Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación

Diseño de la Red de Área Local Inalámbrica para el Edificio de Aulas de la Facultad de Ciencias de la UCV

Trabajo Especial de Grado
presentado ante la Ilustre
Universidad Central de Venezuela
por el Bachiller:

Felix Edward García Espinoza
C.I. 14689650
fege_ucv@yahoo.es

para optar al título de Licenciado en Computación

Tutora: María E. Villapol

Caracas, Noviembre 2010

Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación
Laboratorio de Comunicación y Redes

ACTA DEL VEREDICTO

Quienes suscriben, Miembros del Jurado designado por el Consejo de la Escuela de Computación para examinar el Trabajo Especial de Grado, presentado por el Bachiller Felix E. García C.I. 14689650, con el título **"Diseño de la Red de Área Local Inalámbrica para el Edificio de Aulas de la Facultad de Ciencias de la UCV"**, a los fines de cumplir con el requisito legal para optar al título de Licenciado en Computación, dejan constancia de lo siguiente:

Leído el trabajo por cada uno de los Miembros del Jurado, se fijó el día 1 de Noviembre de 2010, a las 9:00 AM, para que sus autores lo defendieran en forma pública, en el Laboratorio de Internet2, lo cual estos realizaron mediante una exposición oral de su contenido, y luego respondieron satisfactoriamente a las preguntas que les fueron formuladas por el Jurado, todo ello conforme a lo dispuesto en la Ley de Universidades y demás normativas vigentes de la Universidad Central de Venezuela. Finalizada la defensa pública del Trabajo Especial de Grado, el jurado decidió aprobarlo.

En fe de lo cual se levanta la presente acta, en Caracas el 1 de Noviembre de 2010, dejándose también constancia de que actuó como Coordinadora del Jurado el Profesora Tutora María Villapol.

Profa. María Villapol
(Tutora)

Prof. Carlos Acosta
(Jurado Principal)

Prof. David Pérez
(Jurado Suplente)

RESUMEN

Título:
Diseño de la Red de Área Local Inalámbrica para el Edificio de Aulas de la Facultad de Ciencias de la UCV.

Autor:
Felix Edward García Espinoza

Tutora:
Profa. María Villapol

El presente trabajo especial de grado tiene como objetivo elaborar y proponer el diseño de una solución inalámbrica basada en el estándar IEEE 802.11 para la conectividad del Edificio de Aulas de la Facultad de Ciencias de la UCV con su red de datos existente, extendiendo a su vez, la WLAN actual de la Facultad.

Este trabajo surge debido a las deficiencias de la red LAN actual de la Facultad de Ciencias en cuanto su cobertura en el Edificio de Aulas, ya que cada aula dispone de un sólo punto de conexión a dicha red, y en los cuales no se dispone de ningún mecanismo de autoconfiguración en cuanto a la asignación de direcciones IP (por ejemplo, DHCP), además de la carencia cables de red (*patch cord*) para la conexión de los dispositivos de los usuarios a la red. Así mismo, la WLAN actual de la Facultad no le da cobertura al Edificio de Aulas donde se llevan a cabo las actividades académicas más importantes.

Para la elaboración del diseño se siguió un procedimiento conocido como *Site Survey (Estudio del Sitio)*, el cual facilita el proceso de diseño e implementación de una WLAN basada en el estándar IEEE 802.11, dicho procedimiento se describe en el presente documento.

Como producto de este trabajo especial de grado, se obtuvieron dos esquemas de diseño para la WLAN del Edificio de Aulas, y se realizó el respectivo análisis comparativo entre ambos en cuanto al hardware de red necesario para la implementación de cada uno, así como de la calidad de las señales RF y rendimiento de la red, con el fin de determinar a futuro la conveniencia del diseño a implementar.

Palabras Claves: Red de Área Local Inalámbrica, IEEE 802.11, Wi-Fi, WLAN, Site Survey (Estudio de Sitio), Antena, Radiofrecuencia (RF).

Agradecimientos

En primer lugar, mi agradecimiento a mi familia, especialmente a mi madre y hermano, por el apoyo brindado en distintas formas durante mis estudios universitarios.

A la Profesora María Elena Villapol, por su tutoría, disposición, diligencia, y apoyo en todo lo relacionado con el presente trabajo especial de grado, facilitando el camino para su desarrollo y culminación, y dejando ejemplo de lo que es una tutora.

A todo el grupo docente y demás miembros (preparadores, pasantes, tesistas, etc.) del Laboratorio de Redes Móviles e Inalámbricas (ICARO), al igual que a los miembros del Centro de Computación, por su colaboración, en distinta medida, durante el desarrollo del trabajo especial de grado.

Al personal de limpieza de la Facultad de Ciencias, por su colaboración en cuanto a facilitar la apertura de las aulas, y la vigilancia del material utilizado durante la ejecución de este trabajo.

A mis compañeros más cercanos, con quienes compartí conocimientos, experiencias, al igual que momentos de sano esparcimiento durante mi vida universitaria.

Finalmente, a la Universidad Central de Venezuela como institución por la disposición de sus distintos espacios, recursos, y servicios ofrecidos a sus estudiantes (incluyendo mi persona), apoyando así una formación integral, tanto en lo profesional como en lo humano.

Felix E. García E.

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE ANEXOS

1. INTRODUCCIÓN

En la actualidad, las redes de datos *LAN (Local Area Network, Red de Área Local)* juegan un rol importante y obligatorio de comunicación en cualquier organización. Tradicionalmente, las tecnologías que implementan este tipo de redes hacen uso de medios de transmisión guiados como cables, lo que puede hacer complicado y costoso su mantenimiento, modificación y ampliación, según el tamaño de la red y complejidad del cableado.

En los últimos años se han venido desarrollando tecnologías alternativas inalámbricas, que si bien, no intentan sustituir a las tecnologías cableadas, se presentan como un complemento de las mismas, en el sentido de brindar conectividad a la red en lugares donde el cableado es difícil, costoso, o no permitido para su implantación. Donde este último, es el caso de la UCV (Universidad Central de Venezuela).

Una red LAN que usa tecnología inalámbrica se conoce como *WLAN (Wireless LAN, LAN Inalámbrica)*.

En este sentido, el presente trabajo especial de grado tiene como objetivo elaborar y proponer el diseño de una solución inalámbrica para la conectividad del Edificio de Aulas de la Facultad de Ciencias de la UCV con su red de datos existente. Dicha solución representa a su vez, una extensión de la WLAN actual de la Facultad de Ciencias.

El diseño de la WLAN del Edificio de Aulas está basado en el estándar IEEE 802.11. La elaboración de dicho diseño siguió el procedimiento conocido como *Site Survey (Estudio del Sitio)*, descrito en la metodología del capítulo 3 de este documento, y que facilita el proceso de diseño e implementación de una WLAN basada en el estándar IEEE 802.11.

1.1. Planteamiento del problema

En la actualidad, la Facultad de Ciencias de la UCV cuenta con una red de datos LAN cableada, la cual se divide en subredes entre los distintos departamentos y escuelas. Esta LAN cableada se extiende hasta el edificio de aulas de dicha facultad, donde cada aula posee sólo un punto de conexión a dicha red, en los cuales no se dispone de ningún esquema de autoconfiguración (por ejemplo, DHCP), así como de cables de red (*patch cord*) para la conexión de los dispositivos de los usuarios con la red.

Adicionalmente, la Facultad de Ciencias dispone de una WLAN que sirve de extensión a la red cableada, la cual ofrece acceso inalámbrico a los usuarios móviles (profesores, empleados, estudiantes y demás miembros de la comunidad de la Facultad de Ciencias) en lugares donde no es posible acceder a la LAN cableada (por ejemplo, biblioteca Alonso Gamero, Auditorio Tobías Lasser, etc.) o donde los equipos de computación no satisfacen la demanda de cantidad de usuarios (por ejemplo, Sala de Micros). Esta WLAN cubre buena parte de la Facultad, pero omite un lugar crítico que es el

edificio de aulas, donde se llevan a cabo las actividades académicas más importantes.

1.2. Justificación

En un lugar como el edificio de aulas de la Facultad de Ciencias, es útil y necesario cualquier medio que soporte las actividades académicas y de docencia. Uno de los medios más importantes de información en las últimas décadas es la Internet, la cual juega un papel importante en el soporte didáctico para profesores y alumnos dentro de las aulas de clase. Así mismo, la facultad provee diversos recursos de información y herramientas en línea en los servidores pertenecientes a su intranet. Estos recursos y medios de información pueden ser accedidos mediante la interconexión del edificio de aulas a la red de datos de la Facultad de Ciencias.

El crecimiento en la utilización de dispositivos portátiles (como *Laptops* y PDAs) con facilidades de comunicación inalámbrica por parte de la comunidad de la Facultad de Ciencias, sumado a la escasa cantidad de puntos de conexión a la LAN cableada en cada aula, hace posible y necesaria la extensión de la red de datos de la Facultad de Ciencias hacia el edificio de aulas mediante el empleo de tecnologías inalámbricas, complementando así la WLAN que opera actualmente en la institución.

1.3. Objetivo general

Proponer una solución WLAN para la interconexión del edificio de aulas de la Facultad de Ciencias de la UCV con su red de datos actual, especificando: hardware a utilizar, sugerencias de instalación, y configuración.

1.4. Objetivos específicos

Los objetivos específicos del trabajo especial de grado incluyen:

- Determinar los requerimientos de los usuarios de la red (seguridad, rendimiento, movilidad, etc.) y su área de cobertura.

- Estudiar el sitio donde operará la WLAN, incluyendo el comportamiento de las ondas *RF (Radio Frequency, Radiofrecuencia)* e interferencias, además de la ubicación, configuración e instalación de los dispositivos de red.

- Analizar los resultados del estudio con el fin de recomendar una solución que incluya las mejores opciones de configuración e instalación de la WLAN.

1.5. Distribución del documento

A continuación se describe la distribución de los capítulos del presente documento, resumiendo muy brevemente su contenido.

1. INTRODUCCIÓN: Comprende el presente capítulo introductorio de este documento.

2. MARCO TEÓRICO - ESTÁNDAR IEEE 802.11: En este capítulo, se explica cada uno de los componentes de la arquitectura, servicios que ofrece a los dispositivos móviles. Se describe la arquitectura de protocolos, mecanismos de seguridad, y finalmente, una breve descripción de las funcionalidades que agrega cada una de las versiones que se han desarrollado a la especificación.

3. METODOLOGÍA - *SITE SURVEY*: Describe un procedimiento "paso a paso" para el levantamiento de información, análisis del *sitio* donde se implementará la WLAN, ejecución de diversas pruebas, y el registro de los resultados para su análisis.

4. DISEÑO DE LA WLAN: Este capítulo presenta el procedimiento realizado para el diseño de la WLAN para el Edificio de Aulas de la Facultad de Ciencias, siguiendo la metodología descrita en el capítulo 3. Finalmente, se describen los esquemas de diseño sobre los cuales se ejecutaron las pruebas.

5. ANÁLISIS DE LOS RESULDADOS DE LAS PRUEBAS: Este capítulo plantea en definitiva el diseño de la WLAN del Edificio de Aulas para cada esquema presentado, resultado de las pruebas ejecutadas, así mismo se analizan los resultados obtenidos durante la ejecución de las pruebas del *Site Survey*, con el fin de obtener una noción comparativa entre los diseños planteados.

6. CONCLUSIÓN: Esta capítulo describe una síntesis de la interpretación de los resultados obtenidos, al igual que la contribución, limitaciones, y recomendaciones. Además se dan una serie de ideas para trabajos futuros para la contribución en el ámbito del trabajo realizado.

2. MARCO TEÓRICO - ESTÁNDAR IEEE 802.11

En la industria de las WLANs se han desarrollado diversos estándares que buscan la interoperabilidad entre los dispositivos en el contexto de las WLANs, entre ellos, el que ha ganado mayor popularidad por su evolución, masiva distribución y bajo costo, es la especificación del *IEEE (Institute of Electrical and Electronics Engeneers, Instituto de Ingenieros Eléctricos y Electrónicos)* conocida como IEEE 802.11 del comité IEEE 802 [1].

El desarrollo de esta especificación se inicia dentro del grupo de trabajo IEEE 802.4, donde el interés inicial era desarrollar una WLAN en la banda ISM que utilizase un mecanismo similar al paso de testigo (*token-passing*) utilizado en las redes *token-bus* de la especificación 802.4 para el acceso al medio en la capa MAC. Posteriormente, se determinó que este mecanismo no era adecuado para un medio *RF (Radio Frequency, Radiofrecuencia)* por el uso ineficiente del espectro RF. Por lo tanto, el IEEE 802 decidió conformar un nuevo grupo de trabajo, el IEEE 802.11, dedicado exclusivamente a desarrollar capas MAC y PHY (capa física) en las WLANs [3].

2.1. Componentes de la arquitectura 802.11

El modelo desarrollado por el grupo 802.11 del IEEE, está conformado de una serie de componentes que interactúan entre sí para proporcionar a una WLAN de transparencia a las capas superiores en cuanto a la movilidad de los dispositivos cliente (estaciones). Estos componentes se describen a continuación [3] [4]:

- **Estación:** En el estándar IEEE 802.11, una estación es cualquier dispositivo que implementa las especificaciones de las capas MAC y PHY 802.11 [3].

- **AP (Access Point, Punto de Acceso):** Es una entidad conformada por una estación que ejecuta cierta lógica que provee de acceso al DS (se explica a continuación) a las demás estaciones. También se le conoce como estación base de una celda en una WLAN.

- **DS (Distribution System, Sistema de Distribución):** Se utiliza para interconectar varios BSSs (se explica a continuación) y otras LANs integradas a la WLAN. El DS puede ser implementado con cualquier tecnología, como una LAN cableada, una WLAN, etc.

- **BSS (Basic Service Set, Conjunto de Servicios Básicos):** Es el bloque de construcción básico de una WLAN IEEE 802.11. Consiste en un grupo de estaciones (dos o más) ejecutando el mismo protocolo MAC y compitiendo por el acceso al medio compartido dentro de un área específica conocida como *BSA (Basic Service Area, Área de Servicios Básicos)*, conformando así lo que también se conoce como una celda. Esta celda o BSS puede estar aislada para conformar un *IBSS (Independent BSS, BSS Independiente)* implementando una red

ad hoc (Ver Figura 2.1), o puede estar conectada a un DS backbone a través de un AP, configurando así una red de infraestructura (Ver Figura 2.2) 0.

- **ESS (Extended Service Set, Conjunto de Servicios Extendido):** Consiste en la interconexión de dos o más BSSs por medio de un DS. Donde el DS no forma parte del ESS, solo los BSSs interconectados, como se muestra en la Figura 2.3.

- **Portal:** Se utiliza para integrar redes de cualquier otra tecnología, como una LAN cableada, a la WLAN, interconectándose mediante el DS. La lógica de un portal se implementa en algún dispositivo como un puente o router [3].

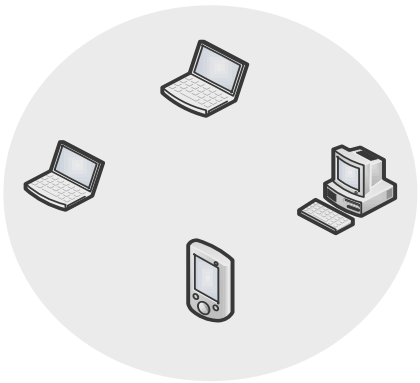


Figura 2.1: IBSS conformando una red ad hoc

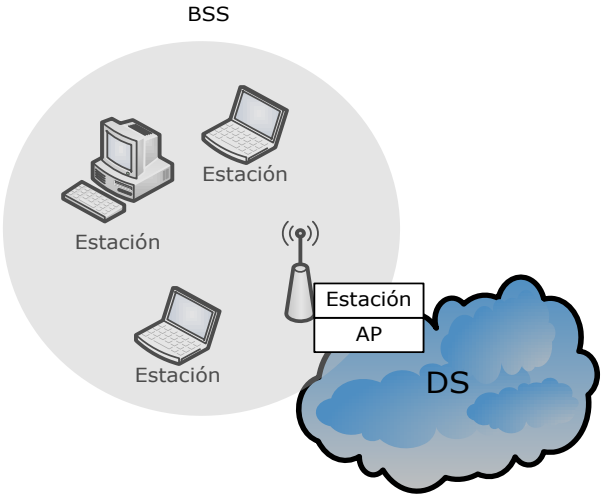


Figura 2.2: BSS conformando una red de infraestructura.

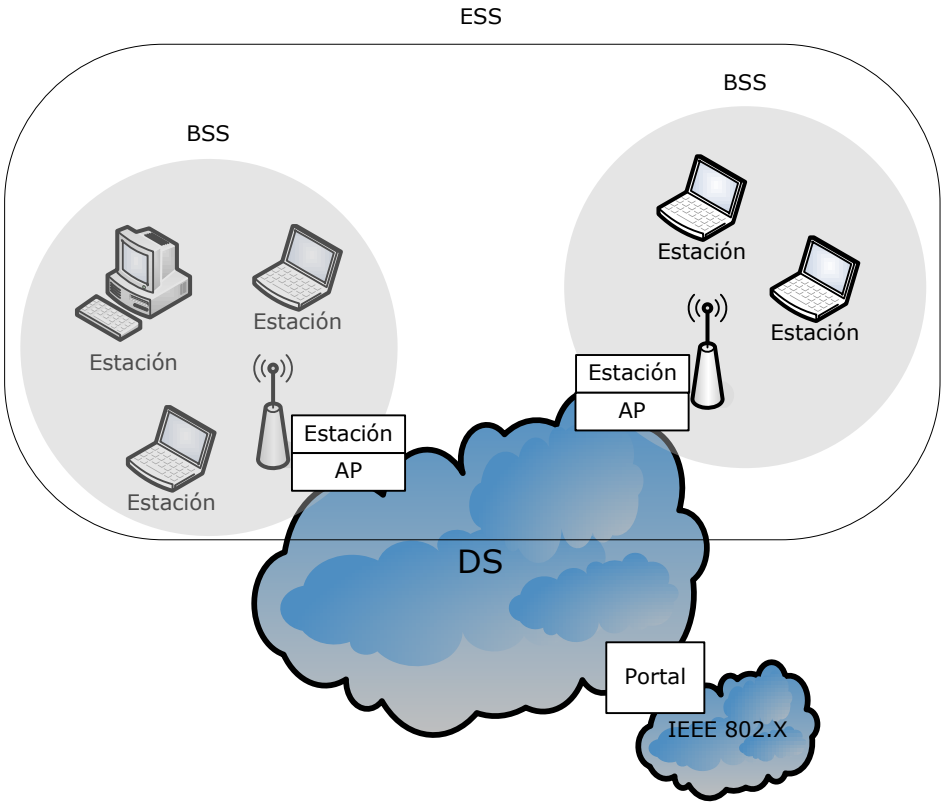


Figura 2.3: Arquitectura de una red IEEE 802.11

2.2. Servicios

El DS puede implementarse con cualquier tecnología de red. Por lo tanto, estándar IEEE 802.11 no especifica detalles de la implementación del mismo, en su lugar, especifica un conjunto de servicios [4]. Los servicios están relacionados con los diferentes componentes de la arquitectura. Este conjunto de servicios se divide básicamente en dos categorías (Ver Tabla 2.1):

- **SS (Station Services, Servicios de Estación):** Son provistos por todas las estaciones IEEE 802.11 (incluyendo APs).

- **DSS (Distribution System Services Servicios del Sistema de Distribución):** Son provistos por el DS, esto es, entre BSSs. Específicamente, se implementan en los APs o algún otro dispositivo de propósito específico conectado al DS.

Servicio	Tipo	Uso	Especificación que lo incorpora
Entrega de MSDU	SS	Transporte de MSDU	802.11 original
Distribución	DSS	Transporte de MSDU	802.11 original
Integración	DSS	Transporte de MSDU	802.11 original
Asociación	DSS	Transporte de MSDU	802.11 original
Re-asociación	DSS	Transporte de MSDU	802.11 original
Disociación	DSS	Transporte de MSDU	802.11 original
Autenticación	SS	Acceso y seguridad	802.11 original
Des-autenticación	SS	Acceso y seguridad	802.11 original
Privacidad	SS	Acceso y seguridad	802.11 original
DFS	SS	Manejo del espectro	802.11h
TPC	SS	Manejo del espectro	802.11h
Sincronización de temporizador en capas superiores	SS/DSS	Calidad de Servicio	802.11e
Programación de tráfico QoS	SS/DSS	Calidad de Servicio	802.11e

Tabla 2.1: Clasificación básica de los servicios IEEE 802.11.

2.2.1. Entrega de MSDU

Es el servicio más básico. Se encarga de tomar un bloque de datos pasado desde las capas superiores, pasando por la capa más *inmediata LLC (Logical Link Control, Control Lógico del Enlace,)* a la capa MAC 802.11 para conformar un *MSDU (MAC Service Data Unit, Unidad de Datos del Servicio MAC)*, en el cual es encapsulado en un PDU MAC 802.11 (o trama) que es entregado a la capa física para su transmisión sobre el medio inalámbrico. Si el MSDU es muy largo, este puede ser fragmentado por este servicio y transmitido en múltiples tramas MAC 802.11.

2.2.2. Distribución

Es el principal servicio utilizado por las estaciones para intercambiar tramas MAC dentro de un ESS, esto es, atravesando el DS.

Dentro de un ESS, cuando una estación en un BSS envía un mensaje de datos a una estación en otro BSS, la estación emisora envía su trama MAC

a través del medio inalámbrico, siendo recibida por el AP de su BSS (AP de entrada), el cual se encarga de entregar el mensaje al DS para su distribución. El servicio de distribución del DS se hace responsable por hacer llegar el mensaje al destino apropiado dentro del DS, es decir, al AP del BSS donde se encuentra la estación destino (AP de salida), el cual, una vez recibe el mensaje, lo entrega la estación destino como una trama MAC 802.11 a través del medio inalámbrico.

La manera en que el DS distribuye el mensaje es ajena al estándar IEEE 802.11, y depende de la implementación del DS. La obligación del estándar para la distribución, se reduce a proveer la información necesaria al DS para que éste pueda determinar el punto de salida correspondiente al destino (BSS destino) del mensaje. Para esto, se utilizan los servicios de asociación, re-asociación y disociación (se explica más adelante).

En caso de que la estación destino se encuentre dentro del mismo BSS que la estación origen del mensaje, el AP de entrada y de salida es el mismo, de modo que el servicio de distribución no hace uso del DS.

2.2.3. Integración

Si al momento de invocar el servicio de distribución, este determina que el receptor del mensaje es miembro de una LAN integrada, entonces el punto de salida es un portal.

El servicio de integración invocado por el DS es responsable por llevar a cabo las operaciones necesarias (por ejemplo, traducción de direcciones) para llevar el mensaje del medio de transmisión del DS al medio de transmisión de la LAN integrada. Cuando el DS recibe un mensaje de la LAN integrada para una estación IEEE 802.11 a través de un portal, este debe invocar al servicio de integración antes de distribuir el mensaje.

Los detalles del servicio de integración dependerán de la implementación específica del DS.

2.2.4. Asociación

Antes que una estación móvil tenga permitido enviar datos a través de un AP, debería asociarse primero a este. Esta acción de asociarse implica invocar el servicio de asociación, el cual provee un mapeo estación-AP (o estación-BSS) al DS. El DS utiliza esta información para poder llevar a cabo el servicio de distribución.

El servicio de asociación soporta la movilidad de dentro de un mismo BSS (movilidad de *no-transición*), y es necesario pero no suficiente para soportar la movilidad entre dos o más BSSs dentro de un ESS (movilidad de *transición-BSS*).

Una estación puede estar asociada a un solo AP (BSS) a la vez, lo que asegura al DS una sola respuesta en cuanto a que AP se encuentra

determinada estación. Por otro lado, un AP puede estar asociado a varias estaciones móviles a la vez.

2.2.5. Re-asociación

Se necesita funcionalidad adicional a la asociación para soportar movilidad de transición entre BSSs, la cual es provista por el servicio de re-asociación. Este servicio es invocado para "mover" una asociación de un AP a otro, manteniendo al DS informado del mapeo actual entre una estación y el AP en lo que la estación se mueve de un BSS a otro dentro del mismo ESS. La re-asociación siempre es iniciada por la estación móvil, pero es un servicio del DS (DSS).

2.2.6. Disociación

Se utiliza para terminar una asociación existente entre una estación móvil y un AP. El servicio le dice al DS que invalide toda información existente sobre la asociación terminada, ya que la disociación es una notificación, no una solicitud-respuesta, de modo que no puede ser rechazada por ninguna de las partes. Además, los intentos de enviar mensajes a través del DS a una estación disociada no tendrán éxito.

Una estación móvil debería intentar disociarse cuando deja la red, aunque el protocolo MAC no depende de que la estación invoque el servicio de disociación, ya que está diseñado para ajustarse a la pérdida de comunicación con las estaciones asociadas.

2.2.7. Autenticación

Este servicio provee de un control de acceso al medio de la WLAN análogo al acceso físico de las estaciones al medio guiado de una LAN cableada. El servicio de autenticación opera a nivel del enlace entre las estaciones IEEE 802.11, no provee autenticación *end-to-end* de alto nivel (usuario-a-usuario) entre origen y destino del mensaje.

La autenticación establece la identidad entre todas las estaciones que se comunican entre sí, tanto en un ESS como en un IBSS. Si no se ha establecido un nivel mutuamente aceptable de autenticación entre dos estaciones, no se podrá establecer una asociación entre las partes.

Los mecanismos de autenticación provistos por el estándar IEEE 802.11, se describen en la sección 2.3.1.3.

2.2.8. Des-autenticación

La des-autenticación es invocada para finalizar con una autenticación existente entre dos estaciones. Dado que la autenticación es un requisito para la asociación, la invocación al servicio de des-autenticación deberá

conllevar a la disociación de la estación que invoca. La des-autenticación, al igual que la disociación, es una notificación que no puede ser rechazada, y que puede ser invocada por cualquiera de las partes autenticadas.

2.2.9. Confidencialidad de datos (Privacidad)

Este servicio provee a la WLAN IEEE 802.11 de la privacidad análoga implícita en el medio guiado de una LAN cableada, ya que a diferencia de los cables, el medio no guiado de las WLANs IEEE 802.11 puede ser escuchado por cualquier dispositivo con las características de las capas física y MAC del estándar.

El estándar provee diversos algoritmos de encriptación para proteger el tráfico, los cuales se describen en la sección 2.3.1.3. Las estaciones proveerán algún medio para configurar el algoritmo a utilizar en determinada asociación.

