ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE SISTEMAS

“ANALISIS Y DISEÑO DE UNA WLAN 802.11.”

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO ESPECIALISTA EN INFORMATICA MENCIÓN EN REDES

ANA CONSUELO ORBE OLMEDO
WILSON MEDARDO PANCHO MALES

DIRECTOR: ING. CARLOS BADILLO

Quito, Septiembre 2006

DECLARACIÓN

Nosotros, Ana Consuelo Orbe Olmedo, Wilson Medardo Pancho Males, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

---------- ----------

Ana Orbe Wilson Pancho

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Ana Consuelo Orbe Olmedo y Wilson Medardo Pancho Males, bajo mi supervisión.

Ing. Carlos Badillo
DIRECTOR DEL PROYECTO

AGRADECIMIENTO

Damos gracias primero a DIOS que siempre nos iluminó y ayudó para llegar a culminar éste trabajo.

Y luego agradecemos a nuestros maestros y compañeros por las enseñanzas y la sincera amistad que nos brindaron en todo momento. Además les agradecemos al personal de FLACSO, quienes nos proporcionaron todo el apoyo e información que nos ha ayudado en gran parte a desarrollar nuestro trabajo.

DEDICATORIA

Este trabajo esta dedicado a mis padres ya que ellos me apoyaron en cada momento y etapa de mi carrera, que a mas de ser el ejemplo que guiaron cada paso de mi vida son mis amigos incondicionales, que con su apoyo y esfuerzo me han ayudado a cumplir con este objetivo.

.

Ana Orbe.

DEDICATORIA

Dedico este trabajo a mis hijas quienes me dieron todo su amor, apoyo y comprensión para alcanzar este objetivo.

Wilson Pancho.

TABLA DE CONTENIDO

INDICE DE FIGURAS

RESUMEN

El presente trabajo busca brindar una solución para el acceso a la red de FLACSO sede Ecuador a los usuarios que cuentan con un dispositivo inalámbrico WiFi.

Este documento se ha estructurado en 5 capítulos y cuatro anexos. En ellos se resumen las ideas más importantes y necesarias para el adecuado funcionamiento de una WLAN 802.11.

En el capítulo primero se redacta lo referente al marco teórico de la tecnología inalámbrica WiFi, en el segundo capítulo se analiza la situación actual de la red de la institución, en el tercer capítulo se realiza el diseño de la WLAN, el cuarto capítulo analiza la factibilidad de implementación de la WLAN, tomando tres aspectos: técnico, operativo y económico; finalmente el capítulo quinto presenta las recomendaciones y conclusiones.

Es deseo que este documento contribuya tanto a la formación como a la ayuda en la toma de decisiones por parte de los agentes involucrados, y que redunde en un beneficio para la institución.

INTRODUCCION

La Sede de FLACSO es un organismo internacional establecida en Ecuador desde 1975 mediante un acuerdo entre el Estado ecuatoriano y el sistema internacional de FLACSO.

Desde la década de los 80 se ha constituido en un centro de formación en el área de las ciencias sociales de estudiantes para un desempeño de excelencia en carreras académicas y en profesiones aplicadas.

La institución forma parte del sistema universitario ecuatoriano y fue reconocida por la Ley de Educación Superior en el año 2000.

El campus académico de FLACSO esta conformado por 9 pisos altos, el nivel 0 y un piso bajo (nivel -1) en el cual funciona un centro de convenciones que cuenta con acceso directo desde la calle, se compone de dos auditorios (capacidades 350 y 160 asientos), tres aulas magistrales de 60 personas cada una, 2 salas de sesiones y hall de exposiciones.

El edificio es moderno y su infraestructura cuenta con tecnología de punta, con conexiones de cableado estructurado de fibra y cable trenzado categoría 6, que brinda todas las facilidades de conexión y comunicación fija a todos los usuarios de la sede.

De acuerdo a la naturaleza del edificio concebido principalmente para la academia de ciencias sociales y afines, y tomando en cuenta la cantidad de eventos que se efectúan en su centro de convenciones, lo cual atrae gran cantidad de visitantes diarios locales, nacionales e internacionales, de variada ideología y formación, status social, religión, raza, etc.; que demandan de servicios de comunicación y acceso a la información en tiempo real sin las limitaciones que supone estar atado a una ubicación fija o por cable y contando con muy altas velocidades de conexión, es por ello que se debe pensar en soluciones rápidas y eficaces sin que para ello se tenga que modificar

ostensiblemente la arquitectura de la red de datos cableada implementada en la actualidad, además de las molestias que ocasionaría a los usuarios y visitantes las labores de construcción y adecuación de nuevos puntos de cable para el acceso a la red.

Una solución confiable es el acceso inalámbrico que mejorará la flexibilidad de la organización ya que el tamaño de la red se puede modificar con gran facilidad en función de la creciente demanda, además de facilitar la integración de nuevos dispositivos como los asistentes digitales personales (PDA) y Tablet PC, Ipaq, etc. Finalmente se debe considerar que el costo de dotar el acceso a la red, se reduce considerablemente.

La implementación de una red inalámbrica, se convierte en el complemento ideal de la red cableada permitiendo bajo ciertos criterios de administración y seguridad compartir los recursos y servicios que la sede brinda a sus usuarios, tales como, servicio de Internet continuo, eventos en línea, ventas de sus productos en línea, consulta de situación académica, administrativa y financiera de sus estudiantes.

Una WLAN combina la conectividad a la red de datos con la movilidad de los usuarios.

Este documento busca brindar una solución para esa creciente demanda de servicios de los usuarios continuos y ocasionales.

CAPITULO 1: MARCO TEORICO

El desarrollo tecnológico de las redes esta orientado a la consecución de mayor rapidez, eficiencia y seguridad en los procesos que se ejecutan y se comparten en ellas, así cómo a una mayor comodidad para el usuario y control de la naturaleza y el entorno.

Dentro del desarrollo tecnológico, es posible destacar los dos elementos que más han influido beneficiosamente en los últimos años[1]:

- La mejora del acceso, especialmente en sus componentes de capacidad y ubicuidad, representadas en particular por la banda ancha, las nuevas tecnologías de difusión y la movilidad.
- La interoperabilidad de redes y servicios, en particular mediante el empleo de los servicios abiertos y del paradigma IP.

  Son estos tres conceptos: banda ancha, movilidad y servicios abiertos los que van a marcar el éxito de una tecnología.

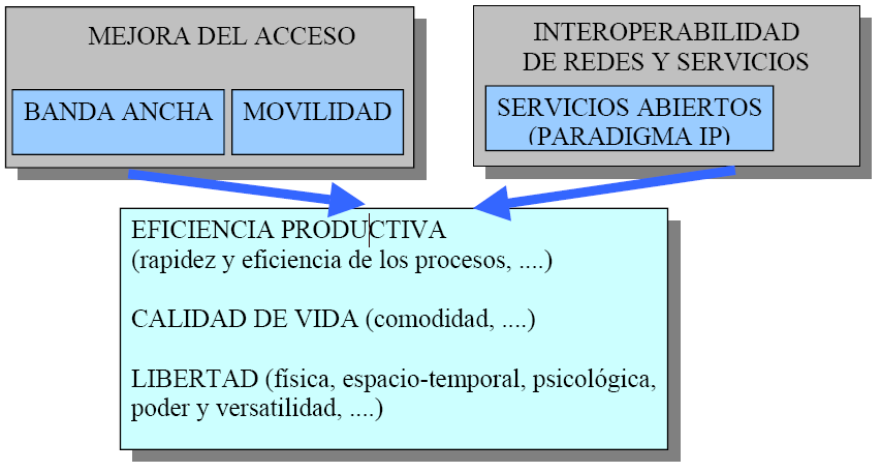


Figura 1.1: Objetivos tecnológicos actuales y beneficios que reportan

Las redes inalámbricas de área local (WLAN) cumplen cada vez un rol más importante en las comunicaciones actuales. Debido a su facilidad de instalación y conexión, se han convertido en una excelente alternativa para ofrecer

[1] La situación de las Tecnologías basadas en el estándar IEEE 802.11 variantes (“Wi-Fi”). Colegio Oficial de Ingenieros de Telecomunicación Grupo de Nuevas Actividades Profesionales

conectividad en lugares donde resulta inconveniente o imposible brindar servicio con una red alambrada. La utilización de las WLAN se ha hecho tan popular a tal punto que los fabricantes de computadores y motherboards están integrando dispositivos para su acceso en sus equipos; tal es el caso de Intel[2], que fabrica el chipset Centrino para computadores portátiles.

La tabla siguiente recoge las características más importantes de las tecnologías de acceso más exitosas, con el fin de poder compararlas de una forma rápida y destacar sus principales ventajas e inconvenientes.

Red	Normalización	Medio físico	Topología	Terminales	Alcance
Satélite	DVB, ETSI	Radio, 11-14 GHz(Ku) 20-30 GHz(Ka)	Multipunto	Fijos (móviles a pocos Kbit/s)	Visión directa
LMDS	IEEE.802.16	Radio, 3.5GHz, 26GHz y superiores	Multipunto	Fijos	Visión directa 3Km(26GHz) 8Km(2.5GHz)
LANs Inalámbricas (WLAN)	IEEE.802.11 ETSI	Radio, 2.4GHz(.11b y.11g), 5GHz(.11a)	Multipunto	Móviles	50-150 m
UMTS	3GPP	Radio, 1.7-2.2GHz	Multipunto	Móviles	50m-3Km
TV digital terrestre (TDT)	DVB, ETSI	Radio, 800MHz(UHF)	Multipunto	Fijos	32Km
Cable (HFC)	DOCSIS, DVB	Fibra y coaxial	Multipunto	Fijos	40Km
xDSL	ITU-T, ETSI	Par telefónico	Punto a punto	Fijos	300m-6Km
Fibra hasta X (FTTX)	FSAN, ITU-T	Fibra óptica sola o fibra y par telefónico	Punto a punto o multipunto (PON)	Fijos	20Km
Ethernet 1a milla (EFM)	IEEE.802.3ah	Par telefónico o fibra	Punto a punto o multipunto (PON)	Fijos	750m-2.7Km (sobre par telefónico)
Power line comm.(PLC)	PLC forum, CENELEC, ETSI	Red eléctrica (segmento de baja tensión)	Multipunto	Fijos	200m

Tabla 1.1: Características más importantes de las tecnologías de acceso

[2] Intel Centrino Mobile Technology. http://www.intel.com/products/mobiletechnology/

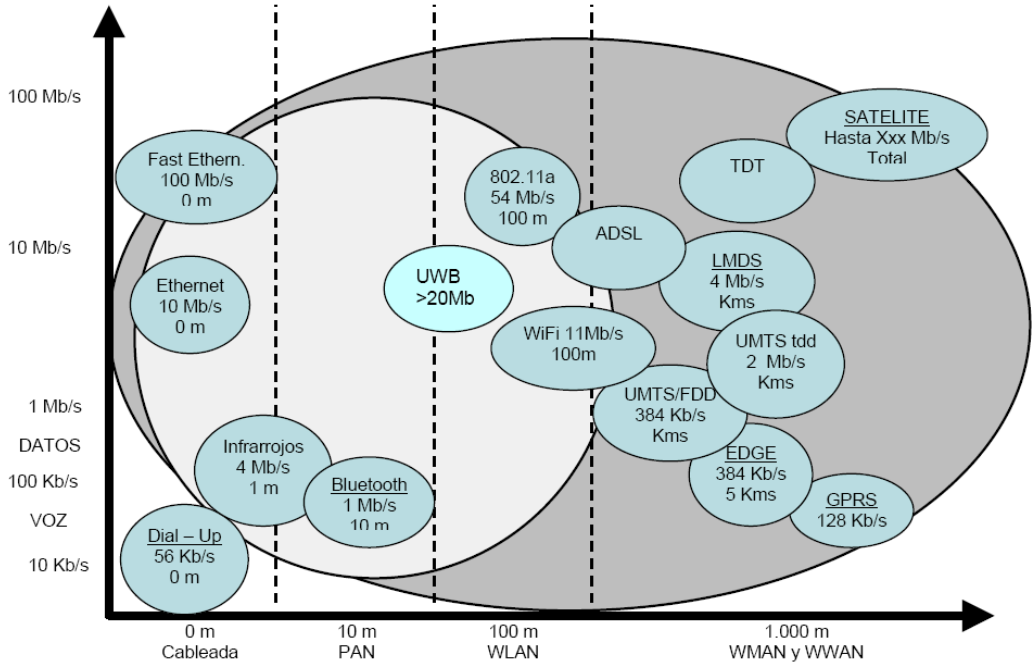


Figura 1.2: Posicionamiento de las distintas tecnologías de acceso

La figura 1.2, brinda una idea del posicionamiento de las tecnologías de acceso en base a dos parámetros como son el alcance y la capacidad de transmisión que puede lograrse a través de radio frecuencia. Estos parámetros están ligados al diseño e implementación de la red en su totalidad y del uso que se hace de la misma.

1.1. TECNOLOGÍA INALÁMBRICA

El uso de tecnología inalámbrica ha tenido un crecimiento agresivo en los últimos años, debido a la creciente necesidad de permitir el acceso a la información desde cualquier sitio físico ya sea al interior o exterior de una organización, sin tener los limitantes de una ubicación fija y sin ataduras a cables.

En la actualidad la tecnología inalámbrica es usada por millones de personas a nivel mundial, y el uso que se da a las redes con acceso inalámbrico es

variado, encontrando redes en sitios de acceso tanto público (bibliotecas, aeropuertos, estaciones de buses, supermercados, etc.) como privado (universidades, pequeñas y medianas empresas, etc.).

El fundamento de las redes inalámbricas es la radiodifusión. La primera red inalámbrica fue desarrollada en la Universidad de Hawai en 1971 para enlazar ordenadores de cuatro islas sin utilizar cables de teléfono. ALOHANET fue el primer sistema creado para enviar paquetes de datos a través de radios con una velocidad de operación de 9600 bps.

En los años 80 entraron en el mundo de los ordenadores personales las redes inalámbricas, debido a la popularidad de la idea de compartir datos, algunas de las primeras redes inalámbricas no utilizaban ondas de radio, sino que utilizaban transceptores de infrarrojos. Lastimosamente los infrarrojos no tuvieron el despunte necesario puesto que tenían limitantes de velocidad, distancia y que no podía atravesar objetos físicos, es decir se necesitaba un paso libre entre los dispositivos para que puedan transmitir, limitante que hasta la actualidad se mantiene.

En 1985 se comercializa la tecnología gracias a los cambios en las regulaciones de la parte 15 de la FCC[3] que permitieron el uso de radios a través del espectro extendido en las aplicaciones comerciales.

Telesystems SLW fue creada una año más tarde que se efectuaron los cambios en la regulación del FCC, para explotar este desarrollo. El sistema desarrollado por Telesystems en realidad era de espectro extendido, en realidad usaba una variación, en lugar de hacer que una señal de banda angosta saltara de una frecuencia a la siguiente a través de un ancho de banda establecido empleo un sistema que se conoce como secuencia directa, donde una señal de banda angosta se extiende a través del ancho de banda determinado al multiplicar el ancho de la señal a través de un conjunto de frecuencias más grande (Anexo I).

[3] Comisión Federal de Comunicaciones (Federal Communications Comisión)

En 1988 se introduce el primer sistema comercial basado en tecnología de secuencia directa en el espectro extendido DSSS[4], que operaba en la banda sin licencia establecida por la FCC en los 902 y 928 Mhz. Lastimosamente la banda de los 900 Mhz, era una frecuencia sin licencia únicamente en Estados Unidos, Canadá y Australia por lo que luego y por razones de globalizar su uso se utilizo la banda sin licencia en Europa y Japón de los 2.46 Mhz.

Las LAN inalámbricas basadas en radio se iniciaron en los 90, lastimosamente su implementación era costosa y eran de productos propietarios lo que provocaba la incompatibilidad entre ellos, por ende no se podían comunicar, debido a ello a mediados de los 90 la atención se centro en el naciente estándar 802.11 que fue ratificado recién en 1997 por la IEEE.

Existen 3 especificaciones para las WLAN. El 802.11b que es el estándar de redes inalámbricas más común en todo el mundo; Bluetooth que es un reemplazo del sistema de cable de corto alcance que no consume mucha batería; y HomeRF, orientado al pequeño consumidor de unir teléfonos inalámbricos, dispositivos multimedia, controles de televisión por cable e Internet.

1.1.1. HOMERF

Es un estándar desarrollado por el grupo HRFWG[5]. Está basada en el Protocolo de Acceso Inalámbrico Compartido SWAP[6], que define una interfaz inalámbrica diseñada para soportar voz y datos. Utiliza salto de frecuencias FHSS[7] en la banda de los 2.4 Ghz., la misma banda de frecuencia que los estándares 802.11b y 802.11g, pero como cuenta con el método de salto de frecuencia SWAP no interfiere con conexiones Bluetooth.

---

[4] Espectro extendido por secuencia directa (Direct Sequence Spread Spectrum)
[5] HomeRF Working Group, encargado de mantener interoperatibilidad entre productos de diferentes empresas.
[6] Shared Wireless Access Protocol
[7] Espectro extendido por salto de frecuencia (Fecuency Hopping Spread Spectrum)

Entre las características técnicas de este estándar se menciona que añade un subconjunto de estándares DECT[8], para proporcionar los servicios de voz (hasta seis conversaciones).

Corresponde a una tecnología inalámbrica de hogares, desarrollada principalmente en Europa. La idea es comunicar teléfonos inalámbricos, ordenadores o electrodomésticos simultáneamente con fiabilidad a través de la misma red sin la necesidad de utilizar cable.

Su desarrollo al contrario de las otras tecnologías inalámbricas toma el camino opuesto es decir va de voz a datos, es por ello que se convierte en el único estándar que puede transportar el tráfico de voz con la calidad de llamadas telefónicas normales, brindando capacidades como: identificador de llamadas, llamadas en espera, regreso de llamadas e intercomunicación dentro del hogar. Esto se atribuye directamente a que el estándar se basa en un estándar de voz desarrollado por las compañías telefónicas.

Para la transmisión utiliza una combinación de CSMA/CD[9] para los datos en paquetes y TDMA[10] para el tráfico de voz y vídeo, con el fin de optimizar el flujo del tráfico sobre una base principal.

La capa física utiliza la modulación por frecuencia FSK[11], que proporciona velocidades entre 800 Kbps y 1.6 Mbps en la banda de 2.4 Ghz.

Para la seguridad usa un cifrado de 128 bits, aumentado por medio de la mejora en la seguridad original de la modulación FHSS en la capa física. Esta combinación debe proporcionar un nivel alto de resistencia a los ataques de denegación de servicio.

---

[8] Digital Enhanced Cordless Telecommunications
[9] Carrier Sense Multiple Access with Collision Detection
[10] Time Division Multiple Access
[11] Frequency Shift Keying

Su alcance es de alrededor de 50 metros, consiguiendo unas velocidades de transferencia que pueden llegar hasta los 2 Mbps, conectando un total de hasta 127 dispositivos.

Se intento el estándar HomeRF2 que usa 15 canales de Mhz. para canales de 5 y 10 Mbps, en la capa física incluye el salto de frecuencia inteligente para evitar la residencia de transmisiones en canales que están muy congestionados debido a la interferencia. Lastimosamente no hubo mucha inversión en esta tecnología por parte de los constructores

1.1.2. BLUETOOTH

Se considera como un estándar cerrado, puesto que las empresas que brindan soporte para el estándar están encerradas en torno a las compañías de desarrollo principales, como es el caso de IBM que es el patrocinador principal de Bluetooth.

Es un estándar de red ad – hoc de corto alcance que utiliza la misma banda de 2.4 Ghz que el estándar 802.11b, diseñado para ir a una velocidad de 1 Mbps o con un rendimiento de red de 700 Kbps. Pese a ser un estándar de WLAN, se tiene la errada idea de que compite con los otros estándares HomeRF y 802.11, pues no es así ya que su principal objetivo es la conectividad de dispositivos en un rango pequeño de hasta 5 metros con velocidades de datos lentas.

Utiliza el salto de frecuencias en lugar de secuencia directa, trabaja en el rango de frecuencias de 2,402 GHz a 2,480 GHz. Se trata de una banda de uso común que se puede usar para aplicaciones ICM y que no necesita licencia.

La primera versión de Bluetooth, transfiere datos de forma asimétrica a 721 Kbps. y simétricamente a 432 Kbps. Se puede transmitir voz, datos e incluso vídeo. Para transmitir voz son necesarios tres canales de 64 Kbps. Para transmitir vídeo es necesaria la compresión a formato MPEG-4 y usar 340 Kbps

para conseguir refrescar 15 veces por segundo una pantalla VGA de 320x240 puntos.

Los dispositivos cambian de frecuencia 1600 veces por segundo, lo que lo hace un estándar muy resistente a las interferencias y obstrucciones, y permiten que muchos tranceptores en especial del estándar HomeRF, funcionen en el mismo espacio sin interferirse unos con otros.

El principal propósito es conectar computadoras portátiles con teléfonos celulares, PDA con computadoras portátiles y teléfonos celulares. Su limitante es la velocidad de 1.5 Mbps., lo que equivale aproximadamente una décima parte de la velocidad del estándar 802.11b y una fracción de la velocidad que ofrecen los estándares 802.11a y 802.11g.

Tiene 2 puntos fuertes:

1. Tamaño. Le permite instalarse en relojes de mano, PDA y otros dispositivos electrónicos pequeños, en los que el tamaño es un criterio de diseño importante.
2. Ahorro de energía. Utiliza 30 microamperes, que representa una cantidad mínima de energía, esta característica permite a la industria crear dispositivos, como auriculares inalámbricos, basándose en la cantidad de energía que se requiere de una batería, para proporcionar un período de operación continua y para alargar la vida de los ordenadores de bolsillo, los móviles y otros tipos de aparatos que pueden trabajar con chip bluetooth incrustados.

Bluetooth es un enlace de radio de corto alcance que aparece asociado a las Redes de Área Personal Inalámbricas o WPAN[12]. Este concepto hace referencia a una red sin cables que se extiende a un espacio de funcionamiento personal con un radio de hasta 10 metros.

[12] Wireless Personal Area Network

Las WPAN constituyen un esquema de red de bajo costo que permite conectar entre sí equipos informáticos y de comunicación portátil y móvil, como ordenadores, PDAs, impresoras, ratones, micrófonos, auriculares, lectores de código de barras, sensores, displays, localizadores, teléfonos móviles y otros dispositivos de electrónica de consumo. El objetivo es que todos estos equipos se puedan comunicar e ínter operar entre sí sin interferencias.

1.1.3. ESTÁNDAR 802.11

En 1997 el IEEE adopto el estándar 802.11 y se convirtió en el primer estándar WLAN. La certificación Wi-Fi de la Alianza de compatibilidad de Ethernet inalámbrico WECA (Wireless Ethernet Compatibility Alliance) que es una organización internacional, sin ánimo de lucro, formada en 1999 para certificar la interoperabilidad de productos inalámbricos de WLAN basados en la especificación del IEEE 802.11. El objetivo de los miembros de la Wi-Fi Alliance es enriquecer la experiencia de los usuarios a través de la interoperabilidad de sus productos.

Figura 1.3: Logotipo y etiquetado de certificación de productos de la Wi-Fi Alliance

Este estándar abarca la mayor parte del mercado de tecnología inalámbrica, por que a captado la atención de los proveedores principales de esta tecnología, puesto que de los estándares vistos anteriormente es el único que

soporta realmente banda ancha, esto se debe a que el desempeño es superior al de los otros. El estándar 802.11 tiene un conjunto de variantes: 802.11a, 802.11b, 802.11d, 802.11e, 802.11f, 802.g, 802.11h, 802.11i. En la tabla 1.2 se muestra un cuadro con las principales características de las variantes del estándar 802.11[13].

Estándar	Frecuencia portadora	Velocidad de datos	Resumen
802.11a	5.1 – 5.2 Ghz 5.2 – 5.3 Ghz 5.7 – 5.8 Ghz	54 Mbps	La potencia máxima es 40 mW en la banda 5.1, 250 mW en la banda 5.2 y 800 mW en la banda 5.7 (En Estados Unidos)
802.11b	2.4 – 2.485 Ghz	11 Mbps	Es el estándar que más se vende
802.11d	N/D		Múltiples dominios reguladores
802.11e	N/D	N/D	Calidad de servicio
802.11f	N/D	N/D	Protocolo de conexión y de puntos de acceso IAPP
802.11g	2.4 – 2.485 Ghz	36 o 54 Mbps	
802.11h	N/D	N/D	Selección dinámica de frecuencia DFS
802.11i	N/D	N/D	Seguridad

Tabla 1.2: Tabla de estándares IEEE 802.11

802.11 controla principalmente las capas 1 y 2 del modelo OSI, capa física y capa de enlace respectivamente.

1.1.3.1. Capa MAC de 802.11

La principal característica del estándar 802.11 es la movilidad, es decir la facilidad de un usuario de moverse de un punto de acceso a otro y seguir conectado a la red.

La capa MAC controla aspectos de movilidad en las WLAN 802.11. Realiza funciones de capas superiores tales como: controla el inicio y fin de sesión (función de la capa 5 en la pila OSI); seguridad (función de la capa 6 en la pila OSI), para ello utiliza la privacidad equivalente al cableado WEP que es un método que maneja claves y cifrado de datos.

[13] 802.11 Manual de redes inalámbricas, Neil Reid y Ron Seide

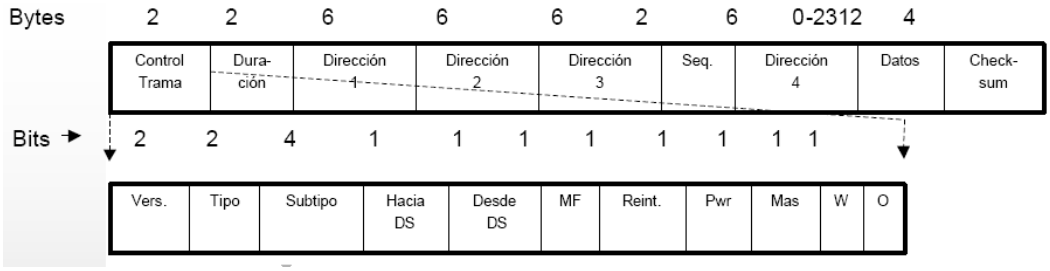


Figura 1.4: Trama 802.11

Vers.: Permite la coexistencia de varias versiones del protocolo
Tipo: Indica si se trata de una trama de datos, de control o de gestión
Subtipo: Indica por ejemplo si es una trama RTS o CTS
Hacia DS, Desde DS: Indica los AP de origen y destino en caso de ruta por un ESS
MF: Indica que siguen más fragmentos
Reint.: Indica que esta trama es un reenvío
Pwr: Para 'dormir' o 'despertar' a una estación
Mas: Advierte que el emisor tiene más tramas para enviar
W: La trama está encriptada con WEP (Wireless Equivalent Privacy)
O: Las tramas que tiene puesto este bit se han de procesar por orden
Duración: Dice cuanto tiempo va a estar ocupado el canal por esta trama
Dirección 1,2,3,4: Dirección de origen(1), destino(2), AP origen (3) y destino(4)
Seq.: Número de secuencia (cuando la trama es un fragmento)

La capa MAC es un subconjunto de la capa de enlace y controla la conectividad de 2 o más puntos a través de un esquema de direcciones, a su vez es adyacente a la capa física en una red basada en IP.

La capa 1 en una red 802.11 realiza tres funciones esenciales:

1. Funciona como interfaz entre la capa MAC entre 2 o más dispositivos.
2. Realizan la detección de los sucesos CSMA/CD
3. Efectúan la modulación y demodulación de la señal. El esquema de modulación puede ser DSSS o FHSS.

Maneja la "técnica de cambio de velocidad" debido a cambios de distancia, calidad y fuerza de la señal, en la modulación DSSS la velocidad de transmisión varia desde 1 a 11 Mbps, y la modulación por FHSS varia de 1 a 2 Mbps.

En las redes Ethernet tradicionales (IEEE 802.3) el protocolo de acceso al medio es CSMA/CD (Carrier Sense Multiple Access/ Collision Detection): en este entorno cuando una estación va a transmitir, primero escucha el medio de transmisión para determinar si éste está o no en uso. Si el medio está en uso, la estación difiere su transmisión. Si el medio no está en uso la estación transmite. Si dos estaciones escuchan el medio, comprueban que está vacío y transmiten al mismo tiempo, entonces se producirá una colisión. Si se detecta una colisión las estaciones involucradas esperarán un tiempo aleatorio y volverán a intentar transmitir.

