunas de las ventajas más importantes son la fácil y rápida instalación sin la necesidad de usar cableado estructurado, además permiten que los usuarios tengan movilidad, y a diferencia de las redes cableadas, éstas tienen mucho menor costo de implementación y mantenimiento.

Actualmente las redes inalámbricas han tenido una gran demanda no sólo en los hogares, también en el sector corporativo, educativo y gubernamental donde ha surgido la necesidad de diversificar sus servicios y aprovechar las bondades que éstas redes ofrecen. Una de las malas concepciones que aún persisten en las redes inalámbricas es la seguridad de los datos, esto debido a que la información está en el ambiente a través de ondas de radio frecuencia y los métodos débiles de encriptación que las primeras implementaciones mostraron, y que aún prevalecen en diversos sitios, han generado esa mala reputación acerca de su confiabilidad.

Actualmente las empresas requieren de servicios de correo electrónico, archivos compartidos, impresión, internet, voz y video donde no es posible llegar mediante cables, ya sea falta de presupuesto o limitaciones por renta de espacios en oficinas han generado que la tecnología inalámbrica haya tenido un crecimiento enorme en los últimos años. Estas necesidades han motivado el desarrollo de la tecnología, uno de los más importantes es el cambio de paradigma inalámbrico descentralizado (Autónomo) a uno más robusto y confiable, redes inalámbrica Unificadas, con mejores niveles de seguridad y mayor ancho de banda.

En los fundamentos necesarios para la correcta comprensión de este informe se cubrirán los estándares de la IEEE 802.11, las bandas A, B, G y N, así como conceptos importantes de redes como VLAN, interfaces, Trunks, SSID, encriptación, autenticación, comparación entre una solución autónoma y una unificada y las opciones de seguridad existentes en la actualidad, esta información se incluye a continuación.

Introducción a la Tecnología Inalámbrica

En un nivel muy básico podemos entender una red switchheada la que está compuesta con cables y una red inalámbrica es aquella no los requiere, esta concepción es muy lógica y simple pero es la mayor de las diferencias en la capa física del modelo OSI (Capa 1).

Una red tradicional Ethernet está definida por el estándar IEEE 802.3. Cada conexión debe operar bajo las ciertas condiciones establecidas, especialmente hablando de un estado de link, es decir velocidad, modo dúplex, etc. De la misma manera las redes inalámbricas se rigen bajo ciertas condiciones, en este caso es el estándar IEEE 802.11.

Las redes Ethernet cableadas deben transmitir y recibir paquetes de acuerdo al método Carrier Sense Multiple Access/Collision Detection (CSMA/CD). En una red Ethernet compartida con una PC comunicándose en half-duplex, la PC debe escuchar el medio antes de mandar información, esto para evitar colisiones. En el caso de conexiones full-dúplex se tiene comunicación bidireccional.

Una red inalámbrica es un medio compartido, donde la información va en el aire y es susceptible a colisiones, es decir que su comportamiento puede entenderse como una red half-duplex. La razón por la cual las redes inalámbricas presentan colisiones es porque usan la misma frecuencia (Hz) para enviar y recibir datos.

Otro punto en contra de las transmisiones RF es que las ondas son absorbidas, refractadas o reflejadas por paredes, agua y superficies metálicas las cuales generan degradación de la potencia de la señal.

Debido a estas situaciones las redes inalámbricas se tornan un tanto inestables por los factores ambientales y por lo tanto no deben ofrecerse como redes tan robustas con las cableadas (no para una operación CORE), es decir no como la conexión primaria de una empresa. Sin embargo ofrecen grandes ventajas y cada día su comportamiento es más estable y seguro.

Uno de los retos más fuertes en las redes inalámbricas es la distorsión de la señal y esto sucede frecuentemente cuando se aumenta la potencia (ganancia) de las antenas para cubrir un mayor espacio, lo cual no es necesariamente lo correcto. Por otro lado si se desea transmitir a mayor ancho de banda debe hacerse en frecuencias altas, sin embargo el área de cobertura (distancia) decrece de manera proporcional. Por el contrario si deseamos cubrir distancias mayores se debe hacer en bajas frecuencias lo cual generará menor velocidad de transmisión. Este punto es importante cuando se trabaja en los requerimientos del cliente ya que las situaciones siempre son distintas.

El estándar inalámbrico (802.11) es un conjunto de especificaciones desarrolladas por diversas agencias y grupos para marcar la pauta en esta tecnología, esto para generar comunes denominadores que puedan ser utilizados por todos los fabricantes. Las agencias más importantes son las siguientes:

Tabla Anexo 1.0 Estándares IEEE

Agencia	Actividad
Institute of Electrical and Electronic Engineers (IEEE)	Crea y mantiene los estándares en Operación
Federal Communications Commission (FCC)	Regula los dispositivos inalámbricos en Estados Unidos
European Telecommunications Standards Institute (ETSI)	Genera estándares comunes en Europa
Wi-Fi Alliance	Prueba y promueve la interoperabilidad de las redes inalámbricas

Debido a que las redes inalámbricas se transmiten a través de radio frecuencias estas deben ser reguladas de la misma manera como lo hace la radio AM/FM. La FCC regula el uso de dispositivos inalámbricos y la IEEE toma esas regulaciones para crear estándares.

La FCC tiene tres bandas no licenciadas para uso público: 900 MHz, 2.4 GHz y 5.7 GHz. Las bandas de 900 MHz y 2.4 GHz son conocidas como Industrial, Scientific, and Medical (ISM) Bands y la banda de 5 GHz es conocida como Unlicensed National Information Infrastructure (UNII).

Es decir que si se quiere realizar una implementación fuera de estas tres bandas se debe solicitar una licencia específica de la FCC. Al ofrecer las bandas no licenciadas muchas empresas se dedicaron a desarrollar productos dentro de este espectro dentro de las cuales la que más auge ha tenido es la banda 802.11b/g la cual opera en 2.4GHz. La Wi-Fi Alliance se ha encargado de certificar la interoperabilidad de todos estos productos que se encuentran en el mercado.

Estándar 802.11

802.11 es un conjunto de estándares para las redes inalámbricas (WLAN) que usan frecuencias en las bandas 2.4 y 5 GHz los cuales fueron creados para sentar las bases de las comunicaciones y definir protocolos. La siguiente tabla muestra los estándares existentes en la actualidad.

Tabla Anexo 1.1 Estándar inalámbricos

IEEE 802.11 ^a	54Mbps, 5GHz standard
IEEE 802.11b	Enhancements to 802.11 to support 5.5 and 11Mbps
IEEE 802.11c	Bridge operation procedures; included in the IEEE 802.1D standard
IEEE 802.11d	International roaming extensions
IEEE 802.11e	Quality of service
IEEE 802.11F	Inter-Access Point Protocol
IEEE 802.11g	54Mbps, 2.4GHz standard (backward compatible with 802.11b)

IEEE 802.11h	Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) at 5Ghz
IEEE 802.11i	Enhanced security
IEEE 802.11j	Extensions for Japan and U.S. public safety
IEEE 802.11k	Radio resource measurement enhancements
IEEE 802.11m	Maintenance of the standard; odds and ends
IEEE 802.11n	Higher throughput improvements using MIMO(multiple input, multiple output antennas)
IEEE 802.11p	Wireless Access for the Vehicular Environment (WAVE)
IEEE 802.11r	Fast roaming
IEEE 802.11s	Extended Service Set (ESS) Mesh Networking
IEEE 802.11T	Wireless Performance Prediction (WPP)
IEEE 802.11u	Internetworking with non-802 networks (cellular)
IEEE 802.11v	Wireless network management
IEEE 802.11w	Protected management frames
IEEE 802.11y	3650–3700 operation in the U.S.