El estado de confidencialidad de datos por defecto es "ninguno". Si el servicio de confidencialidad de datos no es invocado, entonces todos los mensajes se envían sin protección. Si la política no es aceptada por el emisor, entonces este no enviará tramas de datos. Si en el extremo del receptor, la política no es aceptada, éste descartará todas las tramas de datos que le lleguen. Por otro lado, las tramas rechazadas que no cumplen con la clave de autenticación, no son notificadas a la subcapa LLC o al DS (si aplica), en su lugar, son confirmadas con el fin de no desperdiciar ancho de banda del medio con retransmisiones.

2.2.10. DFS (Dynamic Frequency Selection, Selección Dinámica de Frecuencias)

Introducido por la especificación 802.11h, define un mecanismo para evitar la interferencia de las señales de radar con los canales en las WLANs que operan en la banda de los 5 GHz ISM, satisfaciendo las regulaciones para ciertas regiones. Además, asegura la utilización uniforme de los canales disponibles mediante una planificación automática de la utilización de las frecuencias.

Este servicio permite:

- Asociación de las estaciones con el AP de un BSS en base a los canales soportados por dichas estaciones.
- Verificación de la presencia de señales de radar en un canal antes de ser usado o durante la operación en el mismo.
- Finalización de la operación actual en un canal determinado al momento de detectar la presencia de radar para evitar interferencias.
- Detección de señales de radar en un canal en utilización, así como en los demás canales en base a requerimientos regulatorios.

- Reporte de mediciones realizadas en todos los canales.

- Selección y notificación de un nuevo canal con el fin de asistir la migración de un BSS o IBSS, luego de la detección de señales de radar.

2.2.11. TPC (Transmit Power Control, Control de Potencia de Transmisión)

Introducido por la especificación 802.11h, define un mecanismo para satisfacer las regulaciones locales en cuanto a la máxima potencia de transmisión para cada canal en las WLANs que utilizan la banda de los 5 GHz ISM, con el fin de reducir las interferencias con algunos servicios satelitales.

Este servicio permite:

- Asociación de las estaciones con el AP de un BSS en base a la potencia de transmisión de dichas estaciones.

- Especificación del máximo nivel de potencia de transmisión para cada canal según las regulaciones locales.

- Selección del nivel de potencia para cada transmisión dentro de las restricciones regulatorias en el respectivo canal.

- Adaptación de la potencia de transmisión en base a información del enlace (incluyendo, pérdida en el espacio libre, etc.).

2.2.12. Sincronización de temporizador en capas superiores

Introducido por la especificación 802.11e, este servicio provee un mecanismo para la sincronización de temporizadores entre las capas superiores en algunas aplicaciones donde se aplica calidad de servicio (tales como, transmisión de video y voz sobre IP).

2.2.13. Programación de tráfico QoS (Quality of Service, Calidad de Servicio)

Introducido por la especificación 802.11e, este servicio permite una transferencia de tramas con calidad de servicio a nivel del enlace dentro de un mismo BSS. Donde una entidad de programación de tráfico en la estación selecciona una trama de un conjunto de colas de tráfico para su transmisión, basándose en ciertos parámetros de especificación de tráfico, o en niveles de prioridad para cada trama.

2.3. Arquitectura de protocolos 802.11

Las pilas de protocolos de los estándares del comité IEEE 802 tienen muchas similitudes entre sí (Ver Figura 2.4). De modo que la capa física corresponde correctamente a su par en el modelo OSI, pero la capa de enlace de datos en todas las especificaciones IEEE 802 se divide en dos o más subcapas. En el estándar IEEE 802.11 la subcapa MAC controla el acceso al medio compartido, determinando a que estación le toca hacer uso del medio en determinado momento. Sobre la capa MAC se encuentra la subcapa LLC, que se encarga de ocultar las diferencias entre las variantes IEEE 802 a las capas superiores.

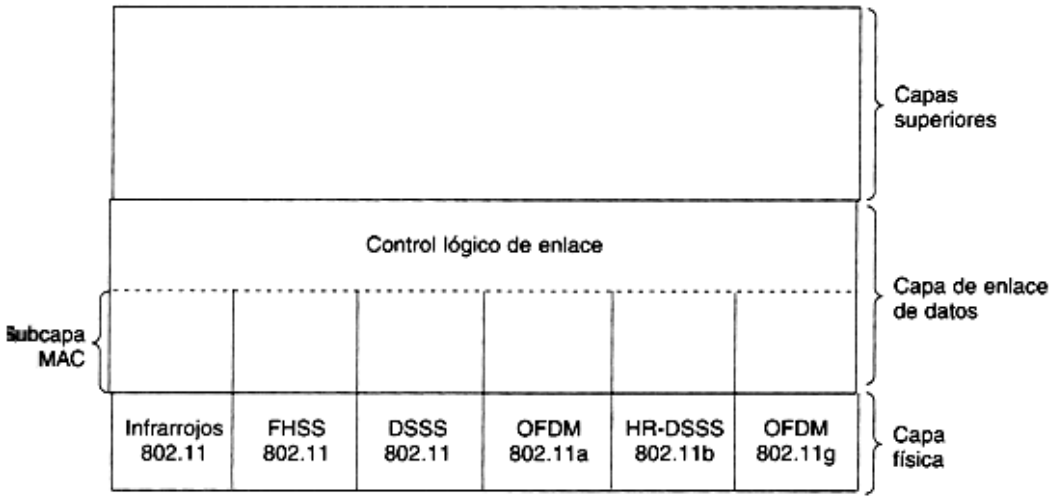


Figura 2.4: Vista parcial de la arquitectura de protocolos IEEE 802.11 [1]

2.3.1. Especificación de la subcapa MAC

La subcapa MAC del estándar IEEE 802.11 se encarga de la entrega de datos confiable a nivel del enlace físico, así como del control del acceso al medio inalámbrico compartido. Adicionalmente, proporciona características de seguridad análogas a las que presta el medio guiado en una LAN cableada en cuanto al acceso físico al medio y privacidad.

2.3.1.1. Descripción funcional de la subcapa MAC

La subcapa MAC 802.11 define un protocolo basado en un algoritmo *stop-and-wait (parada y espera)* junto con un mecanismo de detección de errores para la *entrega de datos confiable*, que consiste en el intercambio de tramas de datos (por parte del emisor) y tramas de confirmación (por parte del receptor) para notificar la recepción exitosa de los datos, de modo que cuando una trama no es recibida en un tiempo determinado o esta se recibe con errores, no es confirmada y se procede a la retransmisión de la misma por parte del emisor luego de un tiempo determinado [1] [3].

Por otra parte, el estándar define un algoritmo para el *control de acceso al medio* conocido como *DFWMAC (Distributed Foundation Wireless*

MAC) que integra dos mecanismos para el control de acceso: Un mecanismo base distribuido conocido como *DCF (Distributed Coordination Function, Función de Coordinación Distribuida)* que distribuye la decisión de acceso al medio entre todos los nodos. Y un mecanismo centralizado opcional conocido como *PCF (Point Coordination Function, Función de Coordinación Puntual)* donde existe un ente central que determina el nodo que hace uso del medio en determinado momento. Desde el punto de vista de diseño de la arquitectura de protocolos IEEE 802.11, la subcapa MAC queda dividida en dos subcapas, la subcapa DCF, y la subcapa PCF, de manera que el modelo mostrado en la Figura 2.4 queda refinado como se muestra en la Figura 2.5.

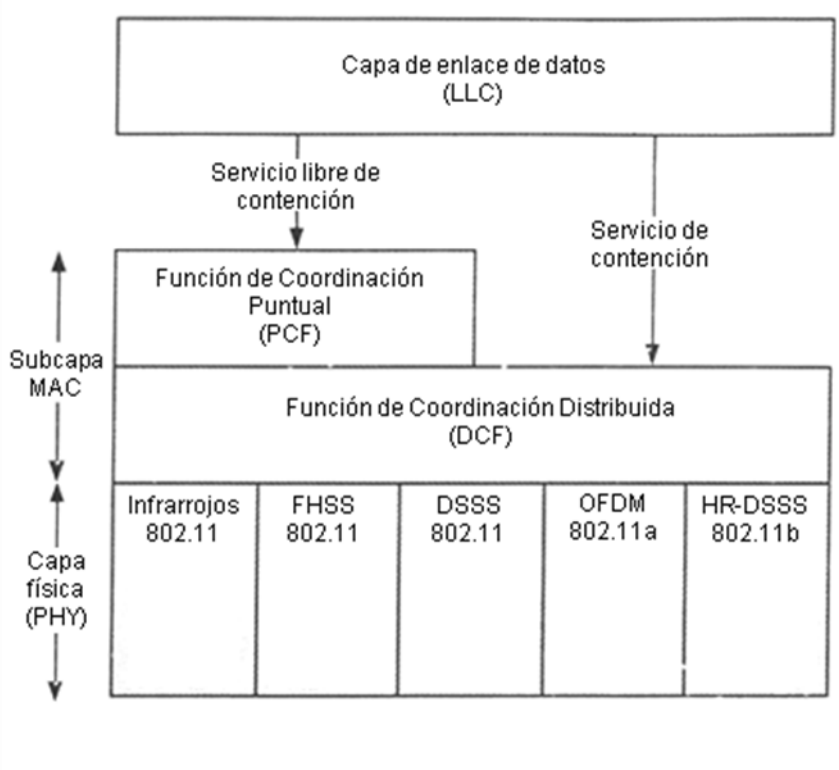


Figura 2.5: Vista detallada de la arquitectura de protocolos IEEE 802.11.

- **DCF**

  Esta subcapa provee un servicio de contención, donde las estaciones compiten de manera distribuida por el acceso al medio, operando tanto en redes ad hoc (IBSS) como en redes de infraestructura (BSS). Utiliza un protocolo *CSMA/CA (Carrier Sense Medium Access/Collision Avoidance, Acceso al Medio por Detección del Canal con Evasión de Colisiones)*, el cual establece dos modos de detección del canal: detección física y detección virtual.

  La detección física del canal es realizada por la capa física, y consiste en escuchar las perturbaciones electromagnéticas en el medio inalámbrico para detectar la portadora de la señal en un rango de frecuencias determinado.

  La detección virtual del canal, que se muestra en la Figura 2.6, se realiza mediante una variante de CSMA/CA para redes inalámbricas

conocida como *MACAW (Multiple Access Collitions Avoidance Wireless, Acceso Multiple con Evasión de Colisiones Inalámbrico)*, la cual evita el "problema de la estación oculta" y el "problema de la estación expuesta" en las WLANs. Este mecanismo consiste básicamente en un intercambio de tramas de control previo a la trasmisión de datos entre un emisor (que ha ganado el acceso al medio) y un receptor dentro de un BSS. El emisor envía una trama RTS (Request-To-Send, Solicitud de Envió) a la dirección MAC del receptor, el cual, responde mediante una trama CTS (Clear-To-Send, Despejado para Enviar), notificando al emisor que puede enviar las tramas de datos. Las tramas RTS son recibidas por las estaciones dentro del área de cobertura del emisor, y las tramas CTS son recibidas por las estaciones dentro del área de cobertura del receptor, proporcionando a dichas estaciones (mediante el campo de duración de la trama MAC 802.11) cierta información para la estimación del tiempo en que permanecerá ocupado el medio para la transmisión de la subsecuente trama de datos. De este modo cada estación establece para sí un canal virtual representado por un intervalo de tiempo conocido como *NAV (Network Allocation Vector, Vector de Asignación de Red)*, en que las estaciones se abstendrán de realizar cualquier actividad en la WLAN, incluyendo la detección física del canal.

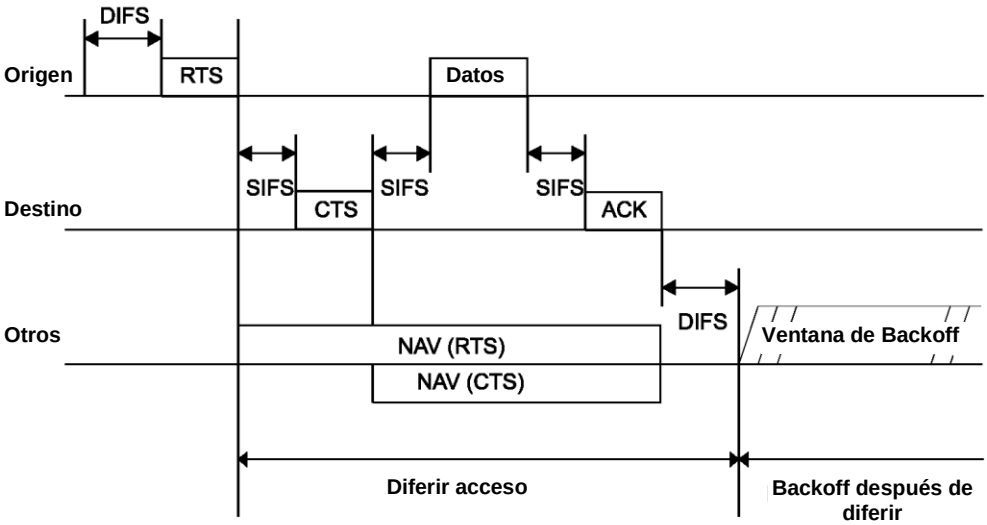


Figura 2.6: Detección virtual del canal mediante MACAW.

- **PCF**

Esta subcapa esta implementada sobre la subcapa DCF, de modo que explota algunas características de esta última. Implementa un mecanismo opcional que provee un servicio libre de contención (contention-free) mediante un control de acceso al medio centralizado, y que opera solo en redes de infraestructura (dentro de un BSS).

El mecanismo consiste en un esquema de sondeo (*polling*) por parte de un *PC (Point Coordinator, Coordinador de Punto)* implementado en el AP de un BSS, y que opera de manera opcional. Durante el servicio libre de contención, el PC sondea a las estaciones asociadas a él mediante la transmisión periódica de tramas *beacon* con una política

de round-robin. Si una estación (configurada para tráfico libre de contención) sondeada tiene algo que transmitir, esta obtiene el acceso al medio inalámbrico para la transmisión de sus tramas de datos. Todas las estaciones que reciben una trama *beacon*, asociadas o no al BSS, pero dentro de su área de cobertura, establecen un NAV (una de las características "heredada" de la subcapa DCF) acorde a información de duración del período libre de contención indicada en la trama de *beacon*, con el fin de que estas cedan el control al PC por ese período de tiempo antes de poder competir nuevamente por el medio mediante DCF.

- **Uso de IFS**

  Para que dos mecanismos como DCF y PCF puedan ser interoperables entre sí, el estándar define un conjunto de intervalos de tiempo conocidos como *IFS (Inter-Frame Space, Espacio Inter-Trama)*. Básicamente, durante un IFS las estaciones escuchan el medio mediante la detección física del canal antes de transmitir una trama, en caso de que el canal se encuentre desocupado se realiza la transmisión de la(s) trama(s), en caso contrario, se espera a que se desocupe para volver a escuchar el medio durante otro IFS antes de transmitir.

Adicionalmente a los mecanismos para la entrega de datos confiable y control de acceso al medio expuestos, el estándar ofrece diversos mecanismos de *seguridad* para proveer a las WLANs de las características de privacidad que ofrece el medio guiado en las LANs cableadas. Para esto, dichos mecanismos de seguridad en las WLANs 802.11 comprenden dos aspectos básicos:

- **Confidencialidad de datos:** Mediante la encriptación de los datos, se busca alcanzar una privacidad análoga a la que ofrece el medio guiado y cerrado de una LAN cableada, donde a diferencia del medio inalámbrico en las WLANs, no es posible escuchar o alterar la transmisión de los datos a través de los cables.

- **Autenticación:** En las LANs cableadas, el simple acceso físico mediante cables es requerido para poder transmitir y recibir tramas de datos en el enlace físico. En el medio inalámbrico de las WLANs no existe un acceso físico directo entre los dispositivos, de modo que se utilizan los mecanismos de autenticación para permitir o no la transmisión de tramas en el enlace inalámbrico.

Se han desarrollado diversos mecanismos para soportar la autenticación y la confidencialidad de datos, algunos simples y otros más complejos, los cuales se detallan en la sección 2.3.1.3.

2.3.1.2. La trama MAC 802.11

A continuación, en la Figura 2.7, se muestra el formato general de la trama MAC 802.11, el cual es el mismo para todos los tipos de tramas, y para todas las especificaciones del estándar IEEE 802.11.

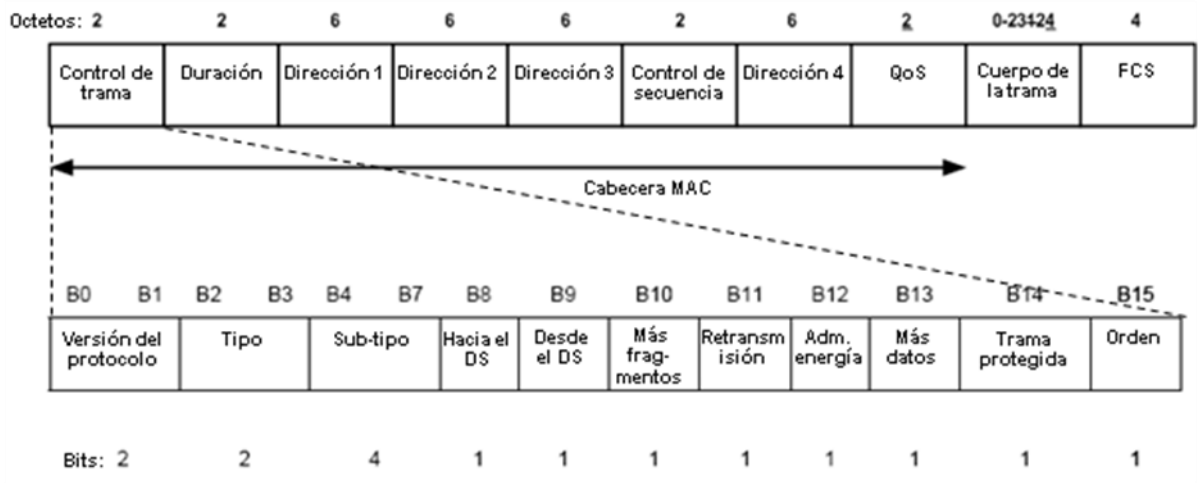


Figura 2.7: Formato general de la trama MAC IEEE 802.11.

Los campos de la trama MAC son los siguientes [3]:

- **Control de trama**: Indica el tipo y subtipo de trama, e incluye información de control. Los sub-campos de esta trama son:
    - **Versión del protocolo:** Versión del protocolo, actualmente la versión es 0.
    - **Tipo:** Indica el tipo de trama (control, gestión, o datos) (Ver Tabla 2.2).
    - **Sub-tipo:** Identifica la función de la trama (Ver Tabla 2.2).
    - **Hacia el DS:** Cuando su valor es 1, indica que la trama va destinada al DS.
    - **Desde el DS:** Cuando su valor es 1, indica que la trama sale del DS.
    - **Más fragmentos:** Cuando su valor es 1, indica que siguen más fragmentos a este.
    - **Retransmisión:** Cuando su valor es 1, indica que la trama es la retransmisión de una anterior.
    - **Administración de energía:** Cuando su valor es 1, indica que la estación transmisora se encuentra en modo de ahorro de energía.

- **Más datos:** Indica que la estación tiene más datos que transmitir a nivel de la capa LLC, de modo, que los mismos pueden ser fragmentados en varios bloques, donde cada bloque puede ser transmitido en varias tramas.

- **Trama protegida:** Indica si la trama ha sido procesada por algún algoritmo de encriptación (valor 1) (como WEP) para el intercambio de datos seguro.

- **Orden:** Cuando su valor es 1, indica que la estación receptora debe procesar las tramas e estricto orden.

- **Duración:** Indica el tiempo en que el canal permanecerá ocupado para la transmisión exitosa (incluido el ACK) de la trama. En algunas tramas de control, este campo contiene un identificador de asociación o conexión.

- **Dirección (1, 2, 3, 4):** Existen cuatro campos de dirección, que corresponden a (no necesariamente en el siguiente orden): *Dirección Destino*, que identifica a la estación destinataria final del MSDU transportado en el campo Cuerpo de la Trama. *Dirección Fuente*, que identifica a la estación fuente que inicio la transmisión del MSDU transportado en el campo Cuerpo de la Trama. *Dirección del Receptor*, que identifica al receptor (no el destinatario) inmediato del MPDU en el medio inalámbrico. *Dirección del Transmisor*, que identifica al transmisor (no la fuente) del MPDU en el medio inalámbrico. Las dos últimas direcciones se utilizan para poder direccionar las tramas dentro de un DS para el tráfico entre dos BSSs [1] [4].

- **Control de secuencia:** Los primeros 4 bits corresponden a un sub-campo de *Número de fragmento* para el re-ensamblaje de los fragmentos de trama recibidos. Los restantes 12 bits corresponden al sub-campo de *Número de secuencia* (Ver Figura 2.8) para numerar y ordenar las tramas enviadas y recibidas.

Figura 2.8: Campo de Control de Secuencia de la trama MAC 802.11.

- **QoS (Quality-of-Service, Calidad de Servicio):** Identifica la *categoría de tráfico* o *flujo de tráfico* al que pertenece la trama entre otros parámetros de calidad de servicio, con el fin de que una entidad MAC configurada para prestar calidad de servicio determine el *nivel de prioridad* o la *especificación del tráfico* con que debe ser tratada dicha trama para su transmisión en el medio inalámbrico dentro de un BSS.

- **Cuerpo de la trama:** Campo de longitud variable. Puede contener un MSDU o fragmento de un MSDU proveniente de la subcapa LLC, así

como información de control de la subcapa MAC, según el tipo de trama.

- **FCS (Frame Check Sequence, Secuencia de Verificación de Trama):** Contiene un Código de Redundancia Cíclica (CRC) de 32 bits, calculado sobre todos los campos de la trama MAC (incluido el cuerpo de la trama).

La trama MAC 802.11 puede ser de tres tipos (subcampo Tipo del campo Control de trama): Tramas de Control, Tramas de Gestión, y Tramas de Datos. En la Tabla 2.2 se muestran las combinaciones validas más importantes de tipo y sub-tipo te tramas) [3] [4].

Valor del campo Tipo	Descripción del tipo	Valor del campo Sub-tipo	Descripción del subtipo
00	Gestión	0000	Solicitud de asociación
00	Gestión	0001	Respuesta de asociación
00	Gestión	0010	Solicitud de re-asociación
00	Gestión	0011	Respuesta de re-asociación
00	Gestión	0100	Solicitud de probe
00	Gestión	0101	Respuesta de probe
00	Gestión	0110 - 0111	Reservado
00	Gestión	1000	Beacon
00	Gestión	1001	ATIM
00	Gestión	1010	Disociación
00	Gestión	1011	Autenticación
00	Gestión	1100	Des-autenticación
00	Gestión	1110 - 1111	Reservado
01	Control	0000 - 0111	Reservado
01	Control	1010	Power Save-poll
01	Control	1011	RTS (Request to Send)
01	Control	1100	CTS (Clear to Send)
01	Control	1101	Confirmación (ACK)
01	Control	1110	CF-end
01	Control	1111	CF-end + CF-ACK
10	Datos	0000	Datos
10	Datos	0001	Datos + CF-ACK
10	Datos	0010	Datos + CF-Poll
10	Datos	0011	Datos + CF-ACK + CF-Poll
10	Datos	0100	Función Nula
10	Datos	0101	CF-ACK (sin datos)
10	Datos	0110	CF-poll (sin datos)
10	Datos	0111	CF-ACK + CF-poll (sin datos)
10	Datos	1000	QoS Datos
10	Datos	1001	QoS Datos + CF-ACK
10	Datos	1010	QoS Datos + CF-Poll
10	Datos	1011	QoS Datos + CF-ACK + CF-Poll
10	Datos	1100	QoS Función Nula
10	Datos	1101	Reservado
10	Datos	1110	QoS CF-poll (sin datos)
10	Datos	1111	QoS CF-ACK + CF-poll (sin datos)
11	Reservado	0000 - 1111	Reservado

Tabla 2.2: Combinaciones validas de tipo y sub-tipo de tramas 802.11.

2.3.1.3. Mecanismos de seguridad para las WLAN 802.11

La especificación original del estándar IEEE 802.11 define un mecanismo básico para la confidencialidad de datos y dos para autenticación, los cuales se describen a continuación:

- **WEP (Wired Equivalent Privacy, Privacidad Equivalente al Cableado)**

  Es el mecanismo de seguridad más básico de encriptación de datos que provee el estándar. Se utiliza para la confidencialidad de datos, así como para apoyar algunos mecanismos de autenticación. Se apoya en el algoritmo de encriptación RC4, el cual es sencillo de implementar y rápido en su ejecución [2].

  WEP se basa en el uso de claves secretas compartidas en formato alfanumérico o hexadecimal (de 40 ó 104 bits) para generar, mediante el uso de RC4 y un *PRNG (Pseudo-Random Number Generator, Generador de Números Pseudo-Aleatorios)*, cadenas o claves pseudo-aleatorias tanto en el emisor como en el receptor. La Figura 2.9 muestra el proceso para la encriptación del tráfico, que se realiza de la siguiente manera:

  i. El cuerpo de la trama, o carga útil (payload), en "texto plano" se envía a un algoritmo de chequeo de integridad (el que calcula el valor CRC-32 para el campo FCS de la trama MAC 802.11), generando un *ICV (Integrity Check Value, Valor de Chequeo de Integridad)*.

  ii. El valor ICV es concatenado al texto plano de la carga útil.

  iii. Un *Vector de Inicialización (IV, Initialization Vector)* de 24 bits es generado y concatenado al inicio de la clave secreta compartida.

  iv. El IV junto con la clave secreta son pasados al algoritmo RC4 para crear un valor semilla para el PRNG.

  v. El PRNG genera un flujo o cadena cifrada (*cipher-stream*).

  vi. Mediante una simple operación XOR entre el flujo cifrado del paso v, y el conjunto ICV + texto plano del paso ii, se obtiene el texto cifrado (*ciphertext*) que representa la data encriptada a proteger.

  vii. Finalmente, el texto cifrado mediante WEP es concatenado al conjunto IV + clave secreta obtenidos en el paso iii para su transmisión en el enlace inalámbrico.

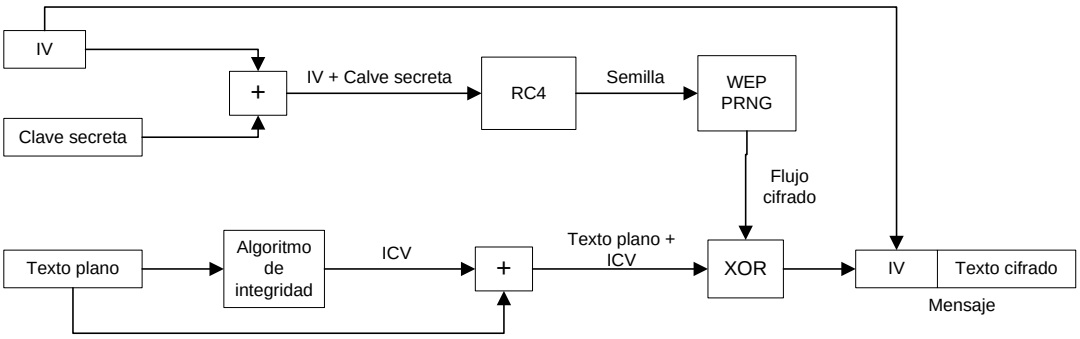


Figura 2.9: Proceso de encriptación con WEP.