En las redes WLAN (IEEE 802.11) el protocolo de acceso al medio es CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance): dada la dificultad que existe en el medio RF para detectar colisiones, el mejor modo de proceder es evitarlas. El acceso al medio se produce de la siguiente manera: Cuando una estación desea transmitir (ya sea un PC inalámbrico o el Access Point), el nivel físico trabaja conjuntamente con el nivel MAC muestreando la energía presente en el medio a la frecuencia de transmisión. La capa física utiliza un algoritmo denominado Clear Channel Assessment (CCA) para determinar si el canal está libre. Para ello compara la energía medida con un determinado umbral. Si esta energía medida está por encima del umbral entonces la transmisión es diferida según las reglas del estándar. Si está por debajo de ese umbral, entonces se considera que el canal está disponible para la transmisión.

Una vez verificado que el medio de transmisión está libre se procede a comprobar que la transmisión se ha completado sin errores, para lo cual existen dos técnicas, que son las siguientes:

a. MAC – Level Acknowledgement: Después de recibir un mensaje completo, la estación receptora debe transmitir una señal de ACK a la estación originadora del mensaje dentro de un determinado margen de tiempo SIFS (Short Inter Frame Space, 10 ms), para verificar que la transmisión ha sido correcta.

La señal de ACK sólo se envía cuando se ha completado una transmisión correctamente. Esta manera de proceder proporciona muy poca sobrecarga de tráfico y es el modo de trabajo recomendado en las WLANs pequeñas. Su principal inconveniente es que no garantiza que no se vaya a producir colisión en el medio de transmisión: pueden aparecer problemas de interferencias o de incapacidad para que una estación detecte la portadora puesta en el medio por otra estación.

Este fenómeno, denominado “Estación Oculta” se puede llegar a producir en configuraciones en las que la WLAN abarque un área física grande (especialmente en exteriores).

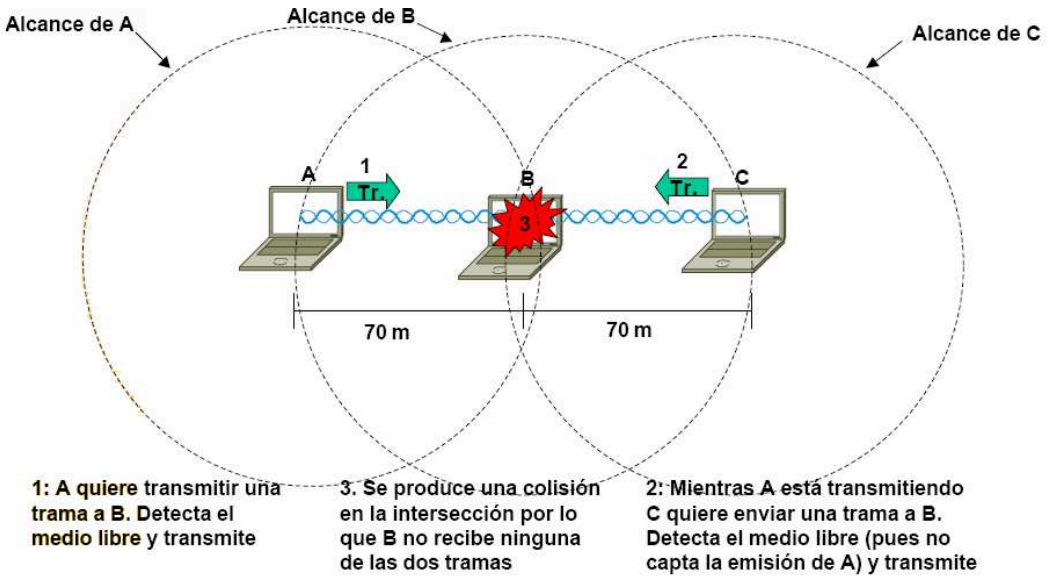


Figura 1.5: Problema de la solución oculta[14]

b. Request-To-Send/Clear-To-Send (RTS/CTS): La comunicación se establece cuando uno de los nodos inalámbricos envía una trama Request-To-Send (RTS). La trama RTS incluye la estación de destino y la longitud del mensaje que se desea transmitir. A partir de la longitud del mensaje se determina cuál será el tiempo que durará la transmisión. La longitud del mensaje se conoce como NAV (Network Allocation

[14] Diego Gachet, Seminario de redes inalámbricas, Escuela Politécnica del Ejército, 2005

Vector). A la recepción de un RTS, la estación receptora envía una trama Clear-To-Send (que contiene la dirección de la estación que envió la trama RTS y el NAV) a la estación que solicitó permiso para transmitir y que, además, alerta al resto de las estaciones de que se va a producir una transmisión y que durante el tiempo que equivale al NAV deben permanecer "en silencio", sin hacer intento de transmitir. Una vez completada la transmisión, el receptor envía una trama de ACK para verificar que se ha completado con éxito la transmisión.

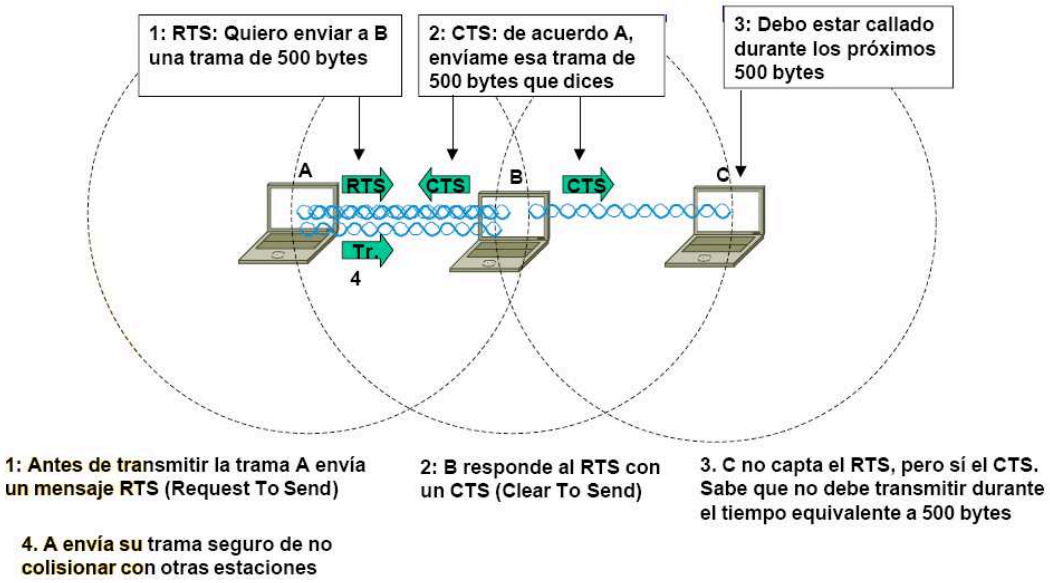


Figura 1.6: Utilización de RTS/CTS para soluciones el problema de la estación oculta[15]

El inconveniente que plantea este procedimiento de transmisión es que añade una gran cantidad de sobrecarga al tráfico de datos. Dado que en el modo de operación normal de una WLAN la mayor parte de las comunicaciones se realizan desde el AP al resto de las estaciones, la presencia de nodos ocultos no será habitualmente un problema grave. Por ello el modo de operación RTS/CTS sólo es utilizado cuando es absolutamente indispensable.

1.1.3.2. IEEE 802.11b

[15] Diego Gachet, Seminario de redes inalámbricas, Escuela Politécnica del Ejército, 2005

Es conocido con el nombre de marca registrada WiFi fidelidad inalámbrica (Wireless Fidelity). Esta estándar se ha convertido en la tecnología de red inalámbrica dominante que se utiliza ampliamente, es fácil de configurar y no tiene costos de espectro, se puede encontrar este tipo de red inalámbrica en oficinas, espacios públicos y hogares.

El comité IEEE 802 se ocupa de las redes; el grupo de trabajo 802.11 se ocupa de las redes de área local inalámbricas (WLAN); y los distintos grupos de tareas (a, b, e, g, h, i) se ocupan de tipos concretos de WLAN o de problemas específicos, como la comunicación entre puntos de acceso y la seguridad. 802.11 utiliza la banda sin licencia de 2.4 Ghz

Las velocidades que admite el 802.11b son: 11 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps y 512 Kbps, va disminuyendo debido a las interferencias que impiden que los datos lleguen a su destino.

WI-Fi es muy similar a ethernet con cable, solo difiere en la parte de la especificación dedicada a la física de movimiento de bits de un lado a otro utilizando señales de radio en lugar de electrones en un cable físico.

1.1.3.3. IEEE 802.11a

Conocido también como WiFi5, fue ratificado como estándar en 1999, utilizando la frecuencia de los 5 Ghz y utiliza la técnica de modulación de radio OFDM[16]. Esta técnica divide una portadora de datos de alta velocidad en 52 subportadoras de baja velocidad que se transmiten en paralelo. Estas subportadoras se pueden agrupar de un modo mucho más integrado que con la técnica de espectro que utiliza el estándar 802.11b.

También se utiliza esta técnica con el estándar WiMax, que es una especificación para redes metropolitanas inalámbricas (WMAN) de banda ancha, que corresponde al estándar 802.16x, promovido por el grupo de la

[16] Ortogonal Frequency Division Multiplexing

industria WiMax (Worldwide Interoperaability for Microwave Access o interoperabilidad global para acceso por microondas), cuyo miembros más representativos son Intel y Nokia. Al igual que sucede con el estándar Wi-Fi, garantiza la interoperabilidad entre distintos equipos.

La diferencia entre estas dos tecnologías inalámbricas está en su alcance y ancho de banda. Mientras que WiFi está pensado para oficinas o dar cobertura a zonas relativamente pequeñas, WiMax es una red que conecta Hot-spots de Wi-Fi, y/o provee una extensión inalámbrica de última milla para instalaciones de cable y DSL al menor costo. Este estándar provee un área de servicio de hasta 50 km lineales y permite conectividad sin línea de vista directa a la estación base. Permite transmisión de hasta 70 Mbps. Mientras que la tasa de transferencia de WiFi es de 11 Mbps y la distancia de hasta 350 metros en zonas abiertas.

802.11a difiere en los siguientes aspectos del 802.11b:

- Usa la banda de 5 GHz
- Tiene 12 canales que no solapan
- La velocidad es de 54 Mbps
- Funciona en distancias más cortas pero tiene mejores protocolos para clasificar la retención de señales en interior.

Ventajas:

- Permite que un número mayor de usuarios aproveche todo el ancho de banda en el mismo espacio físico, ya que tiene los 12 canales no solapados y la banda de 5 GHz no está siendo utilizada por muchos otros dispositivos inalámbricos.
- Un mayor rendimiento y menor solapamiento de canales significa que el 802.11a podría reemplazar o ampliar las redes Ethernet convencionales.
- Varios fabricantes han empezado a lanzar puntos de acceso que combinan el 802.11a y el 802.11b y pueden gestionar el tráfico utilizando simultáneamente los dos estándares.

1.1.3.4. IEEE 802.11g

Basado en el estándar 802.11b, fue aprobado a mediados del año 2003. Más avanzada que su antecesora, trabaja sobre la misma frecuencia de los 2,4 GHz y es capaz de utilizar dos métodos de modulación (DSSS y OFDM), lo que la hace compatible con el estándar de facto en esta industria. Es capaz de incrementar notablemente la velocidad de transmisión, llegando hasta los 54 Mbps que oferta la norma 802.11a, manteniendo las características propias del 802.11b en cuanto a distancia, niveles de consumo y frecuencia utilizada.

En la tabla 1.3 se muestran las ventajas y desventajas de las variantes 802.11a y 802.11g.

	802.11a	**802.11g**
Desempeño	Ventaja: Sólo OFDM, banda de 5 Ghz y la ausencia de células mixtas proporciona una mejor capacidad de salida	Desventaja: Soporte para los estándares elevados, células mixtas y la operación en la banda de 2.4 Ghz que podría estar potencialmente saturada, lo cual posiblemente daría como resultado una capacidad de salida ligeramente menor que la de 802.11ª
Capacidad	Ventaja: Con ocho canales, proporciona una capacidad agregada de 432 Mbps (54 Mbps multiplicados por 8 canales)	Desventaja: Con solo tres canales, proporciona una capacidad teórica agregada de 162 Mbps (54 Mbps multiplicado por 3 canales)
Rango	Desventaja: Una longitud de onda más corta y restricciones reguladoras en la potencia de transmisión y la ganancia de la antena que deterioran el rango de 802.11ª	Ventaja: A pesar de que no proporcionará el mismo rango que 802.11b debido a las velocidades de datos más altas, la física y regulaciones en la banda de 2.4 Ghz permiten un rango más grande que cuando se opera en la banda de 5 Ghz
Interferencia	Ventaja: Las LAN 802.11a inalámbricas operan en las bandas de 5 Ghz que son relativamente grandes, pero aún así están saturadas	Desventaja: Las bandas que no requieren de licencia de 2.4 Ghz son relativamente pequeñas y se están saturando con las LAN inalámbricas, teléfonos inalámbricos y, potencialmente, dispositivos Bluetooth
Migración	Desventaja: Operando a 5 Ghz y proporcionando soporte solo para la transmisión OFDM, no	Ventaja: Al operar en la banda heredada de 2.4 Ghz y soportar DSSS, proporciona la

	proporciona compatibilidad con dispositivos anteriores de 802.11b	característica importante de la compatibilidad con productos anteriores de 802.11b
Flexibilidad de instalación	Desventaja: las regulaciones FCC que se aplican a los cuatro canales inferiores de 802.11a restringen a los fabricantes al uso exclusivo de antenas integradas que no se pueden desconectar	Ventaja: Al igual que 802.11b, permite antenas de 2.4 Ghz auxiliares que pueden estar directamente conectadas o conectadas por cables
Operación a lo largo de todo el mundo	Desventaja: Operación en los países apegados a FCC y Japón, pero aún no se define en Europa	Ventaja: La operación libre de licencia en, prácticamente, todo el mundo

Tabla 1.3: Ventajas y desventajas de 802.11a y 802.11g

1.1.3.5. IEEE 802.11e

Implementa la característica de calidad de servicio (QOS). Capacidad para garantizar la transmisión coherente de los datos, esto es necesario cuando se envía video o se realiza llamadas de teléfono IP. Esta especificación, es aplicable tanto a 802.11b como a 802.11a.

1.1.3.6. IEEE 802.11f

Básicamente, es una especificación que funciona bajo el estándar 802.11g y que se aplica a la intercomunicación entre puntos de acceso de distintos fabricantes, permitiendo el roaming o itinerancia de clientes.

1.1.3.7. IEEE 802.11h

Adaptabilidad. Garantiza que solo se transmitirá en las frecuencias que no están siendo utilizadas por otros transmisores y un control automático de potencia para minimizar los efectos de posibles interferencias.

1.1.3.8. IEEE 802.11i

Acceso Wi-Fi protegido WPA. Este estándar permite incorporar mecanismos de seguridad para WLAN, ofrece una solución interoperable y un patrón robusto

para asegurar datos. Corrige el sistema de cifrado incompleto WEP del 802.11b. Se trata de un complemento de seguridad desarrollado para 802.11a, 802.b y 802.11g, destinado a mejorar el nivel de protección de las WLAN.

1.1.3.9. IEEE 802.11n

Es un estándar nuevo, permitiendo velocidades mínimas de 100 Mbps y tiene previsto operar en la banda de frecuencia de los 5 Ghz y esto promete rangos superiores en comparación con los estándares anteriores.

1.1.4. HIPERLAN/2

Este es el nombre que se le ha dado a la nueva generación de la tecnología WLAN desarrollada por ETSI[17]. Se trata de un sistema de comunicación inalámbrica basado en ATM ("Asynchronous Transfer Mode"), similar a UMTS ("Universal Mobile Telecommunications System"), lastimosamente no incorpora características como QoS ("Quality of Service"), orientación de la conexión para obtener una mayor eficiencia en la utilización de los recursos de radio, búsqueda automática de la frecuencia a utilizar, y sobre todo una elevada velocidad de transmisión, que actualmente puede llegar hasta los 54 Mbps.

Esta tecnología opera sobre la banda de frecuencia de los 5 GHz y utiliza el método de modulación OFDM al igual que ocurre con el estándar 802.11a, manteniendo de igual manera un radio de alcance similar.

1.2. TOPOLOGÍAS WLAN

El elemento fundamental en la arquitectura de las redes 802.11 es la "celda", la cual se puede definir como el área geográfica en el cual una serie de dispositivos se interconectan entre sí por un medio aéreo. Por lo general, esta celda esta compuesta por estaciones y un único punto de acceso.

[17] "European Telecommunications Standards Institute", un organismo similar al IEEE pero a nivel europeo

Las celdas individuales se pueden superponer de manera que se permita una comunicación continua con la LAN cableada, dentro de un entorno determinado. La responsabilidad de los AP será la de hacer "hand off" de los usuarios a medida que se desplazan por el área geográfica de cobertura.

El punto de acceso es el dispositivo que gestiona todo el tráfico generado por las estaciones y que puede comunicarse con otras celdas o redes. Se constituye en un puente que funciona en la capa 2 (subcapa enlace en el modelo OSI), tanto de su celda de cobertura, como a otras redes a las cuales estuviese conectado. A esta estructura se le denomina Grupo de Servicio Básico BSS ("Basic Service Set").

Es posible realizar una configuración en la que existan múltiples AP en la misma red inalámbrica, siempre que estén ajustados a una frecuencia tal que no se interfieran. Tal como se comentó con anterioridad, al utilizar DSSS las características de la modulación empleada son tales que, para que no haya interferencia entre 2 AP adyacentes sus frecuencias de transmisión deben estar separadas 5 canales.

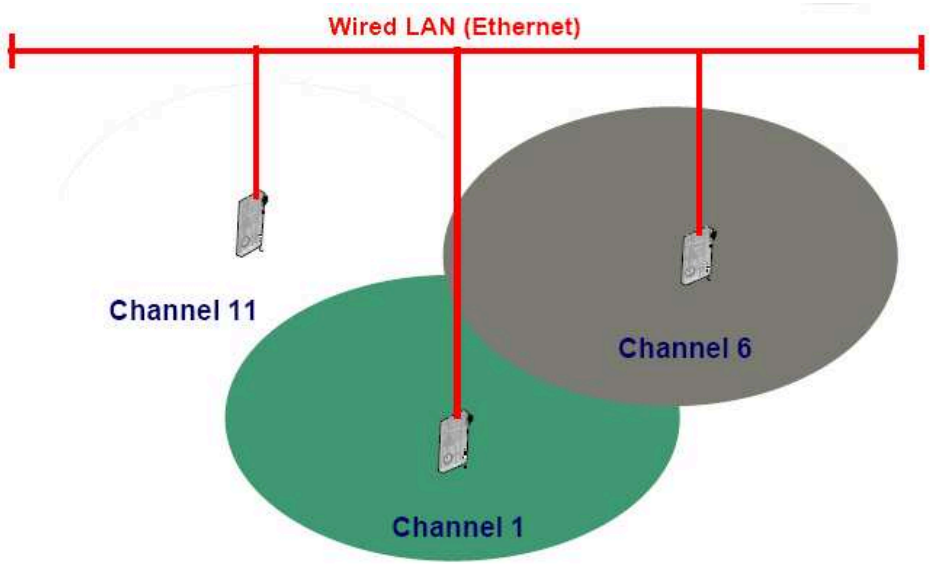


Figura 1.6: WLAN Multicelda[18]

[18] Tecnología de Redes de Área Local Inalámbricas. WLAN. KERN DATANET S.A. Grupo TELINDUS. http://www.kerndatanet.com

El BSS se constituye en una entidad independiente que puede conectarse con otros BSS a través del punto de acceso mediante un Sistema de Distribución (DS, “Distribution System”). El DS comunica el BSS con una red externa generalmente través de cable como por ejemplo una red Ethernet fija, o también inalámbrica, en cuyo caso se denomina Sistema de distribución inalámbrica (“Wireless Distribution System”).

Sobre este concepto básico surge una serie de alternativas de topologías de red inalámbrica:

1.2.1. BSS INDEPENDIENTE (IBSS, “INDEPENDENT BASIC SERVICE SET)

Es una celda inalámbrica en la cual no hay sistema de distribución y, por tanto, no tiene conexión con otras redes.

1.2.2. MODO AD-HOC.

Se constituye en una red independiente que conecta un conjunto de PCs que tienen instalado un adaptador inalámbrico. Cada vez que dos o más adaptadores inalámbricos están uno en el rango del otro, pueden establecer una red independiente que les permita compartir recursos, como unidades de disco, o intercambiar ficheros, algo similar a cuando se utiliza cable ethernet cruzado entre dos puertos de dos ordenadores. Este tipo de redes normalmente no requieren administración ni preconfiguración alguna.

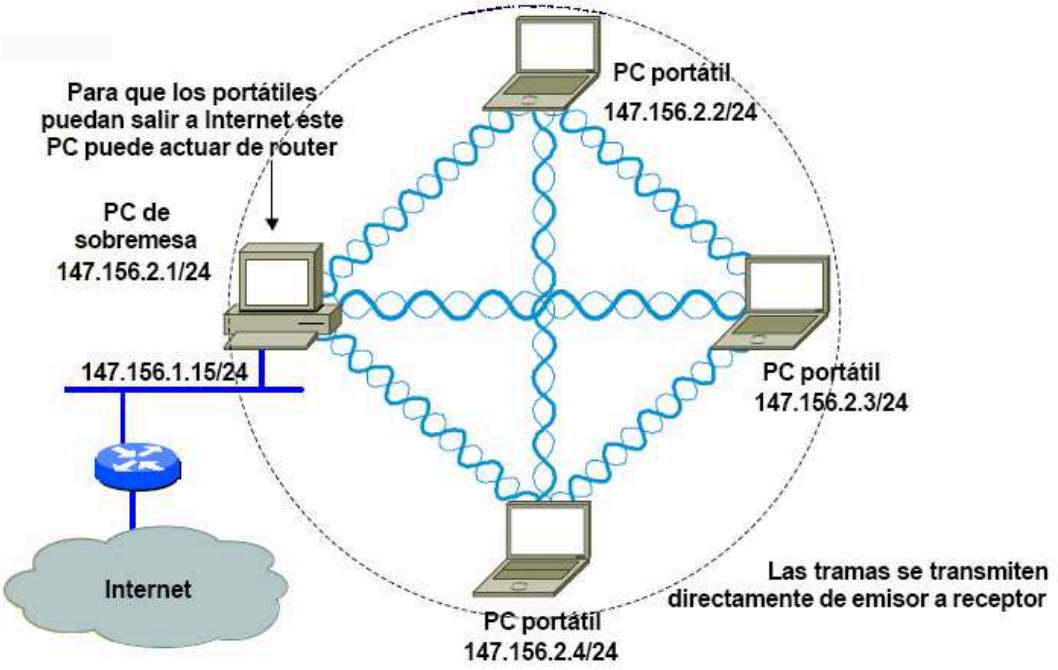


Figura 1.7: WLAN ad-hoc19

Es una variante del IBSS en el cual no hay punto de acceso. Las funciones de coordinación pueden ser asumidas de forma aleatoria por una de las estaciones presentes. El tráfico de información se lleva a cabo directamente entre los dos equipos implicados, sin tener que recurrir a un dispositivo que controle y coordine el acceso (Punto de acceso). La cobertura esta determinada por la distancia máxima entre dos equipos.

1.2.3. MODO INFRAESTRUCTURA

El punto de acceso realiza las funciones de coordinación. Todo el tráfico atraviesa el punto de acceso, razón por lo que se da una pérdida de eficiencia cuando dos estaciones dentro de un mismo BSS desean comunicarse entre sí. Es la arquitectura más generalizada cuando la mayor parte del tráfico se origina o finaliza en las redes externas a las cuales está conectado el punto de acceso.

La cobertura alcanza una distancia aproximada de el doble de la distancia máxima entre punto de acceso y estación.

---

[19] Diego Gachet. Redes inalámbricas de área local. Seminario de Telecomunicaciones. Escuela Politécnica Nacional. 2005

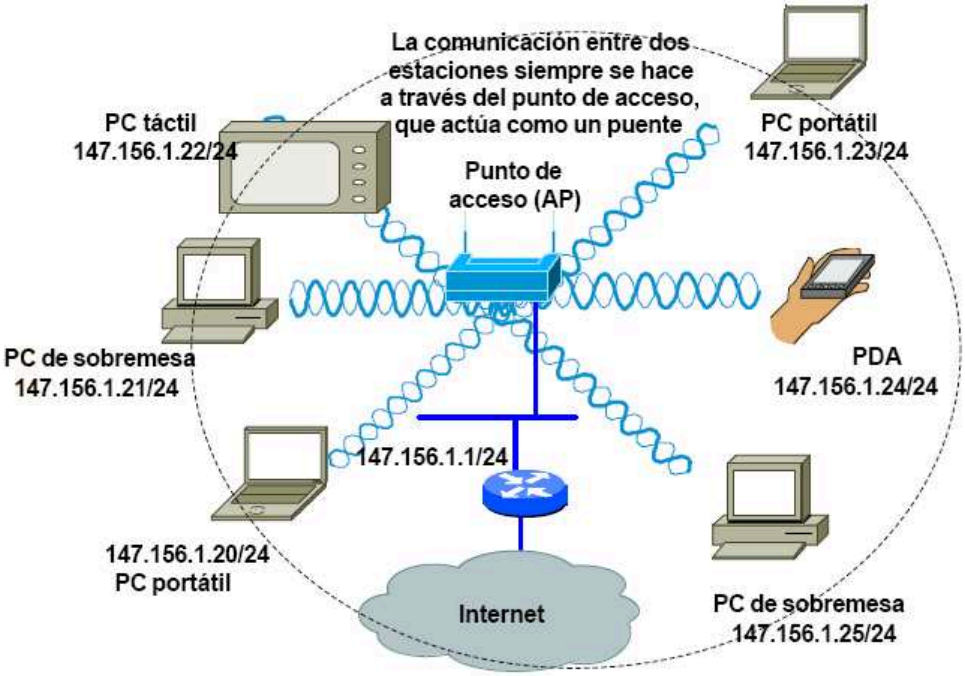


Figura 1.8: WLAN de infraestructura[20]

1.2.4. BSS EXTENDIDO (ESS, "EXTENDED SERVICE SET")

Es un caso específico del modo infraestructura, representado por un conjunto de BSS asociados mediante un sistema de distribución. Esto permite una serie de prestaciones avanzadas opcionales como el roaming entre celdas.

[20] Diego Gachet. Redes inalámbricas de área local. Seminario de Telecomunicaciones. Escuela Politécnica Nacional. 2005

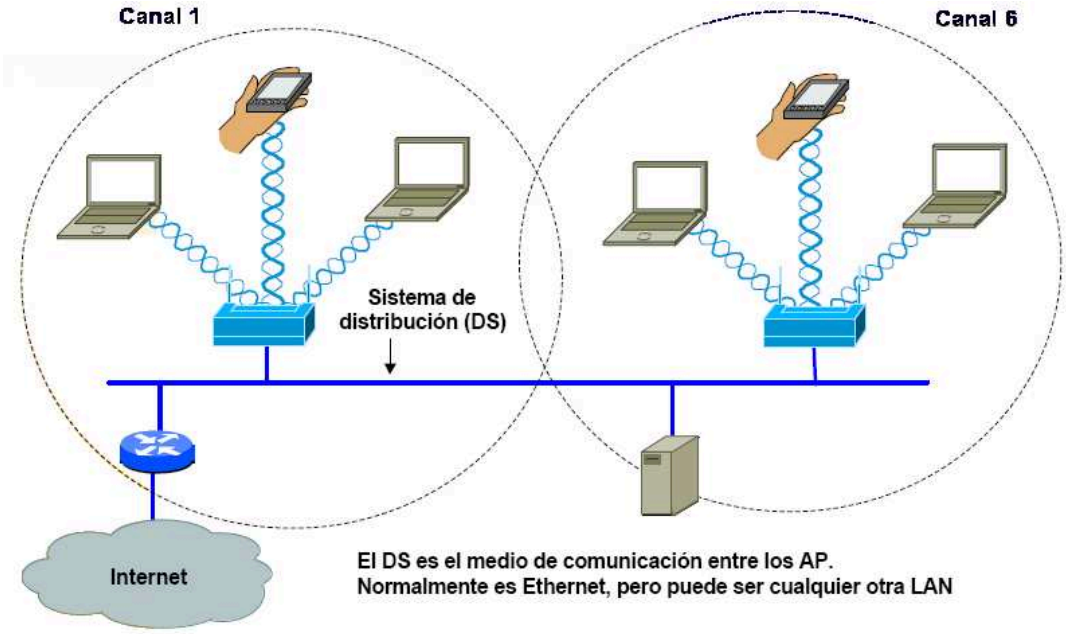


Figura 1.9: WLAN BSS extendido[21]

Servicios de la red 802.11

Una red 802.11 ofrece dos tipos de servicios:

1. Servicios de distribución: son ofrecidos por los puntos de acceso a las estaciones que se encuentran dentro de su alcance
2. Servicios de estación: son utilizados por las estaciones para comunicar dentro de una celda (es decir en un Basic Service Set o BSS)

Servicios de distribución

- Asociación: lo utiliza una estación cuando está dentro del área de cobertura de un AP. Anuncia su identidad y capacidades (velocidades, gestión de energía, etc.)