Estándar 802.11 b (2.4GHz)

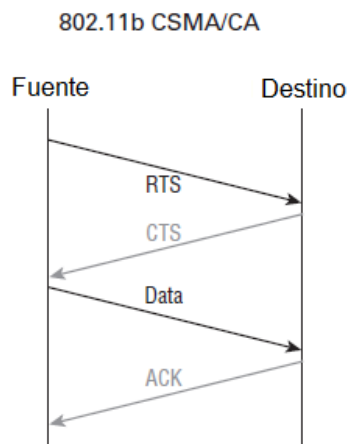
Primero de la lista 802.11 b fue el estándar más implementado en el mercado operando a 2.4 GHz y ofreciendo diversas velocidades de transmisión de hasta 11 Mbps. Un punto interesante de las redes inalámbricas es que tienen la habilidad de moverse a diferentes velocidades de transmisión, es decir una persona pueda estar conectada a 11 Mbps e irse alejando del Access Point y pasar a 5 Mbps, después a 2 Mbps y finalmente seguir conectado a 1 Mbps. Los Access Point tienen la habilidad de ofrecer diferentes velocidades a distintos usuarios dependiendo su ubicación.

El problema de 802.11b recae en la capa 2 (Data link), para resolver los problemas de colisión en el espectro RF se creó el llamado CSMA/CA Carrier Sense Multiple Access with Collision Avoidance o también llamado RTS/CTS Request To Send, Clear To Send, nombre tomado por su manera de operar. Cada paquete enviado por el Access Point debe recibirse un acknowledgment (paquete de recibido), es un proceso engorroso pero realmente funciona.

Estándar 802.11g (2.4GHz)

Este estándar fue ratificado en 2003 y compatible con 802.11b. 802.11g entrega hasta 54Mbps y funciona en la misma banda que 802.11b (2.4GHz).

Tabla Anexo 1.3 Estándar 802.11g



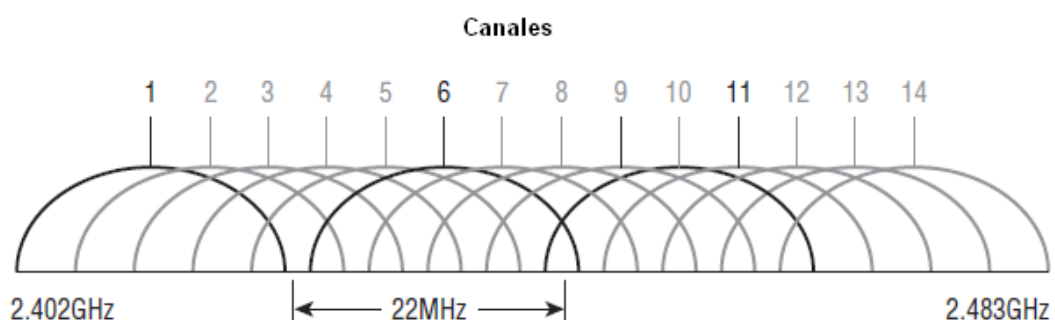
El hecho de que 802.11b/g funcionen en la misma banda de 2.4 GHz hace que una migración de infraestructura entre ellas sea muy suave respecto a los clientes (tipo de tarjetas inalámbricas). Se debe tomar en cuenta que la migración de 802.11b hacia 802.11g no es vía software aunque trabajen en la misma frecuencia, ya que usan diferentes chips en los radios, razón por la cual trabajan a velocidades distintas.

Si se tiene un Access Point en 802.11b y tienen tarjetas 802.11g, la máxima velocidad a la que trabajarán es 11Mbps, y si se tiene un Access Point 802.11g los usuarios en 802.11g trabajarán hasta 54Mbps y los 802.1b hasta 11Mbps, sin embargo si un usuario 802.11 g no logra asociarse en su banda y lo hace en 802.11b puede impactar en el rendimiento de la red, por lo tanto se recomienda deshabilitar el radio b si sólo se tiene clientes en g.

La diferencia de las bandas radica en la técnica de modulación que utilizan, 802.11b usa Direct Sequence Spread Spectrum (DSSS) la cual no es tan robusta como la que usan 802.11 a/g Orthogonal Frequency Division Multiplexing (OFMD), los clientes que trabajan en 802.11 a/g realmente perciben un mejor comportamiento que 802.11b.

La siguiente figura muestra los 14 diferentes canales, cada uno con 22MHz de amplitud permitidos por la FCC para la banda de 2.4GHz. Sin embargo sólo 11 canales son configurables y tres de no traslape (es decir que no se interfieren), 1, 6 y 11. Esto limita a usar sólo estos tres canales en una misma área sin generar interferencia.

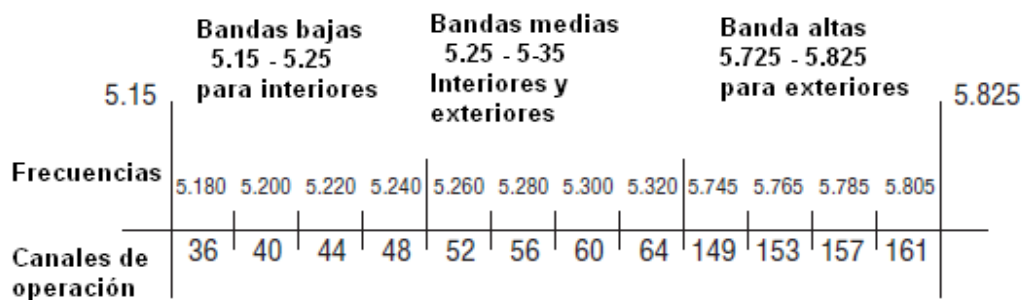
Tabla Anexo 1.4 Canales en 2.4 GHz



Estándar 802.11a (5GHz)

La IEEE ratificó este estándar en el año 1999. 802.11a entrega hasta 54 Mbps con 12 canales sin traslape, lo cual parece muy interesante.

Tabla Anexo 1.5 Canales en 5 GHz



Operar en la banda 5Ghz tiene la ventaja de ser inmune a las interferencias de dispositivos que operan en la banda de 2.4GHz como hornos de microondas, teléfonos inalámbricos y dispositivos Bluetooth. 802.11a no es compatible con 802.11b/g por trabajar en frecuencias distintas pero tienen la posibilidad de convivir sin que se genere conflicto alguno.

También 802.11a es capaz de trabajar a distintas velocidades desde 54Mbps moviéndose a 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps y finalmente a 6Mbps.

Tabla Anexo 1.6 Comparativa de bandas

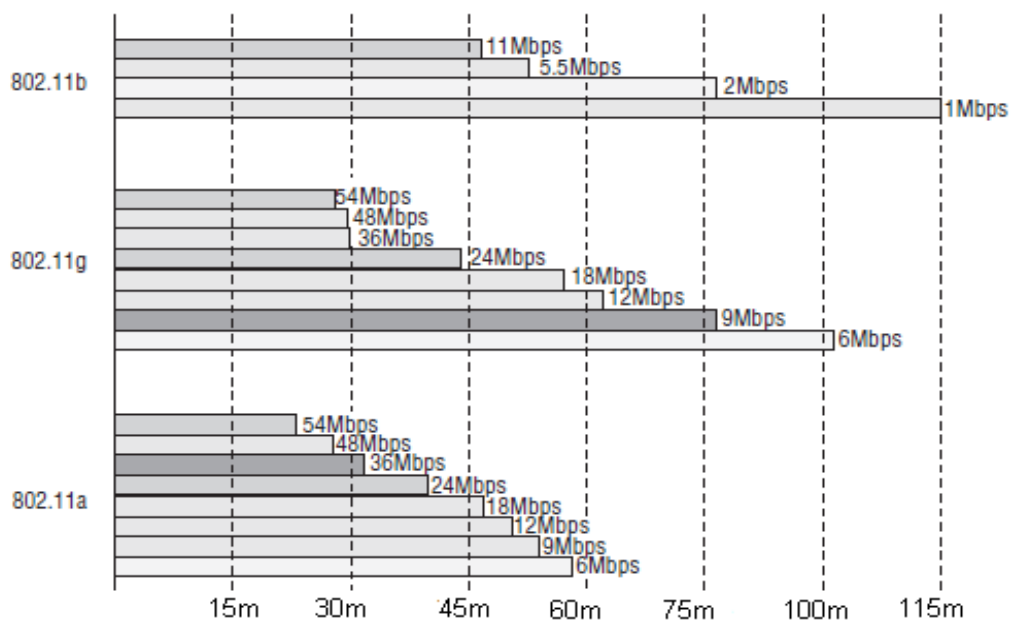
802.11b	802.11g	802.11a
2.4GHz	2.4GHz	5GHz
La más común	Alto rendimiento	El mayor rendimiento
Hasta 11 Mbps	Hasta 54 Mbps	Hasta 54 Mbps