La simplicidad de WEP, lo hace débil y poco confiable, ya que el algoritmo RC4 ha sido implementado de manera inapropiada en WEP.

Parte de su debilidad, se encuentra en la utilización de un IV de 24 bits, tanto para las claves de 64 bits (clave secreta de 40 bits + 24 bits del IV) como para las claves de 128 bits (clave secreta de 104 bits + 24 bits del IV). Ya que en la mayoría de las implementaciones se inicializa este valor en 0, siendo posteriormente incrementado en 1 para cada paquete transmitido, agotando rápidamente los 2^{24} posibles IVs (se estima aproximadamente 5 horas para redes con mucho tráfico). Esto, junto al hecho de que el IV es transmitido sin encriptar, crea una puerta abierta para los hackers con cierto conocimiento sobre WEP y RC4, y con las herramientas de hardware y software apropiadas para perpetrar ciertos ataques a la red, que van desde obtener la clave secreta, a desencriptar el texto cifrado obteniendo el texto plano de la carga útil de las tramas que viajan en el enlace inalámbrico.

Existen dos maneras de asignar las claves secretas compartidas:

- **Claves estáticas:** Las claves estáticas son introducidas manualmente en los APs y estaciones asociadas, y no cambian durante la operación de la red, lo que las hace más susceptibles a ser descubiertas por hackers con los conocimientos y herramientas suficientes para tal fin. Por esta razón, las claves estáticas podrían ser utilizadas como un mecanismo de seguridad básico en redes pequeñas, pero no se recomienda su uso en redes empresariales más grandes.

- **Servidores de claves centralizados:** Los servidores de claves buscan cubrir los siguientes aspectos: Generación centralizada de claves, distribución de claves centralizada, rotación de claves, reducción de la carga de la red en cuanto a todo el manejo de claves. Donde, a diferencia de la asignación de claves estáticas, es un proceso automatizado entre estaciones, APs, y servidor de claves el que se encarga de la tarea de mantener las claves dinámicas. La generación y rotación de claves puede ser por paquete o por sesión, dependiendo de la implementación del servidor, el cual puede ser un servidor *RADIUS (Remote Authentication Dial-In User Service, Servicio al Usuario de*

Marcado de Autenticación Remota) o algún servidor de aplicaciones alojando alguna aplicación específica para tal fin.

- **OSA (Open System Authentication, Autenticación de Sistema Abierto)**

  Es el mecanismo de autenticación más básico que provee el estándar original IEEE 802.11. Este tipo de autenticación no provee beneficio de seguridad alguno, simplemente se limita a el intercambio de tramas de autenticación entre las partes, indicando el tipo de autenticación, así como la identidad de cada estación, donde la estación que inicia la autenticación siempre es aceptada en el IBSS o en el BSS obteniendo acceso al DS [3].

- **SKA (Shared Key Authentication, Autenticación de Clave Compartida)**

  Es el otro tipo de autenticación que provee el estándar. Un poco más avanzado que OSA, requiere de una clave secreta compartida entre las partes a autenticarse. El proceso de autenticación se realiza de la siguiente manera 0:

  i. El transmisor que desea autenticarse con el "autenticador" (un AP o IBSS) envía una trama de autenticación indicando que usará el tipo de autenticación SKA junto con la identificación de estación.

  ii. El autenticador responde con una trama de autenticación que incluye un texto de desafío de 128 bytes, el cual se genera utilizando el PRNG de WEP.

  iii. El transmisor responde con una segunda trama de autenticación que incluye el texto de desafío recibido. Dicha trama es encriptada mediante WEP.

  iv. El transmisor recibe la trama y la desencripta junto con la clave compartida mediante WEP. Si el proceso es exitoso, se compara el texto de desafío recibido con el que fue enviado en el paso ii. Finalmente, envía una trama de autenticación indicándole al transmisor si la autenticación es satisfactoria o no.

Adicionalmente a estos mecanismos básicos de seguridad originales del estándar IEEE 802.11, se han venido desarrollando e implantando en los dispositivos de las WLANs una serie de mecanismos avanzados para solventar las deficiencias de WEP. Entre ellos tenemos:

- **TKIP (Temporary Key Integrity Protocol, Protocolo de Integridad de Clave Temporal)**

  Este mecanismo de confidencialidad de datos resuelve algunos de los problemas de seguridad que posee WEP, mediante la especificación de nuevas reglas para el uso de IV, procedimientos para

la actualización de claves (re-keying), y la utilización de un MIC (Message Integrity Code, Codigo de Integridad de Mensajes) que ayuda a determinar cuando un paquete ha sido modificado por un usuario no autorizado para inyectarlo en la red [2].

TKIP utiliza una clave temporal de 128 bits que es compartida entre todas las estaciones. Esta clave temporales combinada con la dirección MAC del cliente, y luego se le concatena un IV de 16 bytes (mucho más largo que en WEP). Posteriormente, se utiliza el algoritmo de encriptación RC4 para generar el texto cifrado a ser transmitido.

Con el proceso descrito en el párrafo anterior, se evita que dos o más estaciones coincidan con el mismo texto cifrado, y se logra la compatibilidad hacia atrás con WEP. Adicionalmente, la clave temporal de 128 bits cambia cada 10000 paquetes transmitidos (lo cual toma aproximadamente una hora en muchos casos).

La mayoría de los equipos que inicialmente solo soportan WEP pueden ser actualizados para TKIP mediante actualización de firmware.

- **WPA (Wi-Fi Protected Access, Acceso Protegido Wi-Fi)**

Este mecanismo fue introducido por la Wi-Fi Allinance (Alianza Wi-Fi) en 2002 en respuesta de la espera en que se encontraba la industria de la ratificación de la especificación IEEE 802.11i. De modo, que este mecanismo comprende un subconjunto de funcionalidades del 802.11i [9].

WPA ofrece dos métodos de autenticación [6]:

  - **WPA-PSK (Pre-Shared Key):** Se utiliza en ambientes donde no se cuenta con algún servidor de autenticación. Por lo que utiliza claves pre-compartidas estáticas, para generar nuevas claves encriptadas mediante TKIP.

  - **WPA-Empresarial:** Se utiliza en ambientes empresariales con servidores de autenticación (como RADIUS). Al igual que en WPA-PSK, se utiliza TKIP para la encriptación. Además, utiliza como mecanismo de autenticación el estándar IEEE 802.1x basado en *EAP (Extensible Authentication Protocol, Protocolo de Autenticación Extensible)*.

- **IEEE 802.1X**

Es un mecanismo de autenticación basado en el protocolo *EAP (Extensible Authentication Protocol, Protocolo de Autenticación Extensible)* (para detalles sobre EAP, ver [7]), el cual especifica la utilización de RADIUS como servidor de autenticación. La autenticación entre la estación cliente y el servidor RADIUS se realiza a través de un ente "autenticador" implementado en el AP, que a su vez, establece un puerto lógico a través del cual los clientes inalámbricos obtienen acceso a la red cableada [6] [2].

El flujo de este mecanismo funciona de la siguiente manera [2]:

i. El cliente solicita una asociación con el AP.

ii. El AP (autenticador) responde con una *solicitud de identidad EAP*.

iii. El cliente envía una *respuesta de identidad EAP* al AP.

iv. La respuesta de identidad EAP del cliente es reenviada por el AP hacia el servidor de autenticación.

v. El servidor de autenticación envía al AP una *solicitud de autorización*.

vi. El AP reenvía la solicitud de autorización recibida al cliente.

vii. El cliente responde enviando una *respuesta de autorización EAP* al AP.

viii. El AP reenvía la respuesta de autorización EAP del cliente al servidor de autenticación.

ix. El servidor de autenticación envía un mensaje de éxito (*EAP Success*) al AP.

x. El AP reenvía el mensaje de éxito del servidor al cliente y coloca el puerto de este en *modo de reenvío (forward mode)*.

- **IEEE 802.11i**

  Es el estándar de seguridad propio del grupo de trabajo IEEE 802.11 ratificado en el 2004. También conocido como WPA2 según la alianza Wi-Fi, ya que anteriormente, WPA implementaba parte de este estándar cuando aún se encontraba en desarrollo. De modo que estándar 802.11i (WPA2) introduce la misma funcionalidad que WPA con algunas mejoras, como el uso obligatorio del protocolo *CCMP (Counter mode with Cipher-block chaining with Message authentication code Protocol)* (para detalles sobre CCMP, ver [7]), el cual está basado en el algoritmo *AES (Advanced Encryption Standard, Estándar de Encriptación Avanzado)* para sustituir a WEP en la encriptación y confidencialidad de datos. Asimismo hace uso del estándar 802.1X con EAP para la autenticación [4] [9].

Finalmente, el uso de cualquiera de estos mecanismos por sí solos no garantiza la seguridad absoluta de la red, por lo tanto, se recomienda su uso acompañado con mecanismos adicionales tradicionales como el filtrado de direcciones MAC, filtrado de protocolos, políticas empresariales para la asignación de claves, entre otros [2].

2.3.2. Especificación de la capa física

La capa física (PHY) IEEE 802.11, básicamente define el medio de transmisión inalámbrico a utilizar, y las técnicas de modulación y codificación de la señal para la transmisión efectiva de las tramas MAC en dicho medio, las cuales difieren en tecnología y velocidad (tasas de transferencia) [1].

La capa física IEEE 802.11 ha sido publicada en diversas etapas (ver Figura 2.4):

- **PHY 802.11 original**

  La primera parte corresponde al estándar original conocido simplemente como 802.11. Esta capa física permite tres modos de transmisión:

  - **DSSS (Direct Sequence Spread Spectrum):**

    Es una técnica de modulación de espectro expandido sobre una señal RF en la banda de los 2,4 GHz ISM. La cual divide dicha banda en tantos canales según el ancho de banda permitido por el ente regulador local de telecomunicaciones, por lo general estos canales tienen un ancho de banda de 5 MHz.

    La técnica consiste en lo que se conoce como un *código de chipping* o secuencia de pseudo-ruido para codificar cada bit de datos, generando una secuencia de bits que luego es modulada en cada canal mediante alguna técnica de modulación digital-analógica. En el caso particular de la PHY 802.11, se utiliza un código de chipping conocido como *secuencia de Barker* para codificar los datos, junto con la técnica de modulación DBPSK para alcanzar una tasa de 1 Mbps, y DQPSK para una tasa de 2 Mbps.

    Una de las ventajas de la secuencia de Barker es su resistencia a las interferencias y la poca sensibilidad al multi-trayecto.

  - **FHSS (Frecuency Hopping Spread Spectrum):**

    Es otra técnica de modulación de espectro expandido sobre una señal RF en la banda de los 2,4 GHz ISM. Utiliza canales de 1 MHz, donde la cantidad de canales dependerá del ente regulador local a cada país o región.

    La técnica consiste en un esquema de saltos de frecuencia, donde la señal cambia de manera pseudo-aleatoria entre los distintos canales en base a una secuencia de *pseudo-ruido*, donde emisor y receptor deben estar sincronizados con la misma semilla al iniciar cada comunicación para "saltar" al mismo tiempo entre los distintos canales. Como técnica de

modulación, se utiliza GFSK de dos niveles para una tasa de 1 Mbps, y GFSK de cuatro niveles para una tasa de 2 Mbps [3].

Esta aleatoriedad en el salto de frecuencias de FHSS, permite una repartición justa del ancho de banda de 2,4 GHz ISM, evitando posibles interferencias entre los dispositivos. También proporciona cierto nivel de seguridad, ya que se hace poco predecible el canal utilizado por ambas partes de la comunicación en determinado momento. La técnica ofrece además, cierta resistencia a los efectos de la propagación multi-trayecto [1].

- **Infrarrojo:**

Opera en una banda de frecuencias más alta del espectro electromagnético, con una longitud de onda entre los 850 nm y 950 nm.

En la PHY 802.11 original, la transmisión infrarroja es omni-direccional o de difusión, donde es posible un rango de 20 m. El esquema de modulación utilizado se conoce como *16-PPM (Pulse Position Modulation, Modulación por Posición del Pulso)*, donde cada grupo de 4 bits de datos es mapeado a una cadena de 16 bits o *símbolo 16-PPM* compuesta por quince 0s y un 1 para una tasa de 1 Mbps. Para una tasa de 2 Mbps, cada grupo de 2 bits de datos se mapea a una cadena de 4 bits (*4-PPM*). La transmisión física en sí, utiliza un esquema de modulación de intensidad, donde a presencia de señal, corresponde a un 1 binario, y la ausencia de señal a un 0 binario [3].

Debido a que las señales infrarrojas no atraviesan objetos opacos, las celdas se encuentran aisladas a áreas muy limitadas. Además, la luz infrarroja es afectada por la luz solar. Todo esto, sumado a la baja tasa de transferencia, hace que este modo no sea muy popular [1].

- **PHY 802.11a**

Es considerada la primera especificación para WLANs de alta velocidad del IEEE, la cual fue publicada en 1999.

Esta especificación opera en la banda de los 5 GHz ISM, utilizando la técnica de modulación *OFDM (Orthogonal Frecuency División Multiplexing, Multiplexión por División de Frecuencias Ortogonal)* o *Modulación Multi-portadora*, que consiste en una señal con múltiples portadoras de diferentes frecuencias para distribuir la transmisión de los bits de datos (de un solo origen) entre múltiples canales. Esto da como resultado, que la señal es dividida en una banda más estrecha, a diferencia de las técnicas de espectro expandido.

El sistema utiliza hasta 52 sub-portadoras, que son moduladas como se indica en la Tabla 2.3.

Tasa de transferencia	Esquema de modulación
6 Mbps	BPSK
9 Mbps	BPSK
12 Mbps	QPSK
18 Mbps	QPSK
24 Mbps	16-QAM
36 Mbps	16-QAM
49 Mbps	16-QAM
54 Mbps	16-QAM

Tabla 2.3: Modulación OFDM.

- **PHY 802.11b**

  Esta especificación no pretende ser una continuación o mejora de la PHY 802.11a, ya que se aprobó y salió al mercado antes [1]. Utiliza una variante de DSSS conocida como *HR-DSSS (High Rate DSSS, DSSS de Alta Velocidad)* en la banda de los 2,4 GHz ISM, junto con el mismo esquema de modulación que el modo DSSS de la PHY 802.11 original.

  La técnica HR-DSSS utiliza una técnica de modulación compleja adicional a la que provee DSSS conocida como *CCK (Complementary Code Keying)* para lograr tasas de transferencia más altas que DSSS (5.5 Mbps y 11 Mbps) [3].

- **PHY 802.11g**

  Surge en 2001 como una mejora a la PHY 802.11b. Utiliza la misma técnica de modulación que 802.11a (OFDM) logrando las mismas tasas de transferencia, pero en la banda de 2,4 GHz ISM, lo que lo hace compatible con 802.11b y ampliamente utilizado en los dispositivos de red IEEE 802.11.

2.4. Especificaciones existentes del estándar IEEE 802.11

El grupo de trabajo IEEE 802.11 ha desarrollado, a partir del estándar original, una serie de especificaciones (o versiones) en el ámbito de las WLANs con distintos objetivos en cuanto a la evolución, compatibilidad y seguridad de las mismas. Se describen a continuación [5]:

- **IEEE 802.11a**

  Fue publicado en 1999 como un estándar de alta velocidad que soporta tasas de transferencia de hasta 54 Mbps en la banda de los 5 GHz ISM, usando el esquema de modulación OFDM.

- **IEEE 802.11b**

  Es el estándar dominante de las WLANs, soportando velocidades de hasta 11 Mbps en la banda de los 2,4 GHz ISM. Utiliza una variante de DSSS de alta velocidad llamada HR-DSSS. Esta especificación fue una ratificación de 1999 del estándar original 802.11, permitiendo comparar a la funcionalidad inalámbrica con Ethernet. Esta especificación es compatible con 802.11g.

- **IEEE 802.11g**

  En Junio del 2003 se aprueba esta nueva especificación basada en el 802.11b. Funciona en la banda de los 2,4 GHz ISM y es capaz de utilizar dos métodos de modulación, DSSS y OFDM, lo que lo hace compatible con el estándar de facto.

- **IEEE 802.11d**

  Permite la comunicación 802.11 e países que tienen restricciones sobre el uso de las frecuencias en las que opera el estándar. De esta forma se puede usar en cualquier parte del mundo.

- **IEEE 802.11e**

  El objetivo de esta especificación es introducir nuevos mecanismos a nivel de la capa MAC para soportar las aplicaciones que requieren garantías de calidad de servicio (QoS), manejando tráfico en tiempo real en cualquier entorno y situación.

- **IEEE 802.11f**

  Incorpora el protocolo IAPP (Inter-Access Point Protocol, Protocolo Inter-AP o entre puntos de acceso), cuyo objetivo es lograr la interoperabilidad entre APs de diferentes redes, logrando como consecuencia, capacidades de roaming entre dichas redes.

- **IEEE 802.11h**

  Es una adaptación de la especificación 802.11a en cuanto a potencia de transmisión y gestión de las frecuencias (asignación dinámica de canales) para su aplicación en Europa. Alcanza una tasa de transferencia de hasta 54 Mbps en la banda de los 5 GHz, con modulación OFDM. Incorpora los servicios DFS y TPC descritos en las secciones 2.2.10 y 2.2.11 respectivamente.

- **IEEE 802.11i**

  Busca corregir la vulnerabilidad existente en la seguridad para protocolos de autenticación y codificación. Abarca los protocolos 802.1x, TKIP y AES (para detalles, ver sección 2.3.1.3).

- **IEEE 802.11j**

  Ésta especificación aprobada en el 2004, principalmente busca adaptar el estándar a las regulaciones del mercado y el gobierno japonés, en cuanto a la potencia de transmisión, modos de operación, y distribución de los canales. Opera en una nueva banda de 4,9 GHz y en la banda de los 5 GHz ISM [10] [11].

- **IEEE 802.11n**

  Especificación aprobada en el 2009, introduce una nueva tecnología conocida como *MIMO (Multiple-Input Multiple-Output, Múltiple Entrada Múltiple Salida)*, que consiste en el uso de múltiples antenas (Diversidad de Antenas) para dividir la señal en flujos separados independientes mediante *SDM (Spatial Division Multiplexing, Multiplexión por División Espacial)*, junto con el uso de canales de 40 MHz para lograr tasas de transferencia de hasta 600 Mbps. Utiliza la técnica de modulación OFDM, y puede operar en las bandas de 2,4 GHz y 5 GHz ISM, manteniendo la compatibilidad hacia atrás con las especificaciones a y g anteriores [8].

3. METODOLOGÍA – *SITE SURVEY*

El *Site Survey (Estudio del Sitio)* es una guía o procedimiento "paso a paso" donde se estudia el comportamiento de las ondas RF en cuanto a cobertura e interferencias, y se determina la ubicación apropiada de los dispositivos de red en las instalaciones del *sitio*, con el fin de realizar recomendaciones acerca de las mejores opciones en cuanto al hardware a utilizar, instalación y configuración de la WLAN [2]. El objetivo principal de este procedimiento es asegurar que los usuarios móviles experimenten un buen nivel de señal RF de forma continua a medida que se mueven por el sitio, manteniendo al mismo tiempo la conectividad de sus aplicaciones de trabajo, así como con otros dispositivos (móviles o fijos).

Un *site survey* determina especificaciones detalladas sobre cobertura, fuentes de interferencia, ubicación de equipos de red, consideraciones de energía y de cableado.

Todos los resultados del *site survey* deben ser registrados, ya que la documentación sirve como guía para el diseño e instalación de la red, así como para la verificación de la infraestructura inalámbrica.

3.1. Preparación para el *site survey*

La planificación de una WLAN involucra la recolección de información y toma de decisiones. Algunos asuntos puntuales a definir antes de ejecutar el *site survey* son los siguientes [2]:

3.1.1. Análisis de las instalaciones

Se debe tomar en cuenta el número de usuarios, requerimientos de seguridad, requerimientos de ancho de banda, presupuesto, impacto de otros equipos cercanos (maquinaria, artefactos eléctricos y electrónicos, etc.) en cuanto a su interferencia en las señales RF, etc.

3.1.2. Análisis de las redes existentes

Involucra lo siguiente:

- **Redes (cableadas o inalámbricas) en el sitio:** Se debe determinar si la red se va a implementar desde cero, o si funcionará con alguna infraestructura existente. En el último caso, se debe conocer en qué consiste dicha red, por lo tanto, hay que tomar en cuenta cualquier documentación sobre el hardware existente, frecuencias utilizadas, número de usuarios, rendimiento, etc. que ayude a determinar cómo afectará la inclusión de nuevo hardware de red.

- **Ubicación de cuartos de cableado:** Es muy común que al determinar la mejor ubicación para un AP, ésta resulte encontrarse

lejos de algún cuarto de cableado o punto de red, haciendo difícil su conexión a dicha red. La ubicación de los cuartos de cableado debe ser documentada en copias de mapas y diagramas, tanto de las instalaciones como de la topología de la red, lo que ahorrará tiempo en el sitio.

- **Convención de nombres de APs:** De no existir una infraestructura de WLAN en el sitio, se debe idear una convención para los nombres de los APs, lo que facilitará tanto su administración, como la documentación de la ubicación de los mismos.

3.1.3. Determinación del área de utilización

Involucra lo siguiente:

- **Área de operación de la WLAN (interiores o exteriores):** Se debe determinar si el *site survey* se realizará en interiores, exteriores, o ambos. Luego, se debe obtener cualquier documentación (como mapas y diagramas) que esté disponible. En interiores, los documentos deben mostrar cualquier información sobre la distribución de los pisos, muros, estructura de la edificación, cuartos de cableado, etc. En exteriores, la documentación debe mostrar cuán lejos se puede extender la WLAN con cierto nivel de seguridad contra intrusiones, así como posibles obstáculos y fuentes de interferencia de las señales RF. En el caso de exteriores, también se deben tomar en cuenta la influencia de los elementos de la naturaleza (viento, lluvia, polvo) sobre las antenas y los APs, así como los dispositivos que se pueden utilizar para protegerlos.

- **Requerimiento de torres:** Durante la ejecución del *site survey*, puede ser necesario instalar alguna torre de antena (por ejemplo, en el tope de una edificación) para superar algún obstáculo en el camino de un enlace inalámbrico en exteriores. En tal caso, se debe determinar: Adecuación del edificio para soportar dicha torre, permisos necesarios, personal calificado para realizar dicha instalación, etc.

3.1.4. Propósito de la WLAN y requerimientos de negocio

Los usos de las WLANs pueden variar sustancialmente dependiendo de la organización en que se implementan, de modo, que se deben conocer las necesidades de la organización con el fin de realizar el *site survey* de manera efectiva. Se debe determinar exactamente el uso que los usuarios desean darle a la WLAN y que aplicaciones serán ejecutadas dentro de la red. Mediante la documentación exhaustiva de dichas necesidades, se hará posible el diseño de una solución que cumpla con todas las necesidades de los usuarios, así como de la administración de la red.

3.1.5. Levantamiento de los requerimientos de *roaming* y ancho de banda

Involucra lo siguiente:

- **Requerimientos de *roaming* y ancho de banda:** Se deben determinar la tecnología final a implementar y la tecnología que será utilizada para la ejecución del *site survey*, incluyendo: velocidad, alcance, y rendimiento por usuario. Lo cual permitirá crear una solución rentable y que cumpla con las necesidades de los usuarios. Para esto, se debe tomar en cuenta que la mayoría de las organizaciones están divididas en departamentos, donde cada departamento puede tener diferentes requerimientos y usos para la WLAN.

- **Cantidad de usuarios para un área determinada:** Se requiere tener una noción de la cantidad de usuarios localizados en determinada área del sitio para calcular el rendimiento (*throughput*) que cada usuario experimentará, y por ende, ayuda a determinar la tecnología que se ajustará mejor a las necesidades de dichos usuarios.

- **Tipo de aplicaciones a utilizar:** Se deben analizar y documentar los requerimientos de las aplicaciones (ancho de banda, sensibilidad al tiempo, si es orientada a conexión o no, etc.) antes de realizar el *site survey*, con el fin de tomar decisiones más acertadas durante las pruebas.

- **Cambios atípicos en el tiempo de las necesidades de la red en áreas particulares:** Son cambios que pueden ser tan simples como la variación en la cantidad de usuarios en un área y momento determinados, o algo más complejo como cambios climáticos (cambio de temporada, humedad, lluvia, etc.) que afecten el comportamiento de las señales RF.

- **Cobertura necesaria para movilidad:** Es importante documentar la posible necesidad de los usuarios de moverse con sus dispositivos en interiores, exteriores o ambos, así como en situaciones complejas al cruzar limites de algún router de la red o mantener conectividad VPN, etc., ya que es un factor más a tomar en cuenta para el diseño de la solución.

3.1.6. Análisis de los recursos disponibles

Involucra lo siguiente:

- **Recursos disponibles:** Es importante conocer el presupuesto del proyecto, así como el tiempo estimado para el mismo, y la disponibilidad de personal entrenado para la administración de WLANs. Asimismo, se debe recolectar toda documentación disponible como planos y diagramas de la topología de red, y de las instalaciones en estudio, lo cual facilitará la realización del *site survey*.

- **Disponibilidad de planos de las instalaciones:** Será útil y necesario solicitar cualquier tipo de planos o diagramas que muestren la distribución de las instalaciones (el sitio). De no estar disponible esta documentación, se debe crear un diagrama que refleje las dimensiones del sitio, paredes, cuartos de red y/o de cableado, tomas de corriente, puntos de red, etc., lo cual puede ser una tarea que consuma tiempo.

- **Disponibilidad de informes de algún *site survey* anterior:** Si anteriormente se ha realizado un *site survey* en el sitio, es recomendable obtener el informe de dicho procedimiento, ya que implicará un gran ahorro de tiempo para el nuevo estudio.

- **Restricciones de seguridad de las instalaciones:** Puede ser requerido solicitar algún pase, permiso, o compañía por parte de personal de seguridad para poder ingresar a algunas áreas del sitio estudiado.

- **Acceso físico a los techos y cuartos de cableado:** Puede ser necesario el acceso a los techos y cuartos de cableado para estudiar y determinar la ubicación de antenas y puntos de conexión de red.