  Cuando una estación se enciende busca un AP. Si recibe respuesta de varios atiende al que le envía una señal más potente.

  La estación se asocia con el AP elegido. El AP le incluye su MAC en la tabla de asociados

[21] Diego Gachet. Redes inalámbricas de área local. Seminario de Telecomunicaciones. Escuela Politécnica Nacional. 2005

El AP se comporta para las estaciones de su celda como un hub inalámbrico. En la conexión entre la celda y el sistema de distribución el AP actúa como un puente

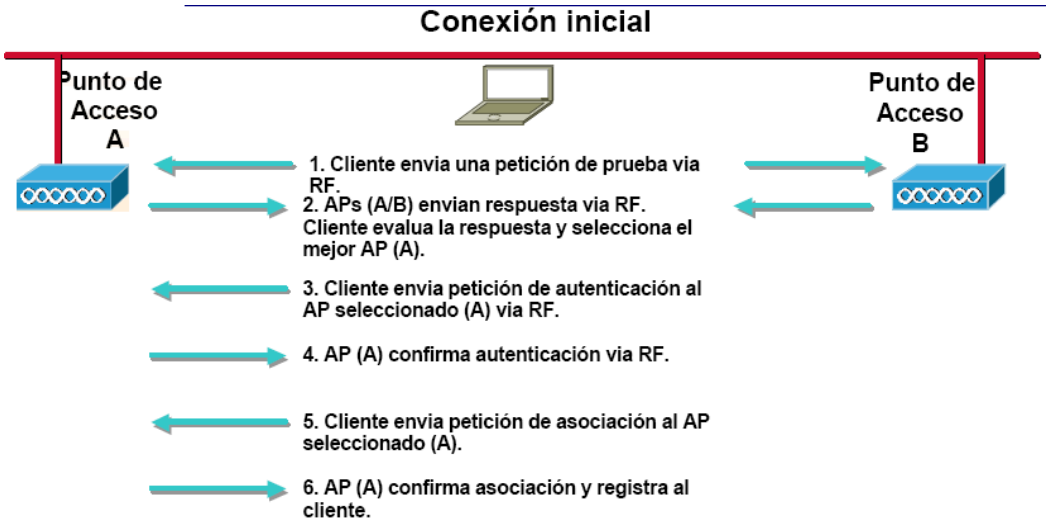


Figura 1.10: Proceso de asociación[22]

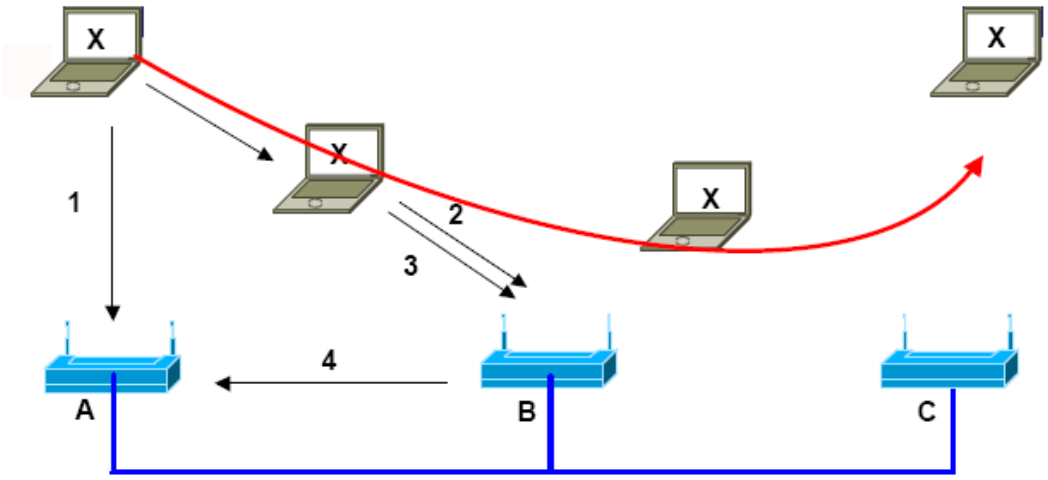
- Desasociación: cuando la estación o el AP quiere despedirse (por ejemplo porque se va a apagar)
- Reasociación: se utiliza cuando una estación se mueve y cambia al área de cobertura de otro AP dentro del mismo ESS (handover)

  Los AP envían regularmente (10-100 veces por segundo) mensajes de guía (beacon) para anunciar su presencia a las estaciones que se encuentran en su zona.

  Si una estación se mueve y cambia de celda detectará otro AP más potente y cambiará su registro. Esto permite la itinerancia ('handover') sin que las conexiones se corten.

  Para que el handover pueda hacerse correctamente debe haber una zona de solapamiento entre las dos celdas (entrante y saliente) y la estación debe permanecer el tiempo suficiente en ella. Por tanto el handover depende del tamaño de la zona de solapamiento y de la velocidad con que se mueve la estación

[22] Diego Gachet. Redes inalámbricas de área local. Seminario de Telecomunicaciones. Escuela Politécnica Nacional. 2005



1: La estación se enciende. Se autentifica y asocia con el AP A (el más próximo)

2: La estación se mueve y se pre-autentifica con el AP B

3: La estación decide reasociarse con B

4: B notifica a A la nueva ubicación de X con lo que X se desasocia de A. A envía a B cualquier trama para X en curso

5: X sigue moviéndose por lo que más tarde repite el proceso con C

Figura 1.11: Proceso de Handover[23]

- Distribución: determina como enrutar las tramas según el destino esté en la misma celda o no
- Integración: se encarga de la traducción a formatos diferentes cuando parte del trayecto se hace por una red no 802.11

Servicios de estación

- Autenticación: una vez se ha efectuado la asociación se ha de validar a la estación solicitante.

  SSID. Los clientes y el punto de acceso se asocian mediante un SSID (System Set Identifier) común.

  El SSID sirve para la identificación de los clientes ante el punto de acceso, y permite crear grupos 'lógicos' independientes en la misma zona

[23] Diego Gachet. Redes inalámbricas de área local. Seminario de Telecomunicaciones. Escuela Politécnica Nacional. 2005

Normalmente cada SSID se asocia a una VLAN diferente en la red alámbrica y a una subred IP diferente

Algunos APs permiten configurar varios SSID en un mismo equipo. En este caso el AP se conecta a un puerto 'trunk'

El SSID permite organizar y gestionar varias WLANs que tengan que coexistir en una misma ubicación, incluso si comparten un mismo canal

- Desautenticación: para terminar la comunicación ordenadamente primero hay que desautenticar y luego desasociar. Una vez desautenticado no se puede usar la red.
- Privacidad: se encarga de la encriptación/desencriptación de la información. El algoritmo utilizado es el RC4. Se han puesto de manifiesto varios errores en las funciones de privacidad las redes 802.11
- Entrega de los datos: se encarga del envío de los datos por el enlace de radio una vez se han cumplido todos los requisitos previos (asociación, autenticación y privacidad)

1.3. SEGURIDAD

La popularidad de las redes inalámbricas, debido a sus mejoras y el aumento de la movilidad, eficiencia organizacional y productividad en general no representan nada cuando una WLAN provoca problemas de seguridad en una organización siendo este, el problema más grande de este tipo de redes.

En términos de seguridad se refiere tanto a la seguridad física como, a la seguridad de la información, su integridad y a la no accesibilidad de terceros.

Una situación clara de la situación anterior podemos decir lo siguiente: Cualquier equipo o dispositivo que se encuentre próximo a un punto de acceso, podría tener acceso a la WLAN. Por ejemplo, si una empresa que funciona en un mismo edificio, y cada piso dispone de una punto de acceso, el equipo de un funcionario podría encontrarse en cierto momento en el área de influencia de dos o más puntos de acceso, pudiéndose conectar (intencionalmente o no) a la red de un departamento que no es el suyo. Un caso extremo, puedes ser

que, debido a que las ondas de radio pueden salir del edificio, cualquier persona que posea un equipo móvil y entre en el área de cobertura de la red, podría conectarse a la red de la empresa.

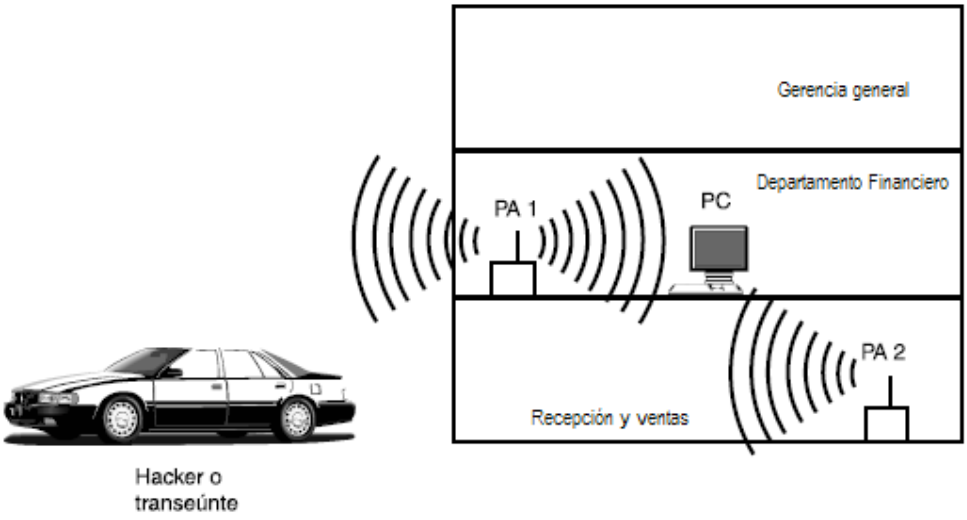


Figura 1.12: Conexión a WLAN

Según la gráfica anterior, queda claro que, cualquier usuario externo puede utilizar libremente las redes corporativas o domésticas.

Normalmente en un entorno empresarial, es común encontrar redes en las que el acceso a Internet se protege adecuadamente con un firewall, pero al interior de la red existen puntos de acceso inalámbrico totalmente desprotegidos, irradiando señal al exterior del edificio. Cualquier persona (posiblemente un hacker) que desde el exterior capte la señal del punto de acceso, tendrá acceso a la red de la compañía, con la posibilidad de navegar gratis en Internet, utilizar la red de la compañía como punto de ataque de otras redes y luego desconectarse para no ser detectado, robar software y/o información, introducir virus o software maligno, etc.

Un punto de acceso inalámbrico mal configurado se convierte en una invitación a vulnerar por completo la seguridad informática de una compañía. Un estudio publicado en 2003 por RSA Security Inc.4[24] encontró que de 328 puntos de

[24] Dennis Fisher. Study Exposes WLAN Security Risks. Marzo 12 de 2003. http://www.eweek.com/print_article/0,3048,a=38444,00.asp

acceso inalámbricos que se detectaron en el centro de Londres, casi las dos terceras partes no tenían habilitado el cifrado mediante WEP. Cien de estos puntos de acceso estaban divulgando información que permitía identificar la empresa a la que pertenecían, y 208 tenían la configuración con la que vienen de fábrica.

Una vez que un intruso localiza y logra ingresar a la red puede realizar 2 tipos de ataques:

1. Ingresar y hacer uso ilegal e inadecuado de los recursos
2. Configurar un punto de acceso propio, para de esa manera los usuarios de la red se conecten al punto de acceso del intruso y comiencen a transmitir a través de él, procediendo al robo de información o instalación de software maligno.

Para poder considerar una red inalámbrica segura se debe considerar lo siguiente:

a. Limitar las ondas de radio lo máximo posible, aunque resulta muy complicado se puede lograrlo utilizando antenas direccionales y con una adecuada configuración de la potencia de los puntos de acceso.
b. Establecer un mecanismo de autentificación en ambos sentidos, es decir que el cliente esta seguro de la red a la que se conecta y que el punto de acceso este seguro que el cliente es quien dice ser, además de tener permisos de acceso.
c. Cifrar la información que se transmite, para evitar que otros equipos a los que no esta dirigida los datos puedan leer la información.

1.3.1. WARWALKING Y WARDRIVING

Existen prácticas bien conocidas para obtener información de localización y configuración de redes inalámbricas Wi-Fi.

Warwalking.- esta práctica consiste en caminar por la calle con una portátil o PDA que cuente con un dispositivo Wi-Fi, buscando señal de puntos de acceso. Una vez localizado se pinta con un símbolo especial a manera de graffiti en la acera o la pared para marcar zonas de cobertura de puntos de acceso y si la red es segura o no.

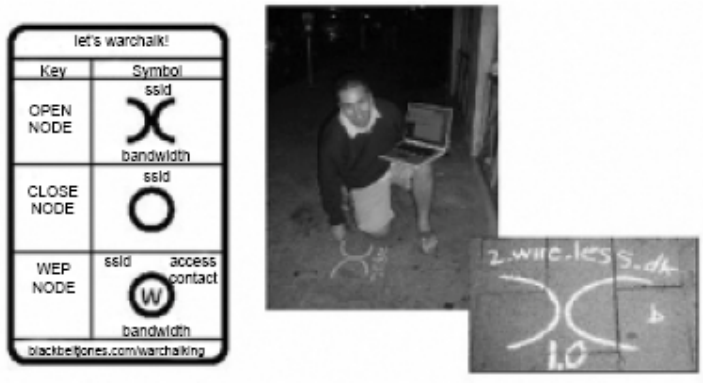


Figura 1.13: Warwlaking y su simbología[25]

Wardriving[26].- Esta práctica localiza puntos de acceso desde un automóvil, para lo cual se utiliza un portátil dotado de un dispositivo Wi-Fi, una antena direccional, GPS y software para detectar redes inalámbricas que se consigue de manera gratuita en Internet. Así elaboran mapas disponibles en Internet donde se indica la situación de todas las redes inalámbricas encontradas y su nivel de seguridad (ver http://www.wifimaps.com).

Actualmente existen diversas iniciativas en marcha y se cuentan por miles el número de Hot-spots (puntos de acceso de conexión en zonas públicas como aeropuertos, hoteles, cafés, restaurantes, etcétera) distribuidos por el mundo. A través de Internet podemos encontrar localizadores de Hot-spots que nos sitúan geográficamente los puntos donde poder conectarnos, el operador que da el servicio, cómo acceder al mismo, y hasta sus tarifas.

1.3.2. MÉTODOS DE AUTENTICACIÓN INALÁMBRICA

[25] Warchalking. http://www.warchalking.org
[26] Wardriving http://www.wardriving.com

Se encarga de verificar que un dispositivo (cliente) es quien dice ser, par lo cual hace uso de credenciales. Cada punto de acceso contiene un identificador de servicio SSID, que es proporcionado por el fabricante, se lo considera básicamente como el nombre de la red antes que como una contraseña. El SSID puede ser activado como medio de identificación de un punto de acceso o una red entera cuando varios puntos de acceso tienen el mismo SSID.

1.3.2.1. Sin autenticación

Se trata del método por defecto de la mayoría de los puntos de acceso. No requiere autenticación, por lo que cualquier usuario se puede conectar siempre que se encuentre dentro del área de cobertura del PA y disponga de una tarjeta de red inalámbrica. Lo peor es que muchos PA tienen habilitada por defecto la transmisión automática de sus SSID (identificador de servicio) facilitando aún más su localización.

Normalmente, los puntos de acceso difunden su SSID para que cada cliente pueda ver los identificadores disponibles y así realizar la conexión al que ellos seleccionen. Se puede inhabilitar la difusión de este SSID en el punto de acceso, de este modo dificultar el descubrimiento de la red inalámbrica por parte de personas ajenas.

1.3.2.2. Filtrado de direcciones MAC

Este método consiste en la creación de una tabla de direcciones en cada uno de los puntos de acceso que componen la red inalámbrica, lo que permite la creación de listas de control de acceso ACL (Access Control List). Dicha tabla contiene las direcciones MAC de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

No es el método más seguro, sin embargo su ventaja es su sencillez, por lo cual se puede usar en redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes:

- Contiene problemas de escalabilidad, debido a que siempre que se autoriza o da de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso. Mientras más grande es la red inalámbrica es más complejo la administración de los dispositivos que la componen.
- El formato de una dirección MAC no es amigable (formato hexadecimal), lo que conlleva generalmente a cometer errores en la manipulación de las listas.
- Las direcciones MAC se trasmiten sin cifrado por el aire. Razón por la que un intruso (hacker) puede capturar esas direcciones MAC registradas en la red empleando un olfateador (sniffer), para luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, pudiéndose hacer pasar por un usuario valido. Se pueden utilizar programas como AirJack6 o WellenReiter.
- En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un punto de acceso el problema es más serio, puesto que el dispositivo contiene toda la tabla de direcciones válidas.

1.3.2.3. Autenticación de claves WEP

El esquema WEP utiliza claves de cifrado, permite transmitir una de sus claves para autentificar el acceso al punto de acceso. Se trata de una técnica de seguridad en redes inalámbricas. Sin embargo, WEP ya ha sido descifrado con el ataque Fluhrer, Martin y Shamir. Ahora, ya es posible obtener las claves WEP mediante un ataque man-in-the-middle (de suplantación), con el cual un hacker falsifica un punto de acceso perteneciente a la red, por uno no autorizado y así capturar información de los usuarios sin que éstos se den

cuenta. Hay utilidades como Ettercap[27] que son capaces de configurar un punto de acceso no autorizado como dispositivo de paso al punto de acceso legítimo a fin de capturar todos los paquetes de datos que pasen por él.

1.3.2.4. Sistema de autenticación RADIUS[28]

El estándar 802.1x está compuesta de 3 principales componentes: un solicitante (dispositivo cliente), un autenticador (puntos de acceso) y un servidor de autenticación, inicialmente concebidos como servidores de autenticación de usuarios remotos que se conectaban a la red vía telefónica, han sido mejorados permitiendo la autenticación de usuarios que se conectan por un medio inseguro como son las ondas de radio.

El proceso de autenticación funciona de la siguiente manera:

1. El cliente obtiene el acceso al medio inalámbrico a través de CSMA/CA y se asocia a un punto de acceso.
2. El punto de acceso acepta la asociación pero ubica al cliente en un "área de espera" hasta que sea autentificado, mientras permanece bloqueado su acceso a la LAN
3. El usuario envía su identificación con el nombre de usuario y contraseña, al recibir esta información el punto de acceso reenvía estos datos al servidor de autenticación RADIUS. Mientras el usuario es autenticado en el servidor el cliente permanecerá en el área de espera.
4. El servidor RADIUS buscará el nombre de usuario en la base de datos, generalmente buscarán en base de datos de usuarios separadas. como por ejemplo, Active Directory de servidores Windows. Windows 2000/2003 incorporan uno llamado IAS y también hay otros para Linux sin costo.
5. Una vez que el usuario ha sido identificado por el servidor RADIUS, el servidor realiza una serie de cuestionamientos al cliente. El cliente debe

[27] Alan Sugano. Solución de problemas en redes, editorial Anaya. Cáp. 8.
[28] Remote Autentication Dial-in User Service

responder estas preguntas hasta que el servidor RADIUS determina que el usuario es válido.

6. Además de autenticar al usuario también se debe autenticar la red a la cual se está conectando el cliente, por lo que luego de ser autenticado el cliente, este también realiza un proceso de pregunta similar al realizado por parte del servidor al cliente, así puede verificar que se esta conectado a un punto de acceso válido de la red.
7. Una vez que el usuario ha sido autenticado se abre la conexión para que el usuario pueda hacer uso de los servicios que la WLAN brinda.

Actualmente ya algunos de los puntos de acceso incorporan servidores RADIUS. Debido a que el acceso se gestiona desde un servidor de manera centralizada, existe la posibilidad de agregar o eliminar un usuario de manera rápida.

1.3.2.5. Autenticación RADIUS con mecanismos de certificación o tarjetas inteligentes

Se considera uno de los métodos más seguros para autenticar el acceso al punto de acceso. En las WLAN no sólo se debe autenticar al cliente, sino que además de proveer un nombre de usuario y contraseña para que se registren en el servidor RADIUS, necesitan un certificado válido tanto para el equipo Wi-Fi como para el usuario que debe ser emitido por un servidor de certificación.

1.3.2.6. Cifrado inalámbrico

Antes de realizar una transmisión de radio en una red segura, los datos se codifican. Si un hacker intercepta tráfico de la WLAN, lo datos obtenidos aparecerán como un lista de caracteres ilegibles y sin sentido, lo que permite proteger la información que se envía desde un punto a otro en un enlace inalámbrico.

1.3.2.7. Sin cifrado

Por defecto la mayoría de los puntos de acceso no tienen habilitado el mecanismo de seguridad a través de cifrado, en resumen los datos se transmiten sin protección y cualquier usuario que intercepte la información que circula en el enlace inalámbrico con un sniffer, podrá ver la información que contiene.

1.3.2.8. Protocolo equivalente al cableado WEP

WEP hace que una conexión inalámbrica sea segura, ofrece interoperabilidad dentro del 802.11. WEP utiliza el método de cifrar los datos con el fin de proteger el enlace inalámbrico. Las claves que se usan para cifrar los paquetes son estáticas (permanecen iguales hasta que alguien las modifican de manera manual) y la clave de cifrado se comparte entre todos los usuarios de la LAN

El algoritmo WEP forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado. WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas

WEP utilizan la técnica de un “secreto compartido”, que es una clave de cifrado compartido por todos los usuarios de la red. El adaptador de la red inalámbrica utiliza la clave de cifrado para codificar todos los datos antes que salgan del ordenador. El punto de acceso cuando llegan los datos, utiliza la clave para decodificarlos a su forma original.

Los usuarios deben ingresar manualmente la clave WEP en cada cliente que vaya a formar parte de la red protegida por WEP. La clave se genera en el sistema de numeración hexadecimal. Gran parte de los usuarios no tienen idea de manejar los números hexadecimales. Si se combina la confusión de los usuarios con lo complejo que resulta inventar e introducir cadenas de números hexadecimales, se puede tener una idea por que utilizar WEP es molesto.

Vector de inicialización es un fragmento de 24 bits de una clave WEP de 64 o 128 bits, que se supone que ayuda a aumentar el número de claves diferentes posibles generadas a partir de los bits restantes, variando las claves con el tiempo. Desafortunadamente el uso del vector de inicialización es optativo y muchos fabricantes no lo utilizan. Los ataques que utilizan el vector de inicialización incluyen vigilar la reutilización de claves.

El algoritmo WEP cifra de la siguiente manera

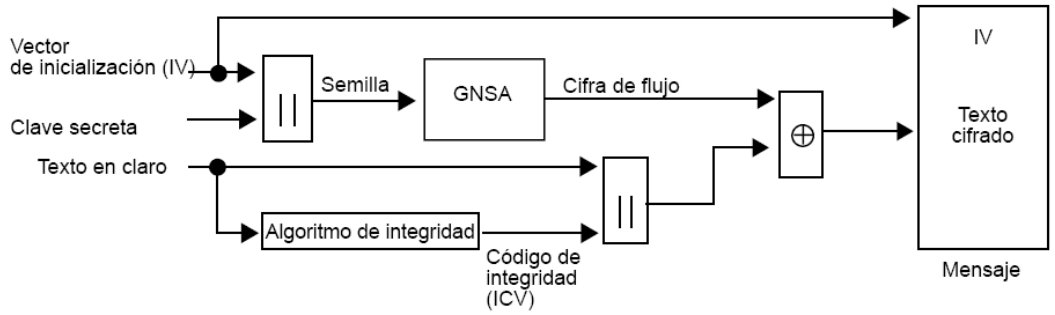


Figura 1.14: Cifrado WEP[29]

- A la trama de datos se le aplica el algoritmo CRC-32 para generar el código de integridad ICV[30]. Dicho ICV se junta a la trama de datos (trama en claro), y es empleado por el receptor para comprobar si la trama ha sido alterada durante la transmisión.
- Se selecciona una de las claves secretas compartida entre el emisor y el receptor. En caso de emplear siempre la misma clave secreta para cifrar todas las tramas, dos tramas en claro iguales generarán tramas cifradas similares. Para evitarlo, se concatena la clave secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits. El IV cambia con cada trama.
- A la concatenación de la clave secreta y el IV (conocida como semilla) se aplica el algoritmo RC4 de números seudo-aleatorios, generando una

[29] Juan Manuel Madrid Molina. Seguridad en redes inalámbricas 802.11. Universidad Icesi. Sistemas & Telemática
[30] Integrity Check Value

secuencia o cifra de flujo, del mismo tamaño de la trama a cifrar más 32 bits (para cubrir la longitud de la trama y el ICV).

- Se realiza un XOR bit por bit de la trama con la cifra de flujo, obteniéndose como resultado la trama cifrada.
- Finalmente el IV y la trama se transmiten juntos.

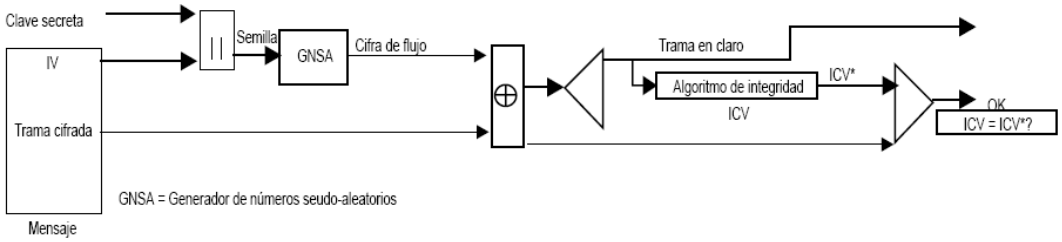


Figura 1.15: Descifrado WEP[31]

- El receptor genera la semilla que utilizó el transmisor, con el vector de inicialización y la clave secreta compartida.
- Utilizando el algoritmo RC4 genera la cifra de flujo a partir de la semilla, comparándola con la usada en la transmisión.
- Luego realizando un XOR bit a bit, entre la cifra de flujo y la trama cifrada, se obtiene la trama de datos original con el ICV.
- Finalmente a la trama se le aplica el algoritmo CRC-32, para obtener un segundo ICV y se lo compara con el ICV de la trama recibida y si son iguales la trama se acepta, caso contrario se rechaza.

A pesar de resolver el problema de cifrado entre el emisor y el receptor, WEP presenta problemas de seguridad como:

- Las claves WEP son claves de cifrado estáticas (se configura una clave en el punto de acceso y no se la cambia nunca, o muy de vez en cuando). Pudiendo hacer que un atacante capture grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque.

[31] Juan Manuel Madrid Molina. Seguridad en redes inalámbricas 802.11. Universidad Icesi. Sistemas & Telemática

- El IV que se utiliza es de longitud insuficiente (24 bits). Dado que cada trama se cifra con un IV diferente, solamente es cuestión de tiempo para que se agote el espacio de 2^{24} (16 777 216) IV distintos. Esto no es problema en una red casera o con bajo tráfico, pero en una red que posea alto tráfico se puede agotar el espacio de los IV en más o menos 5 horas. Si el atacante logra conseguir dos tramas con IV idéntico, puede efectuar un XOR entre ellas y obtener los textos en claro de ambas tramas mediante un ataque estadístico. Con el texto en claro de una trama y su respectivo texto cifrado se puede obtener la cifra de flujo; conociendo el funcionamiento del algoritmo RC4 es posible entonces obtener la clave secreta y descifrar toda la conversación.

- WEP no ofrece servicio de autenticación. El cliente no puede autenticar a la red, al contrario; basta con que el cliente y el punto de acceso compartan la clave WEP para que se establezca la comunicación.

1.3.2.9. Red privada virtual (VPN) inalámbrica

Una red privada virtual VPN emplea tecnologías de cifrado para crear un canal (túnel) virtual privado sobre una red de uso público. Las VPN resultan atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP.

Una analogía se la puede realizar con la transmisión de información segura por un medio inseguro como es el caso de Internet, de manera similar se plantea el problema de transmitir información segura por un medio inseguro como es la transmisión por radio frecuencia.