DSSS	DSSS/OFDM	OFDM
3 canales de no traslape	3 canales de no traslape	Hasta 23 canales de no traslape
Alrededor de 25 clientes por célula	Alrededor de 20 clientes por célula	Alrededor de 15 clientes por célula
Distancia limitada por Multipath	Rendimiento degradado por clientes en 802.11b	Poca penetración en el Mercado

Estándar 802.11n (2.4GHz/5GHz)

802.11n fue creada sobre el estándar previo 802.11 agregando MIMO (Multiple-Input Multiple-Output) lo cual emplea múltiples antenas que reciben y envían para incrementar el rendimiento. 802.11n puede manejar hasta ocho antenas, sin embargo la mayoría de los Access Point de hoy en día sólo usan cuatro. Frecuentemente son llamadas antenas inteligentes, por ejemplo si se tienen cuatro antenas, dos son usadas para transmitir y dos para recibir de manera simultánea. Esta característica ofrece mayor ancho de banda que 802.11a/b/g, aproximadamente 300 Mbps. Este estándar fue ratificado en Septiembre de 2009.

Tabla Anexo 1.7 Comparativa de cobertura

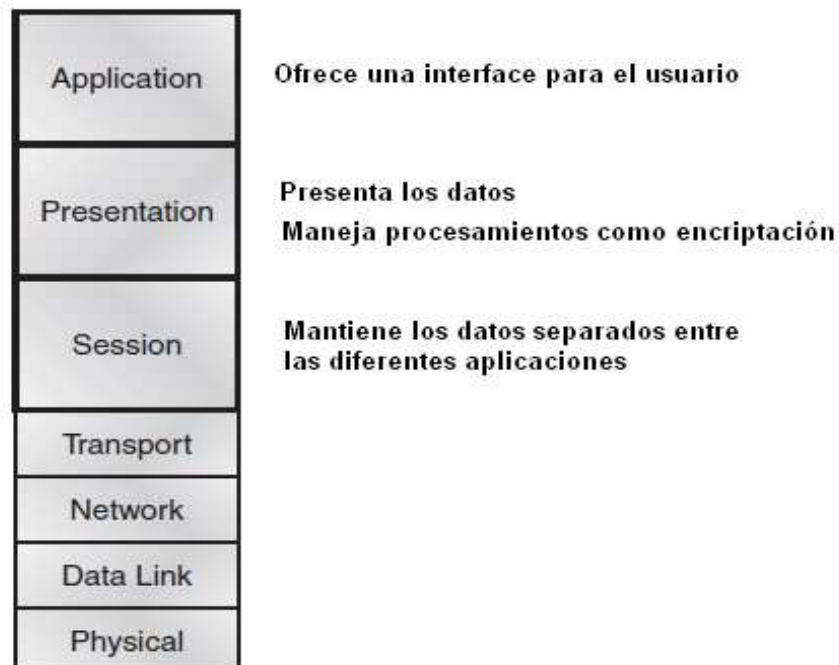


El Modelo OSI

El Open System Interconnection Reference Model (OSI) es una descripción abstracta para las comunicaciones y el diseño de los protocolos de red. Fue desarrollado por Open Systems Interconnection (ISO). En su forma básica divide la arquitectura de red en siete capas las cuales son de arriba hacia abajo, Aplicación, Presentación, Sesión, Transporte, Red, Datos y Física.

Una de las grandes funciones de OSI es asistir en la transferencia de datos entre distintos hosts, por ejemplo es capaz de comunicar y transferir información entre un PC y una Mac o un host Linux. Las tres capas superiores definen como las aplicaciones entre host se comunican de un lado al otro. Las otras cuatro capas definen como se transmiten los datos.

Tabla Anexo 1.8 Modelo OSI



Aplicación

La capa de Aplicación es la más cercana al usuario final, lo cual significa que el usuario interactúa directamente con el software. Algunos de los protocolos en esta capa son HTTP, FTP, SMTP, Telnet, etc.

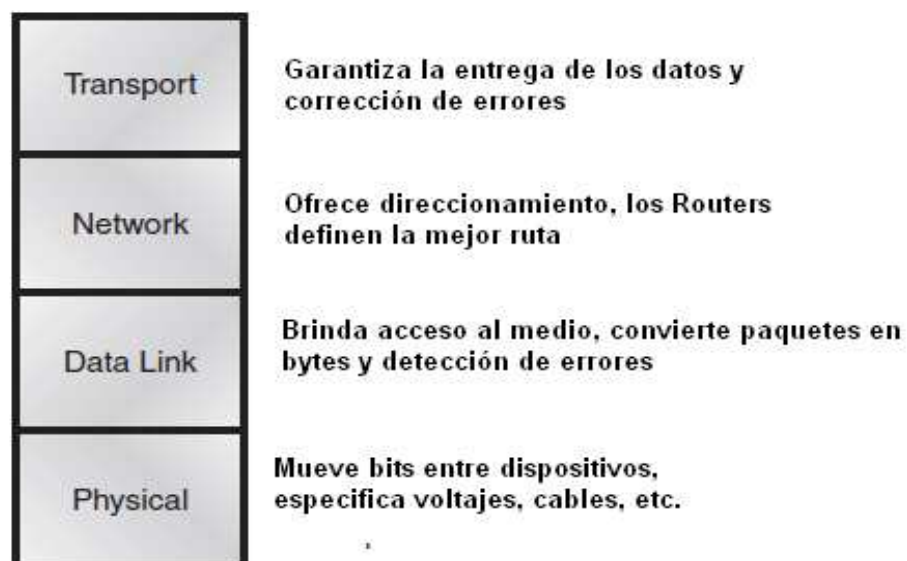
Presentación

La capa de Presentación consigue su nombre de su comportamiento, presenta los datos a la capa de Aplicación y es responsable de traslación de datos y codificación. Tareas como compresión, descompresión, encriptación, desencriptación se llevan a cabo en esta capa.

Sesión

Esta capa es responsable de iniciar, administrar y finalizar las sesiones entre los usuarios.

Tabla Anexo 1.8.1 Modelo OSI



Transporte

Esta capa es encargada de segmentar los datos y reensamblarlos así como del transporte de los mismos estableciendo una conexión lógica entre ambos nodos y corrección de errores, un ejemplo es TCP.

Red

Esta capa administra el direccionamiento de los equipos, localiza la ubicación de los equipos en la red y determina la mejor ruta para comunicarlos, los Routers se ubican en esta capa.

Datos

Esta capa ofrece transmisión física de datos y manejo y notificación de errores, topología de la red y control de flujo. Ejemplos de esta capa son ARP, Frame Relay y PPP. Aquí es donde se ubica el estándar 802.11.

Física

Esta capa es la encargada de enviar y recibir bits. Aquí se definen las especificaciones eléctricas, es decir la relación entre el dispositivo y el medio. Incluye voltajes, especificaciones de cables y el más claro ejemplo son los Hubs y Repetidores.

Comunicación Inalámbrica

Una PC con una tarjeta inalámbrica es encendida en cualquier lugar y requiere conectarse a una red, naturalmente hay ciertos paquetes de negociación que necesita enviar y recibir antes de iniciar una comunicación con otro dispositivo. ¿Qué información necesita?

SSID

En la terminología de la IEEE cualquier grupo de dispositivos inalámbricos es conocido como *Service Set* los dispositivos deben compartir un común *Service Set Identifier (SSID)* la cual es una cadena de texto incluida en cada paquete enviado. Si el SSID coincide entre el transmisor y el receptor los dispositivos podrán comunicarse.

La PC como un usuario final se convierte en un cliente de la red inalámbrica, la cual debe tener un adaptador (tarjeta de red) y un suplicante (software que interactúa con los protocolos inalámbricos).

IBSS

El estándar 802.11 permiten que dos o más dispositivos inalámbricos se comuniquen directamente entre ellos sin la conectividad de una red. Esto se conoce como red inalámbrica *Ad-Hoc* o Independent Basic Service Set (IBSS).