3.1.7. Levantamiento de requerimientos de seguridad

Involucra lo siguiente:

- **Nivel de seguridad de la red necesario:** El cliente, o beneficiario de la red, puede tener fuertes demandas de seguridad o no requerir ningún tipo de medidas. Sin embargo, es importante informar al mismo de las distintas opciones y mecanismos de seguridad en las WLANs, así como de su justificación, con el fin una mejor toma de decisiones en cuanto al diseño de la solución.

- **Políticas de seguridad existentes en la administración de la WLAN:** En caso de ya existir una infraestructura WLAN en el sitio, se deben revisar las políticas de seguridad existentes antes de iniciar el *site survey*. De no existir política de seguridad alguna, es recomendable levantar cualquier requerimiento al respecto, los cuales pueden variar según el tipo y tamaño de la instalación de la red.

3.2. Ejecución del *site survey*

Una vez que se ha reunido y documentado toda la información necesaria acerca del sitio y los requerimientos de los usuarios, así como la preparación del equipo necesario, es momento de visitar el sitio para ejecutar las diversas pruebas del *site survey*. Las actividades de este proceso se resumen a la recolección y registro de información. Se recomienda iniciar el *site survey* con la recolección de la información no relacionada con el ámbito RF [2].

3.2.1. Estudios en interiores

Para estudios en interiores, se debe localizar y registrar en alguna copia de los planos o diagramas del sitio, lo siguiente [2]:

- Tomas de corriente AC.
- Recintos a prueba de agua y receptáculos de corriente en exteriores.
- Puntos de conexión a redes cableadas.
- Escaleras o elevadores que pueden ser necesarios para la instalación de APs.
- Posibles obstáculos para la señal RF como puertas metálicas de emergencia, ventanas con mayas metálicas, blindajes metálicos, etc.
- Posibles fuentes de interferencia como: hornos microondas, motores eléctricos, monitores para bebes, teléfonos inalámbricos en una banda de 2,4 GHz, etc.
- Áreas de desorden como cubículos de oficina.

3.2.2. Estudios en exteriores

Para estudios en exteriores, se debe registrar en un esquema del sitio lo siguiente [2]:

- Obstrucciones entre ambos extremos de un enlace, como árboles, edificaciones, lagos, etc.
- Según la temporada, identificar árboles cuyas hojas crecerán en distintas épocas del año causando obstrucción a la señal RF.
- LOS óptica y LOS efectiva entre transmisor y receptor.
- Distancia del enlace (de ser superior a 11,7 Km, tomar en cuenta la compensación por la curvatura de la superficie terrestre).
- Elementos climáticos (viento, lluvia, nieve, relámpagos, etc.).
- Accesibilidad a las torres de antenas, o necesidad de una nueva torre.
- Accesibilidad y altura del techo (para colocación de antenas).

3.2.3. Antes de iniciar

De los elementos expuestos anteriormente (sección 3.2.1 y sección 3.2.2), se pueden requerir mayores detalles a registrar para el *site survey*, incluyendo [2]:

- Personal o dependencia de la organización (cliente) que proveerá escaleras o elevadores necesarios para la instalación de los APs.

- Posibilidades y disposición para remover los obstáculos que interfieren con la zona de Fresnel.

- Permisos para la instalación de nuevas torres de antena, en caso de ser necesarias.

- Permisos para la instalación de antenas en techos, y evaluación de la resistencia del techo para soportar una torre (de ser necesaria).

Por otro lado, puede ser necesaria la utilización de escaleras o elevadores. En caso que el cliente provea dichas herramientas, junto con el personal para realizar las instalaciones, es recomendable permitir que sean ellos quienes realicen dicho trabajo.

3.2.4. Recolección de información en el ámbito RF

La siguiente actividad consiste en la ejecución de pruebas, recolección y registro de datos en cuanto al comportamiento de las señales RF en el sitio, mediante la medición y documentación sistemáticas en cada una de las siguientes áreas [2]:

- **Alcance y patrones de cobertura**

  Consiste en colocar un AP en una ubicación arbitraria para realizar mediciones del área de cobertura, realizando cambios de ubicación y repitiendo dichas mediciones hasta encontrar el lugar optimo que cumpla con la cobertura deseada. Una vez determinada la mejor ubicación para el AP, se debe marcar la misma (por ejemplo, con cinta adhesiva de color), y puede ser fotografiada para posterior documentación. Adicionalmente, es recomendable asegurarse de la orientación de las antenas.

  Las mediciones pueden iniciar en cualquier punto del sitio estudiado (por ejemplo, el centro o una esquina), pero cada punto debe ser estudiado caminando lentamente alrededor del sitio con una *laptop* o PDA ejecutando la(s) herramienta(s) apropiada(s) para el *site survey*, y registrando los resultados de las mediciones.

  Las mediciones a registrar incluyen:

  - Tasa de datos (en Mbps).

- Fuerza de la señal (en dBm).
- Suelo de ruido (en dBm).
- SNR (en dB).

Para las áreas de cobertura en exteriores, se requerirán caminatas más largas y mayor registro de datos. Por lo general, existen pocas ubicaciones posibles para un AP, por lo cual, a diferencia del *site survey* en interiores, es poco común la necesidad de cambiar constantemente de lugar el AP o antena para las pruebas. Además, hay que tomar en cuenta que puede existir una cantidad mayor de fuentes de interferencia y obstrucciones de la señal RF en exteriores.

Es importante registrar los resultados de las pruebas realizadas en zonas generales que incluyen, los puntos más alejado del AP, cada rincón, y cada punto donde no llega señal o la tasa de datos cambia (crece o decrece).

Cualquier información relativa a la ubicación, *roaming*, y tipo de usuarios (aplicaciones que utilizan, carga de la red), y lugares como salas de descanso donde exista la presencia de hornos de microondas generadores de ruido en el medio inalámbrico, puede ayudar a determinar puntos importantes donde realizar mediciones del entorno RF.

- **Límites de las tasas de datos**

Esto tiene que ver con las zonas concéntricas alrededor de un AP, que van desde el centro del AP hacia afuera, como se indica en la Figura 3.1, donde los límites de cada zona van indicados por los puntos donde la tasa de datos decrece (por ejemplo, en una WLAN 802.11b, de 11 a 5.5 Mbps, de 5.5 a 2 Mbps, y así sucesivamente), y los cuales deben ser registrados.

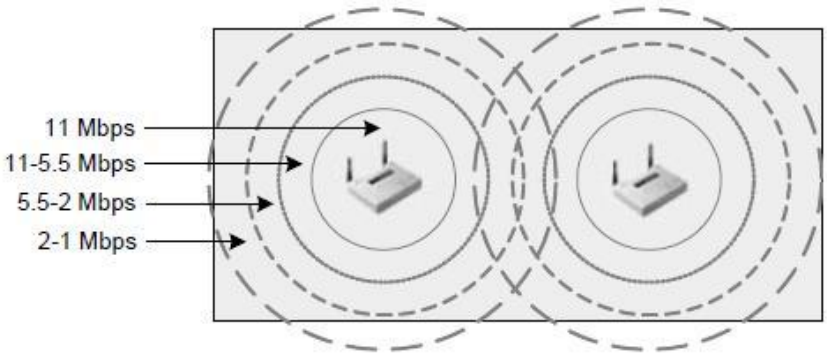


Figura 3.1: Ejemplo de los límites de las tasas de datos

- **Documentación**

Cuando se realizan las pruebas con el AP en determinado lugar, los resultados de las mediciones quedarán registrados sobre copias de

planos y diagramas. Lo cual se repite en cada prueba para distintas ubicaciones del AP hasta encontrar un lugar donde se obtenga la cobertura y tasas de datos deseadas, generando así nueva documentación.

Documentar solo los casos con la mejor cobertura puede ahorrar tiempo. Así mismo, se pueden realizar todas las pruebas hasta encontrar la mejor ubicación para el AP, y luego dedicarse a realizar la documentación. Estas decisiones que afectan el uso del tiempo son importantes, ya que ejecutar un *site survey* es una actividad que consume una cantidad considerable de tiempo.

- **Pruebas de rendimiento y planificación de capacidad**

Además de documentar las áreas de cobertura y tasas de datos, la realización de pruebas de rendimiento (como transferencias de archivos FTP) de la red puede proveer valiosa información para la toma de decisiones al diseñar la solución, así como dar una visión más detallada del comportamiento de la red que experimentaran los usuarios.

La planeación de la capacidad de la red es algo importante para satisfacer el uso que los usuarios pueden dar a la red. Motivo por el cual, se debe conocer el tipo y cantidad de usuarios, y el uso que la darán a la red en cada área.

Toda esta información es añadida y documentada junto con la que ya se ha obtenido en las demás pruebas.

- **Fuentes de interferencia**

En este punto, se busca determinar posibles fuentes de interferencia en las señales RF, tanto de banda estrecha como de espectro expandido.

  - **WLANs operando en instalaciones cercanas:** Cualquier WLAN existente en las cercanías del sitio puede traer dificultades en la ejecución del *site survey*, dado que cualquier permiso para deshabilitaras (si es necesario) podría no ser concedido. Además, deshabilitar WLANs existentes en ambientes de producción puede no ser posible, de modo que, se tendría que realizar las actividades del *site survey* en fuera de horarios de producción.

  - **Planes de instalación de futuras WLANs:** Se debe determinar si existe alguna otra WLAN en proyecto que deba ser considerada para el análisis, ya que podría afectar a futuro la implementación de la WLAN en cuestión.

  - **Planificación, y existencia de otras WLANs en edificios multi-empresariales:** En edificios multi-empresariales, es posible que otras organizaciones en el mismo edificio posean o

planifiquen implementar una WLAN que pueda afectar el *site survey* (Ver Figura 3.2).

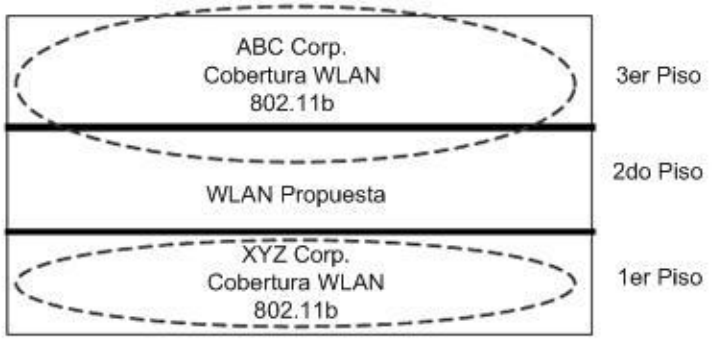


Figura 3.2: WLANs en edificios multi-empresariales.

- **Existencia de fuentes comunes de interferencia en la banda ISM de la WLAN en el sitio:** Se debe documentar cualquier potencial fuente de interferencias que pueda afectar a la WLAN y la ejecución del *site survey*, tales como: Hornos de microondas, teléfonos inalámbricos en la banda de los 2,4 GHz ISM, equipo de radiología, monitores para bebes, entre otros. Asimismo, se deben tomar en cuenta otras WLAN en el área cuya tecnología opere en la misma banda ISM (como 2,4 GHz, o 5 GHz) que la red en estudio.

- **Pérdida de la señal inducida por obstáculos**

Todas las fuentes de interferencia deberían ser localizadas y registradas durante las mediciones de las áreas de cobertura (Ver Figura 3.3).

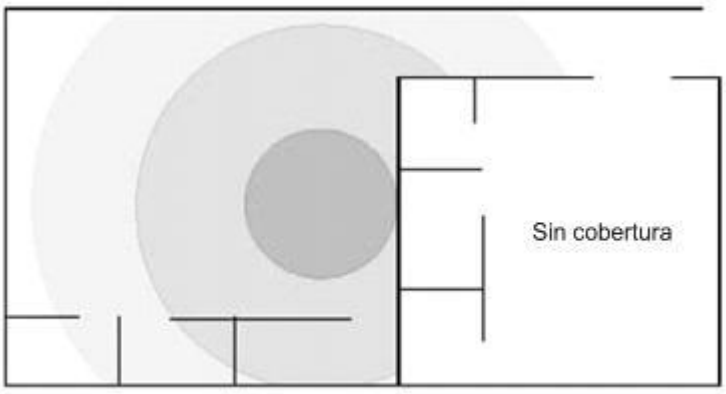


Figura 3.3: Ejemplo de obstáculo para las señales RF.

Existen obstáculos comunes a considerar en interiores, como cubículos de maya metálica, ventanas con maya metálica, puertas metálicas de emergencia, paredes de concreto macizo, motores eléctricos, equipo de telemetría, transformadores, luces fluorescentes,

así como objetos apilados de diverso material que puedan bloquear las señales RF.

En exteriores, existen también diversas fuentes de interferencia, y algunas pueden cambiar por su naturaleza. Por lo tanto, se deben localizar y documentar los efectos de los siguientes elementos:

- Árboles, edificaciones, lagos, entre otras obstrucciones u objetos reflexivos.

- Algunos árboles que podrían crecer o cuyas hojas pueden crecer según la época del año interfiriendo con la zona de Fresnel.

- Tráfico automovilístico, que pueda afectar a un enlace o puente inalámbrico que atraviesa un camino.

Se debe registrar y documentar cada fuente de interferencia, su ubicación, y sus efectos sobre la cobertura, alcance, y rendimiento de la WLAN, tanto en el diagrama del sitio como en algún formato para futura referencia.

- **Conectividad a redes cableadas y requerimientos de energía**

Durante las pruebas y el constante cambio de lugar del AP, tanto en interiores como en exteriores, podría no ser posible colocarlo en las mejores posiciones, ya que su ubicación está restringida a la cercanía de tomas de corriente AC y puntos de conectividad a la red cableada. Por lo tanto, se deben ubicar y marcar en los planos del sitio todas las tomas de corriente AC, así como los puntos de conexión a la red troncal, lo que conlleva a facilitar la ubicación (no necesariamente en el mejor lugar para la cobertura) de cada AP.

Algunos aspectos a considerar durante la búsqueda de la mejor ubicación para hardware WLAN:

- **Disponibilidad de energía AC:** De no disponer de alguna fuente de energía AC en un lugar determinado, se requerirá de los servicios de algún electricista para realizar la instalación y conexión de tomas de corriente AC.

- **Disponibilidad de conexiones a tierra:** La apropiada conexión a tierra de todo dispositivo WLAN, provee protección adicional al equipo contra altas y bajas de tensión.

- **Disponibilidad de conexión a la red cableada (troncal):** De no disponer de conectividad a la red cableada, se podría implementar un puente inalámbrico o utilizar un AP configurado como repetidor, lo cual debería evitarse. Si la distancia entre el AP y el punto de conexión a la red cableada es superior a los 100 metros, un cable STP (Shielded Twisted Pair, Par Trenzado Apantallado) o un AP que soporte cableado de fibra óptica pueden ser utilizados. Por lo tanto, deben estimarse las

longitudes de cable requeridas para la conectividad a los puntos de red, tratando de mantenerlas por debajo de los 90 metros.

- **Obstrucciones físicas:** Obstrucciones como puertas, muros y techos de concreto, entre otros, pueden traducirse en costos de remodelación de ser necesaria su modificación para permitir el paso a las conexiones de energía y/o de red para la interconexión de APs, antenas y redes cableadas.

- **Ubicación de antenas de exteriores**

Para la colocación de antenas en exteriores se registra la ubicación y disponibilidad de, conexiones a tierra, torres o mástiles, y posibles lugares de instalación. En general, la conexión a tierra es un asunto fácil de ignorar, pero se debe generar consciencia de su necesidad. Es necesario tomar en cuenta y especificar lo que se requiere para "llevar la red fuera de la edificación", incluyendo: cableado, energía, protección contra los elementos climáticos, así como protección contra vandalismo y robo.

- **Chequeos puntuales**

Algunas pruebas puntuales después de la completa instalación de la WLAN pueden servir de ayuda para mejorar la solución de problemas cuando ésta se encuentre en producción.

Algunos aspectos a comprobar son:

- Cobertura en áreas perimetrales.
- Cobertura solapada para *roaming*.
- Interferencia entre canales en todas las áreas.

4. DISEÑO DE LA WLAN

Este capítulo presenta el procedimiento realizado para el diseño de la WLAN para el Edificio de Aulas de la Facultad de Ciencias, siguiendo la metodología descrita en el capítulo 3.

4.1. Preparación para el *Site Survey*

Esta sección describe y analiza los requerimientos de la WLAN capturados y demás información levantada relativa al sitio en estudio, los cuales permitieron definir el diseño de la WLAN, el cual se plantea al final de esta sección producto de este análisis.

4.1.1. Análisis de las instalaciones

- **Sitio en estudio:** Edificio de Aulas de la Facultad de Ciencias de la UCV, consistente en un edificio alargado de dos plantas en un área aproximada de 2720 mts^2 (ambas plantas), que se divide en 35 aulas (áreas de cobertura).

- **Áreas de cobertura:** Comprende las áreas de interés a estudiar, donde se requiere la cobertura de la WLAN. Esto incluye las 35 aulas de clase, la Dirección de la Escuela de Biología, la Dirección de Postgrado de Matemáticas, y la Unidad de Idiomas.

- **Impacto RF:** El impacto de las señales RF de la futura WLAN podría causar interferencias en dispositivos inalámbricos cercanos, y viceversa, por lo tanto, durante la ejecución de las pruebas se determinaron los canales de operación de los dispositivos de la nueva WLAN, de modo que se solapasen lo menos posible con los dispositivos cercanos.

- **Seguridad:** Como es natural, se detecto la necesidad de tomar medidas de seguridad en cuanto al hardware de red, así como a nivel de software.

    - **Hardware:** Se contemplaron en el diseño las maneras de ubicar el hardware de red fuera del alcance y vista de posibles usuarios malintencionados que puedan tomar o dañar los dispositivos.

    - **Software:** Los requerimientos de seguridad en este aspecto se describen en la sección 4.1.6.

4.1.2. Áreas de utilización

Dada la naturaleza de las instalaciones del Edificio de Aulas de la Facultad de Ciencias, se identificaron las áreas de operación de la siguiente manera:

- **Interiores:** Involucra las áreas de cobertura (las 35 aulas de clase, Dirección de la Escuela de Biología, Dirección de Postgrado de Matemáticas, y la Unidad de Idiomas), así como la ubicación del hardware de red.

- **Exteriores:** Involucra posibles lugares donde ubicar las antenas que darán cobertura, y su respectivo cableado.

4.1.3. Requerimientos de la WLAN

El paso más importante durante la planificación y levantamiento de información se le atribuye a la captura de requerimientos de la WLAN, los cuales vienen determinados según los siguientes factores:

- **Propósito de la WLAN:** Básicamente, acceso a Internet y a los servidores (aplicaciones, base de datos, correo electrónico, etc.) de la red interna de la Facultad de Ciencias para el soporte académico en las aulas de clase.

- **Aplicaciones:** Se contemplan aplicaciones para el tráfico de datos de "mejor esfuerzo" (como: HTTP, FTP, SSH, e-mail, acceso a bases de datos, mensajería instantánea, etc.). No se contempla tráfico de voz y multimedia.

- **Tipo de usuarios:** Estudiantes, profesores y personal administrativo de la Facultad de Ciencias que requieren acceso a Internet y a las herramientas de la red de datos de la Facultad y de la UCV.

- **Instalaciones donde operará la WLAN:** Edificio de Aulas de la Faculta de Ciencias (descrito en la sección 4.1.1).

En base a estos factores, se determinaron los requerimientos de la WLAN, al igual que su nivel de necesidad e importancia, como se resume en la Tabla 4.1.

Requerimiento	Prioridad/Necesidad					
	N/A	Baja	Media	Alta	Crítica	Justificación
Alcance				**X**		Debe cubrir las 35 aulas del edificio.
Tasa de datos				**X**		Según sea posible
Rendimiento (Capacidad)					**X**	Manejo de volumen de usuarios.
Seguridad			**X**			Autenticación/Encriptación.
Movilidad		**X**				Se limita al interior de un aula, solo si hay solapamiento entre BSSs dentro de un aula.
Disponibilidad				**X**		Principalmente durante los periodos de actividad académica.

Tabla 4.1: Requerimientos de la WLAN.

4.1.4. Recursos disponibles

Para el estudio del sitio se tomaron en cuenta los recursos disponibles (de diversa índole) para la ejecución de pruebas, al igual que los necesarios para la futura implementación de la WLAN.

- **Tiempo:** Se estima realizar el estudio del sitio en un tiempo comprendido de dos a tres meses. El tiempo de implementación de la WLAN se encuentra fuera del alcance de este documento.

- **Personal para la administración de la WLAN:** El Centro de Computación tiene el personal capacitado para la futura implementación y administración de la WLAN.

- **Documentación:** Se recuperó diversa documentación asociada a la red de datos actual de la Facultad de Ciencias y de estudios anteriores para el diseño de una WLAN, entre otras. Esta documentación, aunque escasa, resulto de cierta utilidad para facilitar el presente estudio. Por otra parte, también fue necesario el levantamiento de cierta información de importancia que no se encontraba documentada. Entre la documentación obtenida, y levantada se tienen:

    - **Informes de estudios anteriores:** Se obtuvo el TEG (Trabajo Especial de Grado) titulado "Diseño de la Red Inalámbrica de la Facultad de Ciencias de la Universidad Central de Venezuela" elaborado por el Lic. Rubén Camacho [16], el cual sirvió de apoyo para facilitar la ubicación de los dispositivos. Así mismo, este documento presenta la estructura de la red de datos de la Facultad de Ciencias.

    - **Planos de las instalaciones:** Fue necesario el levantamiento manual de la distribución de las aulas en el Edificio de Aulas en ambas plantas, con el fin de tener una ayuda visual para determinar tanto la ubicación de los dispositivos como la

cobertura de los mismos en el sitio durante la ejecución de las pruebas.

- **Permisos de seguridad y accesibilidad:** Entre los recursos necesarios para acceder a ciertas áreas de las instalaciones, se requirió de ciertos permisos que fueron solicitados en los departamentos correspondientes, así como el apoyo del personal técnico (según el área) para lograr instalar los dispositivos para las pruebas. Entre estos recursos, fue necesario:

    - **Permisos para el acceso al techo del Edificio del Decanato:** Se le solicitó a la Coordinación Académica de la Facultad de Ciencias la permisología respectiva para poder acceder al techo del Decanato para ubicar las antenas.

    - **Apoyo del personal de electricistas y Servicios Generales de la Facultad de Ciencias:** Se requirió y obtuvo el apoyo del personal de electricistas de la Facultad de Ciencias para la instalación de puntos de corriente en el techo del Decanato para la conexión de los dispositivos utilizados en las pruebas.

    - **Apoyo del Centro de Computación:** Se requirió y obtuvo el apoyo necesario del Centro de Computación, para el levantamiento de información de todo lo referente a la red de datos de la Facultad de Ciencias, al igual que para la disposición de los puntos de red cableados y direcciones IP para los dispositivos involucrados en las pruebas.

- **Herramientas de hardware:** Para la ejecución de las pruebas se dispuso del siguiente hardware de red:

    - **APs**

Para ejecutar las pruebas se dispuso de un AP del fabricante *Cisco Systems*, modelo *Aironet 1200*, el cual puede operar con hasta dos radios de dos tipos, uno en la banda de los 2,4 Ghz (802.11g o 802.11b) y otro en la banda de los 5 Ghz (802.11a). Para las pruebas del presente estudio se utilizo el radio de 2,4 Ghz 802.11g, en este sentido, la Tabla 4.2 describe las características de interés para este estudio de dicho dispositivo.

Característica (Con radio 2,4 Ghz 802.11g)	Descripción
Configuración de antenas (Radio 2,4 Ghz)	2 conectores RP-TNC Macho (Diversidad/Individual).
Potencia de salida	100, 50, 30, 20, 5, o 1 mW.
Tasa de datos (adaptativa)	1, 2, 5.5, y 11 Mbps. 6, 9, 12, 18, 24, 36, 48, y 54 Mbps.
NAT	No
Administración	1 Puerto de consola (para cable RJ-45 a DB9). TELNET. SSH.
Conexión a red cableada	1 Puerto Ethernet RJ-45 10BASE-T/100BASE-T.
Fuente de corriente	Adaptador de corriente AC 110 V. PoE.

Tabla 4.2: Características del AP Cisco Aironet 1200

- **Antenas**

Entre las antenas disponibles para realizar las pruebas, se tienen (Tabla 4.3):

Fabricante/Modelo	Tipo	Ganancia	Terminal	Cantidad
HyperLink/HG2409RD-RTP	Omnidireccional	9 dBi	RP-TNC Hembra	2
HiperLink/HG2424G	Direccional	24 dBi	N Hembra	1

Tabla 4.3: Antenas utilizadas en las pruebas

- **Cables**

El cableado disponible, incluye el cableado tanto para la conexión de los APs a la red cableada, como para la interconexión entre los APs y antenas, los cuales se especifican en la Tabla 4.4.

Tipo	Especificación	Longitud	Conectores	Cantidad
UTP	Cat5	15 mts	RJ-45	1
Coaxial	RG-58	0,60 mts	RP-TNC Hembra N Macho	1

Tabla 4.4: Cableado utilizado en las pruebas

- **Adaptador inalámbrico:**

Para la ejecución de las mediciones correspondientes a las pruebas realizadas, se dispuso de un adaptador inalámbrico del fabricante *Broadcom*, modelo *BCM4312*, compatible con la especificación 802.11b/g.

- **Herramientas de software:** Para la ejecución de las pruebas, específicamente, en cuanto a la medición de ciertos parámetros (descritos en la sección 4.2) indicadores de la calidad y rendimiento de la WLAN, se dispuso de las siguientes herramientas de software:

- **Metageek InSSIDer**

Esta herramienta permite analizar el medio inalámbrico en a banda ISM, específicamente en las bandas de los 2,4 GHz y 5 GHz destinadas a las WLANs 802.11, permitiendo determinar la fuerza de la señal y los canales en uso por parte de cualquier AP o BSS dentro del alcance del adaptador inalámbrico [12].

- **NLANR IPerf**

IPerf es una herramienta desarrollada por el *NLANR (National Laboratory for Applied Network Research, Laboratorio Nacional para la Investigación Aplicada de redes)*. Esta herramienta representa una alternativa moderna para generación y medición del rendimiento de flujos de datos TCP y UDP, permitiendo reportar parámetros como *throughput, jitter*, y pérdida de datagramas [13] [14]. La herramienta trabaja con el modelo cliente/servidor. En principio se ejecuta mediante línea de comandos, pero también puede ejecutarse mediante la interfaz grafica JPerf.

- **FileZilla**

Es una solución cliente/servidor para la transferencia de archivos FTP, distribuida bajo la licencia GNU [15].