En este modelo, es donde se realiza el establecimiento de túneles IPSec[32]. Este mecanismo, que asegura el tráfico de datos por una VPN, utiliza algoritmos para la encriptación de datos y la autentificación de paquetes y certificados digitales para la validación de los usuarios. Debido a ello, se han

[32] Internet Protocol Security

implementado soluciones para responder a las necesidades de seguridad en redes inalámbricas, la combinación de la VPN's con el estándar 802.1x

Para configurar una red inalámbrica utilizando las VPN, se empieza asumiendo que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea switching. Está lista de acceso y/o VLAN solamente permite el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN.

Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado, esto brinda una variedad de ventajas:

- La tecnología VPN es una tecnología madura. Las VPN proporcionan una variedad de prácticas de autenticación que se encuentran integrados en los métodos de cifrados como DES, 3DES y AES.
- Aprovechan la experiencia técnica que ya han adquirido el personal técnico en sistemas y redes en la implementación de VPN's.
- Con las VPN existe capacidad de interoperabilidad, las aplicaciones están basadas en una aplicación en el cliente y hardware u otro software en el lado del servidor. Operan en una variedad de sistemas operativos a un costo relativamente bajo.

1.3.2.10. Protocolos LEAP o EAP-TLS

Ante la necesidad de una arquitectura inalámbrica más robusta, escalable y segura, el grupo 802.11 del IEEE creo un grupo de trabajo que se encargaría exclusivamente de la seguridad.

Con la creación de la primera arquitectura de seguridad empresarial de la industria, a principios del año 2001, Cisco Systems lanzó el primer tipo de autenticación, que se llegó a conocer como LEAP. Con LEAP, la contraseña es la credencial de autenticación, habilitando las pantallas de inicio de sesión a la

red en el lado del cliente y desplazando a las bases de datos de los dominios de red. Debido a que Cisco es un fabricante de hardware, originalmente LEAP solo estaba disponible con los dispositivos Cisco, actualmente otros fabricantes tienen la licencia para ofrecerlo, incluido Apple Computer Corporation. LEAP es compatible con el estándar 802.11i.

LEAP permite la autenticación a través de un servidor RADIUS y emplea claves de cifrado dinámicas para asegurar los datos inalámbricos. Hoy en día la mayor parte de las características de seguridad de este protocolo se han incorporado al estándar WPA.

Microsoft añade en su sistema operativo Windows XP un segundo tipo de autenticación alternativo al 802.11i. El tipo de autenticación Protocolo de autenticación extensible con seguridad en la capa de transporte EAP/TLS[33], se basa en certificados en lugar de contraseñas como credenciales de autenticación. Debido a que EAP/TLS reside en el sistema operativo es compatible prácticamente con todos los adaptadores inalámbricos 802.11.

1.3.2.11. Acceso Wi-Fi protegido WPA[34]

Es un estándar propuesto por los miembros de la Wi-Fi Alliance y con la colaboración de la IEEE. WPA tiene varios objetivos de diseño, como son robustez, interoperabilidad, subsanar los problemas de WEP en cuestiones de seguridad, ser actualizable mediante software en los productos existentes con el CERTIFICADO Wi-Fi, ser aplicable tanto para casas como para grandes empresas y estar disponible inmediatamente.

WPA mejora la forma de codificar los datos, para esto utiliza el protocolo de cifrado TKIP (“Temporal Key Integrity Protocol”), Este protocolo realiza el cambio de la clave compartida entre el punto de acceso y el cliente cada cierto tiempo, con el objetivo de evitar ataques que permitan revelar la clave.

[33] Extensible Authentication Protocol with Transport Layer Security
[34] WI-FI Protected Access

Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los vectores de inicialización con respecto a WEP. Además proporciona autenticación de usuarios mediante 802.1x y EAP.

WPA aumenta el tamaño del vector de inicialización de 24 a 48 bits, de esta manera extiende la complejidad del sistema de cifrado. Además los usuarios ya no tienen que introducir complicadas claves WEP (claves en formato hexadecimal), sino una simple contraseña.

Wi-Fi Protected Access será compatible con las especificaciones de seguridad 802.11i que actualmente está desarrollando el IEEE. De hecho, WPA está formada por los componentes ya aprobados del estándar 802.11i. Dichas funciones pueden habilitarse en la mayoría de productos certificados Wi-Fi existentes con una sencilla actualización de software.

Un AP compatible con WPA puede operar en dos modalidades, según la complejidad de la red:

- Autenticación de usuario a nivel empresarial vía 802.1x y EAP
  Para realizar la autenticación, WAP implementa el 802.1x y el protocolo de autenticación extensible (EAP) juntos. Esta implementación provee de un marco estricto de autenticación de usuarios. Utiliza un servidor central de autenticación, como por ejemplo RADIUS, para autenticar a cada usuario en la red antes de permitirle unirse a ella. Además, emplea “autenticación mutua”, por lo que un usuario wireless no puede unirse accidentalmente a una “red infiltrada” donde podría ser robada sus credenciales de red. El servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos

- Modalidad de red casera, o PSK (Pre-Shared Key)
  WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña

coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

Según la Wi-Fi Alliance, todo equipo de red inalámbrica que posea el sello “Wi-Fi Certified” podrá ser actualizado por software para que cumpla con la especificación WPA.

1.4. REGULACIÓN Y NORMATIVAS SOBRE REDES INALÁMBRICAS

En los últimos años, las telecomunicaciones han recorrido un amplio camino, desde un sector con comportamiento lineal y predecible, hacia otro sector tremendamente complejo, multifactorial e impredecible. Gran parte de esta complejidad proviene del fenómeno de la globalización, de la actividad económica y social y del cambio tecnológico que la impulsa.

En el año 2004, el panorama del sector de las telecomunicaciones se ha transformado como resultado del ritmo aplastante con que avanza la globalización del sector.

La fuerte competencia del sector de las telecomunicaciones, surgida como consecuencia del proceso liberalizador iniciado a mediados de los noventa, es el resultado de un acuerdo político multilateral de la mayor parte de los Gobiernos del mundo en torno a los Acuerdos de la Organización Mundial del Comercio (OMC).

Existen aproximadamente 200 países en el mundo, como estados soberanos, cada uno de ellos tiene la autoridad de crear e implementar regulaciones. Afortunadamente pocos son los países que han dictado regulaciones WI-Fi específicas para sus países. La mayoría de los países optan por acoger las

regulaciones internacionales. Un conjunto de países que por lo regular son colindantes y comparten un conjunto de común de regulaciones se conocen dentro de la especificación 802.11 como un "dominio regulador". La siguiente tabla define los dominios reguladores actuales.

Dominio regulador	**Área geográfica**
América o FCC[35] (Comisión Federal de Comunicaciones de EUA)	Norte, Sur y Centro América, Australia y Nueva Zelanda, distintas partes de Asia y Oceanía
Europa o ETSI (Instituto Europeo de Estándares de Telecomunicaciones)	Europa (tanto países de la Comunidad Europea como países que no la conforman), Medio Oriente, África, distintas partes de Asia y Oceanía
Japón	Japón
China	República Popular China (China continental)
Israel	Israel
Singapur*	Singapur
Taiwán*	República de China (Taiwán)
* Las regulaciones de Singapur y Taiwán para las WLAN son específicas para estos países solo en operación en la banda de los 5Ghz.; para la operación en la banda de 2.4 Ghz., Singapur y Taiwán entran en los dominios de ETSI y FCC, respectivamente	

Tabla 1.4: Dominios reguladores actuales para productos Wi-Fi[36]

1.4.1. EL DOMINIO REGULADOR FCC

El espectro de frecuencia fue visto, y se sigue viendo así, como un bien público, cuyo uso esta sujeto a la regulación gubernamental.

El conjunto de regulaciones de FCC que se aplica a la operación de Wi-Fi en la banda de 2.4 Ghz y la de 5 Ghz, es un subconjunto de las regulaciones de la Parte 15 de la FCC, el cual se aplica a una amplia variedad de dispositivos, incluyendo computadores personales además de receptores de televisión y radio.

[35] Comisión Federal de Comunicaciones de EUA, establecida en 1934
[36] 802.11 (WI-FI), Manual de Redes Inalámbricas. Neil Reid y Ron Seide. Editorial Mc Graw Hill. 2003

Dentro de las regulaciones de la Parte 15 se definen tres bandas de frecuencia separadas, 900 Mhz, 2.4 Ghz e infraestructura de información nacional libre de licencia UNII (unilicensed National Information Infrastructure) disponibles para aplicaciones industriales, científicas y medicas libres de licencia. La siguiente tabla describe las principales características de las bandas de frecuencia.

Banda	Nombre común	Rango de frecuencia	Uso común
900 Mhz	900 “meg”	902 a 928 Mhz	Primeras LAN Inalámbricas, teléfonos inalámbricos
2.4 Ghz	Dos-cuatro o 2.4 “gig”	2.400 a 2.4835 Ghz (amplitud de 83.5 Mhz)	LAN inalámbricos Wi-Fi 802.11b y 802.11g. Bluetooth, teléfonos inalámbricos
UNII-1	Euni-uno	5.15 a 5.25 Ghz (amplitud de 100 Mhz)	LAN inalámbricas de uso interno
UNII-2	Euni-dos	5.25 a 5.35 Ghz (amplitud de 100 Mhz)	LAN inalámbricas de uso interno y externo además de puentes inalámbricos de rango corto
UNII-3	Euni-tres	5.725 a 5.825 Ghz (amplitud de 100 Mhz)	Puentes inalámbricos de uso externo de rango amplio

Tabla 1.5: Características de las bandas de frecuencia

La banda de los 900 Mhz, es usada principalmente por teléfonos inalámbricos, WLAN que no cumplen con el estándar y otros dispositivos que no son Wi-Fi.

1.4.1.1. La banda de 2.4 Ghz

Es una banda reservada para la utilización libre de licencia, por todos los dominios reguladores, es decir esta libre de licencia en casi todo el mundo. La regulación describe la operación de los sistemas de Espectro extendido de saltos de frecuencia (FHSS) y en mayor detalle para la operación de los sistemas de Espectro extendido de secuencia directa DSSS.

La compatibilidad de la mayoría de estas regulaciones y la principal responsabilidad de los fabricantes antes que de los usuarios. Se debe tomar muy en cuenta que se pide a los fabricantes que proporcionen “sistemas” compatibles y no solamente “dispositivos” compatibles. En la regulación siguiente que se encuentra dentro de la Parte 15 de la FCC, Subparte C, Subsección 15.203, dice:

> “Un radiador internacional (radio) debe estar diseñado para asegurar que no se debe usar ningún otro tipo de antena que no haya sido elaborada por la parte responsable con este dispositivo. El uso de una antena permanentemente conectada o una antena que usa un dispositivo de acoplamiento único para el radiador intencional debe considerarse adecuado para cumplir con las provisiones de esta sección”.

Normalmente los fabricantes para cumplir con esta sección modifican un conector estándar en la industria de tal forma que se convierte en exclusivo para ellos y por lo general no está disponible en otras fuentes. Por ejemplo, Cisco System modifica un conector de rosca para cable coaxial al invertir la polaridad del acoplamiento. Otros fabricantes realizan modificaciones similares que son fáciles de duplicar; lo que genera la industria de conectores de distintos fabricantes. Por lo tanto es fácil obtener antenas de otros fabricantes con conectores que se ajustarán a los puntos de acceso de los fabricantes líderes en la industria.

La FCC limita el total de la potencia de transmisión y la ganancia de antena menos cualquier pérdida de cable, a no más de 36 dBm o 4 watts. Esta potencia de radiación isotrópica efectiva permite un poco más de flexibilidad en la parte del usuario y el fabricante. Pero la FCC la ha incluido, junto con otros entes reguladores para asegurar que el fabricante no proporcione dispositivos que irradien una cantidad excesiva de energía dentro de un espacio determinado.

Las regulaciones para los amplificadores de la FCC son mucho más restrictivas. Un amplificador es un dispositivo de potencia que se conecta entre el radio y la antena para añadir potencia adicional al sistema. A pesar que la FCC permite la venta de antenas individuales, prohíbe en cambio, la venta de amplificadores externos como dispositivos aislados. Se los puede comprar solo como parte de un kit que incluya al radiador internacional, antena y los cables necesarios: el kit debe estar certificado con la compatibilidad de FCC.

Referente a lo señalado, en la Subseccion 15.204: "…ninguna persona debe usar, fabricar, vender, arrendar, ofrecer la venta o arrendamiento, o importar embarcar o distribuir para el propósito de vender o arrendar, ningún amplificador externo de potencia de la frecuencia de radio o kit amplificador que tenga como fin el uso de radiador intencional de la Parte 15"

En resumen un usuario debe evitar los amplificadores externos, especialmente si no están incluidos como un componente de un elemento certificado en la norma 802.11.

Sin embargo de que la asignación FCC para la banda ISM de 2.4 Ghz está comprendida en las bandas de frecuencia de 2.4 y 2.4835 Ghz, los dispositivos funcionan en términos de canales. Las especificaciones 802.11 b y 802.11g definen el uso de estos canales de la siguiente manera:

ID de canal (Mhz)	**Frecuencia**
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462

Tabla 1.6: Canales disponibles en la banda FCC para Estados Unidos

De acuerdo a la tabla anterior se sugiere que el usuario dispone de 11 canales en la banda de los 2.4 Ghz. En verdad el usuario cuenta con 3 canales que no se solapan, es decir solo 3 canales puede usar el cliente. Se requieren por lo menos 22 Mhz de transmisión para Wi-Fi. Como se puede ver en la siguiente figura los canales de 22 Mhz de amplitud se extienden 11 Mhz fuera del punto central del canal en ambas direcciones. Los únicos canales que permiten la amplitud de 11 Mhz en ambas direcciones sin interferir con otro canal son los canales 1, 6 y 11. Se recomienda el uso de estos tres canales para alcanzar el mejor balance entre capacidad y confiabilidad.

1.4.1.2. Las bandas de 5 Ghz

La FCC ha asignado tres bandas libres de licencia en la porción de los 5 Ghz del espectro de frecuencia que se conoce como las bandas de Infraestructura de información libre de licencia UNII (Unlicensed National Information Infrastruture). Cada una de las tres bandas tiene una amplitud de 100 Mhz. De acuerdo a la tabla 1.5 de este capítulo, las bandas UNII-1 y UNII-2 son contiguas por lo que en 802.11a son tratadas como un espacio continuo de amplitud de 200 Mhz de espectro. La ventaja de tener una amplitud de 200 Mhz es que están divididas hasta en 8 canales que no se solapan, cada uno de ellos con una amplitud de 25 Mhz.

UNII-1

Diseñada para el uso de LAN inalámbricas internas, su uso externo esta prohibido por las regulaciones. De las tres bandas UNII es la que cuenta con las regulaciones más estrictas. Requiere que la antena y el radiador internacional sean dispositivos integrados; el uso de conectores, cables de antenas auxiliares esta prohibido. La ganancia de la antena esta limitada a 6 dBi. La potencia de transmisión no debe ser mayor de 50 mW en el punto más alto y 40 mW de manera nominal. La limitación EIRP (potencia de radiación isotrópica efectiva) resultante es 22 dBm, la cual se parece a la de 36 dBm para la banda de 2.4 Ghz. Como resultado se obtiene que todos los productos

Wi-Fi de 5 Ghz, ofrezcan rangos mucho más cortos y menos opciones de instalación y patrones de cobertura.

UNII-2

Diseñada para uso inalámbrico de aplicaciones internas y externas en rango corto. Para ello la regulación permite el uso de conectores, cable y antenas auxiliares. La limitación EIRP de 29 dBm está diseñada para el uso de puentes inalámbricos de rango amplio. La potencia de transmisión está limitada a no más de 250 mW cuando se usa una antena de 6 dBi.

1.4.2. EL DOMINIO REGULADOR ETSI

El Instituto Europeo de Estándares de Telecomunicaciones es principalmente un instituto consultivo en lugar de regulador Sin embargo como resultado de la Unión Europea, las regulaciones para toda Europa cada día son más comunes. Las regulaciones ETSI están más detalladas y son más estrictas que las regulaciones de la FCC.

Regulación	Descripción
EN 55022	Línea conductora
EN 1000-4-2	Descarga electrostática
EN 1000-4-3	Inmunidad de campo RF (80 Mhz hasta 1 Ghz)
EN 1000-4-4	Rapidez eléctrica momentánea
EN 1000-4-5	Subida en el voltaje/oscilación
EN 1000-4-6	Inmunidad de la línea conductora (150 khz hasta 80 Mhz)
EN 1000-4-11	Voltaje momentáneo
EN 6001-3-2	Armonía en la línea de alimentación
EN 6001-3-3	Fluctuación de voltaje

Tabla 1.7: Regulaciones ETSI

ETSI no permite más de 100 mW EIRP o 20 dBm. Con un radio de 30 mW (15 dBm), las limitaciones EIRP de ETSI restringen la ganancia de la antena a un máximo de 5 dBi. Antenas como las yagis y algunos parches, no son permitidos

en los países ETSI sin que se incluyan reducciones de potencia de transmisión. Se pueden usar otras antenas, pero su uso está limitado más hacia la redirección de la energía de radio frecuencia antes que al incremento del rango.

ETSI proporciona una banda de 2.4 Ghz, más amplia que la que ofrece FCC. Esto lo logra mediante el uso de la misma canalización para 802.11 que utiliza FCC, el resultado es un total de trece canales en lugar de los once que ofrece FCC. En este sentido lo más importante no es la cantidad de canales que utiliza, sino la cantidad de canales que no se solapan. Lamentablemente la cantidad de canales que no se solapan al igual que con FCC son tres. En resumen no se obtiene ningún beneficio por tener más canales.

En la banda de los 5 Ghz, la banda que recomienda es más amplia y va desde los 5.15 hasta 5.7 Ghz. Para ello ETSI obliga a la implementación de dos parámetros que no se incluyen en los productos 802.11, la Selección de frecuencia dinámica (DFS) y el Control de potencia de transmisión (TPC).

DFS funciona permitiendo que un dispositivo escuche primero en toda la banda de frecuencia disponible para él y luego autoasignarse de manera automática el canal menos congestionado. Al escuchar primero el canal antes de seleccionarlo, el punto de acceso y sus clientes asociados no interferirán con los usuarios principales.

TPC es una idea heredada de los teléfonos celulares, la potencia de transmisión de los puntos de acceso y los dispositivos de los clientes puede ser establecida por los usuarios de tal manera que permite distintos tamaños de área de cobertura, en el caso del cliente permite conservar energía de las baterías. El problema se presenta cuando se configura un punto de acceso con una potencia baja y los clientes transmiten con potencias estándares más alta de la que esta configurado el punto de acceso, dando como resultado la emoción innecesaria de energía de radio frecuencia por parte de los clientes, lo cual lleva a elevar el nivel de ruido, limitando el rango y desempeño de todos

los dispositivos Wi-Fi que se encuentren asignados en la misma frecuencia de radio.

1.4.3. EL DOMINIO REGULADOR JAPONÉS

TELEC, organización japonesa equivalente de FCC y ETSI, emite las regulaciones que son adoptadas únicamente en su país. Las regulaciones TELEC son más estrictas en la potencia de transmisión, proporcionando en cambio un mayor ancho de banda. Las regulaciones no están basadas en una limitación de potencia específica sino que se basa en una alimentación relativa a la cantidad de ancho de banda disponible. Para los dispositivos Wi-Fi la limitación es de 10 mW por 1 Mhz EIRP. Como resultado se tiene que los dispositivos de 2.4 Ghz están limitados a máximo 20 mW en la potencia de transmisión con una ganancia de antena de 6 dBi como máximo, y no más de 50 mW con una antena de 0 dBi. Proporciona catorce canales, pero al igual que las anteriores solo tres no se solapan.

Para la operación de 802.11a, TELEC proporciona una amplitud de banda de 100 Mhz que va de los 5.15 a 5.25 Ghz, lo cual restringe bastante el poder de transmisión total.

1.4.4. REGULACIÓN EN EL ESTADO ECUATORIANO

Debido a que nos encontramos en el dominio regulador del FCC, las regulaciones para el estándar Wi-Fi en el Ecuador han sido adoptadas en su totalidad.

El CONATEL es el ente encargado de la administración y regulación de las telecomunicaciones en Ecuador y de la administración de telecomunicaciones del Ecuador ante la Unión Internacional de Telecomunicaciones (UIT).
Está conformado por:

- Un representante del Presidente de la República, quien lo preside
- El señor Vicepresidente de la República

- El Jefe del Comando Conjunto de las FF.AA.
- El Secretario Nacional de Telecomunicaciones
- El Superintendente de Telecomunicaciones
- Un representante designado conjuntamente por las Cámaras de la Producción
- El representante legal del Comité Central Único de los trabajadores de Telecomunicaciones

Las funciones principales del CONATEL son:

- Dictar políticas del Estado con relación a las telecomunicaciones
- Aprobar el plan de desarrollo de las telecomunicaciones
- Establecer términos, condiciones y plazos para otorgar concesiones y autorizaciones para la explotación de servicios finales y portadores de telecomunicaciones
- Expedir los reglamentos necesarios para la interconexión de las redes
- Promover la investigación científica y tecnológica en el área de las telecomunicaciones

EL órgano encargado de cumplir y hacer cumplir las normas y reglamentos dictados por el CONATEL es la Superintendencia de Telecomunicaciones, la cual tiene como principales funciones las siguientes:

- Cumplir y hacer cumplir las resoluciones del CONATEL
- El control de los operadores que exploten servicios de telecomunicaciones
- Supervisar el cumplimiento de las regulaciones que apruebe el CONATEL
- Juzgar a las personas naturales y jurídicas que incurran en las infracciones señaladas en esta LEY

1.4.4.1. Plan nacional de frecuencias[37]

[37] Plan Nacional de Frecuencias. Consejo Nacional de Telecomunicaciones, Secretaria Nacional de Telecomunicaciones. Septiembre 2000

En septiembre del 2000 se crea el Plan Nacional de Frecuencias con el objetivo principal de proporcionar las bases para un proceso eficaz de gestión del espectro radioeléctrico y asegurar una utilización óptima del mismo; así como, la prevención de interferencias perjudiciales entre los distintos servicios.

El Plan para ese entonces buscaba convertirse en el documento de referencia en el desarrollo de las telecomunicaciones en el país. Cubre las necesidades de los servicios tales como la telefonía fija inalámbrica, las telecomunicaciones móviles terrestres y vía satélite, los servicios integrados que vendrán con los Servicios de Comunicación Personal, Sistemas Móviles Internacionales de Telecomunicaciones (IMT-2000), los nuevos sistemas troncalizados, los nuevos servicios según el concepto de última milla, espectro ensanchado, etc

1.4.4.2. Norma para la implementación y creación de Sistemas de Espectro Ensanchado

RESOLUCION 538-20-CONATEL-200038

En Octubre del 2000 se crea la norma para la implementación y creación de Sistemas de Espectro Ensanchado, su principal objetivo es la de regular la instalación y operación de sistemas de radiocomunicaciones que utilizan la técnica de espectro ensanchado.

La norma determina la utilización de las bandas de frecuencias ICM (Aplicaciones Industriales, Científicas y Médicas) de 902 a 928 MHz, de 2.400 a 2.483,5 MHz y 5.725 a 5.850 MHz. La operación de los sistemas en modo de espectro ensanchado de secuencia directa, salto de frecuencia o híbridos, con las siguientes configuraciones: Sistemas fijos punto a punto; Sistemas fijos punto – multipunto; Sistemas móviles; Sistemas de explotación; y, las demás configuraciones que el CONATEL defina.

[38] http://www.conatel.gov.ec/espanol/baselegal/reglmtoespectroensanchado.htm

Los equipos que se comercializan libremente en el país deben contar con el certificado de homologación otorgado por la Secretaria Nacional de Telecomunicaciones. La potencia máxima de salida del transmisor para los sistemas con salto de frecuencia que operen en las bandas de 2.400 a 2.483,5 Mhz ó 5.725 a 5.850 Mhz, será de 1 vatio.

1.4.4.3. Proyecto de norma para la implementación y operación de sistemas de modulación digital de banda ancha

El 11 de noviembre del 2005, mediante Resolución del CONATEL 417, entra en vigencia “La norma para la implementación y operación de sistemas de modulación digital de banda ancha”. Cuyo principal objetivo es de regular la instalación y operación de Sistemas de Radiocomunicaciones que utilizan técnicas de Modulación Digital de Banda Ancha en los rangos de frecuencias que determine el Consejo Nacional de Telecomunicaciones, CONATEL

En este proyecto se cubre adicionalmente a las ya cubiertas por la “Norma para la implementación y creación de Sistemas de Espectro Ensanchado”, las bandas de 5.150 a 5.250 Ghz , de 5.250 a 5.350 y de 5.470 a 5.725.

Todos los usuarios que dispongan de Certificado de Registro para Uso de Tecnología de Espectro Ensanchado que se encuentren vigentes deben proceder a registrarse en la Secretaria Nacional de Telecomunicaciones como Sistemas de Modulación Digital de Banda Ancha. Los Certificados de Registro para Uso de Tecnología de Espectro Ensanchado, se canjean por su correspondiente Certificado de Registro para uso de Sistemas de Modulación Digital de Banda Ancha en la Secretaría Nacional de Telecomunicaciones.

Como disposición final se deroga la Norma para la Implementación y Operación de Sistemas de Espectro Ensanchado aprobado con la Resolución 538-20-CONATEL-2000, publicada en el Registro Oficial 215 del 30 de noviembre del 2000.

CAPITULO 2: SITUACION ACTUAL DE LA RED

2.1. SITUACIÓN ACTUAL DE LA RED LOCAL FLACSO ECUADOR

La Sede de FLACSO en Ecuador fue establecida en 1975 mediante un acuerdo entre el Estado ecuatoriano y el sistema internacional de FLACSO. La institución forma parte del sistema universitario ecuatoriano y fue reconocida por la Ley de Educación Superior en el año 2000.

Su misión es la de producir y difundir conocimiento en el área de las ciencias sociales a través de investigación y docencia de calidad a nivel de postgrado. Actualmente FLACSO sede Ecuador se encuentra ubicado en el sector centro-norte de la ciudad de Quito. El campus académico consta de un edificio moderno y funcional, que cuenta con todas las comodidades de infraestructura tanto física como de tecnología.

El edificio de FLACSO está constituida por dos torres (Torre 1 y Torre 2) de nueve pisos altos cada una, y 4 pisos subterráneos comunes para las dos torres, de los cuales el primer subterráneo esta destinado para un Centro de Convenciones, comprendido de 1 hemiciclo (160 asientos), 1 auditorio múltiple (350 asientos), 3 aulas magistrales para 60 personas, 2 salas de sesiones, una aula virtual (35 asientos), la librería de FLACSO, una sala de Internet (10 equipos) y un hall de exposiciones.

Figura 2.1: Edificio FLACSO sede Ecuador

El edificio cuenta con un atrio con frente hacia la calle, el cual constituye el elemento central de circulación y vinculación de todas las áreas del edificio.

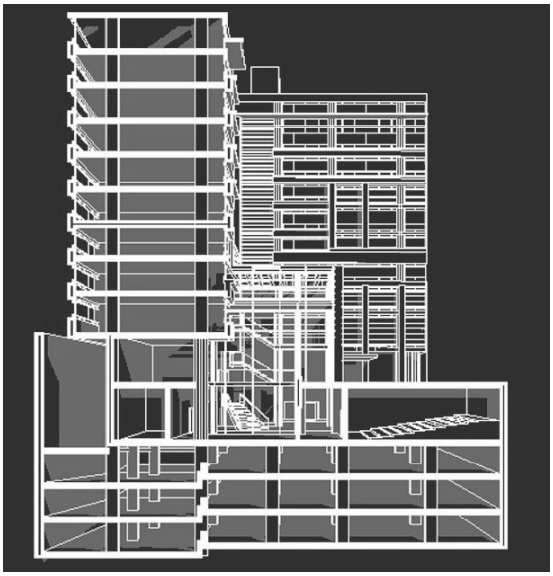


Figura 2.2: Corte frontal - Edificio FLACSO Ecuador

La FLACSO actualmente ocupa para el desarrollo de sus labores la totalidad de la torre 1; además de él piso 1, planta baja y subsuelo 1 de las dos torres en donde funciona la Biblioteca, cafetería, centro de convenciones.

En el subsuelo dos se encuentra un espacio al que se le ha denominado “cuarto inteligente”, en el cual se concentran todos los dispositivos para la gestión, administración y monitoreo del edificio.