BSS

Un Basic Service Set (BSS) centraliza el acceso y el control de un grupo de dispositivos inalámbricos colocando un Access Point (AP) para lograrlo. Cualquier cliente que intente usar esta red deberá tener primero una membresía con el AP. El AP puede requerir uno o más de los siguientes criterios para permitir que un usuario se una a él.

-
- Coincidencia del SSID
 - Compatibilidad inalámbrica de velocidad (802.11a/b/g)
 - Credenciales de autenticación

La membresía con el AP es conocida como *asociación*. El cliente debe enviar un mensaje de petición de asociación, el AP es capaz de aceptarlo o rechazarlo enviando de regreso un mensaje de respuesta. Una vez lograda tal asociación toda la comunicación desde y hacia el cliente debe pasar por el AP. La diferencia con el IBBS (Ad-Hoc) es que el BSS siempre requiere de un AP para comunicarse.

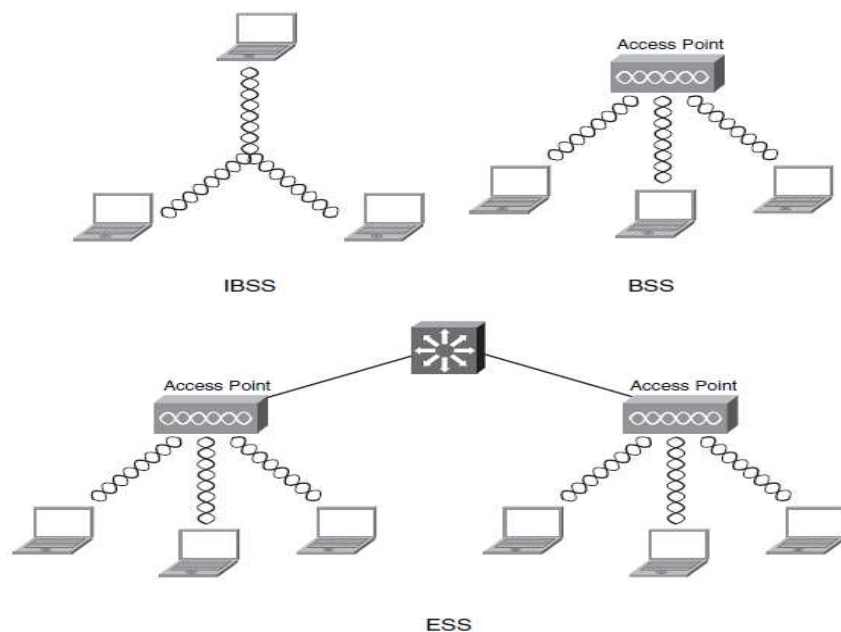
NOTA: Deben tener en cuenta que sin importar el estado de asociación, las PCs son capaces de escuchar y/o recibir paquetes existentes en el medio inalámbrico. Estos paquetes viajan libremente en el ambiente esperando que alguien dentro de su rango los reciba.

Un AP no es un dispositivo pasivo como un Hub, el AP es capaz de darse cuenta de la existencia de los usuarios asociados y controlar el proceso de comunicación, es capaz de evitar colisiones mientras fluyen los datos.

ESS

Extended Service Set es el escenario cuando dos AP están comunicados a través de una red cableada (Switch) un cliente es capaz de moverse estando asociado del AP1 al AP2 sin perder la comunicación (Roaming).

Tabla Anexo 1.10 Comparación entre Service Sets



Operación de los Access Point

La función principal de un Access Point es ser un puente para los datos inalámbricos hacia una red cableada. Un AP acepta conexiones de un número de usuarios, los cuales se convierten en miembros de la red WLAN de la misma manera que lo hacen los usuarios cableados (LAN).

Un AP puede actuar como un puente entre dos redes LAN divididas por una distancia considerable. En este caso se debe contar con una línea de vista entre los AP los cuales son instalados típicamente para ofrecer conectividad entre dos edificios.

Cisco ha desarrollado plataforma de Access Point que pueden intercambiar tráfico de AP a AP lo cual permite que una gran área pueda ser cubierta con sólo dispositivos inalámbricos sin la necesidad de cableado de red. Los AP forman una topología de malla (Mesh) muy parecida el ESS, donde los usuarios son capaces de mantener la comunicación pasando sus servicios de una AP a otro.

Un Access Point funge como un punto central de acceso (de ahí su nombre), controlando el acceso de los clientes a la red. Cualquier usuario que intente usar la red inalámbrica primero debe establecer una asociación con el AP. El AP puede permitir un acceso abierto donde cualquier usuario podría asociarse o también podría limitar el ingreso con credenciales de autenticación o algún otro criterio configurado previamente.

La operación de una red inalámbrica está amarrada a un comportamiento de retroalimentación de un dispositivo con un AP. Por ejemplo, los clientes deben negociar con un AP antes de su asociación para poder usar los recursos. En su nivel más básico esto asegura una conexión en dos vías porque ambos dispositivos (AP y cliente) son capaces de enviar y recibir paquetes de petición y aceptación. Este proceso elimina cualquier posibilidad de comunicación unidireccional, donde el cliente puede escuchar al AP pero el AP no puede escuchar al cliente.

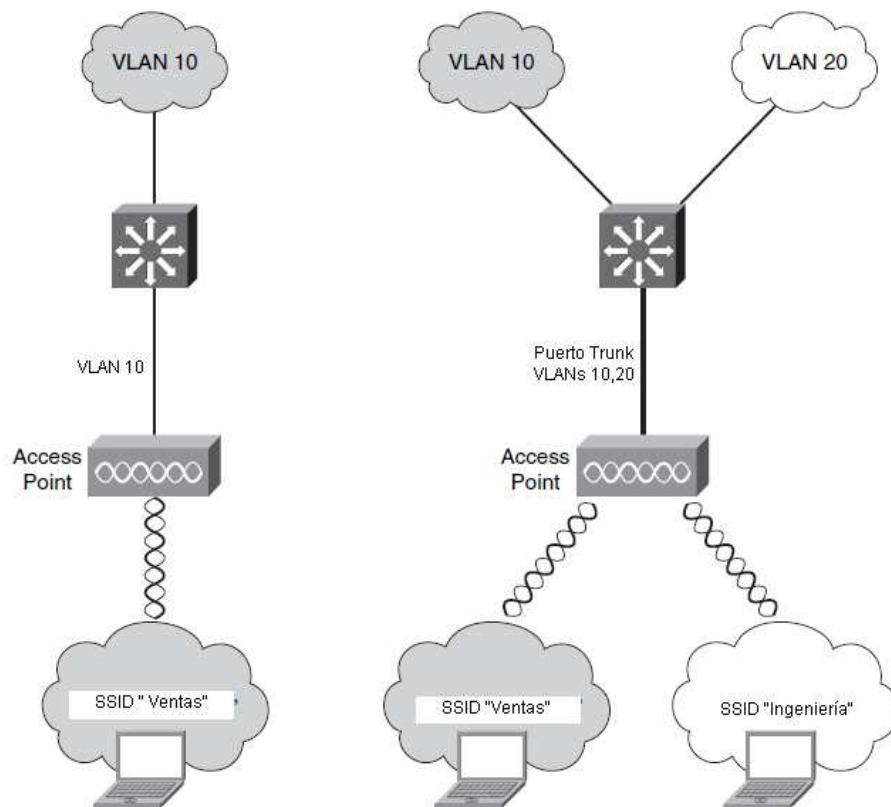
También el AP puede solicitar diversos aspectos de control para su acceso en cada SSID, por ejemplo el AP puede requerir soporte de ciertas velocidades de transmisión, condiciones de seguridad, credenciales de asociación, encriptación, etc.

Un AP es capaz de mapear (relacionar) un SSID con una VLAN. La parte izquierda de la siguiente figura se muestra que la VLAN 10 de la red cableada genera una extensión a través de AP conectado a un puerto de acceso del Switch. El AP mapea la VLAN 10 a una red inalámbrica usando el SSID "Ventas". Los usuarios asociados al SSID "Ventas" aparecerán conectados a la VLAN 10.