4.1.5. Redes existentes

Actualmente la Facultad de Ciencias cuenta con una infraestructura de red cableada, la cual cubre ampliamente las diversas dependencias y escuelas de la Facultad, incluyendo el Edificio de Aulas (aunque con escasos puntos de conexión). Por otra parte, la Facultad cuenta con una WLAN, la cual no brinda cobertura al Edificio de Aulas, de donde se deriva la justificación del presente estudio.

El análisis de la red de datos de la Facultad de Ciencias y el efecto que trae la inclusión de la WLAN en estudio, se dividió en dos partes: el análisis de la red cableada y el análisis de la red inalámbrica (secciones 4.1.5.1 y 4.1.5.2 respectivamente).

4.1.5.1. Análisis de la red cableada

La red cableada de la Facultad de Ciencias, proveerá una infraestructura troncal a la WLAN en estudio, permitiendo mediante la conexión de los APs a dicha red, la conectividad de los clientes inalámbricos, a los diversos recursos de la red de la Facultad de Ciencias, de igual manera, el acceso a la red de datos de la UCV y a Internet.

Cabe destacar que el segmento de red que cubre el Edificio de aulas no dispone de mecanismos de "autoconfiguración" (por ejemplo DHCP) en cuanto al direccionamiento IP, por lo tanto, será necesario que los APs de la futura WLAN tengan la tarea de proveer las direcciones IP a los clientes

inalámbricos mediante el mecanismo DHCP. A esto se le suma el hecho de que, en caso de que los APs a utilizar en una posible implementación de la WLAN no dispongan del mecanismo *NAT (Network Address Translation, Traducción de Direcciones de Red)*, el Centro de Computación puede verse en la necesidad de reservar y asignar un *pool* o conjunto de direcciones para que sean asignadas por los APs, o algún otro servidor DHCP, a los clientes inalámbricos.

4.1.5.2. Análisis de la red inalámbrica

Como se describe en la sección 1.1, la WLAN actual de la Facultad de Ciencias no tiene cobertura en el Edificio de Aulas. Por lo tanto la WLAN correspondiente al presente estudio extenderá dicha cobertura, pasando a formar parte de la infraestructura existente. En consecuencia, la WLAN en estudio debe "absorber" ciertas características de configuración de la infraestructura inalámbrica actual, incluyendo:

- Nomenclatura de los APs.
- Nombre del SSID: Identificador actual de la WLAN de la Facultad de Ciencias: "CIENCIAS".
- Modalidad de direccionamiento IP.
- Políticas de seguridad: Se describen en la sección 4.1.6.

4.1.6. Requerimientos de seguridad

Se identificaron los requerimientos de seguridad, específicamente en cuanto al control de acceso a la WLAN (autenticación) y a la encriptación de los datos como niveles de seguridad necesarios y requeridos, los cuales se describen a continuación. Posteriormente se revisaron tanto los mecanismos disponibles como los utilizados en la WLAN actual:

- **Niveles de seguridad necesarios:** Se establecieron mediante el análisis de los requerimientos de la WLAN descritos en la sección 4.1.3.
- **Niveles de seguridad requeridos:** Es el tipo o nivel de seguridad que requiere la Facultad de Ciencias como "dueña" de la WLAN en estudio.

En la Tabla 4.5 se presentan los niveles de seguridad necesarios y requeridos para la futura WLAN.

Tipo de nivel	Requerimiento		Justificación
	Autenticación	Encriptación	
Necesario	Medio	Bajo	Dado el propósito académico de la WLAN, tanto los usuarios como las aplicaciones manejarán escasa data sensible de interés para usuarios mal intencionados y que pueda perjudicar a la institución y su comunidad.
Requerido	Alto	Bajo	Representa los requerimientos cubiertos por la WLAN actual de la Facultad de Ciencias.

Tabla 4.5: Requerimientos y niveles de seguridad para la WLAN.

Debido que la WLAN en estudio representa la extensión para el edificio de aulas de la WLAN actual de la Facultad de Ciencias, solo es necesario tomar en cuenta los niveles de seguridad requeridos por la Facultad en lugar de los que se determinaron mediante el análisis (niveles necesarios), de modo que la futura WLAN cumpla los mismos requerimientos que la red actual, de la misma manera en que debe adaptarse a las características de configuración descritas en la sección 4.1.5.2.

En el análisis, también se contemplaron los distintos mecanismos de autenticación y encriptación que provee el estándar IEEE 802.11 así como en los dispositivos sugeridos para la implementación de la WLAN. Donde se determinó que se deben "absorber" los mecanismos de seguridad implementados en la WLAN actual, de modo que toda la red (actual y en estudio) inalámbrica sea lo más homogénea posible en este aspecto. En este sentido, se tiene lo siguiente:

- **En cuanto a la autenticación**: El Centro de Computación de la Facultad de Ciencias dispone de un servidor RADIUS, el cual maneja la autenticación y autorización mediante un usuario y contraseña personalizados, de modo que cada AP de la WLAN es configurado para autenticar a los clientes inalámbricos mediante este servidor y permitirles o no el acceso a la WLAN. Este mecanismo resuelve el problema de tener una clave compartida entre un gran número de usuarios como ocurre con otros mecanismos de autenticación como SKA y WPA-PSK.

- **En cuanto a la encriptación y confidencialidad de datos:** La WLAN actual no implementa ningún mecanismo de encriptación de datos, por lo que los datos viajan sin cifrar. Por lo que se sugiere la implementación de algún mecanismo como WPA-Empresarial o 802.11i (WPA2), los cuales proveen encriptación de datos adaptándose al esquema de un servidor RADIUS para la autenticación de los usuarios.

4.1.7. Planteamiento del diseño de la WLAN

El análisis presentado hasta este punto de la sección 4.1, permite plantear los posibles esquemas a seguir para definir el diseño de la WLAN del Edificio de Aulas, y sobre los cuales se ejecutaron las pruebas del *site survey* (capítulo 3), cuyos resultados permiten determinar el mejor esquema de diseño para una futura implementación.

El presente estudio plantea dos esquemas o "versiones" para el diseño de la WLAN (ver secciones 4.1.7.1 y 4.1.7.2).

4.1.7.1. Esquema de diseño 1 - WLAN con antenas omnidireccionales

Este esquema plantea una configuración "clásica" de WLAN mediante la colocación de los APs con antenas omnidireccionales de 9 dBi dentro de las aulas a intervalos de distancia regulares entre ellos de acuerdo a la cobertura alcanzada (en términos de aulas por cada AP) a ambos lados de su ubicación. De esta manera tanto la conexión a la red cableada como la toma de corriente para cada AP puede obtenerse dentro del aula donde se ubica el mismo.

4.1.7.2. Esquema de diseño 2 - WLAN con antenas direccionales

Este esquema plantea la ubicación de antenas direccionales de 24 dBi en el techo del edificio del Decanato enfocadas hacia diversos sectores del Edificio de Aulas, con el fin de cubrir las distintas áreas reduciendo la cantidad de antenas y APs necesarios, manteniendo un rendimiento de la red similar o superior a este último. Así mismo, se plantea la ubicación de los APs dentro de las oficinas del Decanato, los cuales conectan a las antenas direccionales en el exterior mediante cables coaxiales de baja pérdida. De modo que, tanto la conexión a la red cableada como la toma de corriente de cada AP pueden obtenerse fácilmente dentro de dichas instalaciones.

4.2. Ejecución de las pruebas (*Site Survey*)

Para cada esquema de diseño, las pruebas realizadas consistieron en la medición sistemática de diversos parámetros en cada una de las áreas de cobertura de interés, con el fin de determinar la ubicación de los dispositivos inalámbricos (APs y antenas) para lograr la cobertura apropiada. Esto mediante la aplicación del procedimiento descrito en la sección 3.2 del capítulo 3.

En ambos esquemas se tomaron en cuenta los siguientes parámetros a medir, así mismo, para cada uno de ellos se determinó (mediante la experiencia) el rango de valores necesario para lograr una conectividad adecuada:

- **Potencia de la señal (en dBm):** Medición realizada con la herramienta inSSIDer. Para una conectividad adecuada se determino un rango que va entre los -77 dBm en adelante.

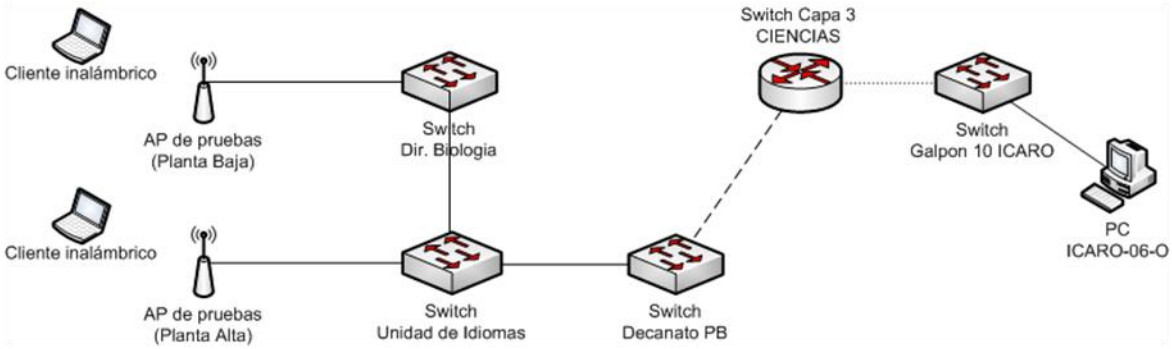
- **Tasa de datos adaptativa (teórica):** Valor mostrado por el driver del adaptador de red inalámbrico, el cual varía mediante el cambio de la técnica de modulación que utiliza el hardware de red (adaptador inalámbrico y APs) de acuerdo a la distancia y calidad de la señal (tasa de datos inversamente proporcional a la distancia entre los dispositivos y directamente proporcional a calidad de la señal). Para una conectividad adecuada se determinó un rango que va entre los 18 Mbps hasta los 54 Mbps (802.11g).

- **Rendimiento:** Involucra la medición de una serie de parámetros que se detallan a continuación. Dado que las herramientas utilizadas siguen un modelo cliente/servidor, dichas pruebas se ejecutaron mediante el esquema de conectividad ilustrado en la Figura 4.1a para el esquema de diseño 1, y la Figura 4.1b para el esquema de diseño 2, donde se muestra la conectividad entre un cliente inalámbrico (corriendo las aplicaciones cliente) y una estación fija (corriendo las aplicaciones servidor) ubicada en el Laboratorio de Redes Móviles e Inalámbricas ICARO durante las pruebas realizadas:

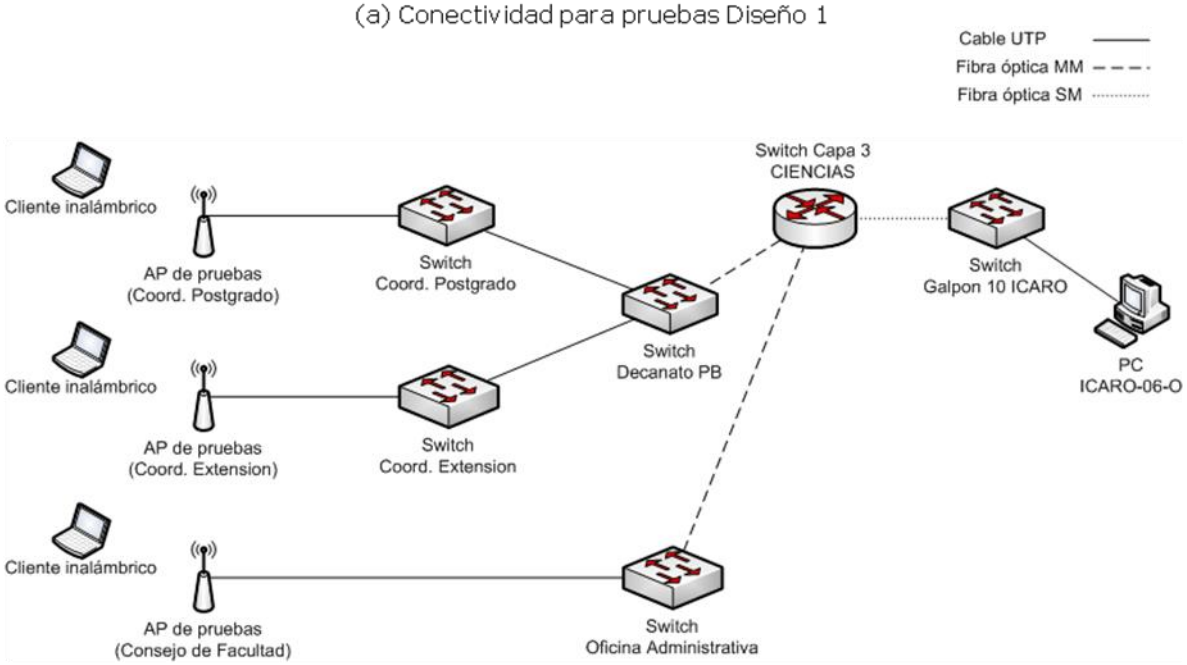
    - ***Throughput* (en Mbits/seg):** Medición realizada mediante la generación y envió de grandes volúmenes de paquetes TCP con la herramienta IPerf.

    - **Pérdida de paquetes (%):** Medición realizada mediante la generación y envió de datagramas UDP a una tasa de transferencia fija con la herramienta IPerf.

    - **Tiempo de transferencia de archivos:** Medición realizada mediante la descarga de archivos a través del protocolo FTP, para lo cual se empleó el software FileZilla para la descarga de un archivo de tamaño fijo (8 MB) en todas las pruebas.



(a) Conectividad para pruebas Diseño 1



(b) Conectividad para pruebas Diseño 2

Figura 4.1: Esquema de conectividad para las pruebas de rendimiento

Así mismo se analizaron los canales en uso de otras WLANs en el área que pudiesen interferir y afectar la calidad de la señal de la WLAN en estudio (con el empleo de la herramienta de software inSSIDer), esto con el fin de determinar los canales a utilizar en cada celda o BSS evitando el solapamiento de canales entre celdas contiguas, y de esta manera conocer las configuraciones necesarias en cada AP en cuanto a la configuración del canal y potencia de salida de la señal.

4.2.1. Esquema de diseño 1 – Antenas omnidireccionales

En esta sección se describe el procedimiento ejecutado para realizar las pruebas que ayudaron a determinar la ubicación de los dispositivos para dar la cobertura apropiada bajo este esquema.

La Tabla 4.6 describe el hardware de red utilizado para ejecución de estas pruebas:

Hardware	Cantidad	Detalles/Configuración	
AP	1	**SSID**	CIENCIAS
		Canal	Automático
		Potencia de la señal	Según ubicación y cobertura requerida (ver Tabla 5.3)
		Antenas	Diversidad
Antenas	2	**Tipo**	Omnidireccionales 9 dBi
		Conexión con el AP	Adaptadas directamente al AP
Cableado de red	15 mts	**Tipo**	UTP Cat5, con conectores RJ-45

Tabla 4.6: Hardware de red para pruebas - Esquema de diseño 1

A continuación se describe el procedimiento realizado para llevar a cabo las pruebas para este esquema:

i. Ubicación inicial: Para este esquema, se eligió (de manera arbitraria) como ubicación inicial para el AP, un punto central en la edificación (aula 9 en la planta baja), ya que esto permitiría conocer el área cobertura del AP en las aulas aledañas (tanto en la planta baja como en la planta alta), mediante la medición de cada uno de los parámetros descritos al inicio de la sección 4.2, donde se determinó que un AP puede cubrir de manera adecuada hasta 3 aulas de cada lado aproximadamente.

ii. Estimación de la ubicación de los dispositivos: En base a la cobertura de la ubicación inicial, se estimó el área de cobertura y ubicación para el resto de los APs a lo largo de cada planta.

iii. Colocación y prueba de los dispositivos: Se procedió a la colocación del AP en cada una de las ubicaciones estimadas en el paso ii para comprobar (mediante las mediciones respectivas) si se obtiene la cobertura esperada por el AP en cada ubicación.

iv. Ajustes en el diseño: En algunas situaciones donde no se obtuvo los resultados esperados en el paso iii, se procedió a realizar los ajustes necesarios en cuanto a la estimación de la ubicación de los APs, y en cuanto a la configuración de los mismos. Seguidamente se procedió nuevamente a la ejecución del paso iii.

v. Registro definitivo del diseño: Una vez obtenida la cobertura apropiada en todas las áreas en el paso iii, se procedió a especificar y registrar las ubicaciones definitivas para los dispositivos, al igual la configuración de cada AP involucrado en el diseño.

4.2.2. Esquema de diseño 2 – Antenas direccionales

En esta sección se describe el procedimiento ejecutado para realizar las pruebas que ayudaron a determinar la ubicación de los dispositivos para dar la cobertura apropiada bajo este esquema.

La Tabla 4.7 describe el hardware de red utilizado para ejecución de estas pruebas:

Hardware	Cantidad	Detalles/Configuración	
AP	1	**SSID**	CIENCIAS
		Canal	Automático
		Potencia de la señal	100 mW (max)
		Antenas	Simple – derecha (principal)
Antenas	1	**Tipo**	Direccional, 24 dBi
		Conexión con el AP	Pig-tail RG-58 N a RP-TNC
Cableado de red	15 mts	**Tipo**	UTP Cat5, con conectores RJ-45
Cableado de antena	0,60 mts	**Tipo**	RG-58, con conectores N y RP-TNC

Tabla 4.7: Hardware de red para pruebas - Esquema de diseño 2

Determinar la cobertura de la antena direccional en determinada área de la edificación resultó ser un poco más complicado que en el esquema 1, debido a los siguientes factores:

- Obstáculos en el camino de la señal: La vegetación de los jardines que se encuentran entre el Decanato y el Edificio de Aulas supone un importante obstáculo para las señales RF, causando una propagación irregular, al igual que un considerado grado de atenuación de las mismas.

- Diferencia en la distancia entre la antena y los puntos a cubrir: Dada la ubicación de cada antena y el área a cubrir, la distancia entre ambas varía en los distintos puntos del área de cobertura, causando variaciones en la pérdida en el espacio libre de la señal (ignorando los obstáculos) en cada punto.

- Patrón de radiación de la antena: A pesar de que la antena tiene un patrón de radiación definido por el fabricante, la propagación de la señal puede variar debido a otros factores como: presencia de obstáculos, ángulo de incidencia de la señal (vertical y horizontal) sobre el área de cobertura.

- Ubicación de la antena: Dependiendo de la ubicación y dirección de la antena, la distancia entre la misma y el punto que enfoca puede variar, afectando la proporción en la fuerza de la señal propagada entre ambas plantas.

En principio, se puede observar la ejecución de las pruebas para este esquema en dos "secciones": Sección Este y sección Oeste del edificio de aulas, donde la delimitación entre ambas correspondería al pasillo que comunica el edificio del Decanato con el Edificio de Aulas.

A continuación se describe el procedimiento realizado para llevar a cabo las pruebas para este esquema:

- Sección Este:

    i Ubicación inicial (Sección Este): Para este esquema, se eligió (de manera arbitraria) como ubicación inicial para la antena direccional, la terraza Noreste del edificio del Decanato, dirigiendo la antena de manera horizontal hacia las últimas aulas en el extremo Este del Edificio de Aulas (aula 17 en la planta baja, y aula 19 en la planta alta), y dirigiéndola de manera vertical hacia la losa que divide las dos plantas, con el fin de dar cobertura en ambas.

    ii Colocación y prueba de los dispositivos: Se procedió a la colocación de la antena y AP en el lugar determinado en el paso i con el fin de comprobar (mediante la medición de cada uno de los parámetros descritos al inicio de la sección 4.2) si se obtiene la cobertura esperada por la antena.

    iii Ajustes en el diseño: En algunas situaciones donde no se obtuvo la cobertura esperada en el paso ii, se procedió a realizar los ajustes necesarios en cuanto a la reubicación y reorientación de la antena, seguidamente se procedió nuevamente a la ejecución del paso ii. En caso de ser necesario, se involucró una antena adicional al diseño para lograr la cobertura, procediendo nuevamente con la ejecución del paso i.

    iv Registro definitivo del diseño: Una vez obtenida la cobertura apropiada en todas las áreas (de la "sección" Este) en el paso ii, se procedió a especificar y registrar las ubicaciones definitivas para los dispositivos, al igual la configuración de cada AP involucrado en el diseño.

- Sección Oeste

    i Ubicación inicial (Sección Oeste): Para este esquema, se eligió (de manera arbitraria) como ubicación inicial para la antena direccional, la terraza Noroeste del edificio del Decanato (encima de la Sala de Conferencias), dirigiendo la antena de manera horizontal hacia las últimas aulas en el extremo Este del Edificio de Aulas (aula 4 en la planta baja, y aula 32 en la planta alta), y dirigiéndola de manera vertical hacia la losa que divide las dos plantas como orientación vertical, con el fin de dar cobertura en ambas.

    ii Colocación y prueba de los dispositivos: Se procedió a la colocación de la antena y AP en el lugar determinado en el paso i con el fin de comprobar (mediante la medición de cada uno de los parámetros descritos al inicio de la sección 4.2) si se obtiene la cobertura esperada por la antena.

iii Ajustes en el diseño: En algunas situaciones donde no se obtuvo la cobertura esperada en el paso ii, se procedió a realizar los ajustes necesarios en cuanto a la reubicación y reorientación de la antena, seguidamente se procedió nuevamente a la ejecución del paso ii. En caso de ser necesario, se involucró una antena adicional al diseño para lograr la cobertura, procediendo nuevamente con la ejecución del paso i.

iv Registro definitivo del diseño: Una vez obtenida la cobertura apropiada en todas las áreas (de la "sección" Oeste) en el paso ii, se procedió a especificar y registrar las ubicaciones definitivas para los dispositivos, al igual la configuración de cada AP involucrado en el diseño.

- Puntos ciegos (ambas secciones)

De existir algún punto ciego donde los obstáculos no permitan la cobertura con las antenas direccionales, se contempló la incorporación de APs con antenas omnidireccionales en el diseño para cubrir la deficiencia.

5. ANÁLISIS DE LOS RESULTADOS

Este capítulo plantea en definitiva el diseño de la WLAN del Edificio de Aulas para cada esquema presentado en la sección 4.1.7, así mismo se analizan los resultados obtenidos durante la ejecución de las pruebas del *site survey* descritas en la sección 4.2, con el fin de obtener una noción comparativa entre los diseños planteados.

5.1. Diseño 1: WLAN con antenas omnidireccionales

En esta sección se detallan cada uno de los elementos del diseño de la WLAN con antenas omnidireccionales en cuanto al hardware de red sugerido, así como la ubicación, cobertura, configuraciones básicas, y elementos de seguridad física del mismo, que permitan una posible y futura implementación de este diseño de manera correcta.

5.1.1. Hardware de red a utilizar

Para la implementación óptima de este diseño se requerirá el siguiente hardware de red (Ver Tabla 5.1): 6 APs, donde cada uno poseerá 2 antenas omnidireccionales de 9 dBi adaptadas directamente al mismo.

Hardware		Cantidad	Detalles
Dispositivo	**Marca/modelo**		
AP	Cisco Aironet 1200	6	Ver sección 4.1.4
Antenas	Indiferente	12 (2 p/AP)	Omnidireccionales 9 dBi, conector RP-TNC hembra
Cableado de red	Indiferente	90 mts (15 mts p/AP aprox.)	UTP Cat5

Tabla 5.1: Hardware de red necesario para el Diseño 1

5.1.2. Ubicación de los APs

Los APs deben colocarse distribuidos a lo largo del edificio de aulas según su cobertura en ambas plantas, como se indica en la Figura 5.1 y más detalladamente en la Tabla 5.2. Donde cada AP se ubicaría dentro de un aula, preferiblemente en el punto más alto y centrado posible de la misma, con el fin de lograr una propagación eficiente de la señal sobrepasando posibles obstáculos de mediana altura (Ejemplo: paredes de cubículos de oficina), así mismo, esto supone un primer "nivel" de seguridad física para los dispositivos (en las aulas que poseen techos de "cielo raso" o *dry-wall*, se sugiere colocar el dispositivo por encima del mismo, siempre y cuando permita el espacio suficiente para las antenas). Con esta ubicación tanto la conexión a la red cableada como la toma de corriente para cada AP puede obtenerse dentro del aula donde se colocará el mismo.

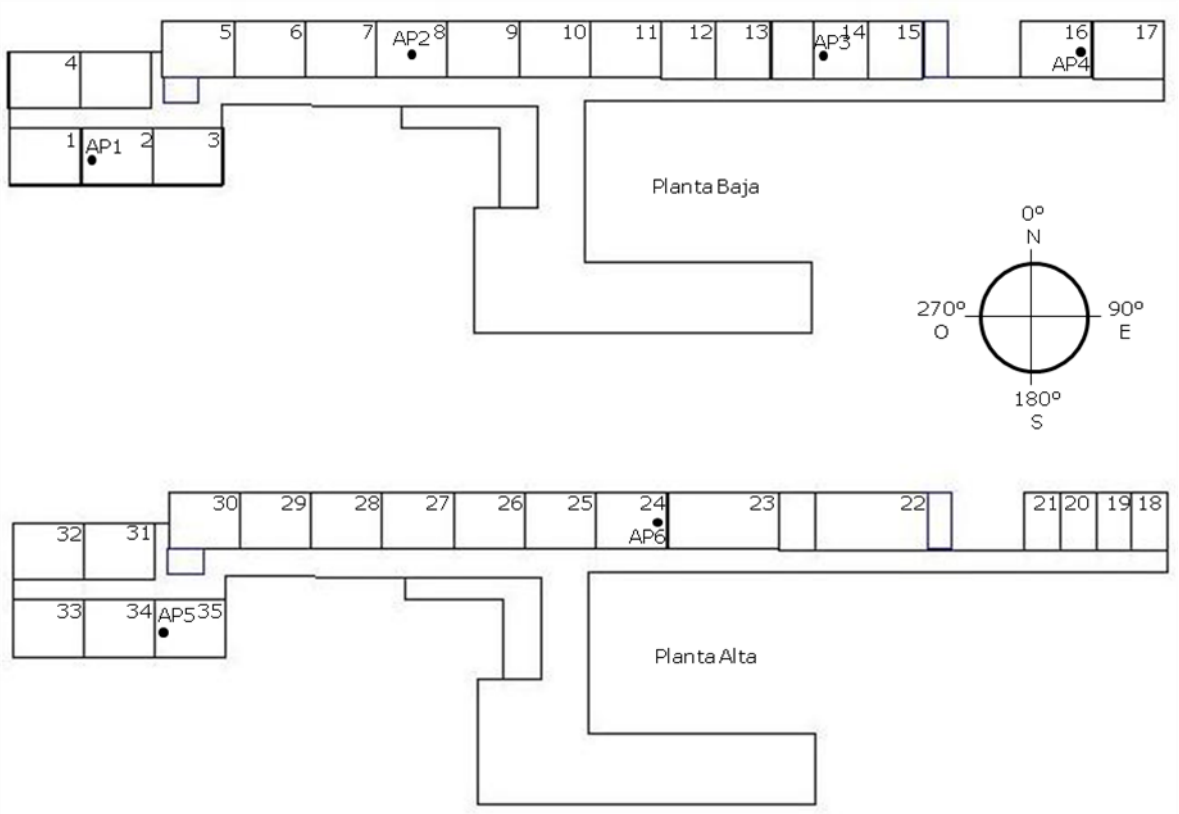


Figura 5.1: Ubicación de los dispositivos - Diseño 1

5.1.3. Cobertura de las celdas

Cada AP y su área de cobertura conforman una celda o BSS en la WLAN como se especifica en la Tabla 5.2. De igual manera, se puede observar gráficamente la cobertura de cada celda en la Figura 5.2.