El cuarto inteligente es el espacio destinado para la ubicación de los servidores y sistemas para el control de generadores, bombas, sistema eléctrico, alarmas contra incendios, aire acondicionado, control de accesos, central telefónica, CCTV, rack’s de distribución central (voz y datos), servidor de voz (central telefónica y mensajería de voz), servidor de base de datos, servidor de aplicaciones, servidor Web, Proxy y de correo electrónico, servidor de protección antivirus y antispam, firewall, switch core, acceso al Internet, etc.

El cuarto inteligente mantiene los niveles adecuados de temperatura, seguridad, respaldos de baterías de energía (UPS), restricciones de acceso del personal, para su funcionamiento continuo.

2.2. DESCRIPCIÓN DE LA INFRAESTRUCTURA DE LA RED.

El campus de FLACSO es un edificio moderno con tecnología de punta que permite la fácil adaptabilidad e interoperatibilidad con las nuevas tecnologías, lamentablemente, en la actualidad no brinda la oportunidad de conectarse a la red de datos de manera inalámbrica, tomando en cuenta la naturaleza académica y de investigación de la institución es de vital importancia contar con acceso inalámbrico tanto para profesores, investigadores, estudiantes y visitantes nacionales e internacionales. Con estos antecedentes el análisis de la infraestructura actual se ha divido en dos grandes partes que son:

1. Parte pasiva de la red
2. Parte activa de la red

2.2.1 PARTE PASIVA DE LA RED

La parte pasiva esta constituida por la parte fija de la red que nunca cambiará o muy rara vez se tendrá que hacer cambios, actualizaciones o reparaciones. En la parte pasiva esta incluida tendido de cables, racks, canaletas, jack´s, patch cords, etc.

La parte pasiva de la red esta constituida en la actualidad casi en su totalidad por tecnología alámbrica, a excepción de la biblioteca que utiliza un pequeño punto de acceso para conectar 4 estaciones que son destinadas exclusivamente para la consulta del fondo bibliográfico de la biblioteca y está restringido el acceso al resto de la red local.

2.2.1.1. Cableado estructurado

El sistema de cableado estructurado esta diseñado para que por él circule tráfico de voz y de datos, esta divido en 2 tipos que son: cableado vertical y horizontal.

El cableado vertical se constituye por el backbone principal de fibra óptica de la red y un backbone de respaldo de cable de cobre. El backbone, tanto de fibra como de cobre unen todos los armarios de distribución (SDF Secondary Distribution Frame) ubicados en varios pisos altos con el armario central de distribución (Main Distribution Frame) del cuarto inteligente.

El cableado horizontal en su totalidad es cable UTP categoría 6 TIA/EIA 568-B2-1 de 4 pares y comprende las redes locales de cada uno de los pisos que se conectan a través del backbone principal de fibra al cuarto inteligente y así poder acceder a los servicios que presta la red de datos de la institución.

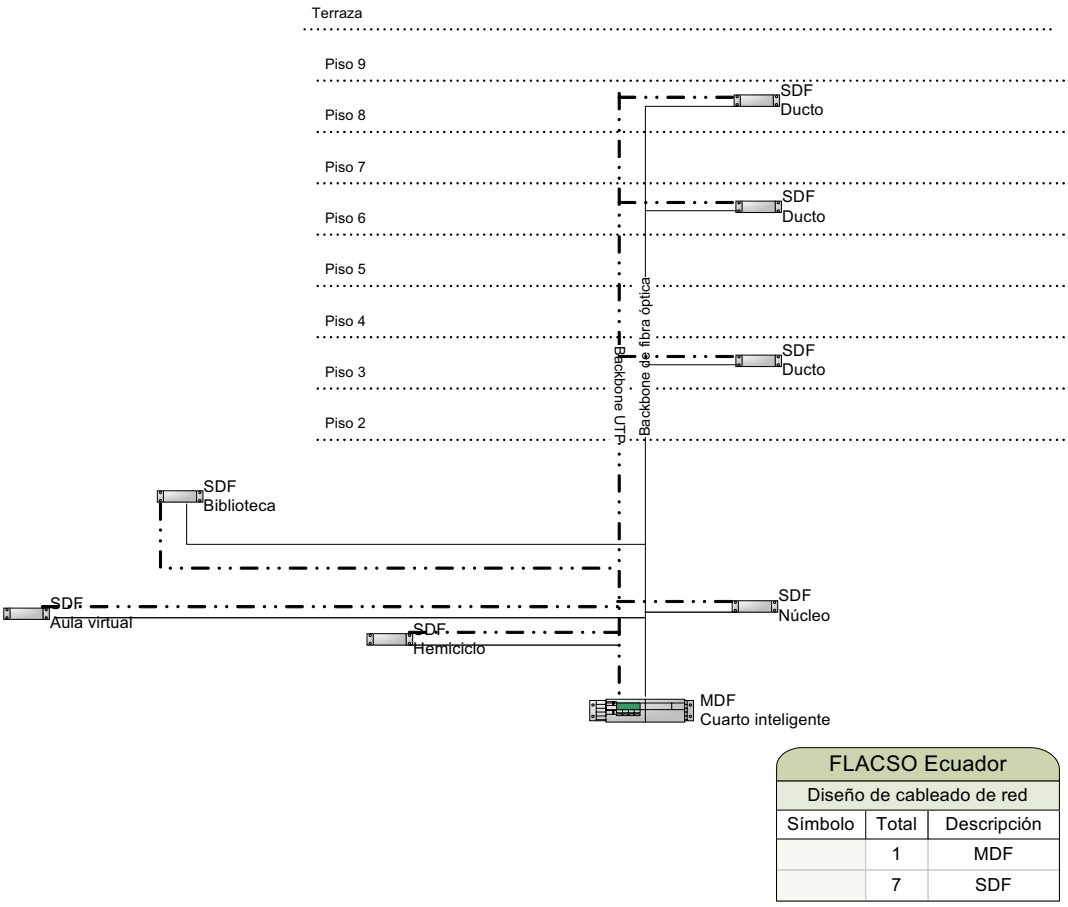


Figura 2.3: Distribución del cableado de red

El cableado horizontal une a través de los equipos de interconexión (parte activa de la red) cada uno de los puntos de conexión de cada cliente que se encuentra ubicado en su espacio de trabajo con el backbone principal y en consecuencia a la red de datos y sus servicios.

2.2.1.2. Armarios de distribución principal (MDF) y secundario (SDF).

Los armarios de distribución MDF (Main Distribution Frame) y SDF (Secondary Distribution Frame) se encuentran distribuidos en el edificio con el objetivo de cubrir las necesidades de conexión de los clientes de la organización. El análisis de necesidades se lo ha hecho tomando en cuenta la asignación de los espacios a cada una de las dependencias que conforman FLACSO y tomando en cuenta la cantidad de funcionarios que laboran en esa dependencia. De acuerdo a ello se han instalado los puertos de red (jack´s) en cada oficina y se han instalado y configurado los equipos de interconexión (switch) pesando en cubrir los requerimientos, dejando por lo menos en los equipos puertos libres para futuros crecimientos.

El continuo crecimiento de la institución, ha provocado que los equipos de conexión y puntos de red en algunos casos han excedido su capacidad, haciéndose necesario la instalación física de más puntos de red cableados, comprar más dispositivos de interconexión, inclusive en otros casos crear redes locales en espacio reducidos (una oficina), afectando al rendimiento de la red, irrespetando los niveles de apilamiento dispuesto por la norma Ethernet y a la estética del edificio.

De ahí que se desprende la necesidad de permitir la posibilidad de crecimiento de una manera ágil, a un menor costo y que brinde todas las bondades que brinda la red de datos actual, sin que ello afecte de manera considerable en el rendimiento ni seguridad de la red, garantizando de esta manera la correcta y oportuna realización de las tareas que cada uno de los funcionarios ejecuta al interior de la organización utilizando la tecnología.

El MDF esta ubicado en el subsuelo 2, en el espacio llamado “cuarto inteligente”, esta oficina esta adecuada para ubicar todos los servidores y equipos de control, monitoreo y mantenimiento del edificio. En él se concentran todas las conexiones de voz y datos tanto desde el interior como del exterior del edificio. Al MDF llega la conexión de las líneas telefónicas, acceso al Internet, líneas ISDN.

Los SDF se encuentran desplegados a lo largo del edificio y cada uno esta pensado para cubrir las necesidades de conexión de los clientes en todos los espacios al interior de la institución.

La distribución, cobertura y número de puertos de red instalados en cada piso se detallan en la tabla No. 2.1

Piso	Cobertura	Puntos
Piso 8	Cubre los pisos 9 (dirección), 8 y 7 (académico)	69
Piso 6	Cubre los pisos 6 (académico), 5 (administrativo financiero) y 4 (estudiantes)	55
Piso 3	Cubre los pisos 3 (centros de computo), 2 y 1 aulas	122
Piso 1	Biblioteca primer piso y planta baja	19
Piso -1	Cafetería, Recepción	7
Piso -1	Hemiciclo, Auditorio, salas de conferencias y sala de exposiciones	39
Piso -1	Aula virtual, sala de Internet, librería y mantenimiento	22
		333

Tabla 2.1: Distribución de SDF

2.2.2. PARTE ACTIVA DE LA RED

La parte activa de la red está constituida por los elementos que se pueden cambiar, modificar o actualizar como son: los Routers, Switchs, Hubs, Servidores, impresoras, estaciones de trabajo.

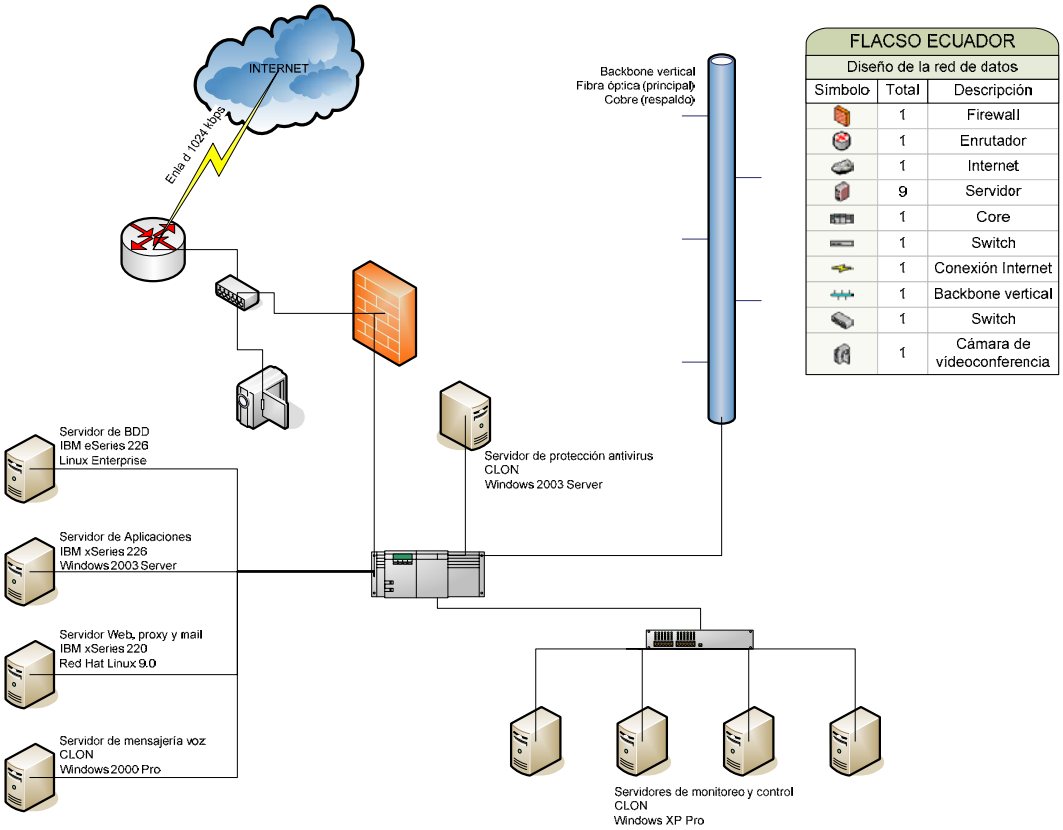


Figura 2.4: Arquitectura actual de la red de datos

2.2.2.1. Router Cisco 1700

El ruteador Cisco 1700 se utiliza para unir la red LAN con la red Internet. En el se encuentran configuradas lista de control de acceso ACL para filtrar el tráfico desde y hacia la red, además de proveer cierto nivel de seguridad contra posibles ataques a la red local.

Procesador	RISC CPU
Memoria Flash	32 MB (ampliable hasta 64 MB)
Memoria DRAM	64 MB
Slots de expansión	1 (ej., para Modulo VPN)
Energía interna	AC (interna solo para Cisco 1760)
Puertos de consola	1 (sobre 115.2 Kbps)

Puertos Auxiliares	1 (sobre 115.2 Kbps)
Conexiones Ethernet máximas	5 (1XFE incluido + 4 puertos WIC-4ESW)
Puertos 10/100 Ethernet	1
Puerto serial de alta velocidad	4
Puertos máximo de ISDN BRI	4 voz, 2 datos
Integra CSU/DSU	Si, soporte opcional T1/E1
Compresión	SW
Encriptación	SW + HW
Soporta VLAN 802.11q	Si

Tabla 2.2: Especificaciones Router CISCO 170039

2.2.2.2. Switch 3Com 4950

Se constituye en el switch principal. Se encarga de la gestión de las VLAN's generadas para la segmentación de la red. Se han configurado listas para el control de acceso (ACL) para el enrutamiento entre las redes virtuales. El conmutador proporciona control de tráfico en toda la red.

Nº total de puertos:	12 puertos 'autosensing' 10/100/1000 para cable de cobre; 6 puertos fijos 1000BASE-SX; 6 puertos GBIC que pueden soportar conectores GBIC 1000BASE-SX, 1000BASE-LX ó 1000BASE-LH70 (Gigabit Ethernet de larga distancia); 1 ranura de expansión
Conexiones soportadas:	RJ-45, MT-RJ
Características de conmutación Ethernet:	Conmutación 'full-rate' sin bloqueos, en todos los puertos Ethernet; auto negociación full-/half-duplex y control de flujo; soporte 802.1Q VLAN, 802.1p y priorización multinivel del tráfico; conmutación de Nivel 3 con soporte para el direccionamiento IP

[39] http://www-search.cisco.com/application/pdf/en/us/guest/products/ps5855/c1031/cdccont_0900aecd8019dc1f.pdf

	unicast; soporte RIP/RIPv2; ARP, ICMP, CIDR, UDP Helper, multiredes IP y listas de control de acceso
Administración:	Administración basada en WEB, Administración por CLI (interfaz de línea de comandos), Administración SNMP vía el software 3Com Network Supervisor.

Tabla 2.3: Especificaciones técnicas switch 3Com 495040

2.2.2.3. Switch SuperStack 3Com 3226 y 3250

Figura 2.5: Switch de piso

Constituyen los equipos de conexión de pisos. El Switch 3226 de 24 puertos 10BASE-T/100BASE-TX con autosensing; el switch 3250 contiene 48 puertos 10BASE-T/100BASE-TX con autosensing. Además ambos equipos tienen 2 puertos Gigabit de uso dual que soportan conexiones 10BASE-T/100BASE TX/1000BASE-T y puertos SFP (fibra) los cuales son los utilizados para unirse al backbone de fibra.

Permiten la segmentación de la red lo que brinda un mejor rendimiento de los grupos de trabajo al enrutar el tráfico segmentándolo localmente a un área o departamento determinado, por ejemplo el departamento financiero, sin que sea necesario enviar el tráfico al núcleo para ser direccionado a su destinatario.

Puertos: SuperStack 3226 SuperStack 3250	 24 puertos 10/100 y dos puertos Gigabit de uso dual 10/100/1000 o de fibra basados en SFP. 48 puertos 10/100 y dos puertos Gigabit de uso dual 10/100/1000 o de fibra basados en SFP
Interfaces con los medios:	RJ-45 para puertos 10/100 y 10/100/1000; para SFPs, dependiendo del módulo SFP específico

[40] http://www.3com.com/prod/es_ES_EMEA/detail.jsp?tab=features&sku=3C17706-US

Características de Switching Ethernet Layer 2:	Velocidad completa (full-rate) sin bloqueo en todos los puertos Ethernet, auto negociación full-/half-duplex y control de flujo, filtrado multicast de layer 2, soporte para 802.1Q VLAN, priorización de tráfico 802.1p, IGMP snooping
Características de Switching Ethernet Layer 3:	Rutas estáticas; rutas Layer 3 dinámicas RIP Soporta routing dinámico (RIP), facilitando la configuración y el mantenimiento continuo de la red

Tabla 2.4: Especificaciones técnicas switch de piso41

2.2.2.4. Switch 3Com 4226T

Permite la conexión de los equipos destinados para el control del edificio. A este equipo se conectan los servidores que administran y almacenan la información generada por los dispositivos de control de accesos, CCTV, sistema contra incendios, etc. Este dispositivo con puertos Ethernet y Fast Ethernet proporciona 24 puertos 10/100 y 2 puertos Ethernet Gigabit 10/100/1000 fijos. Se conecta al switch principal a través de un patch cord de cobre.

Descripción del producto	3Com SuperStack 3 Switch 4226T - conmutador - 24 puertos
Factor de forma	Externo - 1 U
Garantía del fabricante	Garantía limitada de por vida
Características	Control de flujo, capacidad full/half duplex, conmutador MDI/MDI-X, negociación automática, soporte VLAN, activable, apilable multicast Layer 2 filtering, , 802.1p traffic prioritization, IGMP snooping
Cantidad de puertos	24 x Ethernet 10Base-T, Ethernet 100Base-TX
Velocidad de transferencia de datos	100 Mbps
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Cumplimiento de normas	IEEE 802.3, IEEE 802.3U, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1w

[41] http://www.3com.com/prod/es_ES_EMEA/detail.jsp?tab=features&sku=3CR17500-91

Modo comunicación	Semidúplex, dúplex pleno
Protocolo de gestión remota	SNMP, RMON, HTTP
Puertos auxiliares de red	2x10/100/1000Base-T

Tabla 2.5: Especificaciones técnicas switch 3Com 4226T

2.2.2.5. Switch Cnet CNSH-1600

Dispositivo utilizado para la conexión entre router cisco y el firewall, además se conecta una cámara Polycom para video conferencia vía IP. La cámara permite realizar videoconferencia a través de una línea ISND o vía IP para lo cual necesita que se asigne dirección IP real y no se encuentre tras de un servidor Firewall.

Estándares Soportados	10Base-T IEEE 802.3, 100Base-TX IEEE 802.3u , 10Base-T IEEE 802.3 , 100Base-TX / FX IEEE 802.3u
Puertos	16 100Base-TX (15 100Base-TX, un 100Base-FX
Ancho de Banda	100BASE-TX 200 / 100 / 20 / 10Mbps 100BASE-TX 200 / 100 / 20 / 10Mbps 100BASE-FX 200 / 100/ Mbps
Latencia	11 μsec a 100Mbps, mínimo 75 μsec a 10Mbps, mínimo
Memoria en Buffer	4 Mbyte
Modos Duplex	Auto-Negociación, Half y Forzado Full-Duplex por DIP switch (puerto de fibra óptica solamente)
Crossover	15 puertos y un Puerto extra para función de Crossover
Certificaciones	FCC Class A, CE Mark

Tabla 2.6: Especificaciones técnicas switch Cnet42

2.2.2.6. Servidor IBM eServer xSeries 226

Se cuenta con 2 servidores IBM eServer xSeries 226, para la gestión y administración de la red. La información más importante esta almacenada o es administrada por los servidores.

[42] http://www.pcenlinea.com/mp/18357.html

El primer servidor corresponde a un servidor de base de datos, utiliza Sistema operativo Linux Enterprise y como motor de base de datos Oracle. En el se almacena la información financiera, pagos en línea y próximamente, información correspondiente a la gestión académica.

El segundo servidor con sistema operativo Windows 2003 Server realiza principalmente para la gestión de usuarios. Utiliza Active Directory para la administración de usuarios y grupos de usuarios, compartir archivos, gestión de impresoras y aplicaciones. Además es el servidor antivirus con herramientas Symantec corporativas.

Las características principales[43].

- Torre con capacidad de 2-vías con capacidad de rack de 4U vía conjunto opcional de montaje en rack
- Un procesador Intel® Xeon®. 2.8 GHz, con velocidad de bus frontal de 800MHz, 2MB de Cache L2 e Intel Extended Memory 64 Technology proporcionando protección a la inversión
- 512 MB de memoria RAM PC2-3200 DDR2 (Máximo 16 GB)
- Adaptador de hardware ServeRAID 7t previamente configurado para el modelo SATA; ServeRAID 6i previamente configurado más adaptador de hardware para el modelo SCSI
- El modelo SCSI ofrece hasta 6 unidades de disco rígido Ultra320 SCSI hot-swap. El modelo SATA ofrece cuatro HDDs Serial ATA de 250GB de cambio simple (1TB) de capacidad de disco estándar.
- 2 discos duros SCSI de 70 Gb.
- 1 Tarjetas de red Intel Pro/1000
- 1 Tarjeta de red Broadcom NetXtreme Gigabit Ethernet
- Unidad CDROM
- Unidad de CDWRITER
- Microsoft Windows Storage Server 2003 con Print and Storage Manager 2.0 previamente cargados.

[43] http://www.ibm.com/bo/products/servers/

2.2.2.7. Servidor IBM eServer xSeries 220

El servidor IBM eServer corresponde al servidor Web, Proxy y correo electrónico. Corresponde el servidor en el cual reside el portal Web de FLACSO (www.flacso.org.ec), a través de el se permite el acceso al Internet a todos los usuarios que se conectan a la red de FLACSO, sea por conexión con cable o inalámbrica posteriormente.

También se administra el servicio de correo electrónico de la institución. Todo funcionario mantiene una cuenta de correo electrónico. El servidor mantiene reglas de bloqueo para reducir la posibilidad de ataques a través de él, puesto que se constituye prácticamente en la puerta de entrada/salida a la red FLACSO.

Las características principales son:
Dos procesadores Intel Pentium III de 1.01 GHz.; 1 GB. De memoria RAM; Tarjeta de video con 16 Mb; Disk drive de 3.5", 1.44 MB; 3 discos duros de 36.4 Gb SCSI, no hot plegables; 2 Tarjetas de red 10/100 Mbps Intel integrado; CDROM 48X; unidad de tape back up de 12/24 GB; Monitor SVGA color 15".

2.2.2.8. Servidor de comunicaciones

Se encarga de la gestión del correo de voz, se encuentra conectado a la central telefónica, y a través de una aplicación propietaria del proveedor, el equipo almacena los mensajes de voz y luego los envía a la dirección de correo electrónico de cada uno de los usuarios

Características principales:

- Clon procesador AMD Semprom 2200+
- 256 MB de memoria RAM
- Disco duro de 80 Gb.
- Tarjeta de red 10/100 Mbps Intel
- CD ROM 52X.

2.2.2.9. Servidor de filtrado de correo

Con sistema operativo Windows 2003 Server, el equipo se encuentra entre el Firewall y el servidor de Web y de correo, se encarga del filtrado antivirus y antispam de correo electrónico y también se lo utiliza para filtrar el acceso a sitios no autorizados de Internet (páginas con contenido obseno, descargar música y vídeo, etc.).

Características principales:

Clon Pentium IV de 3 GHz
1 GB de memoria RAM
2 discos duros de 120 Gb.
Tarjeta de red 10/100 Mbps Intel
CD ROM 52X.

2.2.2.10. Firewall 3Com SuperStack

Se constituye en el punto de control de la entrada y salida de tráfico de la red de datos de FLACSO. Provee la protección a la infraestructura informática, pero en ningún caso se considera suficiente. Por ello se tiene reglas configuradas reglas en otros equipos de comunicación.

Su administración es muy sencilla y práctica puesto que se la realiza a través de una interfaz gráfica basada en Web. Presenta una conectividad privada virtual basada en IPSec permitiendo un acceso seguro.

Características principales[44]:

Métodos de encriptación soportados: ARC4, DES, 3DES
Asociaciones de seguridad de grupo: 1.000
Clientes VPN soportados: 64.000 simultáneos (modo de clave manual)
Puertos: tres puertos RJ-45 10/100BASE-T (LAN, WAN, DMZ); conector de fuente de alimentación redundante Tipo 1

[44] http://www.3com.com/prod/es_LA_AMER/detail.jsp?tab=features&sku=3CR16110-95-US

Indicadores LED: energía, alerta, indicación de velocidad Ethernet/enlace de puerto, actividad de puerto/configuración duplex
CPU: 233 MHz StrongARM RISC
RAM: 16 MB
Flash: 4 MB
Aceleración: Reloj de tiempo real
Reloj de tiempo real: batería litio-ion
Alto: 4,4 cm (1.7 in)
Ancho: 44 cm (17.3 in)
Fondo: 22,9 cm (9.0 in)

2.2.2.11. Estaciones de trabajo

Las estaciones de trabajo en su gran mayoría están compuestas por estaciones CLONES, en lo que respecta a sus configuraciones y características es muy variada. Existen pocos equipos de marca HP, IBM, Compaq.

El sistema operativo utilizado es Windows 2000 y Windows XP en la mayoría de las estaciones de trabajo, aunque existen todavía 5 estaciones de trabajo con Windows 98.

Las impresoras se encuentran distribuidas a lo largo de todo el edificio, la principal política ha sido la de implementar impresoras máximo 2 por piso, solo se instalan únicamente en áreas que requieran o sea necesario una impresora personal. La marca predominante de las impresoras es HP, además existen dos impresoras Epson y una Samsung. La mayoría son impresoras láser.

En la tabla No. 2.7 se muestra un resumen de la distribución por pisos de las estaciones de trabajo.

Piso	**PC**	**Impresoras**	
		Personales	**Red**
9	7	2	1
8	20	0	2

7	30	0	2
6	30	0	4
5	16	2	2
4	5	3	1
3	41	0	2
2	0	0	0
1	5	0	1
0	10	1	1
-1	5	2	0
-2	8	0	1
-3	0	0	0
-4	1	0	0
Total	178	10	17

Tabla 2.7: Resumen de computadores e impresoras

2.3. SERVICIOS QUE BRINDA ACTUALMENTE

La responsabilidad de la administración, configuración, instalación y operación tanto del hardware como software está delegada al área de las TIC (Tecnologías de Información y Comunicación) que depende de la Subdirección Administrativa Financiera. El departamento de las TIC es la instancia que se encarga de la gestión de todo lo referente a los servicios que se brinda al interior de la sede en lo que respecta a tecnologías, brindando apoyo tanto en las tareas administrativas, financieras, de apoyo y en especial a las labores docentes e investigación.

Los servicios de la red de datos que se brindan en la actualidad a los usuarios son accesibles prácticamente casi en su totalidad a través de una conexión por cable. Solo en biblioteca se encuentra instalado un punto de acceso al cual se conectan 4 estaciones de trabajo que están destinadas exclusivamente para la consulta del fondo bibliográfico de la biblioteca.

TCP/IP es el protocolo utilizado para la conexión y transmisión de información al interior de la institución. Los servicios que se brinda por medio de la red de datos utilizan TCP/IP para su difusión y utilización. La red de datos brinda varios servicios para efecto del presente proyecto nos referiremos específicamente a los servicios que se brindarán a través del acceso inalámbrico de manera directa (Internet) o indirecta (Antivirus corporativo).

2.3.1. SERVICIO DE REGISTRO DE USUARIOS

El servidor IBM xSeries con sistema operativo Windows 2003 Server, en el se realiza la gestión de usuarios y sus perfiles para el acceso al dominio de la red de datos. En el servidor se definen las características y permisos de cada uno de los usuarios o grupos de usuarios dispondrán para el uso de aplicaciones o servicios de la red de datos.

2.3.2. SERVICIO DE ARCHIVOS

Cuando un usuario registrado inicia una sesión se crea una unidad virtual Z: que corresponde a un directorio compartido en el servidor, donde el usuario puede almacenar su información más importante, este espacio cuenta con una cuota previamente establecida y que es común para todos los usuarios. El usuario podrá acceder a esa carpeta desde cualquier estación que se encuentre en el interior del campus ingresando su nombre de usuario y contraseña.

El mismo servidor también se comparte e instalan las aplicaciones que cada usuario o departamento requieren para desarrollar sus actividades; por ejemplo tenemos el grupo que accede a la aplicación para el control de inventarios; la aplicación para la gestión financiera; la aplicación y base de datos para consulta del fondo bibliográfico de biblioteca.