Este concepto puede ser extendido a mapear múltiples VLANs a múltiples SSIDs. Para lograr esto el AP debe estar conectado a un puerto del Switch configurado como puerto Trunk capaz de permitir el paso de las VLANs.

En la parte derecha de la figura VLAN 10 y VLAN 20 pasan vía el Trunk del AP. El AP usa 802.1Q para realizar el mapeo VLAN-SSID. La VLAN 10 está mapeada al SSID "Ventas" y la VLAN 20 al SSID "Ingeniería".

Tabla Anexo 1.11 VLAN en los Access Point



Células Inalámbricas

Un AP sólo puede ofrecer servicio a usuarios que estén dentro de su rango de cobertura. El rango de la señal del AP está definido por el patrón de radiación de la antena.

La ubicación del AP debe ser cuidadosamente planeada para que su rango de cobertura coincida con el área que nos interesa cubrir.

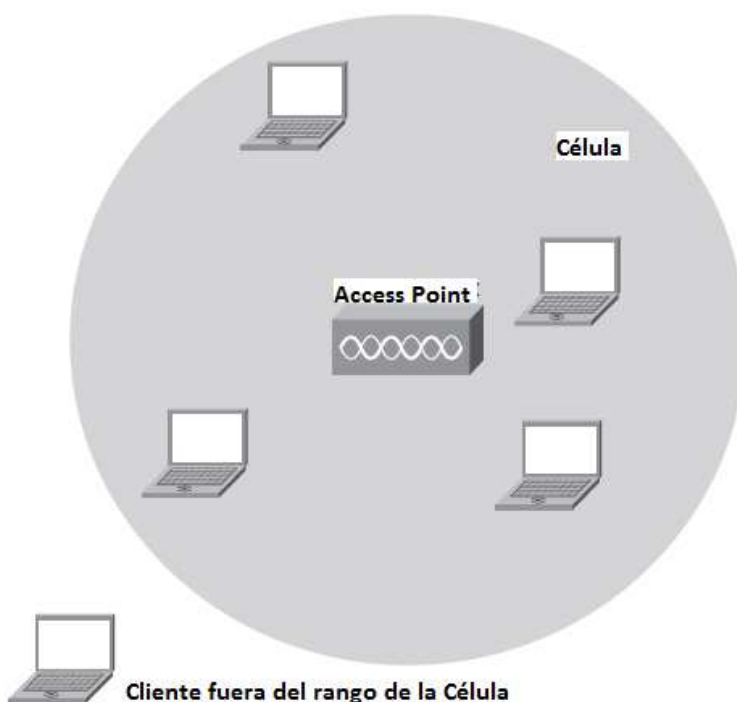
El diseño puede hacerse con un mapa del físico del lugar a implementar, las redes inalámbricas trabajan en condiciones cambiantes por lo tanto se debe poner cuidado especial en las ubicaciones, ya que los AP se mantendrán fijos pero los clientes se estarán moviendo frecuentemente en todos los espacios del inmueble.

El movimiento de los clientes puede ocasionar que las áreas de cobertura no se mantengan como originalmente se planeó, es decir si un cliente está detrás de una pared u objetos dentro de una oficina o cruza una puerta, etc., se puede bloquear la señal que perciben los usuarios y no cumplir con los requerimientos mínimos de cobertura.

Para garantizar una buena ubicación de los AP y la cobertura en cada zona de interés se debe realizar un Site Survey. Un Site Survey es una prueba donde se coloca un AP en un lugar deseable y se realizan recorridos con equipos inalámbricos, aquí se registran valores de potencia y calidad de la señal así como el nivel de ruido en el ambiente. La intención es poder moverse en cada espacio, incluso en aquellos donde normalmente no se encontraría un usuario, pasando por los diferentes obstáculos existentes que generen pérdida de la señal "Signal Loss".

El área de cobertura de un AP es llamada Célula. Los clientes dentro de la Célula pueden asociarse al AP y usar los servicios de la red inalámbrica. En la siguiente imagen un cliente está ubicado fuera de la Célula, es decir más allá del alcance del rango de cobertura del AP, por lo tanto no podrá conectarse a la red.

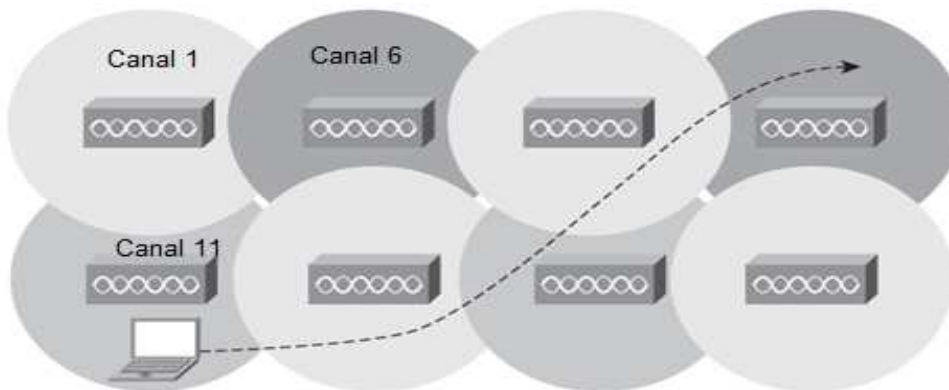
Tabla Anexo 1.12 Célula Inalámbrica



Teóricamente un AP en un espacio interior es capaz de cubrir hasta 30 metros de radio, es decir los clientes podrán moverse dentro de este espacio. Para expandir el área de cobertura de la red inalámbrica otras Células deben ser colocadas alrededor unas de las otras donde los clientes se ubican, aunado a esto se debe garantizar un pequeño porcentaje de traslape (una célula sobre otra), como se muestra en la figura.

En los diseños donde existe un traslape los AP adyacentes no puede operar en la misma frecuencia, si dos AP vecinos usan la misma frecuencia se interferirán, así que en el diseño se debe tener cuidado correcta elección de los canales.

Tabla Anexo 1.13 Canales sin traslape



Como lo muestra la figura, los AP se encuentran en canales distintos y una vez que el cliente se asocia al primer AP será capaz de pasar a través de todo el espacio sin perder la conectividad. Este movimiento se llama Roaming, el cual es el paso de un cliente de un punto a otro, experimentado asociaciones en diferentes AP sin perder la comunicación.

Cuando un cliente se mueve de un AP a otro su asociación debe establecerse con el nuevo AP. Todos los datos que el cliente necesita para el Roaming son enviados del AP original al nuevo AP, de esta manera el cliente sólo está asociado a un AP a la vez. Cuando se diseña una solución de debe tratar de utilizar la máxima área de cobertura que ofrece el AP (configurando este parámetro en el equipo), esto reducirá la cantidad de AP así como el costo del proyecto, sin embargo los requerimientos del cliente pueden ser distintos en cada instalación, es decir se debe considerar la cantidad de usuarios por área, la demanda de ancho de banda para tipos de tráfico como voz y video y distintas aplicaciones.

Características de Radiofrecuencia

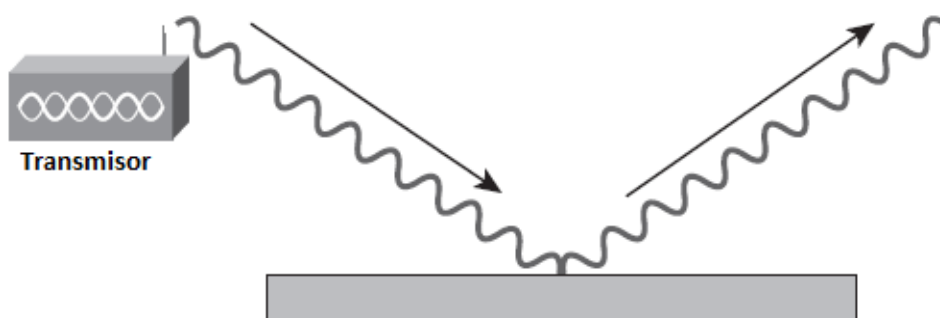
Las señales de radiofrecuencia atraviesan el aire en ondas electromagnéticas, en una situación ideal una señal debería llegar al receptor exactamente como la envía el transmisor, en el mundo real esto no sucede. La señal es afectada por diversos factores, objetos y materiales que se encuentran en su viaje entre el transmisor y el receptor. A continuación explico algunos de estas condiciones.