Nombre	Ubicación	Cobertura
AP1	Aula 2	4 aulas (1, 2, 3, 4) + Dir. Biología
AP2	Aula 8	10 aulas (5, 6, 7, 8, 9, 10, 11, 26, 27, 28)
AP3	Aula 14	5 aulas (12, 13, 14, 15, 23) + Coord. Postgrado Matemáticas + Unidad de Idiomas
AP4	Aula 16	5 aulas (16, 17, 19, 20, 21)
AP5	Aula 35	7 aulas (29, 30, 31, 32, 33, 34, 35)
AP6	Aula 24	3 aulas (23, 24, 25)

Tabla 5.2: Cobertura de las celdas - Diseño 1

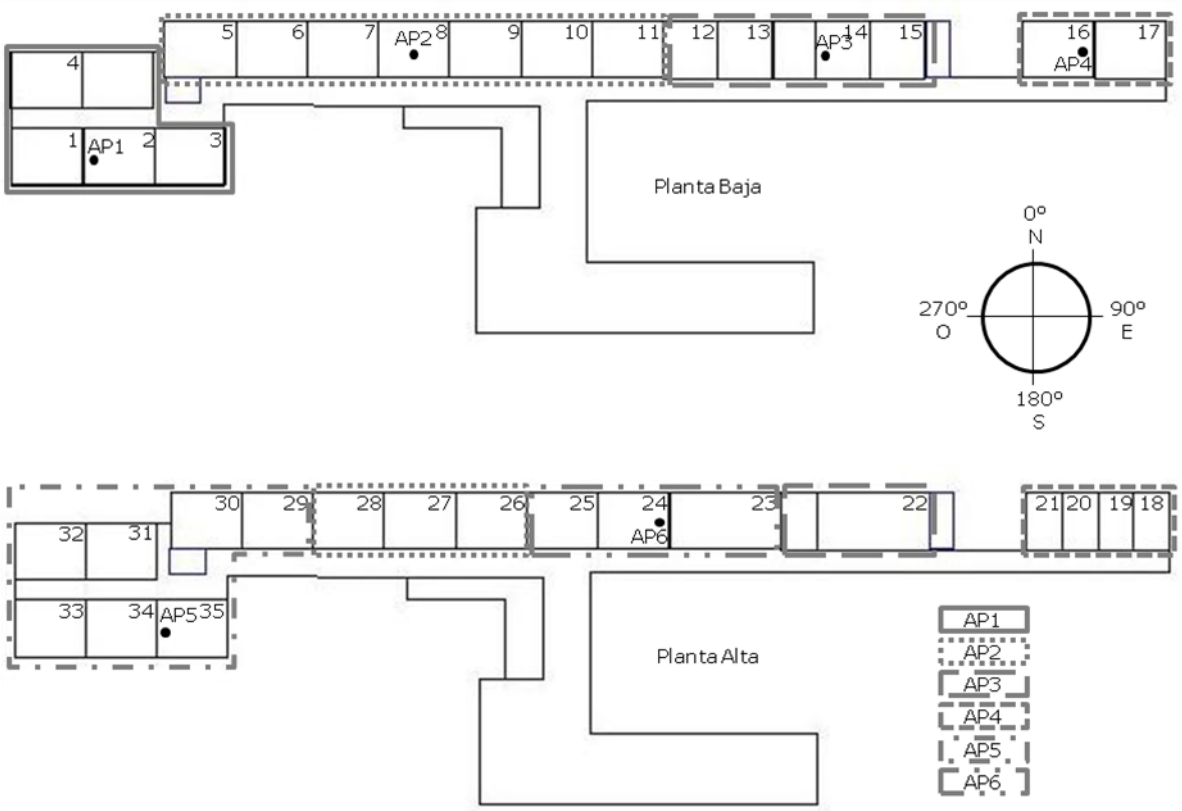


Figura 5.2: Cobertura de las celdas – Diseño 1

5.1.4. Configuración de los APs

En la Tabla 5.3 se especifica la configuración básica que debe poseer cada AP mostrado en la Figura 5.1.

Nombre	SSID	Canal	Potencia de la señal	Antenas	Orientación de las antenas
AP1	CIENCIAS	11	100 mW	Diversidad	Ver Figura 5.3a
AP2	CIENCIAS	6	100 mW	Diversidad	Ver Figura 5.3b
AP3	CIENCIAS	11	100 mW	Diversidad	Ver Figura 5.3c
AP4	CIENCIAS	6	100 mW	Diversidad	Ver Figura 5.3b
AP5	CIENCIAS	3	100 mW	Diversidad	Ver Figura 5.3a
AP6	CIENCIAS	1	5 mW	Diversidad	Ver Figura 5.3d

Tabla 5.3: Configuración de APs - Diseño 1

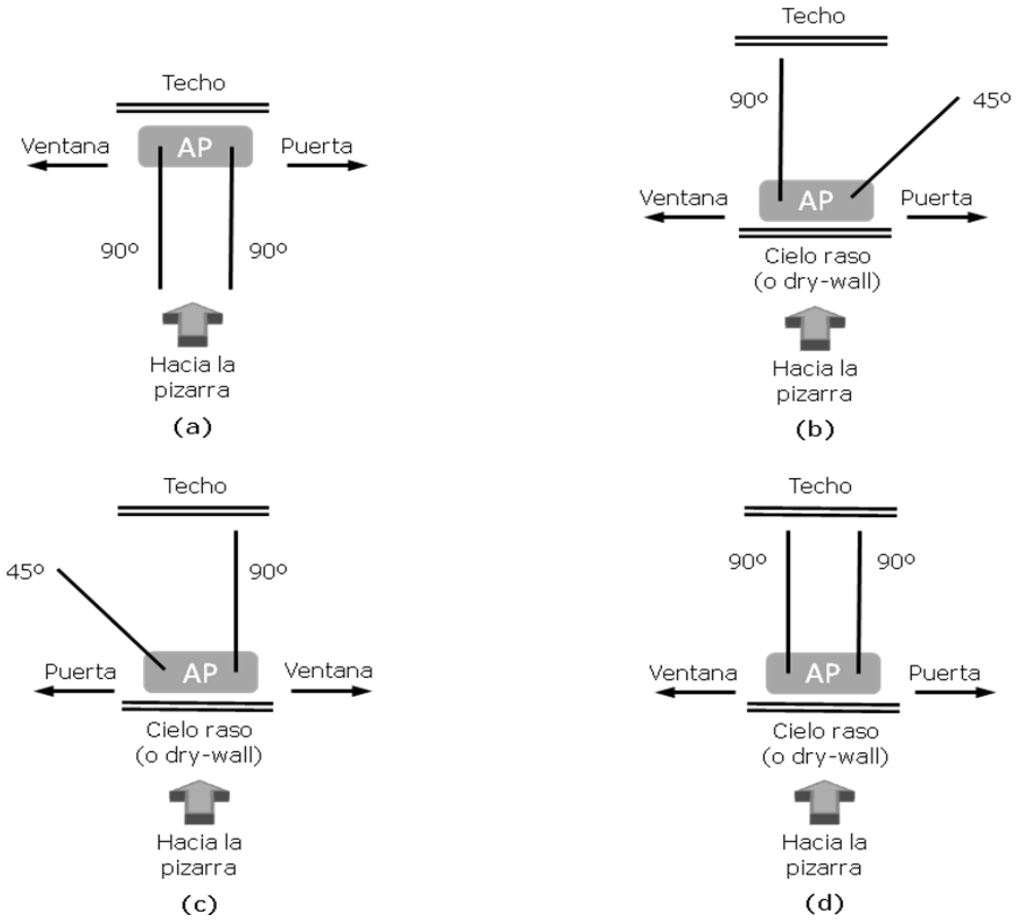


Figura 5.3: Orientación de las antenas – Diseño 1

5.1.5. Esquema de conectividad con la red cableada

En la Figura 5.4 se muestra el esquema de conectividad de los APs con la red cableada de la Facultad de Ciencias.

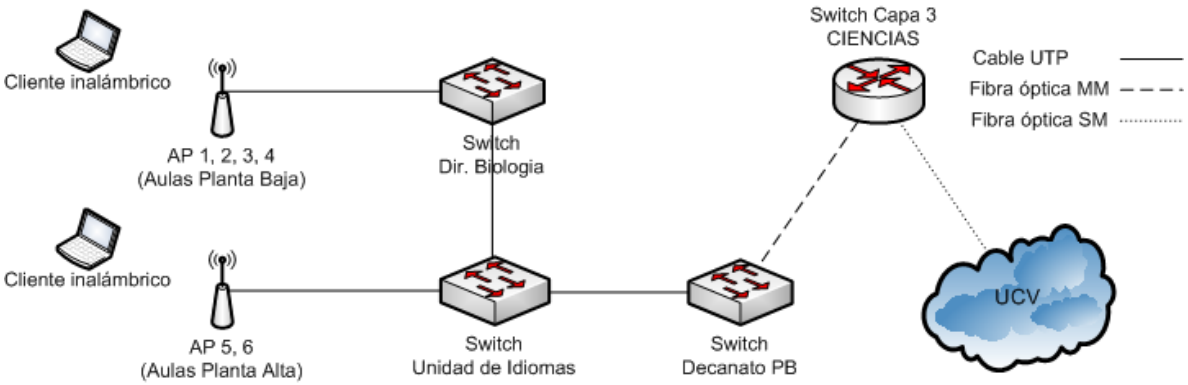


Figura 5.4: Esquema de conectividad - Diseño 1

5.1.6. Seguridad física de los dispositivos

A continuación se dan algunas sugerencias para la seguridad física de los APs:

- Colocar los APs tan alto como sea posible, sugiere una ligera dificultad para el acceso físico al mismo sin despertar alarma en el personal de seguridad de la Facultad.

- Se sugiere la utilización de cajones de seguridad NEMA para brindar un "nivel" más de protección a los APs de ser sustraídos o dañados mediante actos vandálicos.

- El hecho de que cada AP se ubique dentro de las aulas, representa otra implicación más de seguridad, aunque con ciertas limitaciones, ya que el aula respectiva permanecerá asegurada bajo llave durante los periodos en que no hay actividad académica en la Facultad, pero dejando el equipo expuesto durante los periodos de actividad. En este sentido, se sugiere la supervisión especial (en cuanto al resguardo bajo llave) de estas aulas en particular cada vez que esta se encuentre vacía durante cada día de actividad.

- Como medida adicional, se sugiere la colocación o reforzamiento de rejas en las ventanas de cada aula donde se ubique un AP.

5.2. Diseño 2: WLAN con antenas direccionales

En esta sección se detallan cada uno de los elementos del diseño de la WLAN con antenas direccionales en cuanto al hardware de red sugerido, así como la ubicación, cobertura y configuraciones básicas del mismo, que permitan una posible y futura implementación de este diseño de manera correcta.

Así mismo, se presentan los resultados obtenidos durante las pruebas realizadas, reflejando ciertas nociones en cuanto a la calidad de la señal y rendimiento de la red en todas las áreas de cobertura.

5.2.1. Hardware de red a utilizar

Para una implementación óptima de este diseño se requerirá el siguiente hardware de red (Ver Tabla 5.4): 5 APs, donde 3 de ellos poseerán (cada uno) 1 antena direccional de 24 dBi adaptada mediante un cable *pigtail* de baja pérdida, y los 2 APs restantes poseerán (cada uno) 2 antenas omnidireccionales de 9 dBi con el fin de cubrir puntos ciegos donde las antenas direccionales no logran dar cobertura.

Hardware		Cantidad	Detalles
Dispositivo	**Marca/modelo**		
APs	Cisco Aironet 1200 o equivalente	5	Ver sección 4.1.4
Antenas	Hyperlink HG2424G o equivalente	3	Direccionales 24 dBi, conector N hembra (Ver sección 4.1.4)
	Indiferente	4 (2 p/AP)	Omnidireccionales 9 dBi, conector RP-TNC hembra
Cableado de red	Indiferente	Según ubicación de los APs (Ver sección 5.2.3)	UTP Cat5
	LMR 400 Series, equivalente o superior	21 mts (9 mts p/Ant)	*Pigtail* (N macho a RP-TNC hembra)
Lighting arrestors	Indiferente	3 (1 p/antena direccional)	Para la protección de los dispositivos de descargas eléctricas o pulsos electromagnéticos indeseados

Tabla 5.4: Hardware de red necesario para el Diseño 2

5.2.2. Ubicación de las antenas direccionales

Para la implementación de este diseño, se requerirá de la colocación de 3 antenas direccionales orientadas según se especifica en la Tabla 5.5 para dar cobertura en toda la extensión del Edificio de Aulas en las dos plantas como se indica en la Figura 5.5.

Cabe destacar, en cuanto a la orientación horizontal de las antenas direccionales (ver Tabla 5.5), una orientación de la antena de 0º implica que la antena apunta hacia el Norte, enfrentándose perpendicularmente al Edificio de Aulas (ver Figura 5.5). La orientación de cada antena se mide en grados medidos girando en el sentido de las agujas del reloj a partir de los 0°. En cuanto a la orientación vertical, una orientación positiva representa una inclinación de la antena hacia arriba, en cambio, una orientación negativa sugiere una inclinación de la antena hacia abajo.

Antena direccional	Ubicación	Detalles de ubicación	Orientación (Norte=0º)	
			Horizontal	Vertical
Ant1	Terraza Edificio Decanato	0,30 mts del borde Norte de la terraza. 0,45 mts del borde Este de la terraza.	58º	-3º
Ant2	Terraza Edificio Decanato	0,30 mts del borde Norte de la terraza. 12 mts del borde Oeste de la terraza.	0º	-5º
Ant3	Terraza Sala Consejo de Facultad	0,40 mts del borde Norte de la terraza. 0,45 mts del borde Oeste de la terraza.	282º	-4º

Tabla 5.5: Ubicación y orientación de las antenas - Diseño 2

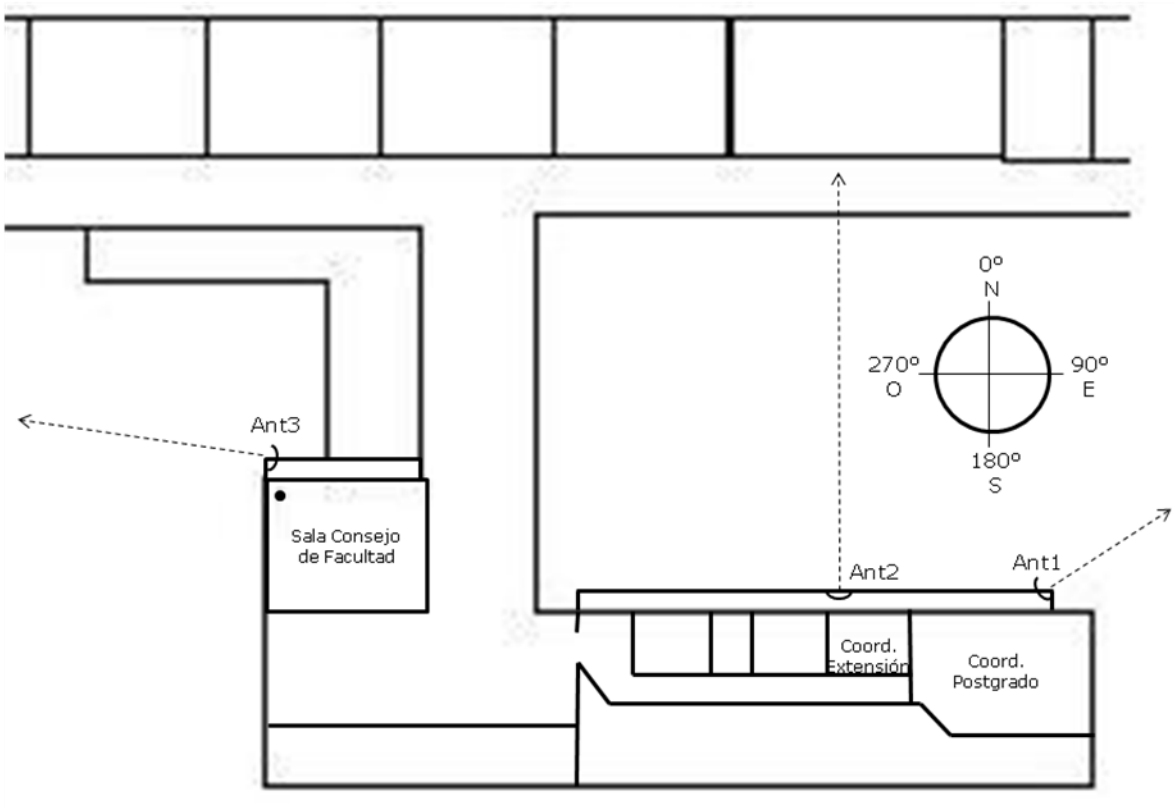


Figura 5.5: Ubicación de antenas - Diseño 2

5.2.3. Ubicación de los APs

En cuanto a la ubicación de los APs, estos deben ubicarse lo más cerca posible de las respectivas antenas que conectan, esto con el fin de reducir la longitud del cable coaxial que conecta cada AP con su antena, reduciendo a su vez, la pérdida de la señal en el cable y el costo del mismo. Por otro lado, la ubicación de cada AP debe resguardar la seguridad física del mismo.

En la Figura 5.6 se sugiere la ubicación de cada AP dentro de las oficinas del edificio del Decanato, por ser este un lugar que representa y requiere un buen nivel de seguridad física hacia dichas instalaciones, y además por la trivial cercanía con las antenas direccionales a ubicar en el exterior del mismo. De modo que, tanto la conexión a la red cableada como la toma de corriente de cada AP pueden obtenerse fácilmente dentro de dichas instalaciones.

Los detalles de ubicación de los APs "AP1" y "AP2" dentro de cada oficina del Decanato se dejan a decisión de, tanto el departamento encargado de la implementación de la WLAN, como a las coordinaciones respectivas. Esto motivado al carácter administrativo de dichas instalaciones donde debe estudiarse la relación funcionalidad/estética dentro de las mismas para este fin.

A pesar de la consideración del párrafo anterior, se sugiere la ubicación de los APs en el techo o alguna pared (en un punto alto) en el interior de cada oficina, manteniendo la suficiente cercanía con la ventana, y en consecuencia con el AP (acortando la distancia del *pigtail*), así como la suficiente distancia para resguardarlo de la visibilidad de intrusos desde el exterior. También debe considerarse que el techo de las oficinas de la planta alta del edificio del Decanato no cuenta con techo de "cielo raso" o *dry-wall* para ocultar los dispositivos.

En el caso del AP "AP3" a ubicar dentro de la Sala del Consejo de Facultad, se sugiere la ubicación del mismo por encima del techo "cielo raso" de dicha sala manteniendo la cercanía con la esquina Noroeste y con la ventana de dicha sala (cerca del AP).

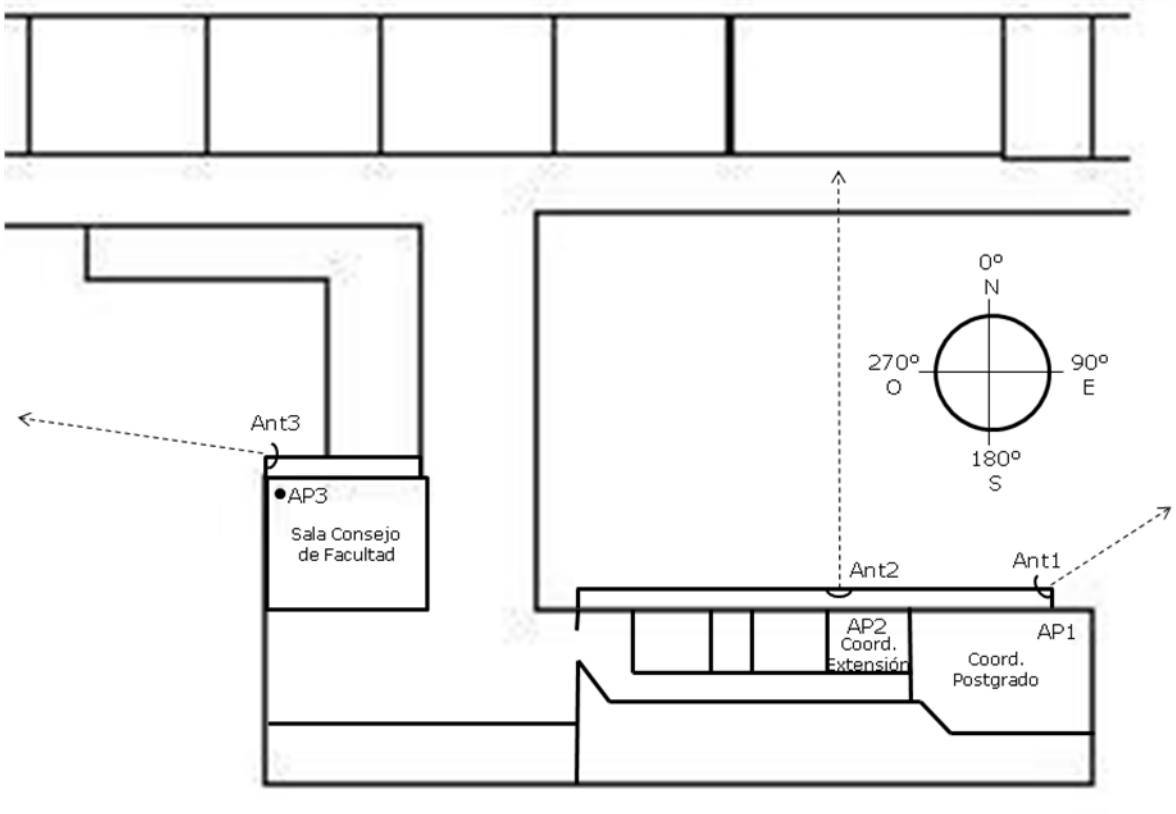


Figura 5.6: Ubicación de APs - Diseño 2

5.2.4. Cobertura de las celdas

Cada antena direccional conectada a su respectivo AP, al igual que los APs con antenas omnidireccionales utilizados para cubrir los puntos ciegos, y su respectiva área de cobertura, conforman una celda o BSS en la WLAN como se especifica en la Tabla 5.6. De igual manera, se puede observar gráficamente la cobertura de cada celda en la Figura 5.7.

Nombre AP	Ubicación	Antena direccional	Cobertura
AP1	Oficina de Coordinación de Postgrado	Ant1	8 aulas (14, 15, 16, 17, 19, 20, 21)
AP2	Oficina de Coordinación de Extensión	Ant2	5 aulas (11, 12, 13, 23, 24) + Coord. Postgrado Matemáticas + Unidad de Idiomas
AP3	Sala de Consejo de Facultad	Ant3	12 Aulas (2, 3, 5, 6, 7, 8, 27, 28, 29, 30, 34, 35)
AP4	Aula 4	N/A	5 aulas (1, 4, 31, 32, 33) + Dir. Biología
AP5	Aula 9	N/A	4 aulas (9, 10, 25, 26)

Tabla 5.6: Cobertura de las celdas - Diseño 2

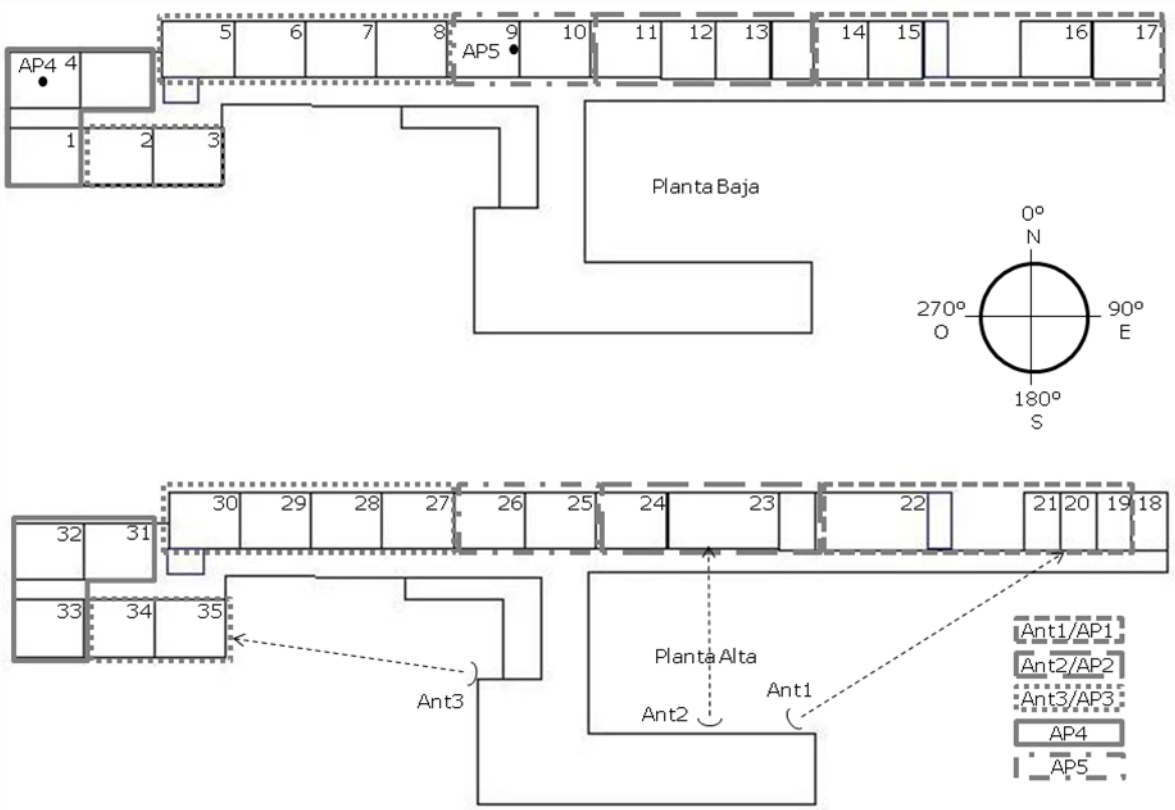


Figura 5.7: Cobertura de las celdas – Diseño 2

5.2.5. Configuración de APs

En la Tabla 5.7 se especifica la configuración básica que debe poseer cada AP mostrado en la Figura 5.6.