2.3.3. SERVICIOS DE IMPRESIÓN

En el interior de institución se tiene como política la instalación de una impresora por área o departamento. Solamente en casos en que no exista la disponibilidad de compartir una impresora entre varios funcionarios, sea por seguridad, ubicación (librería) o por las actividades de un determinado funcionario (elaboración de cheques), se instalan impresoras personales.

Las impresoras de red son instaladas como un equipo completamente independiente, con dirección IP fija y son instaladas en lugar de uso común en los departamentos (máximo 2 por piso) de la institución.

2.3.4. SERVICIO DE CORREO ELECTRÓNICO

La administración y operación del servidor de correo electrónico esta a cargo del departamento de las TIC. Todo usuario académico, investigador, estudiante, administrativo, financiero o de apoyo dispone de una dirección de correo electrónico.

Para acceder a revisar su correo electrónico lo puede hacer desde su puesto de trabajo utilizando la aplicación cliente que viene provista en el mismo sistema operativo (Outlook Express) o desde cualquier sitio que tenga acceso a la red (en el interior del campus) o acceso a Internet (desde el exterior del campus) utilizando un navegador Web (Internet Explorer).

2.3.5. SISTEMAS DE BASES DE DATOS

La gestión y almacenamiento de la información crítica de la sede se encuentra garantizada por el uso de tecnología Oracle. En la actualidad se encuentra en desarrollo una aplicación para la gestión de la información académica y, a la que se podrá acceder a la información proporcionando un nombre de usuario y contraseña a través de un navegador Web por parte de los estudiantes y profesores.

También se publicará para la Web el fondo bibliográfico de Biblioteca, en ella los usuarios además de poder consultar las publicaciones que dispone la Biblioteca, podrán verificar si un libro esta reservado y/o reservar libros.

Finalmente otra aplicación es la que comprende a lo referente a cobros en línea de inscripciones, matrículas, colegiaturas, eventos, publicaciones. La notificación vía correo electrónico a cada una de los funcionarios o departamentos involucrados para su correspondiente registro y en otros casos despacho y envío de los productos que se ofertan.

En cada uno de los casos citados anteriormente cada base de datos tiene o tendrá su aplicación independiente con la cual manipularán la información residente en ellas de acuerdo a los perfiles asignados a cada usuario.

2.3.6. SERVICIO WEB Y PROXY

La institución de igual manera administra y actualiza la página Web[45] en la cual brinda información institucional, docente, investigaciones, eventos, publicaciones, etc.

Uno de los servicios que se pueden encontrar a través del Web es el pago en línea tanto de inscripciones, matrículas, colegiaturas, publicaciones y eventos.

También se incluirá en el Web, el acceso a la información académica de todos los estudiantes de FLACSO. Así como también la consulta y reserva del fondo bibliográfico de la Biblioteca.

Otro servicio que se brinda a través de la página Web es el acceso a los eventos que se programan y que están disponibles en línea sea en vivo o pregrabados.

---

[45] www.flacso.org.ec

Todos los usuarios que se registran y tienen permiso en la red acceden de manera directa a Internet. El uso de Internet es muy importante en el desarrollo de las actividades especialmente docentes y de investigación. Tanto profesores, investigadores, ayudantes y estudiantes requieren de una conexión continua y rápida al Internet. Para ello se provee el acceso a Internet por medio de un servidor Proxy, a través del cual se ha implementado algunas políticas comunes para el uso del Internet.

2.3.7. VIDEOCONFERENCIA

Otro servicio que brinda FLACSO es la de videoconferencia especialmente mediante enlaces ISDN. Se cuenta con tres líneas ISDN de 128 kbps para la conexión, con una cámara Polycom multipunto permitiendo el enlace hasta con 3 puntos de manera simultanea. La videoconferencia a través de IP presenta problemas de retardo en la trasmisión de la señal, en especial el vídeo; debido que es el mismo canal que utilizan el resto de funcionarios de la institución para navegar por Internet, enviar y recibir correos electrónicos, lo que provoca la saturación del canal

2.3.8. EDUCACIÓN VIRTUAL

Un servicio muy importante que brinda FLACSO es la educación virtual[46], para lo cual la institución contrata la plataforma WebCT, y esta alojada en un servidor hosting en Florida, Estados Unidos. La plataforma para la educación virtual la mantienen por alrededor de 3 años aproximadamente.

Los cursos dictados en línea están disponibles tanto para uso de los estudiantes regulares de los postgrados ofertados por FLACSO como para estudiantes externos que se interesan en un curso específico.

[46] www.flacsovirtual.edu.ec

2.3.9. SERVICIO DE PROTECCIÓN ANTIVIRUS

El servicio de protección antivirus esta gestionado de manera corporativa, para lo cual se ha instalado en el servidor IBM y en cada una los clientes una aplicación antivirus y antispam. Las actualizaciones de las definiciones de virus se actualizan diariamente en el servidor y los usuarios las actualizan automáticamente el momento de iniciar una sesión en el servidor.

Adicionalmente, para el filtrado del correo electrónico de virus y correo basura (spam) se ha instalado un equipo CLON con sistema operativo Windows 2003 al cual se lo a ubicado entre el servidor de correo y el firewall, así cada correo es revisado antes de ser entregado al servidor y posteriormente a los clientes.

2.4. ADMINISTRACIÓN DE RED

La administración de la red de datos la efectúa el departamento de las TIC, la gestión de la red se la realiza a través del servidor Windows 2003 Server. El servidor Windows 2003 gestiona el servicio de DNS (flacso.org.ec) al interior de la red LAN. Adicionalmente se realizan tareas de administración en los servidores que brindan otros tipos de servicios:

En el servidor Proxy que esta implementado sobre un servidor Linux, se configuran bloqueos de direcciones no permitidas (direcciones con carácter obsceno, audio, vídeo, juegos, etc.). Se revisan y analizan los logs de transacciones para monitorear su uso.

El servidor de correo utiliza el servicio sendmail de Linux y mantiene una lista de direcciones de correo o dominios no deseadas o están clasificadas en listas negras, de igual manera la configuración para evitar posibles ataques de spam, para no permitir que el servidor sea utilizado para envío y recepción de correo basura.

Se realizan tareas de backup automático y manual para las aplicaciones y bases de datos, así como de los archivos de configuración de los servidores. En la actualidad se encuentran implementando un plan para el respaldo de la información que se almacena en cada una de las estaciones de trabajo.

A través de la herramienta MRTG se monitorea el uso del canal dedicado para el acceso al Internet y que es provisto por Impsat.

De lo expuesto anteriormente no existe una herramienta formal para el monitoreo y gestión de la red. Para poder obtener datos que nos permitan tener una visión clara de la situación actual del uso de la red se ha realizado encuestas al personal que labora, estudia y visita la institución ya sea por eventos, uso de la biblioteca, cafetería, entre otros. También se utilizó la herramienta Sniffer Pro V4.6 de Network Associates.

Del análisis de las 40 encuestas realizadas, se obtienen que 87.5% de los encuestados utilizan la red de datos actual; el 75% no ha tenido ningún problema en el uso de la red local; el 82.5% utiliza la red para navegar en el Internet y para el envío y recepción de correo electrónico; el 25% opina que la red es lenta; otro 25% ha tenido problemas de contagio de virus; y, el 20% tiene problemas de restricciones de acceso debido a las reglas que se mantienen configuradas en el servidor para navegar en Internet. Para mayor información referirse al ANEXO 3.

Luego capturar información del uso de la red con la herramienta Sniffer Pro, se ha determinado, que los protocolos de mayor uso al interior de la red es http, https, smtp y pop3, lo que también se ha reflejado en las encuestas realizadas y que se encuentran en el ANEXO 3. Para mayor información referirse al ANEXO 4.

2.4.1. VLANS

El direccionamiento IP esta segmentado, para lo cual se utilizan VLAN's al interior de la sede. Las VLAN's están organizadas por área o dependencia, conforme se muestra en la tabla No.` 2.8

VLAN	Área	Departamentos
1	Administración TIC	Servidores, core (MDF), switch de pisos (SDF)
2	Dirección	Dirección, subdirecciones y áreas de apoyo
3	Académico	Profesores, investigadores, ayudantes, atención a estudiantes.
4	Administrativo	Coord. Administrativa, RRHH, Servicios generales, bienestar estudiantil, médico.
5	Financiero	Coord. financiera, tesorería, presupuesto, contabilidad, impuestos
6	Estudiantes	Centros de computo, aulas
7	Biblioteca	Biblioteca
8	C. Convenciones	Auditorios, salas de sesiones

Tabla 2.8: VLAN por departamentos

La VLAN 1 se destina para la interconexión de todos los dispositivos que conforman la parte activa de la red (switch, firewall, servidores) y se permite todo tráfico desde y hacia todas las VLAN's. Las reglas de trasmisión o comunicación entre VLAN's se las define en el switch central (core). A continuación en la figura 2.6 se presenta la distribución de las VLAN's en el edificio.

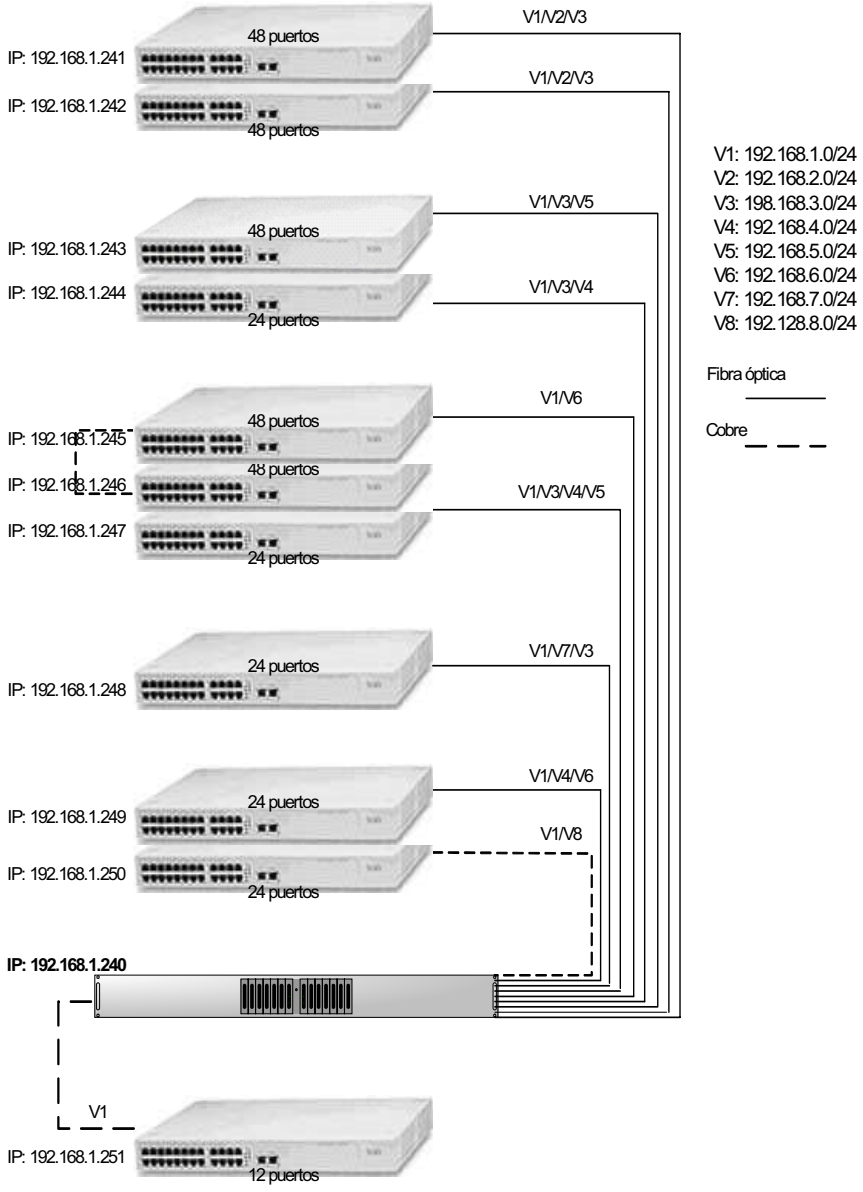


Figura 2.6: Distribución de las VLAN's en el edificio

2.4.2. ANCHO DE BANDA

El ancho de banda utilizado al interior de la sede entre los dispositivos de interconexión tales como servidores, switch de pisos y switch central es de 1 Gb, El tráfico en las redes horizontales en cada piso es de 100 Mbps, esto debido a que cada las interfaces de red de las estaciones de trabajo y los puertos ethernet de los switch de pisos manejan máximo esta velocidad.

Según el análisis realizado con la herramienta Sniffer Pro (Anexo 4), la utilización del ancho de banda de la red local no se encuentra saturado.

2.4.3. GESTIÓN DE USUARIOS

La gestión de usuarios se la realiza con el Active Directory de Windows 2003 Server. La gestión de los grupos de trabajo es jerárquica y toma como base los grupos implementados en las VLAN's en la red, adicionando subgrupos a cada uno de los grupos principales, por ejemplo: La VLAN académica, se divide en subgrupos profesores, investigadores, becarios, asistentes, estudiantes.

Los perfiles se definen y asignan a nivel del subgrupo y/o por usuario.

2.4.4. GESTIÓN DE BASE DE DATOS

La base de datos utilizada para el almacenamiento de la información crítica de la FLACSO es ORACLE y esta implementada sobre un servidor con sistema operativo Linux Enterprise. Entre las aplicaciones que se enlazan con la base de datos esta la aplicación para la gestión financiera que utiliza una interfaz propia; pagos en línea a través de un navegador Web y que se enlaza con el servicio todo1 del Banco del Pichincha; actualmente en desarrollo la aplicación para la gestión de la información docente, con una interfaz que utiliza un navegador Web.

2.5. POLÍTICAS DE SEGURIDAD

La seguridad es preocupación constante en el área de las TIC en el interior de la organización. Entre los temas de seguridad se preocupa tanto de la seguridad física de los equipos como de la seguridad de la información que circula en la red o se almacena en los diferentes repositorios como son bases de datos, estaciones de trabajo, impresoras, etc.

2.5.1. SEGURIDAD FÍSICA

En lo que se refiere a la seguridad física de los equipos además de la seguridad provista por los guardias de seguridad y las puertas con sus respectivas cerraduras, se cuenta con un sistema de accesos a través de tarjetas de proximidad, la tarjeta de proximidad cuenta con un chip en el cual se configura los permisos de acceso a los diferentes espacios, si se puede decir privados del edificio (oficinas). El usuario debe pasar la tarjeta sobre el sensor que se encuentra ubicado en la puerta de ingreso al piso, esto se registra en el servidor de acceso ubicado en el cuarto inteligente del subsuelo 2, la puerta se abrirá siempre y cuando el usuario tengo permiso para acceder a ese piso.

Otro método para la seguridad física del edificio constituye en CCTV (circuito cerrado de televisión), en los hall's principales de cada uno de los pisos altos, en el centro de convenciones, ascensores, parqueaderos y al ingreso al edificio, se instalaron cámaras para el monitoreo de todo el edificio, el video de cada cámara es almacenado en el servidor de CCTV y se mantiene la copia hasta por 30 días.

2.5.2. SEGURIDAD DE LA INFORMACIÓN

Otro punto crítico de seguridad es el que se refiere a la seguridad de la información, tanto la almacenada en los servidores y los pc's personales, como la que circula por el canal de la red.

La seguridad de la información se ha implementado en varios equipos o sistemas. A continuación se describe los niveles de control y seguridad para el acceso a la información.

2.5.2.1. Seguridad en correo electrónico

La gestión del servidor de correo electrónico se lo realiza con el servicio de mail (sendmail) de Linux, el servicio esta configurado para evitar que sea utilizado

como servidor de correo no deseado (spam). Además contiene un archivo que mantiene una lista de direcciones de correo a las cuales se consideran no deseadas y que por lo general se identifican como portadoras de correo o corresponden a cuentas de spam.

Se mantienen también, un filtro de contenido de correo y tipos de archivos adjuntos (.pif, .doc, .xls, etc.), esto se lo realiza a través del servidor de antivirus symantec corporativo.

2.5.2.2. Seguridad para el acceso a Internet

El acceso al Internet por parte de los usuarios se lo realiza a través del servicio de Proxy (squid) de Linux, para el control se mantiene listas de control de acceso ACL, en las cuales se define el orden de navegación y las redes que están autorizadas para navegar por Internet (por ejemplo: la red 192.1.0.0).

Además de mantener filtros de contenidos y direcciones Web (URL), para las cuales no se permiten el acceso a ningún ordenador de la red de FLACSO.

2.5.2.3. Seguridad en las computadoras

Se han generado VLAN's de acuerdo a cada una de las áreas que componen FLACSO Ecuador, por lo que cada computador que se conecta a la red de datos esta asociada a una VLAN. Esto permite que la información que circula en la VLAN 2 no pueda ser interceptada por un equipo que se encuentra en la VLAN 3.

Debido que todas las computadoras contiene sistema operativo Microsoft, la posibilidad de un contagio de virus es mayor; por lo que, cada computador tiene instalado un antivirus que se actualiza diariamente a través del servidor.

Constantemente se actualizan e instalan parches y services pack a los sistemas operativos, con el objetivo de evitar vulnerabilidades en los sistemas.

Una vulnerabilidad que se mantiene corresponde al respaldo de la información residente en cada una de las computadoras. Los respaldos en su mayoría esta ha cargo del propio usuario. Solo se obtienen respaldos los servidores y configuración de los equipos críticos o de comunicación de la red. El respaldo de la información de los usuarios se los realiza únicamente bajo pedido expreso por el usuario al área de TIC.

2.5.2.4. Seguridad en el router

El ruteador es el equipo que une la red local con el Internet, por esta razón, se constituye en el primer filtro de seguridad desde el Internet hacia la red local; para ello se han declarado ACL's, en las cuales se configura para que redes están permitidas el tráfico; los protocolos y puertos que pueden usar para la transmisión de la información.

No se permite el acceso a la administración (telnet, ssh) desde el Internet, solamente se administra desde la red local; además, los únicos equipos que puede administrar el router son los usados por los responsables de las TIC, no cualquier equipo que se conecte a la red local puede acceder a la configuración del router.

2.5.2.5. Firewall

El equipo con plataforma Ethernet 10/100 Mbps preconfigurada ayuda a proteger la intranet de las amenazas de Internet. Se constituye en el equipo central de seguridad de la red local. Contiene tres puertos RJ-45 10/100BASE-T para la LAN, WAN y DMZ.

En el puerto WAN se conecta con el router para la comunicación con el Internet. El puerto LAN se conecta toda la red local de FLACSO incluidos los servidores; y, el puerto DMZ (zona desmilitarizada), actualmente no tiene conectados ningún dispositivo, puesto que como se explico anteriormente los

servidores comparten varios servicios que no pueden ser separados o aislados del Internet y de la red local.

La administración se la realiza a través de una interfaz gráfica basada en Web.

CAPITULO 3: DISEÑO DE LA WLAN

3.1. METODOLOGÍAS DE DISEÑO DE RED

Tener un conocimiento teórico de las tecnologías de redes WLAN, entender como funcionan y como viajan las señales inalámbricas de un lado a otro es muy importante para planificar la red, pero si no se consigue que todos los dispositivos que la conforman se comuniquen entre sí, todo resultaría inútil.

Una definición interesante de metodología es: “Siendo el método un modo ordenado de decir o hacer una cosa determinada, podemos decir que la metodología es un conjunto de métodos que se siguen en una investigación científica”[47].

Una metodología de diseño de red es una serie de pasos fundamentales y necesarios para diseñar la red de manera efectiva, identificando todos los dispositivos que se requieran conectar.

La metodología más adecuada será la que cumpla o se ajuste al objetivo propuesto, para esto debemos apoyarnos en un plano, el mismo que debe estar presente desde el inicio hasta el final del diseño.

3.1.1 METODOLOGÍA CISCO PARA EL DISEÑO DE REDES LAN

Detalla los pasos a seguir para diseñar una red. No es necesario ejecutar todas estas tareas al realizar el proyecto de cableado estructurado. Muchas de las decisiones son tomadas por el diseño de red y el administrador de red existentes. Sin embargo, éste es el proceso que eventualmente se debe seguir.

---

47 http://www.crefal.edu.mx/biblioteca_digital/CEDEAL/acervo_digital/coleccion_crefal/cuadernos/cua16/cap3.pdf

El diseño de red debe tener en cuenta las tecnologías, como, por ejemplo, Token Ring, FDDI y Ethernet. Una vez que se ha decide la tecnología a utilizar, se debe desarrollar una topología de LAN de Capa 1. Se debe determinar el medio y tipo de conexión a utilizar. Se debe generar una topología lógica y una física.

A continuación se desarrolla una topología de LAN de Capa 2, es decir, agregar dispositivos de Capa 2 a la topología a fin de mejorar sus capacidades. Se puede agregar switches para reducir la congestión y el tamaño de los dominios de colisión.

El siguiente paso consiste entonces en desarrollar una topología de Capa 3, es decir, agregar dispositivos de Capa 3, que también aumentan las capacidades de la topología. En la Capa 3 es donde se implementa el enrutamiento, se puede utilizar routers que imponen una estructura lógica en la red que se está diseñando.

También se debe tener en cuenta el enlace de LAN a las WAN e Internet. Como siempre, se debe documentar las topologías física y lógica del diseño de red. La documentación debe incluir ideas, matrices de resolución de problemas y cualquier otra nota que haya realizado mientras tomaba sus decisiones.

Para que una LAN sea efectiva y pueda satisfacer las necesidades de los usuarios, se debe implementar siguiendo una serie sistemática de pasos planificados.

El primer paso en el proceso es reunir información acerca de la organización. Esta información debe incluir:

1. Historia de la organización y situación actual
2. Crecimiento proyectado
3. Políticas de operación y procedimientos administrativos
4. Sistemas y procedimientos de oficinas
5. Opiniones del personal que utilizará la LAN

El segundo paso es realizar un análisis y evaluación detallados de los requisitos actuales y proyectados de las personas que usarán la red.

El tercer paso es identificar los recursos y limitaciones de la organización. Los recursos de organización que pueden afectar a la implementación de un nuevo sistema LAN se dividen en dos categorías principales: hardware informático/recursos de software, y recursos humanos. Es necesario documentar cuál es el hardware y software existentes de la organización, y definir las necesidades proyectadas de hardware y software. Las respuestas a algunas de estas preguntas también le ayudarán a determinar cuánta capacitación se necesita y cuántas personas se necesitarán para soportar la LAN. Entre las preguntas que realice deberán figurar las siguientes:

1. ¿Cuáles son los recursos financieros disponibles de la organización?
2. ¿De qué manera se relacionan y comparten actualmente estos recursos?
3. ¿Cuántas personas usarán la red?
4. ¿Cuáles son los niveles de conocimiento sobre informática de los usuarios de red?
5. ¿Cuáles son sus actitudes con respecto a los computadores y las aplicaciones informáticas?

Si sigue estos pasos y documenta la información en el marco de un informe formal, esto ayudará a estimar costos y desarrollar un presupuesto para la implementación de una LAN.

La siguiente lista incluye parte de la documentación que debe generarse durante el diseño de la red:

- Diario de ingeniería
- Topología lógica
- Topología física
- Plan de distribución
- Matrices de solución de problemas
- Tomas rotuladas
- Tendidos de cable rotulados

- Resumen del tendido de cables y tomas
- Resumen de dispositivos, direcciones MAC y direcciones IP

3.1.2 METODOLOGÍA DE DISEÑO DE RED LOCAL INALÁMBRICA WI-FI

El Colegio Oficial de Ingenieros de Telecomunicación[48] en su documento "La situación de las Tecnologías WLAN basadas en el estándar IEEE 802.11 y sus variantes ("Wi-Fi")", presentan una metodología de despliegue de red inalámbrica que deberá contemplar los siguientes aspectos:

- Especificaciones de la red.
- Dimensionado y determinación del equipamiento.
- Planificación radioeléctrica.
- Cálculo del nivel de emisiones radioeléctricas.
- Despliegue.
- Certificación y puesta en servicio.
- Gestión de Red y Provisión de Servicios.

En la tabla 3.1` se muestran los objetivos que se realizan en cada uno de los apartados propuestos de la metodología.

	Objetivos	Entrada	Salida
Especificaciones	Análisis de los requisitos de red en términos de capacidad, funcionalidad y servicios. Generación de la especificación técnica de la red.	Requisitos y datos del cliente. Estructura de los edificios. Infraestructura de la red cableada. Permisos especiales. Normativa vigente.	Especificación funcional de la red: Capacidad y funciones.
Dimensionado	Determinar las	Especificación de	Estándar

[48] http://www.coit.es

	capacidades y equipamientos necesarios para el funcionamiento de la red.	la red y el servicio. Potenciales usuarios. Información de la zona de despliegue: área de cobertura, tipo de edificio, capacidad esperada. Tipo de servicios. Políticas de seguridad. Condiciones ambientales.	inalámbrico seleccionado. Equipamiento necesario. Arquitectura de red. Capacidades de datos, política de enrutamiento y enlace red troncal. Eficiencia en prestaciones y costes de inversión y explotación.
Planificación	Definir las estaciones fijas y ubicaciones exactas. Determinar prestaciones esperadas de la red en cada punto de servicio.	Dimensionado. Ubicación emplazamientos. Información geográfica detallada. Restricciones geográficas y técnicas.	Emplazamientos concretos. Nivel de señal esperada. Capacidad esperada. Composición de las estaciones: equipos, cables, antenas,… Datos para la conexión a la red
Emisiones	Cálculo de los niveles de emisiones radioeléctricas.	Características y parámetros técnicos de equipos y antenas.	Informe de cumplimiento de acuerdo con los cálculos realizados.

			Medidas de niveles de emisión.
Despliegue	Implementación física de la instalación, APs, cables, antenas, alimentación, accesorios, …	Proyecto de despliegue.	Informes de instalación, pruebas, hojas de incidencias.
Certificación	Aceptación de los emplazamientos. Efectuar puesta en servicio. Verificar conformidad de la red	Proyecto de despliegue. Informes de instalación, pruebas y hojas de incidencias.	Informe puesta en servicio y pruebas de conformidad.
Gestión de Red y provisión de Servicios	Asignación de ancho de banda por servicio y por usuario.		Gestión de Negocio. (Clientes, facturación y reclamaciones) Gestión de red y servicios: Provisión, inventario, incidencias, monitorización de red, mediación para tarificación.

Tabla 0.: Metodología para el desarrollo de proyectos de redes inalámbricas

3.1.3 METODOLOGÍA DE DISEÑO DE RED LOCAL INALÁMBRICA WI-FI EMPRESARIAL

Según Neil Reid y Ron Seide. “Muchas empresas son grandes, formadas de por lo menos cientos de individuos, que a su vez de alguna forma, son usuarios de la infraestructura de información de la organización. No obstante, que estos individuos, pueden estar localizados en un edificio corporativo o universitario, la empresa normalmente está distribuida en forma geográfica, con usuarios repartidos a lo largo de una región, continente, o incluso del mundo”.

El primer paso que hay que dar es establecer los objetivos y luego formular un plan para alcanzarlos. Desplegar una red Wi-Fi en áreas designadas que proporcionen una cobertura confiable y ofrezca el nivel de desempeño esperado sin poner en riesgo la seguridad de la corporación.

3.1.3.1 Designación de áreas

La mayoría de las organizaciones optan al inicio por un despliegue WLAN limitado. Existen distintos criterios para definir la manera en que pueden estar limitados estos despliegues los cuales se describen a continuación.

3.1.3.1.1 Limitación del despliegue a sólo los lugares en los que es más necesario.

Esta estrategia se basa en la suposición de que cuando los usuarios de computadores portátiles están en un área base (oficina, cubículo) pueden acceder a la red a través de una conexión cableada. Por lo tanto, el despliegue Wi-Fi está limitado a los lugares donde las personas tienen a reunirse en un lugar retirado de sus escritorios. Para muchas organizaciones, esta estrategia coincide con la “regla 80-20” –despliega WLAN en 20% de los lugares donde 80% de ellas es requerida.

3.1.3.1.2 Limitación del despliegue a un edificio a la vez

En los entornos universitarios, en especial en aquellas universidades donde distintos edificios o grupos de edificios tienen asignaciones diferentes, es común que se despliegue Wi-Fi mediante un método de edificio por edificio.

3.1.3.1.3 Limitación del despliegue a edificios y grupos de trabajo temporales

En este modelo se despliega Wi-Fi no tanto por la movilidad que proporciona al usuario, sino por la movilidad que proporciona a la infraestructura. Es común que grupos de personas que pertenecen a grupos diferentes e incluso ubicaciones, se reúnan en períodos temporales para un proyecto específico. Este fenómeno ha impulsado la creación del término “redes en movimiento”. En ocasiones las organizaciones empresariales despliegan una red Wi-Fi para satisfacer estas necesidades.