Reflexión

Si una señal que viaje por el aire encuentra un material denso ésta podría reflejarse. Pensemos en una luz emitida desde un bulbo y toda la luz que viaja y lo atraviesa en todas las direcciones, algo puede ser reflejado por los objetos del lugar. La luz reflejada puede regresar a través del bulbo o hacia otras direcciones dentro del mismo lugar.

La siguiente figura muestra esta reflexión. En ambientes interiores se presenta este fenómeno con gabinetes, elevadores o puertas de metal, en exteriores los cuerpos de agua, árboles o la capa atmosférica la generan.

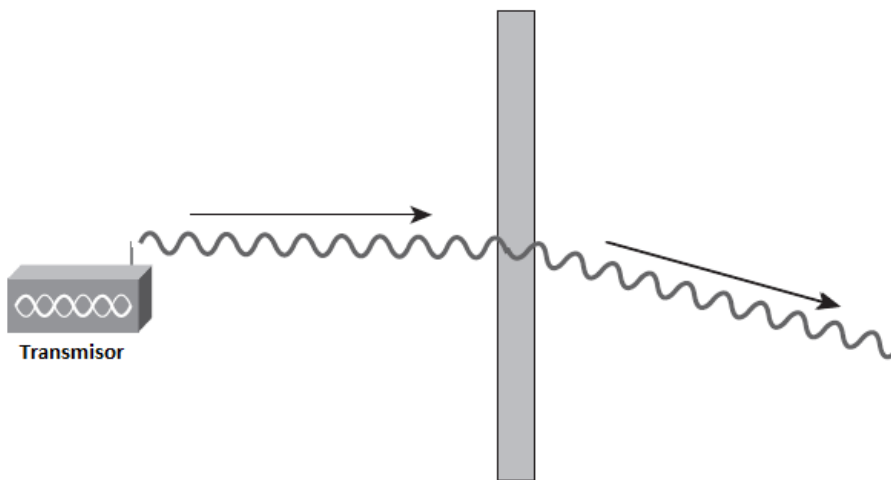
Tabla Anexo 1.14 Reflexión de señal



Refracción

Cuando una señal se encuentra entre dos medios de diferentes densidades puede sufrir refracción. Una señal refractada tendrá un ángulo diferente al original y la velocidad de la onda puede reducirse. La figura muestra este concepto.

Tabla Anexo 1.15 Refracción de señal



Antenas

Un AP sólo puede ofrecer servicio a usuarios que estén dentro de su rango de alcance, este rango es definido por un área de cobertura emitida por una antena. Las antenas son diseñadas para diversos ambientes, la correcta implementación de las antenas en la solución mejora considerablemente la cobertura y el performance de la red. El conocimiento en la elección, el montaje, tipo de conectores, patrones de radiación, etc., maximizarán la zona de cobertura lo cual se reflejará en una correcta implementación.

Las antenas utilizadas por Cisco ofrecen bandas de 2.4- and 5-GHz:

- 2.4 GHz (2.4-2.4835 GHz)-IEEE 802.11b y g
- 5 GHz (5.15-5.35 and 5.725-5.825 GHz)- IEEE 802.11a

Cada rango ofrece características distintas. Las frecuencias bajas tienen mejor rango, pero con un limitado ancho de banda. Las frecuencias altas tienen menor rango y están expuestas a mayores atenuaciones debido a objetos sólidos.

Una antena brinda a un sistema inalámbrico (Access Point) dos propiedades fundamentales; ganancia y dirección. La ganancia es una medida del incremento de la potencia. Dirección es el aspecto que tiene el patrón de transmisión.

El valor de la ganancia es medido en decibeles que es una razón entre dos valores. Esta ganancia referenciada a una antena isotrópica, la cual es una antena teórica con un patrón de radiación uniforme. dBi es usado para comparar el nivel de potencia de una antena con una antena teórica isotrópica. La FCC (Federal Communications Comision) usa dBi en sus cálculos. Una antena isotrópica se dice que tiene una potencia de 0 dB, es decir cero ganancia/perdida cuando se compara consigo misma. A diferencia de las antenas isotrópicas, las antenas dipolares son antenas reales (este tipo de antenas son estándar en Cisco Access Point).

Las antenas dipolares tienen diferentes patrones de radiación, 360 grados en el plano horizontal y 75 grados en el plano vertical (asumiendo que la antena está colocada verticalmente) y forma un patrón similar al aspecto de una dona.

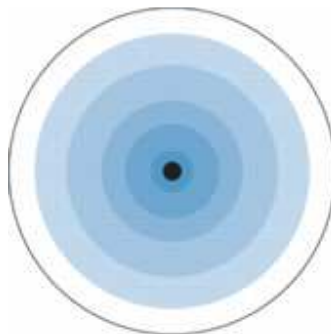
Debido a que el haz está ligeramente concentrado, la antena dipolar tiene una mayor ganancia sobre la antena isotrópica de 2.14 dB en el plano horizontal. Por lo tanto se dice que las antenas dipolares tienen una ganancia de 2.14 dBi en comparación con la antena isotrópica. Por los valores de las antenas son denotadas como dBi.

Tipo de Antenas

La tecnología Cisco ofrece diferentes estilos de antenas para los AP en la frecuencia de 2.4GHz y también para 5 GHz. Estas antenas deber ser probadas y avaladas previamente por la FCC. Cada antena ofrece diferentes capacidades de cobertura. En la medida que la ganancia de la antena se incrementa también lo hace su cobertura. Algunas antenas ofrecen amplias aéreas de cobertura en cierta dirección. Los tipos más comunes de antenas usadas son Omnidireccional, Yagui y Patch.

Una antena omnidireccional está diseñada para ofrecer 360 grados de radiación. Esta antenas son usadas donde se quiere cobertura en todas las direcciones.

Tabla Anexo 1.16 Patrón de antena omni



Antenas direccionales tienen diferentes estilos y aspectos, no significa que estas antenas agreguen la potencia a la señal si no que redireccionan la potencia ofreciendo mayor energía en dicha dirección, debido a que la ganancia se incrementa en este tipo de antenas de la misma manera en ángulo se decrementa, lo cual ofrece mayores coberturas a la distancia.

Ejemplo de estas antenas son Yagi y Patch.

Tabla Anexo 1.17 Patrón de antena patch

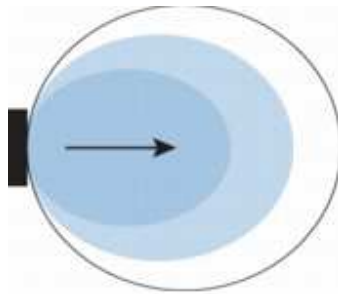
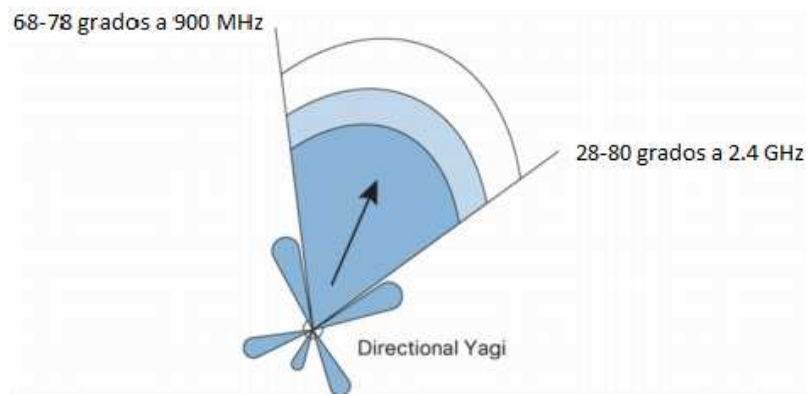


Tabla Anexo 1.18 Patrón de antena yagi



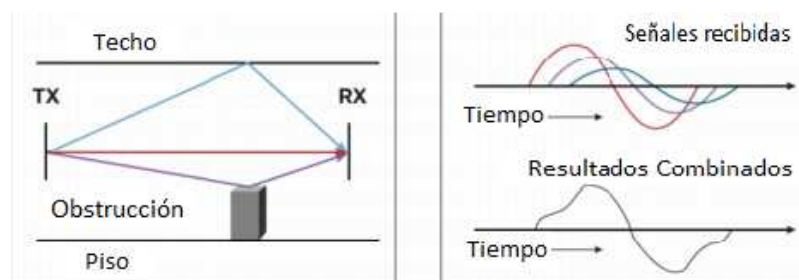
Las antenas en Sistema de Diversidad son usadas para eliminar el fenómeno conocido como Distorsión de Múltiple trayectoria (Multipath Distortion) usando dos antenas idénticas colocadas a cierta distancia para ofrecer mejor cobertura de un área física.