Nombre	SSID	Canal	Potencia de la señal	Antenas	Orientación de antenas
AP1	CIENCIAS	6	100 mW	Derecha (Principal)	Ver Tabla 5.5
AP2	CIENCIAS	1	100 mW	Derecha (Principal)	Ver Tabla 5.5
AP3	CIENCIAS	3	100 mW	Derecha (Principal)	Ver Tabla 5.5
AP4	CIENCIAS	11	10 mW	Diversidad	Análogo a la Figura 5.3c
AP5	CIENCIAS	11	5 mW	Diversidad	Análogo a la Figura 5.3b

Tabla 5.7: Configuración de APs - Diseño 2

5.2.6. Esquema de conectividad con la red cableada

En la Figura 5.8 se muestra el esquema de conectividad de los APs con la red cableada de la Facultad de Ciencias.

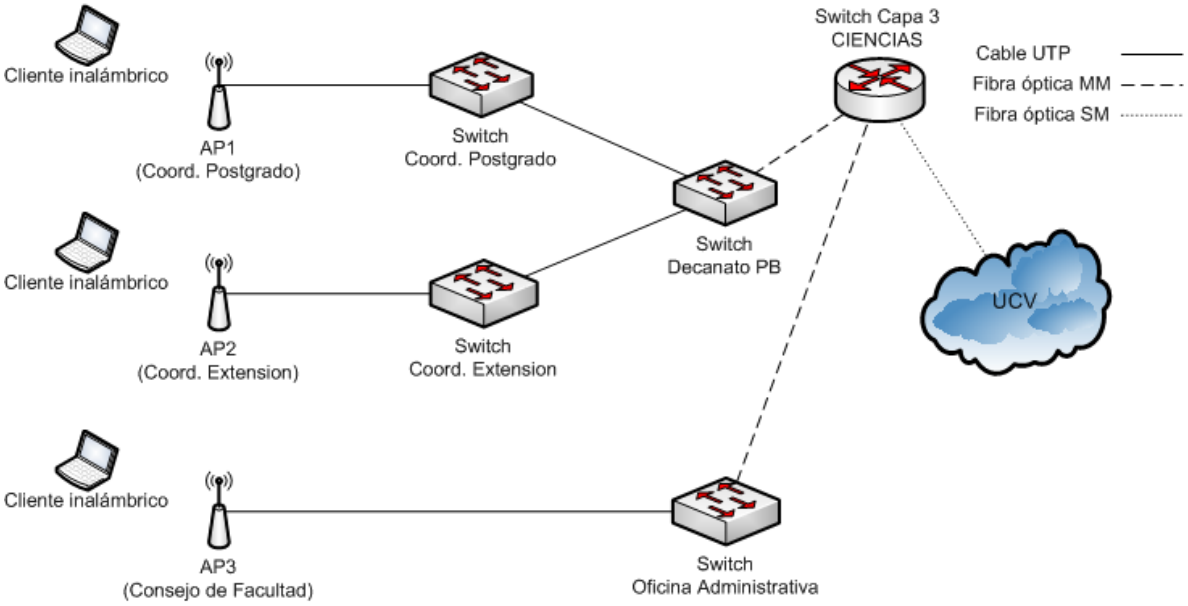


Figura 5.8: Esquema de conectividad - Diseño 2

5.2.7. Seguridad física de los dispositivos

A continuación se dan algunas sugerencias para la seguridad física de los APs y las antenas direccionales:

- La idea de colocar las antenas en el techo del edificio del Decanato supone cierto nivel de dificultad para el acceso, daño y/o sustracción de las mismas sin despertar alarma en el personal de seguridad de la Facultad de Ciencias.

- El hecho de colocar los APs en el interior de las oficinas del decanato supone una obvia "medida" de seguridad física para los dispositivos en este diseño.

- La ubicación de los APs deben permanecer fuera de la vista a través de ventanas y puertas que permitan la visibilidad hacia el interior de las oficinas.

- Se deben aislar con una cinta adhesiva o cualquier otro aislante adecuado las uniones entre conectores del cableado que se encuentre en el exterior (específicamente la interconexión entre cada antena con su AP) para proteger las conexiones de la corrosión causada por los elementos como la lluvia y el sol. Como protección adicional, se puede utilizar una canalización metálica flexible para introducir el cable coaxial a través de ella.

- Se sugiere la utilización de *lighting arrestors* en el exterior para proteger los dispositivos de descargas eléctricas provocadas por diversos factores como las tormentas eléctricas o cualquier desperfecto en los equipos de aire acondicionado o cableado eléctrico cercanos.

5.3. Análisis comparativo de los resultados de las pruebas entre los diseños planteados

Esta sección presenta, de manera comparativa entre los diseños planteados, el análisis de los resultados obtenidos en las pruebas realizadas.

5.3.1. Utilización del hardware de red

En las secciones 5.1 y 5.2 se describió el hardware de red requerido y sugerido para una futura implementación de cada diseño. En esta sección se presenta un análisis comparativo entre ambos diseños en cuanto a la cantidad de dispositivos (APs, antenas, cableado, etc.) necesarios en una posible implementación.

En la Tabla 5.8 se compara la cantidad de hardware de red necesario para los diseños planteados.

Tipo de Hardware		Cantidad Diseño 1	Cantidad Diseño 2
APs		6	5
Antenas	**Omnidireccionales 9 dBi**	12	4
	Direccionales 24 dBi	0	3
	Total antenas	12	7
Cableado de red (UTP Cat5)		90 mts	Según ubicación de los APs (Ver sección 5.2.3)
Cableado para *pigtail* (LMR 400 Series o equivalente)		0 mts	21 mts
Lighting arrestors		0	3

Tabla 5.8: Cantidad de hardware requerido para los diseños planteados

Como se aprecia en la Tabla 5.8, el Diseño 1 requiere cierta cantidad de APs y antenas omnidireccionales para la cobertura apropiada del Edificio de Aulas.

En cuanto al Diseño 2, se puede notar que, a pesar de que éste busca reducir la cantidad de APs mediante la utilización de antenas direccionales de mayor ganancia, no se logra un ahorro tan significativo de dispositivos frente al Diseño 1 como se esperaba, debido a la distancia de propagación, elementos ambientales, y a la gran cantidad de obstáculos en el camino de las señales RF, representados por la densa vegetación de los jardines que se encuentran entre el edificio del Decanato (ubicación de las antenas direccionales) y el Edificio de Aulas, causando la atenuación de la misma. Lo cual trae como consecuencia, la presencia de algunos puntos ciegos donde sería necesario resolver la cobertura con antenas omnidireccionales, traduciéndose en la incorporación al diseño de 2 APs adicionales junto con las antenas omnidireccionales, y cableado respectivos.

Por otro lado, se puede notar que, a pesar de que el Diseño 1 podría requerir una mayor cantidad de hardware de red en cuanto a antenas, APs y cableado de red, el Diseño 2 requiere de ciertos dispositivos un tanto más sofisticados, como lo son: las antenas direccionales, *lighting arrestors*, y el cableado coaxial de baja pérdida para la adaptación de las antenas direccionales a los APs.

En ambos casos, las características de ganancia de la antena, así como su ubicación, impactan en la cantidad de APs necesarios para cubrir determinada área. En consecuencia, el aumento o reducción de APs determina la cantidad de cableado de red necesario.

5.3.2. Calidad de la señal

En esta sección se presenta un análisis comparativo entre ambos diseños en cuanto a los parámetros medidos que se presentan como indicadores para determinar la calidad de la señal RF recibida en el adaptador inalámbrico de las estaciones cliente desde los APs.

- **Fuerza de la señal recibida**

La Figura 5.9 presenta una comparativa entre ambos diseños de las lecturas obtenidas durante las pruebas en cada aula, en cuanto a la fuerza de la señal recibida en el adaptador de red de la estación cliente.

Para este indicador, por tratarse de una pérdida en la señal que llega atenuada al receptor, los valores bajos representan una mejor calidad de la señal.

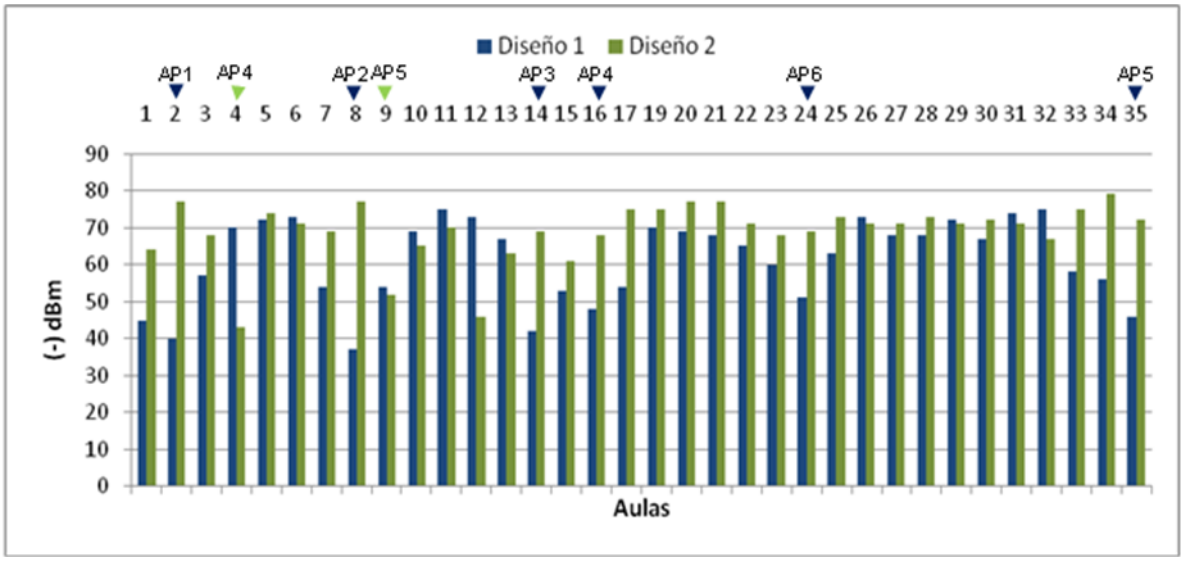


Figura 5.9: Comparativa de la fuerza de la señal recibida absoluta (por aula).

Como se aprecia en la Figura 5.9 las lecturas de la fuerza de la señal recibida en cada aula indican una mejor recepción (con una diferencia variable según el aula) para el Diseño 1.

- **Tasa de datos adaptativa**

La Figura 5.10 presenta una comparativa entre ambos diseños de las lecturas obtenidas durante las pruebas en cada aula, en cuanto a la tasa de datos adaptativa mostrada por controlador del adaptador de red de la estación cliente de acuerdo a la calidad de la señal.

Para este indicador, los valores altos representan una mejor calidad de la señal.

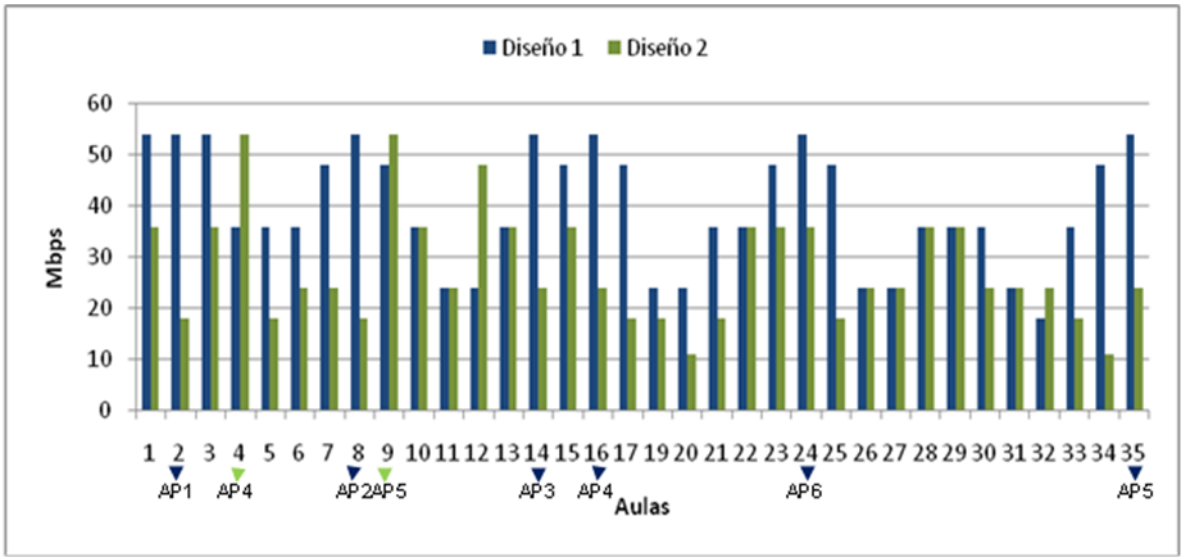


Figura 5.10: Comparativa de la tasa de datos adaptativa absoluta (por aula)

Como se aprecia en la Figura 5.10 las lecturas de la tasa de datos adaptativa utilizada por el adaptador de red y el AP en cada aula, indican una mejor calidad de la señal (con una diferencia variable según el aula) para el Diseño 1.

5.3.3. Rendimiento de la red

En esta sección se presenta un análisis comparativo entre ambos diseños en cuanto a los parámetros medidos que se presentan como indicadores para determinar el rendimiento de la WLAN durante la transmisión de datos en el medio inalámbrico.

- ***Throughput***

La Figura 5.11 presenta una comparativa entre ambos diseños de las lecturas obtenidas durante las pruebas en cada aula, en cuanto al rendimiento (*throughput*) de la red durante el tráfico TCP generado y medido con la herramienta IPerf.

Para este indicador, los valores más altos representan un mejor rendimiento en la transferencia de datos.

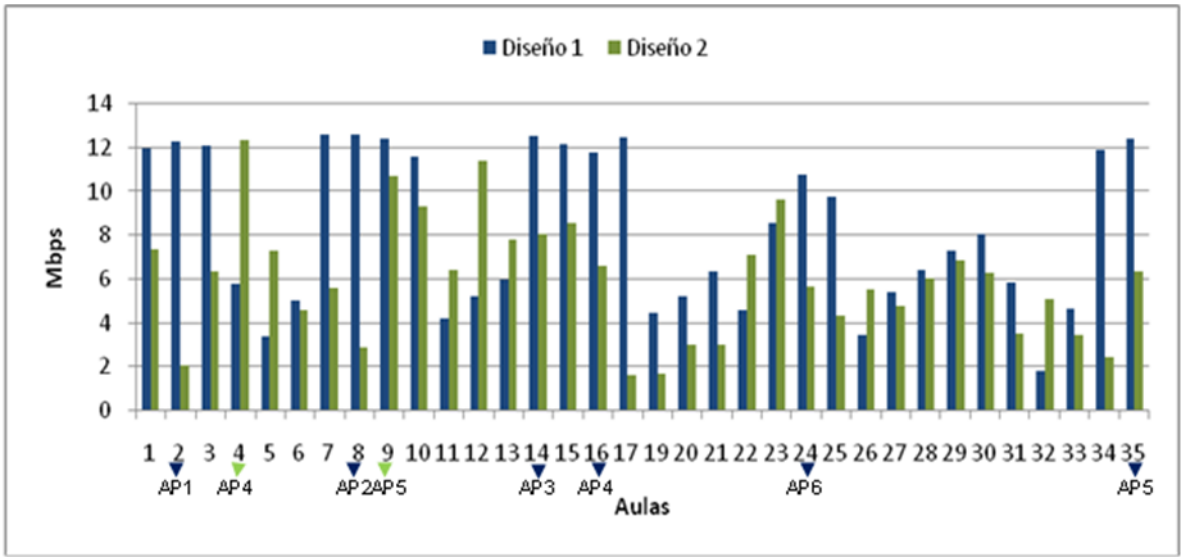


Figura 5.11: Comparativa de rendimiento (*throughput*) absoluto (por aula)

Como se aprecia en la Figura 5.11 las lecturas de *throughput* durante las pruebas en cada aula, indican un mejor rendimiento en cuanto al transporte de datos (con una diferencia variable según el aula) para el Diseño 1.

- **Pérdida de paquetes**

La Figura 5.12 presenta una comparativa entre ambos diseños de las lecturas obtenidas durante las pruebas en cada aula, en cuanto a la pérdida de datagramas durante el tráfico UDP generado y medido con la herramienta IPerf.

Para este indicador, los valores más bajos representan un mejor rendimiento en la transferencia de datos.

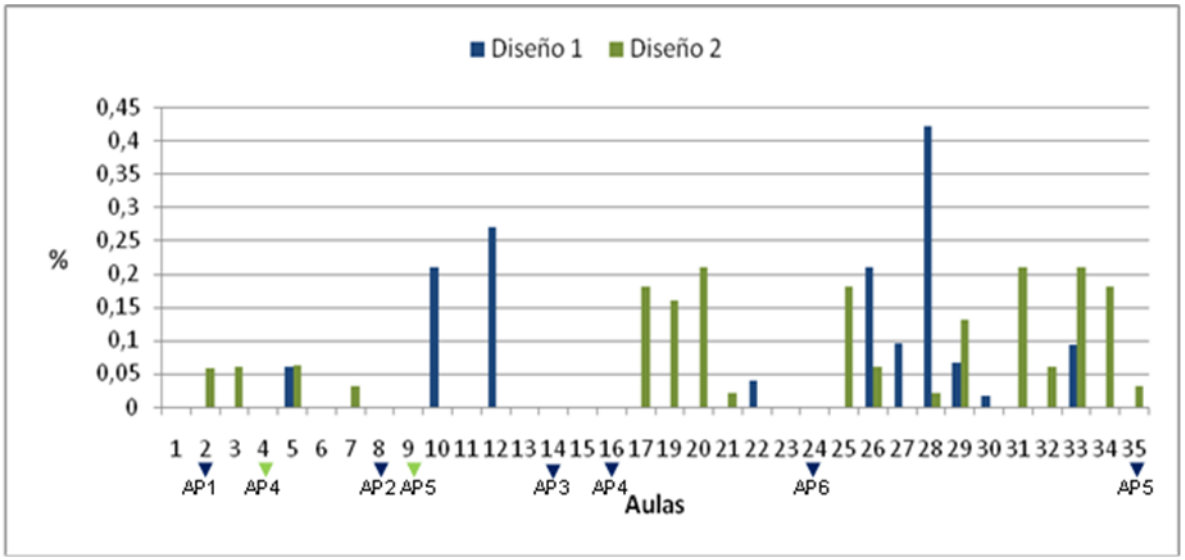


Figura 5.12: Comparativa de la pérdida de paquetes absoluta (por aula)

Como se aprecia en la Figura 5.12 las lecturas de la pérdida de paquetes durante las pruebas en cada aula, indican un mejor rendimiento en

cuanto al transporte de datos (con una diferencia variable según el aula) para el Diseño 1.

En general, se puede decir que la pérdida de paquetes para ambos diseños es relativamente baja.

- **Tiempo de transferencia de archivos**

La Figura 5.13 presenta una comparativa entre ambos diseños de las lecturas obtenidas durante las pruebas en cada aula, en cuanto al tiempo de descarga de un archivo de tamaño fijo para todas las pruebas, mediante la herramienta FileZilla (cliente/servidor FTP).

Para este indicador, los valores más bajos representan un mejor rendimiento en la transferencia de datos.

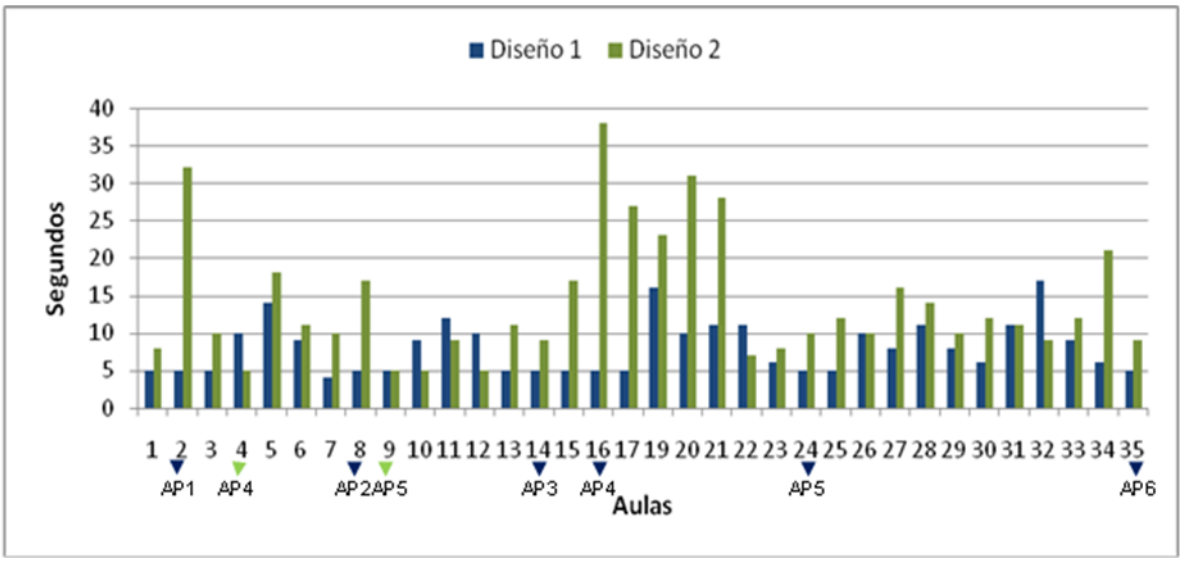


Figura 5.13: Comparativa del tiempo de transferencia de archivos absoluta (por aula)

Como se aprecia en la Figura 5.13 las lecturas en cuanto al tiempo de transferencia de archivos mediante FTP en cada aula, indican un mejor rendimiento en cuanto al transporte de datos (con una diferencia variable según el aula) para el Diseño 1.

5.3.4. Seguridad física de los dispositivos

En esta sección se presenta un análisis comparativo entre ambos diseños en cuanto a la seguridad física ofrecida al hardware de red a instalar en la edificación en una posible implementación de cada diseño.

En las secciones 5.1.6 y 5.2.7 se detallaron una serie de sugerencias para la seguridad física de los dispositivos en ambos diseños, según la naturaleza de ambos esquemas. Se observa que, de implementar dichas sugerencias en su totalidad, se puede encontrar una serie de diferencias notables entre ambos diseños:

- **APs**

A pesar de que el diseño 1 sugiere una serie de medidas para el ocultamiento y resguardo de cada AP dentro de las aulas, de igual manera se tiene que las aulas son áreas que permanecen la mayor parte del tiempo abiertas durante los periodos de actividad académica, así mismo, los mecanismos de resguardo de dichas aulas (cerraduras, rejas, vigilancia, etc.) en los periodos en que no hay actividades, pueden llegar a ser escasos o poco fiables, aumentando el riesgo y exposición de dichos dispositivos a daños o hurto por parte de individuos malintencionados.

En cuanto al diseño 2, existe un menor número de APs expuestos en el edificio de aulas, ya que este esquema intenta (además de reducir la cantidad de dispositivos a utilizar) resguardar los dispositivos ubicándolos en las oficinas del edificio del Decanato, las cuales, dada su importancia, son objeto un mayor número de medidas de seguridad.

- **Antenas**

La seguridad de las antenas a utilizar aplica de manera muy similar al caso de los APs. Ya que, en cuanto al diseño 1, las antenas omnidireccionales se adaptan directamente cada AP conformando una sola unidad.

En cuanto al diseño 2, se plantea la colocación de las antenas direccionales en el techo del edificio del Decanato y sobre la sala del Consejo de Facultad, por lo cual, las mismas se encuentran retiradas en lugares de difícil acceso pero bastante notables en cuanto a la presencia por parte del personal de vigilancia de cualquier irregularidad. A pesar de esto, como se puede apreciar en la Figura 5.5, fue necesaria la incorporación en el diseño de antenas omnidireccionales en algunas aulas para cubrir algunos puntos ciegos que no podían ser cubiertos por las antenas direccionales, quedando de alguna manera más expuestas que estas últimas.

- **Cableado**

Dado que la Facultad de Ciencias, por formar parte de la UCV declarada Patrimonio Mundial de la Humanidad por la UNESCO, no se pueden realizar trabajos de albañilería en las paredes para instalar cableado de red, por lo que sería necesario el empleo de canalizaciones externas para ocultar el cableado de red, aunque estas canalizaciones no son muy robustas para el resguardo del cableado de daños intencionales.

Esto aplica principalmente para el diseño 1, donde el cableado de red UTP seria instalado en el interior del aula para conectar el AP con la red cableada. En cuanto al diseño 2, el cableado UTP se encontraría mejor resguardado dentro de las oficinas del Decanato y la sala del Consejo de Facultad, en cuanto al cableado coaxial que conecta los APs con las antenas direccionales en el exterior, este permanece un poco más expuesto, pero en mejor posición que el cableado UTP en el diseño 1.

6. CONCLUSIONES

La aparición de estándares como el IEEE 802.11, al igual que ciertas agrupaciones de fabricantes de dispositivos inalámbricos (como la *Wi-Fi Alliance, Alianza Wi-Fi*) destinadas a certificar sus productos para su interoperabilidad bajo este estándar, ha convertido a este tipo de redes en una solución de conectividad con diversas ventajas como movilidad, facilidad y rapidez en cuanto a su instalación y actualización, así como su bajo costo, conduciendo a su popularización.

En el presente trabajo especial de grado, se diseñaron y elaboraron dos propuestas de diseño para la futura implementación de una solución WLAN en el Edificio de Aulas de la Facultad de Ciencias de la UCV. Cuya elaboración se apoyó en el *site survey* como metodología para facilitar el desarrollo de ambas propuestas. Alcanzando así, los objetivos planteados.

En cuanto al diseño de la WLAN para el Edificio de Aulas, se contemplaron dos propuestas o esquemas de diseño:

- Diseño 1: Esquema "clásico" de WLAN, mediante el empleo APs con antenas omnidireccionales adaptadas directamente cada AP.

- Diseño 2: Esquema que intenta optimizar el uso de APs y demás hardware de red mediante el uso de antenas direccionales.

Las pruebas realizadas durante el *site survey* determinaron un mejor rendimiento para el Diseño 1 frente al Diseño 2. Así mismo, debido a la necesidad de incorporar APs con antenas omnidireccionales para complementar las deficiencias de cobertura de las antenas direccionales en el Diseño 2, causadas por la distancia de propagación y a la densa presencia de obstáculos en el camino de las señales RF, este esquema no representa un ahorro significativo en cuanto a la cantidad de dispositivos a utilizar como se esperaba. A pesar de estas deficiencias en el Diseño 2, este esquema supone mejores prestaciones en cuanto al resguardo físico de los dispositivos frente al Diseño 1.