3.1.3.1.4 Limitaciones del despliegue desde el exterior hacia adentro.

Controlar las adiciones y cambios en la red es un proceso costoso y que consume tiempo. Como en el caso de un edificio temporal, que puede ser alquilado, y por lo común existen complicaciones en cambios de la infraestructura.

Una LAN Wi-Fi es la mejor opción cuando se va a instalar en oficinas que no son propias, así cuando se termina el contrato es mucho más fácil retirar los equipos inalámbricos e instalarlos en el nuevo sitio de trabajo, en lugar que la red quede inmersa en las paredes del edificio que pertenece a otra persona.

3.1.3.2 Planeación de la capacidad

El siguiente paso debe ser la definición del nivel del servicio WLAN que se necesita proporcionar a los usuarios Wi-Fi. En las WLAN no existen puertos físicos, se debe usar el tamaño y la forma del área de cobertura como un medio para limitar el número de usuarios que normalmente están asociados a un punto de acceso, la cantidad de usuarios varía en la medida en que éstos entren y salgan del área de cobertura, otro factor que influye es la interferencia

y esto hace que disminuya la capacidad de salida, por lo tanto, la planeación de la capacidad para las WLAN está representada por una aproximación.

La principal pregunta que debe ser respondida es: Qué capacidad de salida deberá, en promedio ser proporcionada a cada usuario de la LAN Wi-Fi? De acuerdo a los tipos de usuarios, se tienen diferentes promedios en los requerimientos de capacidad de salida. Por ejemplo, los trabajadores de almacenes y puntos de venta que usan lectores de código de barras, tienen requerimientos bajos, mientras que los usuarios de oficinas y salones de clases que transfieren correo electrónico, exploran el Web e intercambian documentos, tiene requerimientos más grandes.

El objetivo de la planeación de la capacidad es proporcionar a los usuarios lo que necesitan.

3.1.3.3 Planeación de la cobertura: La evaluación en el sitio

El fin de la planeación de la cobertura es proporcionar a los usuarios lo que necesitan donde lo necesitan. Es un proceso mediante el cual un individuo o grupo reúne información para posteriormente hacer recomendaciones específicas sobre los tipos de puntos de acceso, antenas y otros equipos que se deben instalar y las ubicaciones específicas para estas instalaciones.

Esta evaluación toma en cuenta el diseño del edificio y los materiales con los cuales fue construido (se debe revisar planos, diagramas además de una revisión directa), los patrones de tráfico dentro del edificio, los tipos de barreras que posiblemente aparecerán en el edificio, las capacidades de rango y cobertura de los puntos de acceso que se deberán usar y la flexibilidad de esas capacidades, las tecnologías y la capacidad de salida resultante.

3.1.3.4 Diseño interno y externo de los edificios

El efecto que distintos materiales de construcción tienen en la energía de radio representa un buen punto de inicio cuando se evalúe el edificio que se debe cubrir.

Mientras más denso sea el material de construcción, evitará más que la señal RF pase a través de él, esta pérdida de la energía se la conoce como atenuación. La madera, aglomerado, paredes de cubículos, compartimientos de habitaciones contienen una cantidad relativamente de aire, mientras que los ladrillos, cemento, piedras y yeso tiene menos cantidad de aire y por lo tanto son más sólidos. El metal presenta un problema adicional ya que no solo detiene la señal sino que la refleja, creando la propagación de múltiples trayectorias.

3.1.3.5 Opciones de ubicación

Seleccionar la mejor ubicación para la colocación de puntos de acceso y antenas requiere tomar en consideración varios factores como la propagación de la señal, la estética, los costos. Cada edificio presentará distintos parámetros que sugieran la correcta ubicación de los equipos.

La colocación puede ser en las paredes, o en los techos que es generalmente la más común y la que proporciona el área de cobertura más grande (circular y omnidireccional).

3.1.3.6 Evaluación física en sitio

La evaluación en sitio es un paso absolutamente necesario en los despliegues empresariales. En lugares pequeños esta evaluación puede ser un proceso informal. Cuando se trata de lugares grandes, la evaluación puede ser muy sofisticada y requerir de profesionales que tengan un grado de entrenamiento y experiencia. Para cualquier evaluación en sitio se requiere de software, capacidades de instalación temporales, herramientas de medición y

documentación, incluso herramientas adicionales como atenuadores y paquetes de baterías.

Es indispensable realizar una supervisión y un mantenimiento continuo de la infraestructura Wi-Fi empresarial que se ha instalado. Se debe efectuar evaluaciones de sitio frecuentes, mantenimiento de red continua, administración y documentación se incrementa proporcionalmente con el tamaño del despliegue y el nivel de seguridad requerido.

3.1.4 METODOLOGÍA DE DISEÑO DE RED LOCAL INALÁMBRICA WI-FI PARA OFICINAS PEQUEÑAS, SUCURSALES Y OFICINAS DEL HOGAR.

Los aspectos que se deben tomar en cuenta para la instalación de una red Wi-Fi para oficinas pequeñas son básicamente los mismos que para una empresa grande, solo con ciertas excepciones. Para una oficina pequeña no se tiene que administrar una cantidad grande de dispositivos inalámbricos, la instalación de nuevas versiones de software se hará con menor frecuencia que en las empresas grandes.

Aspectos principales cuando se seleccione los dispositivos inalámbricos:

- Cómo se usará la WLAN?
- Quienes usarán la WLAN?
- Qué protocolo se usará 11b, 11a, o 11g?
- Cuántos puntos de acceso son necesarios?
- Qué fabricante seleccionará para los puntos de acceso y los adaptadores de cliente?
- Qué antenas seleccionará para los puntos de acceso y los adaptadores de cliente?
- Qué protocolo de seguridad usará?
- Llevará a cabo una instalación automática o personalizada?
- Dónde adquirirá en el entrenamiento para usar los dispositivos que se desplegarán y la forma de usarlos?

3.1.4.1 Cómo se usará la WLAN?

Se debe determinar la forma en que se va a usar la WLAN. Si se va a transmitir solo datos o también tráfico sensible a la latencia baja como el de voz y video.

3.1.4.2 Quienes usarán la WLAN?

En instalaciones comerciales, el propietario puede permitir que además de los usuarios internos de la pequeña empresa, los visitantes se conecten a su red y otros sitios de Internet. Esto se puede llevar a cabo sin ningún problema mediante el uso de las LAN virtuales (VLAN). Dependiendo del Punto de Acceso se puede establecer el número de VLANs, cada una de estas representa un dominio de colisión virtual y al aislar una de las VLAN en su sitio para el uso no protegido, se puede permitir que otros usuarios accedan al Internet.

La ventaja de una VLAN es mantener la seguridad en el resto de la red, además que el tráfico que proviene de los visitantes no interfiere con el de la LAN de la oficina. Aumenta la eficiencia y velocidad para que un visitante relacionado con la oficina pueda conectarse con sus servidores.

3.1.4.3 Qué protocolo se usará 11b, 11a, o 11g?

En este punto es muy importante la selección del equipo, por lo que se ha optado los AP de banda dual, de esta manera podrán funcionar dispositivos que utilicen el protocolo 802.11b o el 802.11g.

Los estándares 802.11b y 802.11g utilizan bandas de 2,4 gigahercios (Ghz) que no necesitan de permisos para su uso. El estándar 802.11a utiliza la banda

de 5 GHz. La ventaja de utilizar despliegue de estándares mixtos, 11b y 11g es la compatibilidad con productos anteriores.

3.1.4.4 Cuántos puntos de acceso son necesarios?

Para determinar el número de Aps que se necesitarán, se debe tener un promedio de los usuarios y del área en donde se van a instalar.

Según un análisis estadístico realizado por Cisco se puede tener 25 usuarios por cada AP común compatible con el estándar 11gb, funcionando bastante bien.

3.1.4.5 Qué fabricante seleccionará para los puntos de acceso y los adaptadores de cliente?

Se debe considerar lo siguiente al momento de seleccionar un fabricante de equipo 802.11:

- Desempeño
- Confiabilidad
- Interoperabilidad
- Seguridad
- Experiencia en redes
- Estabilidad financiera
- Costo

El desempeño, la confiabilidad y seguridad son 3 de los aspectos más importantes cuando se seleccionan equipos 802.11. La interoperatibilidad también es importante, especialmente debido a que la red crece y lo más común es que 2 o más fabricantes proporcionen equipos 802.11, se debe asegurar la interoperatibilidad entre los dispositivos de distintos proveedores.

La experiencia en redes también se constituye en un factor muy importante al momento de seleccionar un fabricante, puesto que garantiza que los equipos funcionen correctamente. La inversión que realiza el fabricante en la investigación y desarrollo de sus productos y la solvencia financiera de la fabricante, garantiza de cierta manera que los equipos adquiridos gozarán por un buen tiempo (varios años) de soporte y disponibilidad de repuestos.

Otro factor importante en la selección de los dispositivos se constituye la escalabilidad. Se debe considerar que en la actualidad las redes crecen continuamente y los equipos deben estar preparados para permitir su crecimiento y no se constituyan en un elemento limitante en el desarrollo y ampliación de la red.

3.1.4.6 Qué antenas seleccionará para los puntos de acceso y los adaptadores de cliente?

La selección de antenas tiene mayor importancia cuando las instalaciones se realizan en áreas grandes, para un entorno SOHO es suficiente utilizar una antena omnidireccional. Para el uso de interiores, se puede usar una antena de bastidor cuando se desee cubrir una habitación desde una esquina o una pared en la cual se instalará el AP.

Para el uso de exteriores, cuando se tenga que conectar edificios se puede utilizar una antena Yagi, o una antena omnidireccional, o si la distancia es de una milla o más, se utilizará una antena parabólica.

3.1.4.7 Qué protocolo de seguridad usará?

Se recomienda usar las medidas de seguridad máximas disponibles. Algo que se debe tomar muy en cuenta es el balance entre la seguridad y la eficiencia del negocio. El sistema de seguridad seleccionado debe ser en lo posible fácil de usar por parte de los usuarios y de administrar por los administradores, incluyendo además una interfase común a todos los usuarios.

3.1.4.8 Llevará a cabo una instalación automática o personalizada?

Se debe realizar la evaluación en sitio aun cuando se utilice un solo AP, ya que de esta manera se puede saber si existen otros radios 802.11 dentro del rango de su red y responder adecuadamente mediante la selección óptima de canales y con la implementación de medidas de seguridad apropiadas.

La evaluación en sitio se debe realizar regularmente cada cierto periodo, ya que es una herramienta excelente de diagnóstico que ayuda a administrar el entorno de radiación en el cual está la red, para ello se puede hacerlo con un computador portátil que disponga un dispositivo 802.11 e ir probando la calidad de la señal y potencia del AP en el área de cobertura.

3.1.5 SELECCIÓN DE LA METODOLOGÍA

De las metodologías mencionadas anteriormente, se ha seleccionado la METODOLOGIA DE DISEÑO DE RED LOCAL INALAMBRICA WI-FI que se detalla en el punto 3.1.2.

Se selecciona esta metodología de todas las descritas anteriormente, puesto que de acuerdo a nuestro criterio brinda los pasos a seguir de una manera ordenada y clara en el proceso del diseño de una WLAN.

Adicionalmente a la metodología seleccionada se le ha agregado en el diseño lo referente al tema de seguridad de la WLAN.

3.2. ESPECIFICACIONES DE LA WLAN

Para el diseño de la WLAN del campus de la institución se han determinado las especificaciones mínimas que se deberá cumplir.

La red debe ser accesible desde todos los puntos de las zonas de cobertura. El acceso debe, así mismo, estar controlado por el sistema central de autenticación de usuarios de la red de propósito general. Los usuarios podrán acceder tanto al Internet como a Intranet, dependiendo de las claves que se asignen. La red debe estar preparada y equipada para impedir accesos no autorizados a la red.

La cobertura debe ser la totalidad del edificio con un nivel de campo suficiente para alcanzar los 54 Mbps de capacidad pico, el nivel de señal en las zonas de interés debe superar los -80 dBm. El nivel de señal debe cubrir la plaza de ingreso al edificio.

3.2.1 ESTRUCTURA DEL EDIFICIO

El área de cobertura de la WLAN, esta especificada en la figura 3.1, se conforma de la siguiente manera. 7 pisos altos de la Torre I; primer piso, planta baja y subsuelo 1 de las Torres I y II.

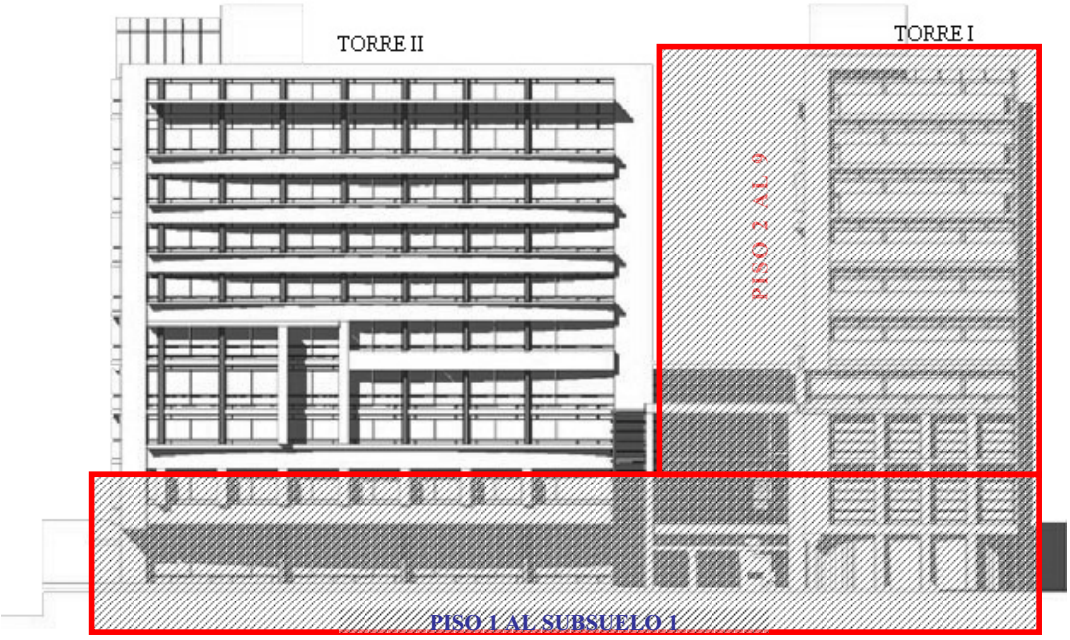


Figura 3-1: Área de cobertura

En la figura 3.2; se muestra un modelo de un piso alto, todos los pisos altos tienen dimensiones similares. Los pisos en su mayor parte las oficinas se encuentran compuestas por divisiones de aluminio y vidrio, puertas de madera.

Solamente en el piso 9 en donde se encuentra la dirección y los pisos 3, 2 y 1 en la zona que corresponde a aulas se encuentran divisiones con paredes de concreto.

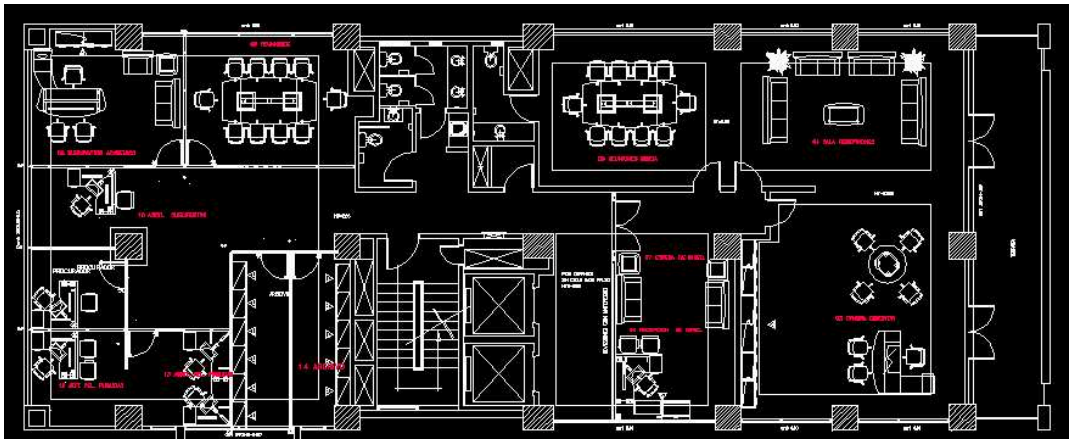


Figura 3-2: Plano piso 9

En la figura 3.3; se muestra un plano de la constitución del subsuelo 1 que corresponde al Centro de Convenciones y se constituye en el área principal en la cual se desea brindar la cobertura de la WLAN

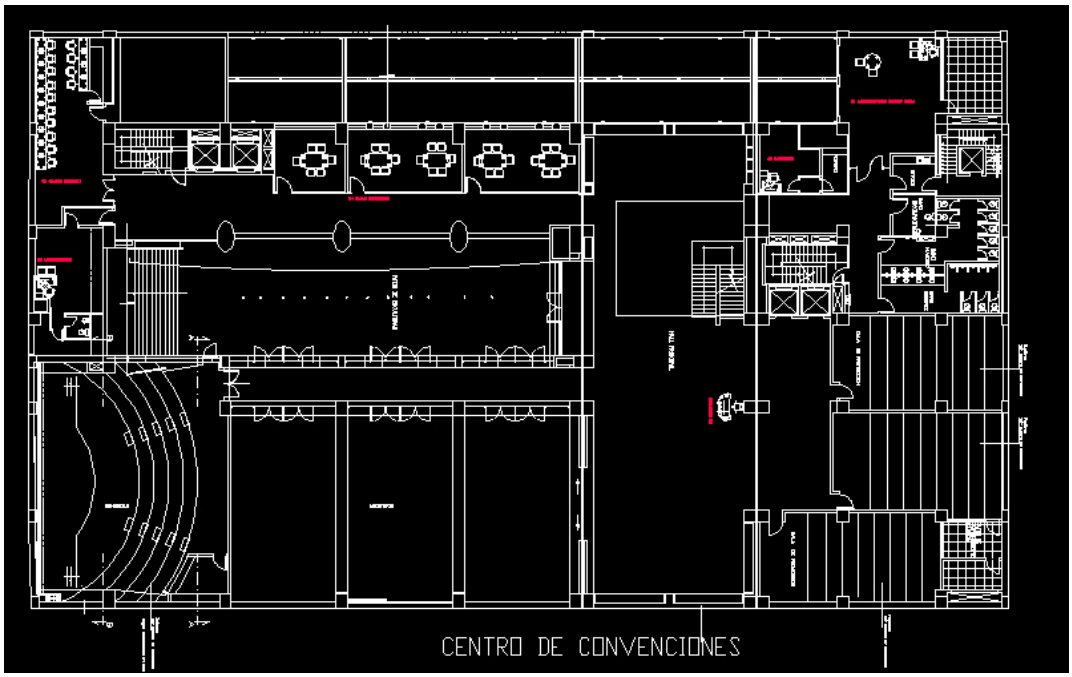


Figura 3-3: Plano Centro de Convenciones

El centro de convenciones en su gran parte se encuentra conformado por estructuras de aluminio, vidrio y madera. Las salas de conferencia cuentan con paredes de concreto pero no cubren del suelo al techo, la parte superior esta compuesta por aluminio y vidrio.

La planta baja que comprende la cafetería, recepción y biblioteca y el primer piso de la biblioteca; se conforman en un 90% de estructuras de aluminio y vidrio. La zona que comprende aulas del primero y segundo piso se las divisiones son de paredes de cemento y puertas de madera.

En la tabla 3.2; se muestra los efectos que los materiales producen sobre la emisión de señales de radio.

Material	Efecto	Ejemplos
Aire	Mínimo	
Madera	Bajo	Divisiones
Plástico	Bajo	Paredes internas
Material sintético	Bajo	Divisiones

Asbestos	Bajo	Techos
Vidrio	Bajo	Ventanas
Agua	Medio	Madera húmeda
Papel	Alto	Archivos
Concreto	Alto	pisos, paredes exteriores
Metal	Muy Alto	mesas, etc.

Tabla 0: Efectos de los materiales sobre Radio Frecuencia

Como se indica en la tabla 3.2 hay materiales que causan interferencia en el paso de la señal de radio frecuencia, causando de esta manera reflexión, refracción o difracción de las ondas. (Anexo 5).

Para solucionar este problema se recurre a la diversidad de espacio que consiste en colocar antenas separadas que se conectan a distintos receptores. De esta forma se mejora la disponibilidad y calidad de la señal recibida.

3.2.2 USUARIOS

Todos los usuarios que se encuentren en el campus académico, deberán contar con la comodidad del acceso al Internet desde su propia portátiles, PDA's y cualquier otro dispositivo que soporte conexión inalámbrica a través del estándar 802.11 en sus variantes a, b, g.

En la tabla 3.3, se detalla la capacidad máxima de personas que se pueden ubicar por piso o área. También se detalla la cantidad de puntos de datos instalados para la conexión a la red local por cable y, finalmente la cantidad de usuarios que actualmente laboran en cada uno de los pisos.

Piso	Área	Capacidad personas	Puntos de datos	Usuarios fijos
Piso 9	Dirección	30	12	8
Piso 8	Académicos	34	27	24
Piso 7	Académicos	40	35	32
Piso 6	Académicos	40	35	32

Piso 5	Administrativos	26	23	16
Piso 4	Estudiantes	6	6	4
Piso 3	Centros computo	94	89	38
Piso 2	Aulas	85	7	2
	Salón de afiches	16	1	0
Piso 1	Aulas	85	7	2
	Biblioteca	42	6	6
PB	Cafetería	60	1	1
	Biblioteca	57	8	5
	Recepción	20	2	2
CC	Hemiciclo	150	4	2
	Auditorio	250	5	0
	Salas de Conf.	180	3	3
	Salas de reuniones	40	2	0
Total		**1255**	**273**	**177**

Tabla 3.3: Usuarios de la LAN

La red inalámbrica debe proporcionar movilidad a los alumnos, profesores y visitantes.

Los estudiantes de la facultad, podrán utilizar la red inalámbrica para tener acceso a la información, el intercambio de la misma, y el aprendizaje.

3.2.3 FUNCIONALIDAD

Una red inalámbrica de área local (Wireless LAN) es un sistema flexible de transmisión de datos implementados como una extensión, o como alternativa, de una red cableada. Utiliza tecnología de radio frecuencia, transmite y recibe datos utilizando como medio el aire, minimizando la necesidad de una conexión de cable, permitiendo la combinación conectividad y movilidad.

La gran acogida que ha tenido las redes inalámbricas se debe, en gran medida, a las ventajas de movilidad para los usuarios y al precio competitivo que tienen en relación con las redes alámbricas convencionales.

En las instalaciones del campus académico, se realizan continuamente convenciones, seminarios, cursos sobre diversos temas, a los cuales asisten gran cantidad de personas, que demandan el servicio de conexión a Internet de manera permanente.

La instalación de la WLAN en estos sitios como son las salas de convenciones, dará un valor agregado a todos los eventos, seminarios y cursos que se realicen. Más que tratar de reemplazarla, la WLAN complementa a la tecnología LAN alámbrica del edificio, proporcionando la siguiente funcionalidad:

Al combinar la red cableada y la inalámbrica, se proporciona movilidad adicional al usuario cuando este requiera trasladarse de una oficina a otra y de un piso a otro.

Despliegue temporal de redes de acceso en los centros de convenciones, en donde el tendido de cableado no tendría sentido, pues la red se retirará una vez concluido el evento.

Otra necesidad, es el establecimiento de grupos de trabajos temporales. Para dar cabida a este tipo de solicitudes, se tiene que analizar la estrategia más adecuada para el redimensionamiento del sistema. El sistema inalámbrico deberá perfectamente acoplarse a la red cableada para mantener los servicios informáticos mientras duren las necesidades de grupos de trabajo temporales. De esta manera se evitará la interrupción total de una actividad o servicio.

Se mantendrá al sistema de cableado como la parte principal y la inalámbrica proporcionará la movilidad adicional al equipo o segmento de red para que los usuarios puedan desplazarse con facilidad dentro del campus de la Universidad.

3.2.4 SERVICIOS DE LA RED LOCAL INALÁMBRICA (WLAN)

La red inalámbrica es un servicio para la comunidad académica, estudiantes, personal de apoyo y gestión; y visitantes, que permita la conexión a la red de datos actual del Campus, sin la necesidad de conectarse físicamente a un nodo a través de un cable.

En una LAN, un ordenador conectado a la red que solicita servicios se denomina cliente. Una WLAN los usuarios podrán compartir archivos, impresoras y otros servicios de la red.

Los servicios que brindará la Red Inalámbrica son:

3.2.4.1 Internet

Acceso a WWW (Internet) de manera ininterrumpida (24x7).

- Navegar por la página WEB institucional: www.flacso.org.ec/, y acceder a los siguientes servicios:
- Acceso a correo electrónico (webmail).
- Realizar consultas en el Sistema Académico ingresando su respectivo nombre de usuario y clave.
- Pago Colegiatura y matrículas.
- Compras y Matrículas en línea
- Inscripciones a futuros eventos
- Compras de las publicaciones editadas por la institución.
- Consulta de los Eventos que se realizaron y realizarán en el presente mes.
- Eventos en línea, poder asistir a un evento en el instante en que se esta realizando o previamente grabado.
- Biblioteca en línea, consultar el fondo bibliográfico de la biblioteca, averiguar si un libro esta prestado, reservar un libro, etc.
- Ingreso a Foros de discusión sobre temas actuales y de coyuntura.
- Acceder a ciertos artículos de investigaciones que se publican de manera gratuita en el portal web de la institución.

3.2.4.2 Acceso

Los usuarios podrán acceder tanto al Internet como a la Intranet, dependiendo de las claves que se asignen. La red debe estar preparada y equipada para impedir accesos no autorizados a la red. Además de brindar servicios de contabilidad y control de accesos. Para esto se instalará un servidor AAA que disponga de herramientas con:

- Directorio de Servicios capaz de RADIUS AAA - autenticación basada en roles, autorización y motor contable por perfiles de usuarios.
- Punto de usuario IPSEC- VPN para defender a los usuarios inalámbricos contra la intercepción de paquetes y escucha espía.
- Enrutamiento.- con capacidades NAT y BiNAT, administre múltiples bloques IP con múltiples puertos físicos y compartición de direccionamiento.
- Servicios de núcleo de red.- Disponga de servicios integrados de asignación dinámica de direcciones DHCP y servidor de nombre de direcciones DNS.
- Cache Web Transparente.- Implícitamente, memorice todas las respuestas http para reducir el consumo de ancho de banda y mejore la velocidad de navegación al usuario final.
- Captura de paquetes.- Archiva todos los paquetes transferidos en una base de datos navegable con disección integrada y con graficación y estadísticas.
- Administración de ancho de banda- refuerza la priorización de paquetes y las políticas de utilización de ancho de banda.
- Firewall Integro.- Filtra paquetes por rango de direcciones IP
- Filtrado de contenido.- Previene que los usuarios puedan tener acceso a sitios Web con contenido ofensivo o que no está relacionado con la institución.
- Sistema de protección de intrusos.- Defiende contra virus y atacantes hackers por medio de la detección de comportamientos anormales en la red y mediante una colocación automática de computadores en una lista de atacantes.

- Administración de Red de Entorno Gráfico Unificado.- Un solo entorno de control administrativo para toda funcionalidad que puede ser accesible desde cualquier navegador Web e incluso los PDAs.

3.3. DISEÑO DE LA WLAN

3.3.1. DIMENSIONAMIENTO

Para el dimensionamiento de la WLAN se han considerado los siguientes valores de usuarios para los pisos altos.

1 usuario/despacho
2 usuarios/sala de reuniones
3 usuarios/aula
3 usuarios/laboratorio
2 usuarios por área de cubículos

Y para las áreas de acceso público un 15% de su capacidad.

Hemiciclo 150 usuarios, el 15% es: 23 usuarios
Auditorio 250 usuarios, el 15% es: 38 usuarios
Plaza de acceso 60 usuarios, el 15% es: 9 usuarios
Sala de lectura biblioteca, 50 usuarios, el 15% es: 8 usuarios
Cafetería 50 usuarios, el 15% es: 8 usuarios
Salas magistrales 50 usuarios, el 15% es: 8 usuarios

Capacidad total máxima que se dará a cada usuario será de 1 Mbps
La capacidad que ofrece cada punto de acceso (AP) dual según la norma IEEE 802.11 es de 54 Mbps brutos que resulta ser el 32 Mbps netos (60% de la capacidad).