La Distorsión de Múltiple Trayectoria ocurre cuando la señal de radiofrecuencia RF tiene más de una trayectoria entre el receptor y el transmisor. Esto ocurre en sitios donde existen espacios metálicos amplios u otras superficies brillantes. De la misma manera que la luz y el sonido rebota en los objetos, la señal de RF también, lo cual significa que hay más de una trayectoria entre la antena que envía y la que recibe los datos.

Esta multiplicidad de señales se combina y causan distorsión de la señal y a su vez esto genera que los datos sean irre recuperables. El tipo y correcta posición de las antenas ayudan a eliminar este problema.

Una analogía a este tipo de fenómeno es cuando detenemos el auto en un semáforo y la señal comienza a perderse, esto es justo porque en ese punto varias señales están convergiendo, sin embargo cuando nos movemos hacia atrás o adelante la señal se estabiliza nuevamente.

Tabla Anexo 1.19 Efecto Multipath Distortion



Red Inalámbrica Unificada

Existe un amplio rango de productos que soportan los estándares 802.11 a/b/g incluso varios para “n” las cuales ofrecen diversas soluciones para ambientes de interiores o exteriores. Estos productos incluyen Access Point, controladores inalámbricos, adaptadores para clientes, servidores de seguridad y administración, dispositivos de administración de la red y resolución de problemas, servicios inalámbricos integrados en Switches y Routers así como antenas y accesorios.

Las redes inalámbricas autónomas (no unificadas) requieren de una configuración independiente en cada equipo, así como la administración y la resolución de problemas de forma individual. Esta característica requiere un numeroso personal de soporte para poder visualizar la red de manera completa así como la atención de incidentes y la reconfiguración de nuevos equipos o la integración de nuevas características en la red. Esto no sólo genera mayor inversión para las empresas sino inconsistencias en configuraciones que se reflejan en intermitencias en el servicio hablando de soluciones que incluyen más de 100 equipos.

¿Podrían pensar en una red que después de una instalación inicial no requiera configuración alguna? Es decir una vez instalada tú red inalámbrica tengas la posibilidad de conectar un AP el cual se configure de manera automática con sólo la configuración del Controlador. El Wireless LAN Controller es un dispositivo ofrece tal ventaja, es capaz de revisar la potencia de la señal requerida para cubrir las necesidades del cliente (suplicante – laptop o cualquier dispositivo con tarjeta inalámbrica), percibe y evita interferencias y canales para usar aquellos que tengan menor demanda y/o ruido en el ambiente de RF, evitar traslapes, etc. Esta característica Cisco la llama “Control Auto RF”.

La solución inalámbrica que comprende Controladores en su conjunto con los Access Point tiene la base de su funcionamiento en una característica llamada Split-MAC Architecture.

Split Mac divide las tareas requeridas para que una red inalámbrica pueda operar de manera correcta, esta división es hecho entre los Access Point y el Controlador.

Las siguientes tareas son realizadas por el Access Point:

- Transmisión de beacons (anuncio de la red en el ambiente RF)
- Respuesta a pruebas de conexión con los clientes
- Forwardeo de notificaciones de las pruebas hacia el Controlador
- Proveer información de la calidad de la señal en tiempo real
- Monitoreo de los canales en relación al ruido e interferencias
- Monitoreo de la presencia de otros Access Point
- Encriptación y desencriptación

El resto de las funcionalidades necesarias para la operación son ofrecidas por el Controlador el cual mantiene una amplia visibilidad de todos los dispositivos asociados a él, las funciones de MAC Layer ofrecidas por el Controlador son las siguientes:

- Autenticación
- Asociación y reasociación (movilidad)
- Translación de frames

Básicamente se puede entender que las funcionalidades que requieren un manejo en tiempo real pueden ser delegadas al Access Point y las que no necesitan esta característica son realizadas por el Controlador.

Protocolo LWAPP

Lightweight Access Point Protocol o LWAPP es el nombre del protocolo que puede controlar múltiples Access Point a la vez. Esto reduce la cantidad de tiempo empleado para configurar, monitorear y administrar grandes redes inalámbricas.

Un sistema centralizado es donde los Access Point se asocian al Controlador quien es encargado de la configuración, versión de sistema operativo y control de las transacciones de autenticación 802.1x. Adicionalmente el protocolo encapsula el tráfico en un túnel entre los Access Point y el Controlador.

Una vez que el Controlador es configurado en una red cableada el siguiente paso es conectar los Access Point, estos envían inmediatamente paquetes para ser agregados al Controlador, mismo que responde dichas peticiones permitiendo que los Access Point inicien un proceso de agregación. Cuando el Access Point esta unido al Controlador descarga el software necesario para operar (si es que las versiones de ambos no coinciden). Después de esto el Access Point depende totalmente del Controlador desde el cual se realizará la configuración deseada.

El protocolo LWAPP asegura que el proceso de agregación entre AP y Controlador sea seguro, para esto requieren intercambiar un certificado de autenticación (X.509), evitando así que Access Point no permitidos (Rogue) sean parte del Controlador.

Seguridad en el medio inalámbrico

La seguridad informática siempre será un punto medular en la implementación de cualquier red de datos y voz. La gran cantidad de ataques existentes han motivado a crear niveles de seguridad más robustos cada día, para evitar que los datos sean interceptados, modificados, denegados, etc. Uno de los dilemas que los clientes enfrentan cuando desean implementar una red inalámbrica y gozar de todos los beneficios que esta ofrece, es la exposición de los datos, es decir el ambiente RF donde viajan los paquetes no está limitado por espacios físicos, cuartos de comunicaciones, conexiones a puertos físicos de la red, etc.

Afortunadamente el mundo inalámbrico se ha expandido y robustecido la seguridad de sus soluciones basándose en estándares que garantizan la seguridad informática en un ambiente RF.

Acceso Abierto

Los Access Point son capaces de ofrecer un acceso abierto, sin algún nivel de seguridad implementado que es útil para cierto tipo de soluciones, estas pueden ser Hot Spots en aeropuertos, restaurantes, universidades donde se ofrece acceso a Internet, sin embargo en ningún caso se recomienda que en un ambiente empresarial se implemente una red con esta característica. La mayoría de estos equipos no tienen seguridad configurada por defecto, esto porque muchas veces el usuario que los adquiere no conoce de computadoras y/o redes y solo necesita conectar el equipos para que este funcione sin ninguna configuración extra.

Características de Seguridad

El diseño del estándar inalámbrico 802.11 fue originalmente creado con ciertas características como el SSID, autenticación abierta y compartida, claves WEP (Wired Equivalency Protocol) y autenticación de Control de Acceso al Medio (MAC). Sin embargo actualmente ninguno de estas características puede garantizar la seguridad de una red, incluso ya no es recomendada para redes en el hogar.

Como ya se mencionó el SSID es el nombre de la red a la cual se conectarán los dispositivos inalámbricos, lo cual indica que si alguien no lo tiene no podría conectarse a la red. Usar la característica de ocultar el SSID para evitar asociaciones no permitidas y tratar de asegurar de esta manera nuestra red es un riesgo inminente. Es fácil saber qué SSIDs están en el ambiente sin que estén “publicados”, este se puede hacer con herramientas de acceso abierto en Internet o incluso con ciertas tarjetas inalámbricas que tienen tal característica y que hacen uno de los paquetes de respuesta que los clientes envían a los Access Point para conectarse.