6.1. Contribuciones

- El presente trabajo especial de grado culmina con la propuesta de dos alternativas de diseño (secciones 5.1 y 5.2) para la futura implementación de la WLAN del Edificio de aulas de la Facultad de Ciencias.

- La ejecución del *site survey* (Ver capítulo 3) realizada en este trabajo especial de grado, representa una experiencia para el diseño de cualquier WLAN a futuro, dentro o fuera de la Facultad de Ciencias siguiendo este procedimiento, o mediante un posible refinamiento u optimización del mismo, de acuerdo a esta experiencia.

6.2. Limitaciones

- Los dispositivos (APs y adaptadores de red) utilizados para las pruebas del diseño se limitaron a la tecnología de la especificación 802.11g, lo que no permitió experimentar con la más reciente especificación de la capa física 802.11n.

- En cuanto al esquema de diseño 2 con antenas direccionales, se dificulta enormemente la remoción o reducción de los obstáculos en el camino de las señales RF representados por la densa vegetación de los jardines que se encuentran entre el edificio del Decanato y el Edificio de Aulas. Trayendo como consecuencia resultados no tan óptimos como se esperaban durante las pruebas bajo este esquema, y por ende, la necesidad de incorporar en el diseño hardware de red adicional para cumplir con la cobertura requerida.

- Los detalles de ubicación de los APs AP1 y AP2 dentro de cada oficina del Decanato se dejan a decisión de, tanto el departamento encargado de la implementación de la WLAN, como a las coordinaciones respectivas. Esto motivado al carácter administrativo de dichas instalaciones donde debe estudiarse la relación funcionalidad/estética dentro de las mismas para este fin. A pesar de esta consideración, se dio una sugerencia general acerca de la ubicación de estos APs.

6.3. Recomendaciones

- Se puede optimizar la calidad de la señal y el rendimiento de la red para el Diseño 2, con la reducción de los obstáculos naturales en el camino de la señal RF, esto mediante la poda o trasplante de los árboles más altos por otros más bajos en los jardines que se encuentran entre el Decanato y el Edificio de Aulas. Trayendo como consecuencia la reducción del hardware de red a utilizar, y así lograr el objetivo del Diseño 2 que es reducir la cantidad de dispositivos frente al Diseño 1, manteniendo un rendimiento similar a este último.

6.4. Trabajos futuros

- Implementación del diseño más conveniente de los planteados en este trabajo para la WLAN del Edifico de Aulas de la Facultad de Ciencias.

- Aprovechando el levantamiento de información y requerimientos, así como el análisis de las instalaciones del Edificio de Aulas realizado en este trabajo especial de grado. Se propone la ejecución de pruebas del el *site survey* con dispositivos compatibles con la tecnología 802.11n.

- Estudiar la factibilidad del diseño de la WLAN realizando pruebas con otros tipos de antenas (Por ejemplo, semidireccionales: Panel, Yagi, etc.).

REFERENCIAS

[1] Andrew Tanenbaum. Redes de Computadoras. Prentice Hall. 2003.

[2] Planet 3. Certified Wireless Network Administrador – CWNA. Mc Graw Hill Osborne. Second Edition. 2003.

[3] Stallings William. Wireless Communications and Networking. Prentice-Hall. 2001.

[4] IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Std 802.11. Junio 2007.

[5] Nasr Marcel. Diseño y Evaluación de un Sistema de Distribución Inalámbrico para la Facultad de Ciencias. 2007.

[6] María E. Villapol. Presentación: IEEE 802.11: Seguridad. 2007.

[7] B. Aboba, L. Blunk, J. Vollbrecht. Extensible Authentication Protocol (EAP). RFC 3748. Junio 2004.

[8] AirMagnet, Inc. 802.11n Primer. Agosto 2008 [http://www.airmagnet.com/assets/whitepaper/WP-802.11nPrimer.pdf]

[9] Wi-Fi Planet [http://wi-fiplanet.com/news/article.php/3373441]

[10] Wi-Fi Planet [http://www.wi-fiplanet.com/news/article.php/3444141]

[11] Wi-Fi Alliance [http://www.wi-fi.org/knowledge_center_overview.php?type=3]

[12] Metageek: [http://www.metageek.net/products/inssider]

[13] SourceForge: [http://iperf.sourceforge.net/]

[14] NLANR: [http://dast.nlanr.net/iperf/]

[15] FileZilla: [http://filezilla-project.org/]

[16] Rubén D. Camacho B. Diseño de la Red Inalámbrica de la Facultad de Ciencias de la Universidad Central de Venezuela. Junio 2005.

ANEXOS

Anexo 1: Lecturas obtenidas durante las pruebas del *site survey*

Diseño 1 – Antenas omnidireccionales						
Aula	**Calidad de la señal**		**Rendimiento**			
	Fuerza de la señal (dBm)	**Tasa de datos adaptativa (Mbps)**	**Throughput (Mbps)**	**Pérdida de paquetes (%)**	**Jitter (ms)**	**Transferencia FTP (8 MB) (seg)**
1	-45	54	11,98	0	8,02	5
2	-40	54	12,31	0	1,16	5
3	-57	54	12,1	0	3,19	5
4	-70	36	5,81	0	2,69	10
5	-72	36	3,43	0,06	3,65	14
6	-73	36	5,06	0	3,02	9
7	-54	48	12,6	0	15,98	4
8	-37	54	12,6	0	5,21	5
9	-54	48	12,4	0	6,2	5
10	-69	36	11,6	0,21		9
11	-75	24	4,22	0		12
12	-73	24	5,22	0,27	10,21	10
13	-67	36	6,02	0		5
14	-42	54	12,53	0		5
15	-53	48	12,2	0	4,18	5
16	-48	54	11,82	0	3,05	5
17	-54	48	12,5	0	0,05	5
19	-70	24	4,45	0	23,64	16
20	-69	24	5,22	0		10
21	-68	36	6,37	0	6,22	11
22	-65	36	4,61	0,04	25,03	11
23	-60	48	8,6	0	3,67	6
24	-51	54	10,8	0	4,62	5
25	-63	48	9,78	0	8.90	5
26	-73	24	3,47	0,21	4,9	10
27	-68	24	5,44	0,096	22,7	8
28	-68	36	6,43	0,42	10,45	11
29	-72	36	7,3	0,067	3,65	8
30	-67	36	8,06	0,016		6
31	-74	24	5,86	0		11
32	-75	18	1,85	0	5,77	17
33	-58	36	4,64	0,094	2,51	9
34	-56	48	11,9	0	4,84	6
35	-46	54	12,43	0		5

Tabla Anexos 1: Resultados de las pruebas Diseño 1

Diseño 2 – Antenas direccionales						
Aula	**Calidad de la señal**		**Rendimiento**			
	Fuerza de la señal (dBm)	**Tasa de datos adaptativa (Mbps)**	**Throughput (Mbps)**	**Pérdida de paquetes (%)**	**Jitter (ms)**	**Transferencia FTP (8 MB) (seg)**
1	-64	36	7,36	0		8
2	-77	18	2,05	0,058	4,93	32
3	-68	36	6,4	0,06	1,01	10
4	-43	54	12,33	0		5
5	-74	18	7,33	0,063	9,44	18
6	-71	24	4,58	0	9,59	11
7	-69	24	5,6	0,032	3,2	10
8	-77	18	2,91	0	8,1	17
9	-52	54	10,69	0		5
10	-65	36	9,36	0		5
11	-70	24	6,42	0		9
12	-46	48	11,4	0		5
13	-63	36	7,82	0		11
14	-69	24	8,08	0		9
15	-61	36	8,56	0		17
16	-68	24	6,63	0		38
17	-75	18	1,61	0,18		27
19	-75	18	1,69	0,16	20,5	23
20	-77	11	3,02	0,21	25,06	31
21	-77	18	3,03	0,021	6,82	28
22	-71	36	7,11	0	3,6	7
23	-68	36	9,62	0	2,3	8
24	-69	36	5,7	0	1,96	10
25	-73	18	4,33	0,18		12
26	-71	24	5,58	0,061		10
27	-71	24	4,8	0	23,67	16
28	-73	36	6,03	0,021		14
29	-71	36	6,87	0,13	19,13	10
30	-72	24	6,29	0	3,81	12
31	-71	24	3,53	0,21		11
32	-67	24	5,11	0,061		9
33	-75	18	3,47	0,21		12
34	-79	11	2,45	0,18	21,89	21
35	-72	24	6,34	0,031	1,82	9

Tabla Anexos 2: Resultados de las pruebas Diseño 2

Anexo 2: Pruebas bajo el esquema de diseño 1 (antenas omnidireccionales)

Figura Anexos 1: Pruebas Diseño 1 – Aula 35

Figura Anexos 2: Pruebas Diseño 1 – Aula 2

Figura Anexos 3: Pruebas Diseño 1 – Aula 14

Figura Anexos 4: Punto de conexión a la red cableada en las aulas

Anexo 3: Pruebas bajo el esquema de diseño 2 (antenas direccionales)

Figura Anexos 5: Pruebas Diseño 2 – "Ant1" (Terraza sobre la Coord. de Postgrado)

Figura Anexos 6: Obstáculos en el camino de las señales RF de la antena "Ant1"

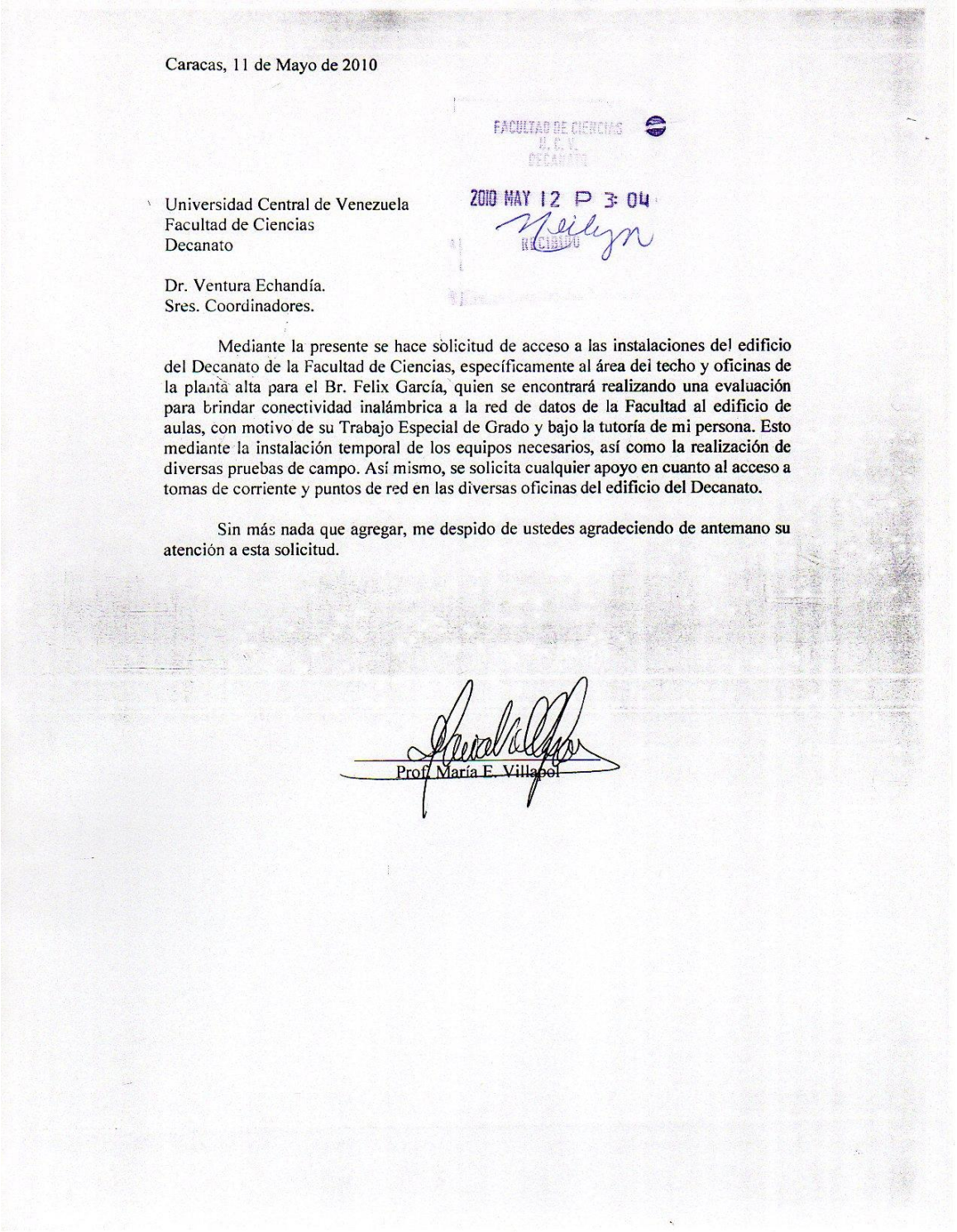
Figura Anexos 7: Pruebas Diseño 2 – "Ant2" (Terraza sobre la Coord. de Extensión)

Figura Anexos 8: Obstáculos en el camino de las señales RF de la antena "Ant2"

Figura Anexos 9: Pruebas Diseño 2 – "Ant3" (Terraza sobre la Coord. de Extensión)

Figura Anexos 10: Obstáculos en el camino de las señales RF de la antena "Ant3"

Anexo 4: Solicitudes administrativas durante la realización del *site survey*



Caracas, 11 de Mayo de 2010

FACULTAD DE CIENCIAS
U. C. V.
DECANATO
2010 MAY 12 P 3:04
RECIBIDO

Universidad Central de Venezuela
Facultad de Ciencias
Decanato

Dr. Ventura Echandía.
Sres. Coordinadores.

Mediante la presente se hace solicitud de acceso a las instalaciones del edificio del Decanato de la Facultad de Ciencias, específicamente al área del techo y oficinas de la planta alta para el Br. Felix García, quien se encontrará realizando una evaluación para brindar conectividad inalámbrica a la red de datos de la Facultad al edificio de aulas, con motivo de su Trabajo Especial de Grado y bajo la tutoría de mi persona. Esto mediante la instalación temporal de los equipos necesarios, así como la realización de diversas pruebas de campo. Así mismo, se solicita cualquier apoyo en cuanto al acceso a tomas de corriente y puntos de red en las diversas oficinas del edificio del Decanato.

Sin más nada que agregar, me despido de ustedes agradeciendo de antemano su atención a esta solicitud.

Prof. María E. Villapol

Figura Anexos 11: Solicitud de acceso al techo del edificio del Decanato

Caracas, 08 de Julio de 2010

U.C.V.
FACULTAD DE CIENCIAS
2010 JUL -8 P 1:29
COORDINACION ADMINISTRATIV

Prof. Santiago Gómez
Coordinador Administrativo
Facultad de Ciencias
Universidad Central de Venezuela

Mediante la presente se hace solicitud del acceso al grupo de aulas descrito a continuación para el Br. Felix García, quien se encontrará realizando un conjunto de pruebas de conectividad para la red inalámbrica del Edificio de Aulas de la Facultad de Ciencias, según el cronograma descrito a continuación:

Día	Horario	Aulas
Jueves 08/06/2010	1PM a 6PM	Planta Baja: 9-17 Planta Alta: 19-26
Martes 13/06/2010	1PM a 6PM	Planta Baja: 9-17 Planta Alta: 19-26
Miércoles 14/06/2010	1PM a 6PM	Planta Baja: 1-8 Planta Alta: 27-35
Jueves 15/06/2010	1PM a 6PM	Planta Baja: 1-8 Planta Alta: 27-35

Sin más nada que agregar, me despido de Ud. agradeciendo de antemano su atención a esta solicitud.

Prof. María E. Villapol

Figura Anexos 12: Solicitud de reservación de aulas para ejecución de pruebas

Anexo 5: Recolección de información en el ámbito RF durante el *site survey*

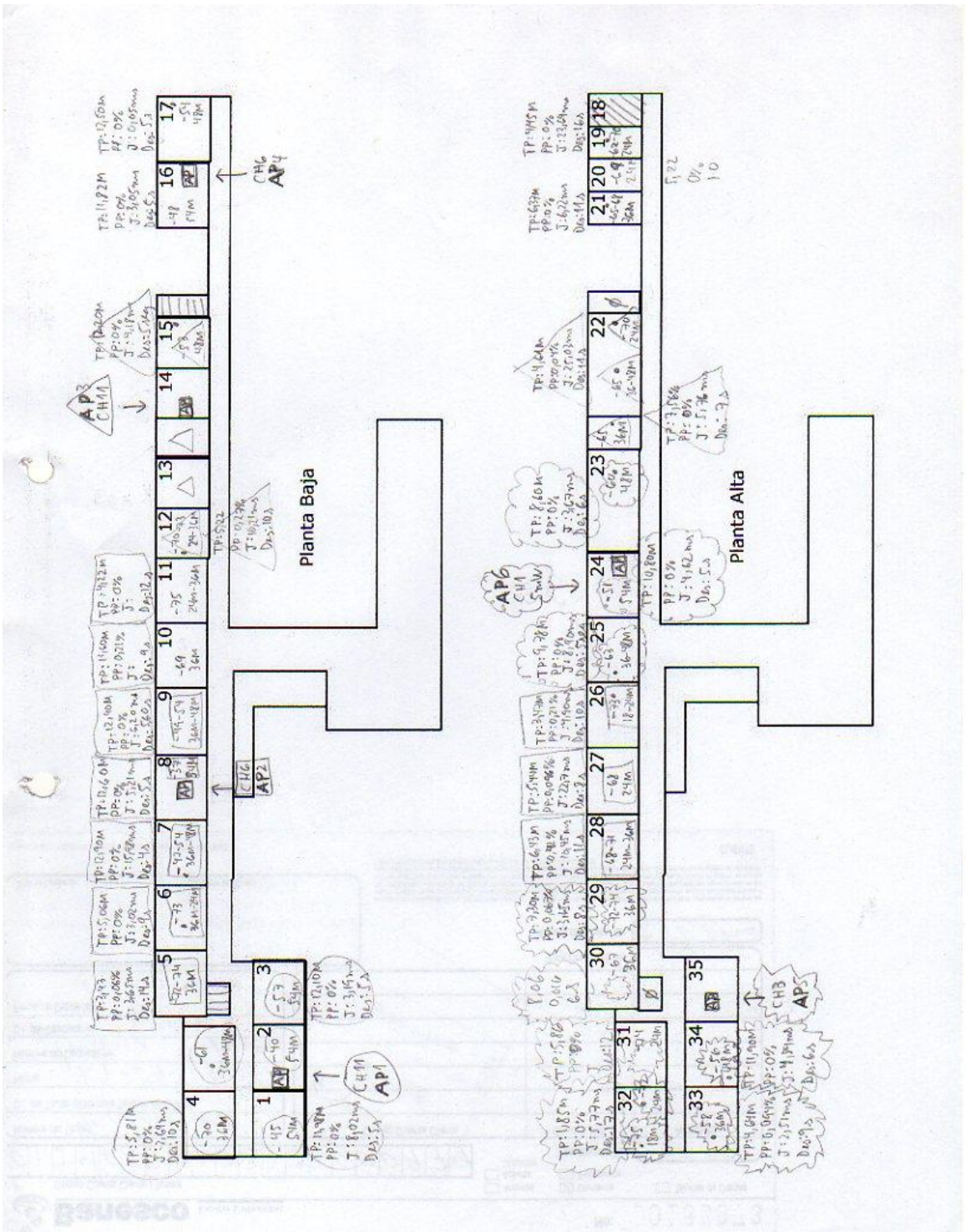


Figura Anexos 13: Registro de resultados en el sitio – Esquema de diseño 1

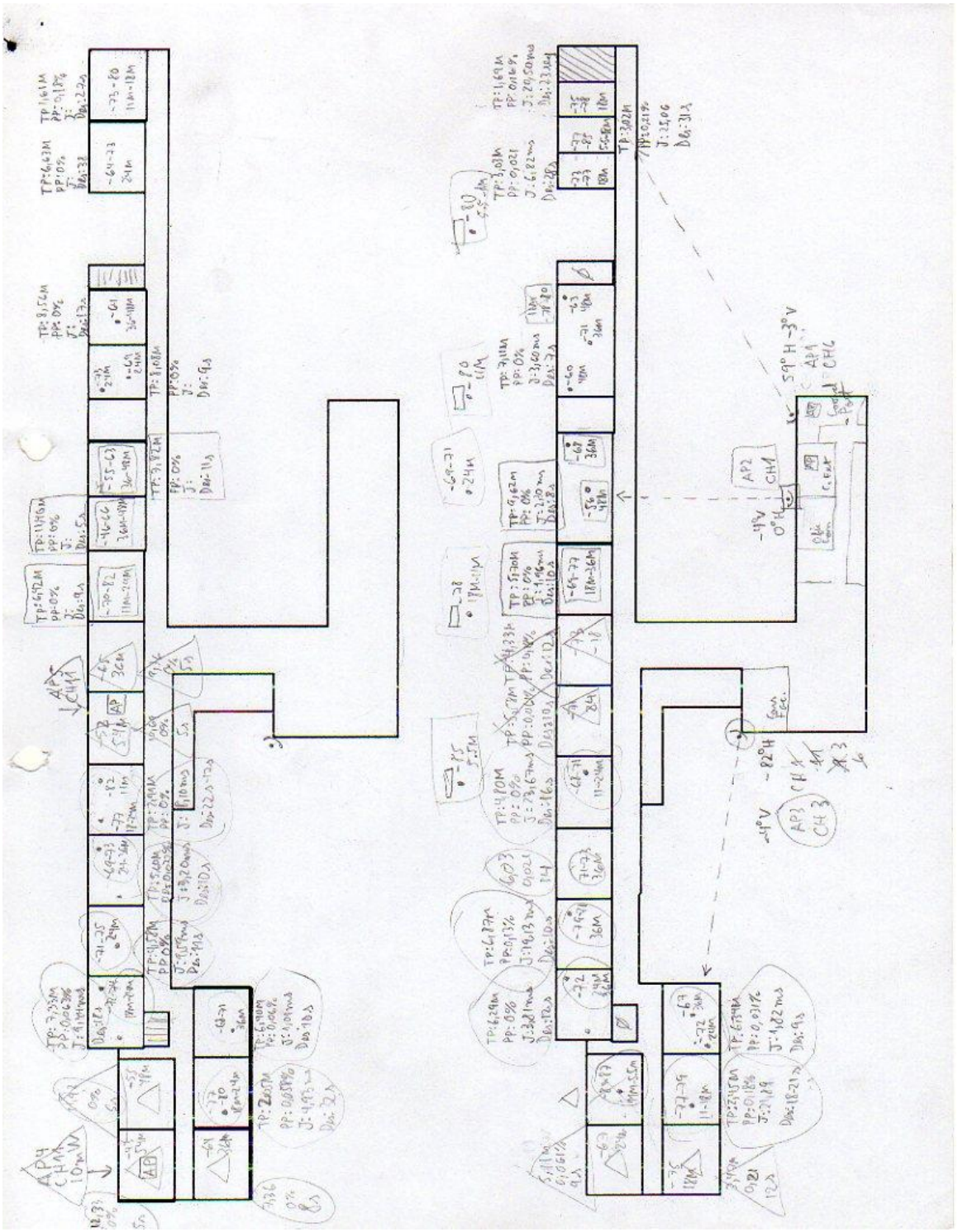


Figura Anexos 14: Registro de resultados en el sitio – Esquema de diseño 2

Anexo 6: Patrones de radiación de las antenas utilizadas en las pruebas

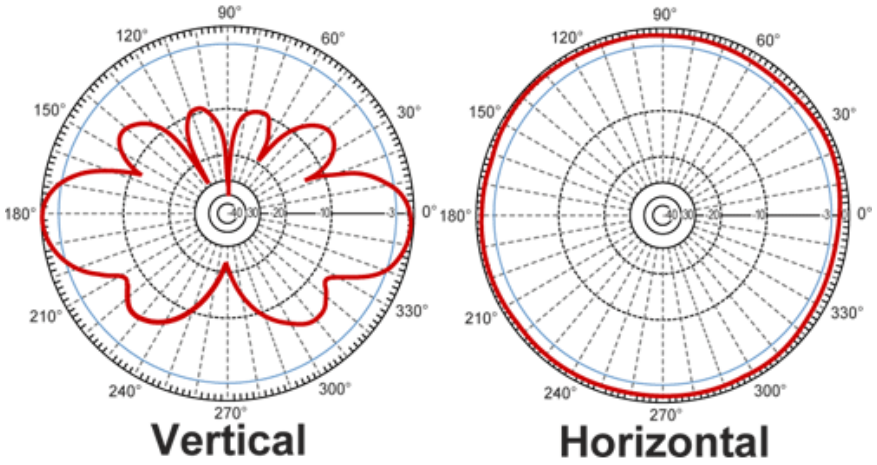


Figura Anexos 15: Patrón de radiación de la antena omnidireccional *Hyperlink HG2409RD-RTP*

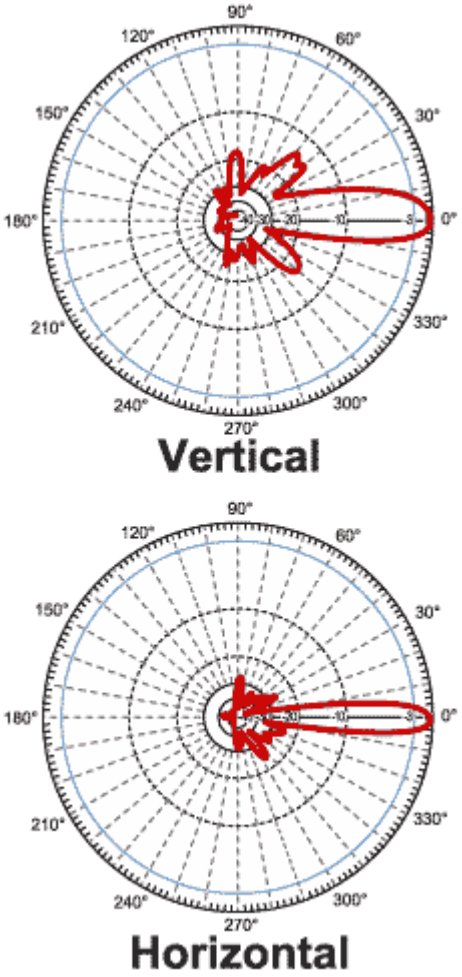


Figura Anexos 16: Patrón de radiación de la antena direccional *Hyperlink HG2424G*