Hay dos tipos de autenticación especificados por la IEEE 802.11: abierto y compartido (open y shared-key). Autenticación abierta aun sigue siendo un método utilizado hoy en día, sobre toda en redes de los hogares.

En la autenticación compartida el Access Point envía un paquete en texto claro (clear text) con el cliente debe encriptar con la correcta llave WEP y regresarla al Access Point, si la llave no es correcta la autenticación fallará y los usuarios no serán capaces de unirse al AP. Sin embargo un intruso fácilmente puede interceptar el texto en claro y el paquete encriptado y poder descifrarlo, por lo tanto este método se considera altamente inseguro y desde hace años ha dejado de ser utilizado.

Con la autenticación abierta el usuario puede asociarse a la red inalámbrica, sin embargo no podrá enviar o recibir información a menos que tenga la llave WEP correcta. Dicha llave está compuesta por 40 o 128 bits, es configurada estáticamente y definida por el administrador de los Access Point. En una red Inalámbrica Unificada el Controlador permite que la llave WEP (así como cualquier tipo de seguridad configurada para un SSID) sea ingresada una sola vez, sin importar la cantidad de Access Point que estén publicando dicho SSID. En el caso de una red Autónoma donde cada AP debe configurarse de manera individual es prácticamente imposible ingresar el mismo valor tantas veces como AP se tengan lo cual hace impensable en un red empresarial de tamaño considerable en estos días. La autenticación vía Mac Address tiene la característica de permitir sólo los valores hexadecimales de las tarjetas permitidas en la red, sin embargo se puede personificar dicho valor y ser usado por otra tarjeta ya que el valor se envía en claro (clear-text), ofreciendou una brecha de seguridad para intrusos, en caso de tener sólo este tipo de seguridad configurada. De la misma manera poder configurar y administrar este tipo de seguridad requiere mucho tiempo, lo cual se minimiza considerablemente en las redes Unificadas.

WPA Pre-shared Key

Este tipo de seguridad sigue siendo considerada básica, sin embargo es mucho mejor que las técnicas anteriormente mencionadas. PSK (Preshared Key-Llave Precompartida) verifica usuarios a través de un código que identificación o password también llamada passphrase tanto en el cliente como en el Access Point. El cliente solo tendrá acceso a la red si dicho password coincide con el AP.

WPA2 también hace uso de TKIP o AES para generar llaves de encriptación por cada paquete de datos transmitido. Aunque PSK es mucho más robusto que WEP el hecho de estar almacenado la computadora o dispositivo inalámbrico llega a comprometer la seguridad del mismo ya que se podría importar el perfil del usuario y exportarlo en otra computadora para obtener acceso a la red.

WPA es un estándar desarrollado por la WiFi Alliance. WPA provee estándares de autenticación y encriptación.

Seguridad en una red inalámbrica unificada

Las redes unificadas de Cisco ofrecen características innovadoras que soportan WPA y WPA2 los cuales proveen un control de acceso a los usuarios que en cada sesión realizan una mutua autenticación y brindan privacidad de los datos así como Calidad de Servicio (garantizar que la información sea intercambiada en caso de saturación de la red), ofrecer movilidad a los usuarios.

Existen una variedad de protocolos que ofrecen técnicas de mutua autenticación los cuales son muy robustos y son implementados con una infraestructura más sólida dedicada especialmente a ofrecer este tipo de servicios. Un ejemplo son las variantes del protocolo EAP (Extensible Authentication Protocol), así como servicios de RADIUS (Remote Authentication Dial In User Service) y servidores de Autenticación, Autorización y Accounting (AAA), como el Cisco Secure Wireless Control Server (ACS).

Las redes inalámbricas utilizan muchos de los dispositivos de detección y prevención de ataques como las redes cableadas, esto para detectar acceso no permitidos, ataques como denegación de servicio o Man in the Middle y Rogue Access Point. Los equipos utilizados para este tipo de vulnerabilidades son Sistemas de Prevención de Intrusos (IPS), NAC (Cisco Network Access Control) y servicios avanzados de ubicación.

Cisco IPS permite a los administradores estar escaneando continuamente el ambiente RF con la finalidad de detectar Access Point y eventos no autorizados, simultáneamente rastrea cientos de dispositivos y mitiga ataques. Cisco NAC tiene la finalidad de proteger a los equipos PC, laptops, Servers y PDA en redes cableadas e inalámbricas que intentan ingresar a los recursos de red y que no cumplen con ciertos estándares de seguridad marcados por la empresa, algunos ejemplos son la falta de actualizaciones del sistema operativo, antivirus, etc.

Controladores Inalámbricos

Las soluciones de Cisco cuentan con varios modelos de Controladores inalámbricos que ofrecen diversas características, una de los diferenciadores más importantes al momento de decidir qué equipo adquirir está en relación directa con la escalabilidad requerida por el cliente. Es decir cuál es la capacidad de la red y qué porcentaje de crecimiento se tiene planeado en el corto plazo.

Uno de los equipos que ofrecen una solución integral para 25 o 50 Access Point es el Cisco SW3750G, el cual es un Switch que tiene integrado un Controlador. Este tipo de equipo es ideal para pequeñas empresas donde el presupuesto es bajo y se aprovechan los puertos del Switch para conectar los Access Point o alguna PC, teléfono IP o cualquier otro dispositivo de red.

Tabla Anexo 1.20 Switch-Controlador Cisco 3750G



Existen equipos modulares (tarjetas) que pueden ser instalados en Swiches o Routers que ofrecen las mismas características inalámbricas, estas son las tarjetas WiSM que se instala en un equipo 6500 o el Network Module para Routers ISR.

Tabla Anexo 1.21 Controlador Cisco WisM

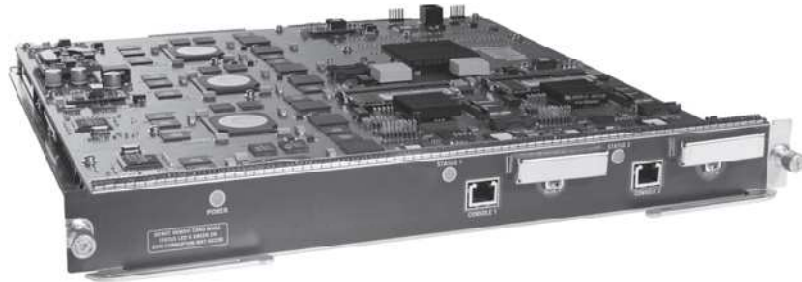
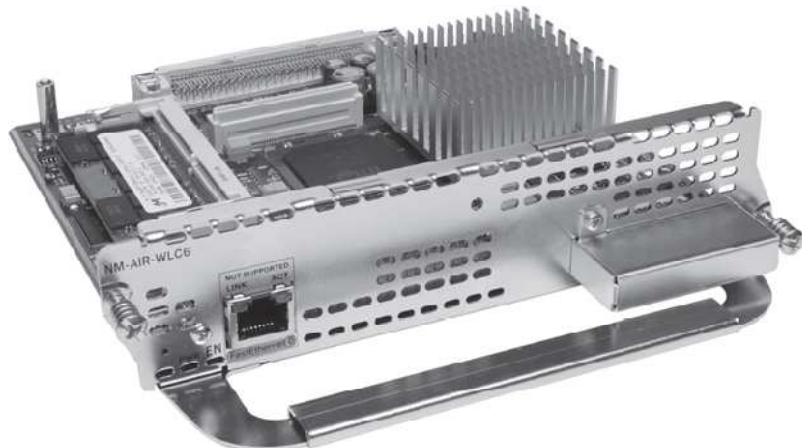


Tabla Anexo 1.22 Modulo Controlador para Router



Sin embargo los más comunes, (utilizados para la solución de este proyecto), son los Controladores 4400 Series. Estos controlados son capaces de soportar desde 1 hasta 100 AP dependiendo las necesidades del cliente. El total de Access Point lo determina una licencia instalada en el mismo.

Tabla Anexo 1.23 Controladores 4402 y 4404



Los equipos cuentan con puertos de fibra (2 para el modelo 4402 y 4 para el modelo 4404) llamados Puertos de Distribución que serán la conexión hacia la red cableada.