3.3.1.1 Dimensionamiento piso 9

Se cuenta con 7 despachos y 3 salas de reuniones, lo que hace, en total, 13 usuarios potenciales.

$C_{máx}$ = 13 usuarios x 1 Mbps/usuario = 13 Mbps

Por tanto para el piso 9 son necesarios los puntos de acceso:

N_{ap} = 13 Mbps/32 Mbps = 0,4 AP ≈ 1 AP

3.3.1.2 Dimensionamiento piso 8

Se cuenta con 12 despachos, 1 salas de reuniones y 2 áreas de cubículos, lo que hace, en total, 18 usuarios potenciales.

$C_{máx}$ = 18 usuarios x 1 Mbps/usuario = 18 Mbps

Por tanto para el piso 8 son necesarios los puntos de acceso:

N_{ap} = 18 Mbps/32 Mbps = 0,6 AP ≈ 1 AP

3.3.1.3 Dimensionamiento piso 7

Se cuenta con 14 despachos, 1 sala de reuniones y 2 áreas de cubículos, lo que hace, en total, 18 usuarios potenciales.

$C_{máx}$ = 18 usuarios x 1 Mbps/usuario = 18 Mbps

Por tanto para el piso 7 son necesarios los puntos de acceso:

N_{ap} = 18 Mbps/32 Mbps = 0,6 AP ≈ 1 AP

3.3.1.4 Dimensionamiento piso 6

Se cuenta con 14 despachos, 1 sala de reuniones y 2 áreas de cubículos, lo que hace, en total, 18 usuarios potenciales.

$C_{máx}$ = 18 usuarios x 1 Mbps/usuario = 18 Mbps

Por tanto para el piso 6 son necesarios los puntos de acceso:

N_{ap} = 18 Mbps/32 Mbps = 0,6 AP ≈ 1 AP

3.3.1.5 Dimensionamiento piso 5

Se cuenta con 10 despachos, 1 sala de reuniones y 2 áreas de cubículos, lo que hace, en total, 14 usuarios potenciales.

$C_{máx}$ = 14 usuarios x 1 Mbps/usuario = 14 Mbps

Por tanto para el piso 5 son necesarios los puntos de acceso:

N_{ap} = 14 Mbps/32 Mbps = 0,4 AP ≈ 1 AP

3.3.1.6 Dimensionamiento piso 4

Se cuenta con 4 despachos y 1 aula, lo que hace, en total, 7 usuarios potenciales.

$C_{máx}$ = 7 usuarios x 1 Mbps/usuario = 7 Mbps

Por tanto para el piso 4 son necesarios los puntos de acceso:

N_{ap} = 7 Mbps/32 Mbps = 0,2 AP ≈ 1 AP

Actualmente se encuentra adecuando 3 aulas, por lo que el número de usuarios de WLAN en 2 meses podría crecer.

3.3.1.7 Dimensionamiento piso 3

Se cuenta con 3 despachos y 3 laboratorios, lo que hace, en total, 12 usuarios potenciales.

$$C_{máx} = 12 \text{ usuarios} \times 1 \text{ Mbps/usuario} = 12 \text{ Mbps}$$

Por tanto para el piso 3 son necesarios los puntos de acceso:

$$N_{ap} = 12 \text{ Mbps}/32 \text{ Mbps} = 0{,}4 \text{ AP} \approx 1 \text{ AP}$$

3.3.1.8 Dimensionamiento piso 2

Se cuenta con 8 aulas, lo que hace, en total, 24 usuarios potenciales.

$$C_{máx} = 24 \text{ usuarios} \times 1 \text{ Mbps/usuario} = 24 \text{ Mbps}$$

Por tanto para el piso 2 son necesarios los puntos de acceso:

$$N_{ap} = 24 \text{ Mbps}/32 \text{ Mbps} = 0{,}8 \text{ AP} \approx 1 \text{ AP}$$

3.3.1.9 Dimensionamiento piso 1

Se cuenta con 7 aulas, lo que hace, en total, 21 usuarios en aulas; en biblioteca se cuenta con 4 despachos y 1 sala de lectura, lo que hace, en total, 33 usuarios potenciales.

$$C_{máx} = 33 \text{ usuarios} \times 1 \text{ Mbps/usuario} = 33 \text{ Mbps}$$

Por tanto para el piso 1 son necesarios los puntos de acceso:

N_{ap} = 33 Mbps/32 Mbps = 1,1 AP ≈ 2 AP

3.3.1.10 Dimensionamiento planta baja y subsuelo 1

Por ser área contiguas en donde no existe mayores interferencias por motivos de paredes, divisiones; se ha tomado como una sola área. Se cuenta con 10 despachos, 1 sala de lectura, cafetería, 2 salas de reuniones, 3 salas magistrales, 1 auditorio, 1 hemiciclo y 1 plaza de acceso, lo que hace, en total, 86 usuarios potenciales.

$C_{máx}$ = 126 usuarios x 1 Mbps/usuario = 126 Mbps

Por tanto para planta baja y subsuelo 1 son necesarios los puntos de acceso:

N_{ap} = 126 Mbps/32 Mbps = 3.9 AP ≈ 4 AP

3.3.2. PLANIFICACIÓN RADIOLÉCTRICA

Para cada piso se han determinado el número de AP necesarios para cubrir el área de cobertura aproximada, esto se indica en la tabla 3.4. La distancia prevista de cobertura de cada AP es de hasta 100m.

Piso	Área de piso	No. AP	Área a cubrir por AP
9	420 m^2	1	420 m^2
8	420 m^2	1	420 m^2
7	420 m^2	1	420 m^2
6	420 m^2	1	420 m^2
5	420 m^2	1	420 m^2
4	420 m^2	1	420 m^2
3	420 m^2	1	420 m^2
2	480 m^2	1	480 m^2
1	860 m^2	2	430 m^2

PB y sub 1	1760 m^2	4	440 m^2

Tabla 3.4: Planificación radioeléctrica

3.3.2.1 Puntos de acceso

Para determinar la ubicación más adecuada de los puntos de acceso se ha realizado un proceso interactivo, mediante el cual se ubican los AP y con ayuda de un computador portátil se ha verificado si se cumplen todos los requisitos de cobertura y calidad de acceso a la red, en caso negativo, se realiza un cambio de ubicación hasta que el resultado sea satisfactorio.

Denominación punto de acceso	P9_AP9
Ubicación	Anexo 2
Canal asignado	Automático
Modo de trabajo	802.11b y 802.11g
Frecuencia de trabajo	802.11b / 802.11g: 2.4 GHz
Porcentaje de área de interés cubierta	100%
Nivel de señal	-73 dBm
Capacidad media de carga	54 Mbps
Cumplimiento con estándares:	Certificación Wi-Fi, IEEE 802.11b, IEEE 802.11g

Tabla 3.5: Punto de acceso P9_AP9

Denominación punto de acceso	P8_AP8
Ubicación	Anexo 2
Canal asignado	Automático
Modo de trabajo	802.11b y 802.11g
Frecuencia de trabajo	802.11b / 802.11g: 2.4 GHz
Porcentaje de área de interés cubierta	100%
Nivel de señal	-73 dBm
Capacidad media de carga	54 Mbps
Cumplimiento con estándares:	Certificación Wi-Fi, IEEE 802.11b, IEEE 802.11g

Tabla 3.6: Punto de acceso P8_AP8

Denominación punto de acceso	P7_AP7
Ubicación	Anexo 2
Canal asignado	Automático
Modo de trabajo	802.11b y 802.11g
Frecuencia de trabajo	802.11b / 802.11g: 2.4 GHz
Porcentaje de área de interés cubierta	100%
Nivel de señal	-73 dBm
Capacidad media de carga	54 Mbps
Cumplimiento con estándares:	Certificación Wi-Fi, IEEE 802.11b, IEEE 802.11g

Tabla 3.7: Punto de acceso P7_AP7

Denominación punto de acceso	P6_AP6
Ubicación	Anexo 2
Canal asignado	Automático
Modo de trabajo	802.11b y 802.11g
Frecuencia de trabajo	802.11b / 802.11g: 2.4 GHz
Porcentaje de área de interés cubierta	100%
Nivel de señal	-73 dBm
Capacidad media de carga	54 Mbps
Cumplimiento con estándares:	Certificación Wi-Fi, IEEE 802.11b, IEEE 802.11g

Tabla 3.8: Punto de acceso P6_AP6

Denominación punto de acceso	P5_AP5
Ubicación	Anexo 2
Canal asignado	Automático
Modo de trabajo	802.11b y 802.11g
Porcentaje de área de interés cubierta	100%
Frecuencia de trabajo	802.11b / 802.11g: 2.4 GHz
Nivel de señal	-73 dBm
Capacidad media de carga	54 Mbps

Cumplimiento con estándares:	Certificación Wi-Fi, IEEE 802.11b, IEEE 802.11g

Tabla 3.9: Punto de acceso P5_AP5

Denominación punto de acceso	P4_AP4
Ubicación	Anexo 2
Canal asignado	Automático
Frecuencia de trabajo	802.11b / 802.11g: 2.4 GHz
Modo de trabajo	802.11b y 802.11g
Porcentaje de área de interés cubierta	100%
Nivel de señal	-73 dBm
Capacidad media de carga	54 Mbps
Cumplimiento con estándares:	Certificación Wi-Fi, IEEE 802.11b, IEEE 802.11g

Tabla 3.10: Punto de acceso P4_AP4

Denominación punto de acceso	P3_AP3
Ubicación	Anexo 2
Canal asignado	Automático
Modo de trabajo	802.11b y 802.11g
Frecuencia de trabajo	802.11b / 802.11g: 2.4 GHz
Porcentaje de área de interés cubierta	100%
Nivel de señal	-73 dBm
Capacidad media de carga	54 Mbps
Cumplimiento con estándares:	Certificación Wi-Fi, IEEE 802.11b, IEEE 802.11g

Tabla 3.11: Punto de acceso P3_AP3

Denominación punto de acceso	P2_AP2
Ubicación	Anexo 2
Canal asignado	Automático
Modo de trabajo	802.11b y 802.11g
Frecuencia de trabajo	802.11b / 802.11g: 2.4 GHz
Porcentaje de área de interés cubierta	100%

Nivel de señal	-73 dBm
Capacidad media de carga	54 Mbps
Cumplimiento con estándares:	Certificación Wi-Fi, IEEE 802.11b, IEEE 802.11g

Tabla 3.12: Punto de acceso P2_AP2

Denominación punto de acceso	P1_AP1A
Ubicación	Anexo 2
Canal asignado	Automático
Modo de trabajo	802.11b y 802.11g
Frecuencia de trabajo	802.11b / 802.11g: 2.4 GHz
Porcentaje de área de interés cubierta	100%
Nivel de señal	-73 dBm
Capacidad media de carga	54 Mbps
Cumplimiento con estándares:	Certificación Wi-Fi, IEEE 802.11b, IEEE 802.11g

Tabla 3.13: Punto de acceso P1_APA1

Denominación punto de acceso	P2_AP1B
Ubicación	Anexo 2
Canal asignado	Automático
Modo de trabajo	802.11b y 802.11g
Frecuencia de trabajo	802.11b / 802.11g: 2.4 GHz
Porcentaje de área de interés cubierta	100%
Nivel de señal	-73 dBm
Capacidad media de carga	54 Mbps
Cumplimiento con estándares:	Certificación Wi-Fi, IEEE 802.11b, IEEE 802.11g

Tabla 3.14: Punto de acceso P2_APA1B

Denominación punto de acceso	P0_AP0A
Ubicación	Anexo 2
Canal asignado	Automático
Modo de trabajo	802.11b y 802.11g

Frecuencia de trabajo	802.11b / 802.11g: 2.4 GHz
Porcentaje de área de interés cubierta	100%
Nivel de señal	-73 dBm
Capacidad media de carga	54 Mbps
Cumplimiento con estándares:	Certificación Wi-Fi, IEEE 802.11b, IEEE 802.11g

Tabla 3.15: Punto de acceso P0_AP0A

Denominación punto de acceso	P0_AP0B
Ubicación	Anexo 2
Canal asignado	Automático
Modo de trabajo	802.11b y 802.11g
Frecuencia de trabajo	802.11b / 802.11g: 2.4 GHz
Porcentaje de área de interés cubierta	100%
Nivel de señal	-73 dBm
Capacidad media de carga	54 Mbps
Cumplimiento con estándares:	Certificación Wi-Fi, IEEE 802.11b, IEEE 802.11g

Tabla 3.16: Punto de acceso P0_AP0B

Denominación punto de acceso	P0_AP0C
Ubicación	Anexo 2
Canal asignado	Automático
Modo de trabajo	802.11b y 802.11g
Frecuencia de trabajo	802.11b / 802.11g: 2.4 GHz
Porcentaje de área de interés cubierta	100%
Nivel de señal	-73 dBm
Capacidad media de carga	54 Mbps
Cumplimiento con estándares:	Certificación Wi-Fi, IEEE 802.11b, IEEE 802.11g

Tabla 3.17: Punto de acceso P0_AP0C

Denominación punto de acceso	P0_AP0D
Ubicación	Anexo 2

Canal asignado	Automático
Frecuencia de trabajo	802.11b / 802.11g: 2.4 GHz
Modo de trabajo	802.11b y 802.11g
Porcentaje de área de interés cubierta	100%
Nivel de señal	-73 dBm
Capacidad media de carga	54 Mbps
Cumplimiento con estándares:	Certificación Wi-Fi, IEEE 802.11b, IEEE 802.11g

Tabla 3.18: Punto de acceso P0_AP0D

3.3.2.2 Descripción de puntos de acceso

Cada punto de accceso deberá cumplir con las siguientes especificaciones:

- Permita la configuración en puente de acuerdo con IEEE 802.1d
- Soporte de SNMP (incluyendo alarmas personalizadas)
- Traspaso transparente entre Puntos de Acceso
- Clear Channel Select escoge el canal menos traficado para brindar conexiones sin problemas
- Opciones de antena externa
- Control de acceso de direcciones MAC
- Encriptación WEP de clave compartida de 40/64 bits y 128/54 bits, y encriptación avanzada WPA
- Rastreo multibanda de RF
- Gestión segura mediante herramienta basadas en Web vía consola local o de forma remota sobre SSL o HTTPS
- Reportes de estado en tiempo real e información de trazadas del protocolo.
- Brinde la opción de PoE (Power over Ethernet)

3.3.2.3 Control de puntos de acceso

Para el control de los puntos de acceso se precisa lo siguiente:

- Pantallas de entrada HTML seguras personalizables y configurables
- Contabilidad mediante RADIUS AAA
- Autenticación a nivel MAC para servicios no-HTTP
- DHCP servidor/Cliente
- Cliente PPPoE
- Asignación dinámica de VLAN
- Enrutamiento IP/IPX
- Redireccionamiento SMTP (E-Mail)
- Autenticación mediante RADIUS AAA
- Firewall (cortafuegos) configurable y personalizable

3.3.4. SEGURIDAD EN LA WLAN

Para la seguridad de la WLAN se plantean la implementación de una VLAN para los usuarios o el grupo de usuarios inalámbricos. Mediante esta VLAN se restringirá el tráfico con los usuarios de la LAN cableada.

Para la implementación del proyecto, será necesaria la activación del servidor DHCP, en el servidor que actúa como controlador de dominio. El rango de las direcciones asignadas por el servidor DHCP estará definido por la VLAN asignada para la WLAN.

Para el control de acceso a la WLAN, se deberá implementar un servidor AAA que utilice RADIUS, el cual se hará cargo de la autenticación y autorización de los usuarios inalámbricos.

El cliente proporcionará su nombre de usuario y contraseña a través de una página web común para todos los usuarios inalámbricos. El servidor RADIUS buscará el ID del usuario en la base de datos del Active Directory de Windows 2003. Una vez que el usuario sea identificado por el servidor RADIUS y este determina que el cliente es legítimo, se abre la red virtual y el usuario podrá acceder a la WLAN.

El servicio que se compartirá con los usuarios de la WLAN será Internet. El servicio de correo electrónico solo estará accesible vía HTTP.

3.4. MATRIZ DE CUMPLIMIENTO

Parámetros	Especificación	Resultado
Números de puntos de acceso	NA	14
Capacidad neta por usuario en carga	1 Mbps	1 Mbps
Capacidad bruta de pico por usuario	54 Mbps	54 Mbps
Nivel mínimo de señal en la zona de servicio	-80 dBm	-73 dBm
Porcentaje total del área de servicio cubierta	100%	100%
Señal fuera de la zona de servicio	Mínima	-80 dBm

Tabla 3.19: Matriz de cumplimiento

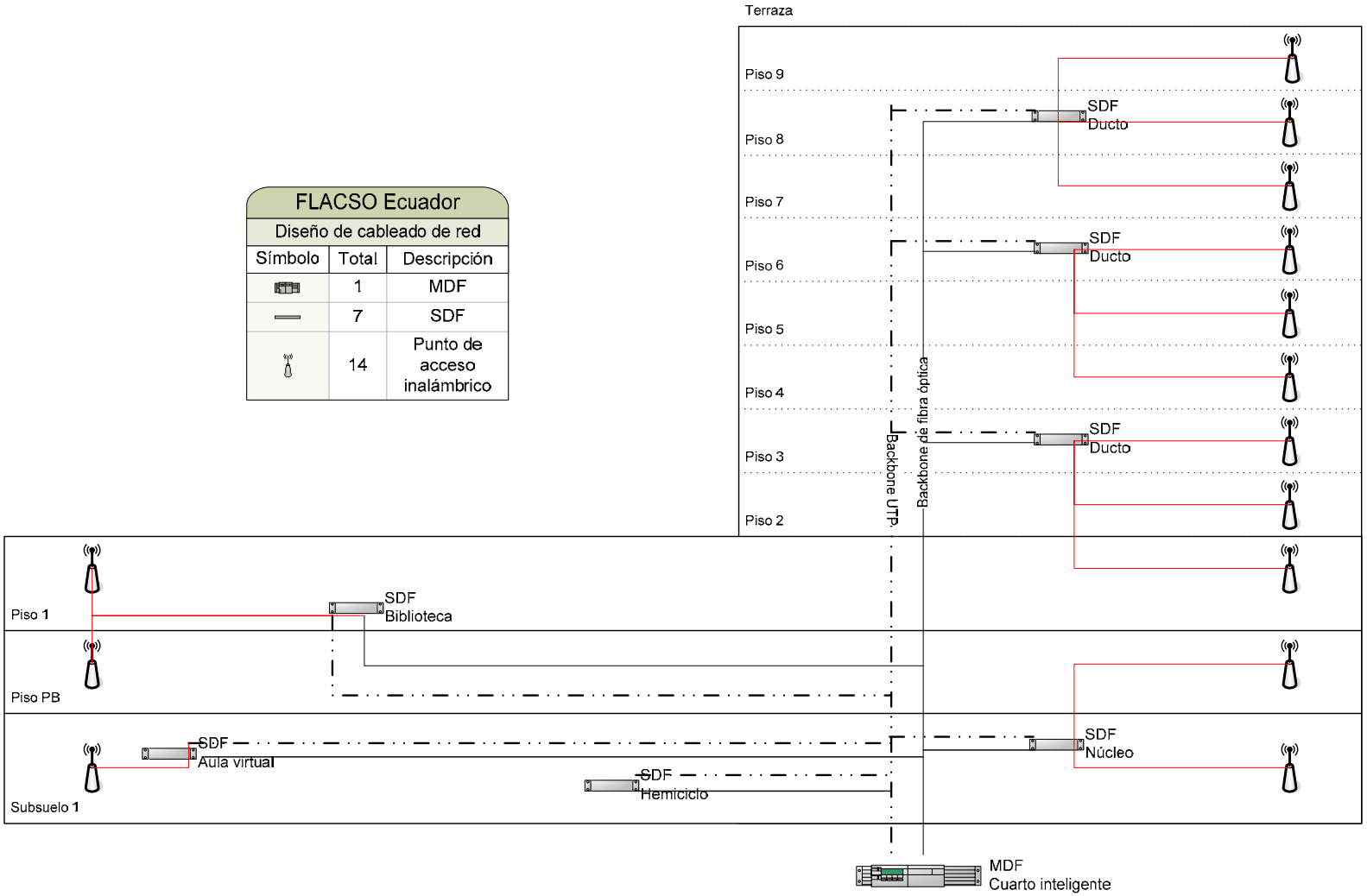


Figura 3-4: Distribución de la `WLAN

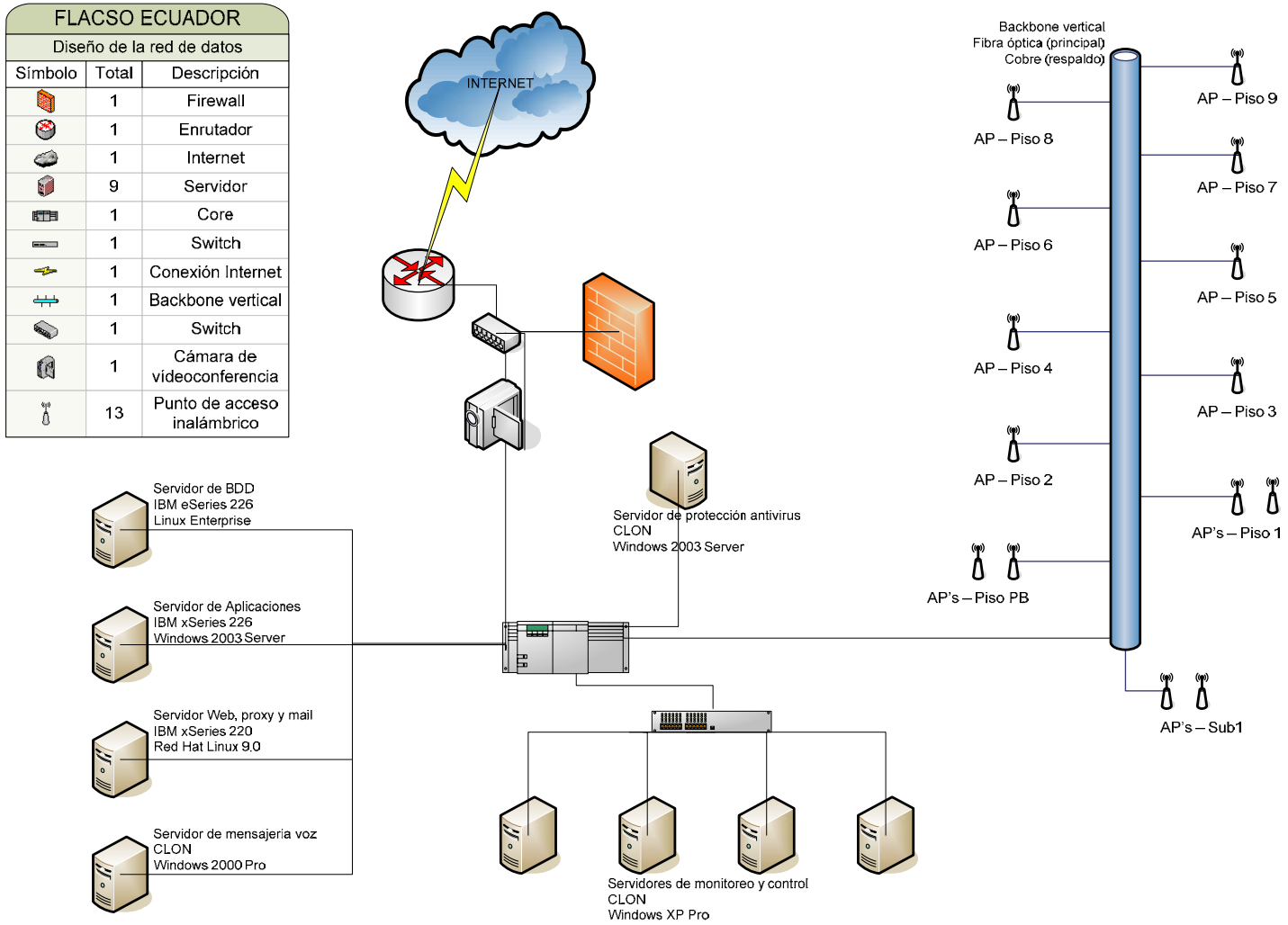


Figura 3-5: Diseño de la WLAN integrada a la red local cableada

CAPITULO 4: FACTIBILIDAD DE IMPLEMANTACION DE LA WLAN

¿Qué es factibilidad?

Es “lo susceptible de ser hecho, lo posible, lo realizable.” (María Moliner, Diccionario del uso del español; P. 1269).

El estudio de la factibilidad sirve para recopilar datos relevantes sobre el desarrollo de un proyecto y en base a ello tomar la mejor decisión, si procede su estudio, desarrollo o implementación.

El estudio de la factibilidad en un proyecto consiste en descubrir cuales son los objetivos de la organización, luego determinar si el proyecto es útil para que la empresa logre sus objetivos. La búsqueda de estos objetivos debe contemplar los recursos disponibles o aquellos que la empresa puede proporcionar, nunca deben definirse con recursos que la empresa no es capaz de dar.

Definición de objetivos

Las organizaciones definen sus objetivos que determinan la posibilidad de factibilidad de algún proyecto sin ser limitativos. Los objetivos básicos que una organización debe plantearse son los siguientes:

- La reducción de errores y mayor precisión en los procesos.
- La reducción de costos mediante la optimización o eliminación de recursos no necesarios.
- La integración de las tareas y subsistemas de la organización.
- Actualización y mejoramiento de los servicios a los usuarios.
- Reducción en el tiempo de realización de las actividades.

Determinación de factibilidad

La factibilidad se define por la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas de una organización, la factibilidad se apoya en tres aspectos básicos:

- Operativo
- Técnico
- Económico

El éxito de un proyecto esta determinado por el grado de factibilidad que se presenta en cada uno de los tres aspectos anteriores.

Presentación de un estudio de Factibilidad

Un estudio de factibilidad debe ser presentado con todas la posibles ventajas para la organización, tomando en cuenta todos los elementos necesarios para que el proyecto funcione. Para esto dentro de los estudios de factibilidad se complementan dos pasos en la presentación del estudio:

- Requisitos Óptimos.
- Requisitos Mínimos.

El primer paso se refiere a presentar un estudio con los requisitos óptimos que el proyecto requiere, estos elementos deben ser los necesarios para que las actividades y los resultados del proyecto sean obtenidos con la máxima eficacia.

El segundo paso consiste en un estudio de requisitos mínimos, el cual cubre los requisitos mínimos necesarios que el proyecto debe ocupar para obtener las metas y objetivos, este paso trata de hacer uso de los recursos disponibles de la empresa para minimizar cualquier gasto o adquisición adicional.

4.1 FACTIBILIDAD TECNICA

El análisis de factibilidad técnica evalúa si el equipamiento y software actual de la organización están disponibles y si tienen las capacidades técnicas requeridas para el diseño que se ha propuesto.

También se considera como la WLAN se complementará a la red LAN cableada que existe actualmente. Así como cuales de los servicios que brinda la red cableada estarán accesibles desde la WLAN.

Finalmente se considera si el personal del área de TIC cuenta con capacidad técnica y experiencia necesaria para implementar, operar y mantener la WLAN.

4.1.1. EQUIPAMIENTO Y SOFTWARE NECESARIO DE LA WLAN

Luego del análisis realizado al equipamiento con el que cuenta en la actualidad de la organización se sugiere lo siguiente:

4.1.1.1.Firewall

Se cuenta de firewall de hardware 3Com, dispone de 3 zonas, LAN, WAN y DMZ. En la actualidad únicamente están activas las zonas LAN y WAN y el tráfico se direcciona directamente entre estas zonas

Se sugiere la activación de la zona DMZ en el firewall y el servidor que se utiliza como servidor de correo, Proxy y servidor Web sea ubicado en esta zona. Y el tráfico de la WAN sea direccionado a la DMZ y de igual forma el tráfico de la LAN también sea direccionado a la DMZ. Lo que provocaría que la red WAN no tenga contacto directo con la LAN de la organización.

4.1.1.2. Servidores

En la actualidad se cuenta con 4 servidores:

1. Servidor de BDD

2. Servidor de control de dominio
3. Servidor de Antivirus
4. Servidor Web, Proxy y Mail

4.1.1.2.1. Servidor de Base de datos

El servidor de BDD cuenta con sistema operativo Red Hat Enterprise 4. Es un servidor con un procesador Intel Xeon de 3.0 Ghz de velocidad, con 512 MB de memoria RAM, 3 discos SCSI de 70 Gb, 2 tarjetas de red 10/100/1000.

El software de aplicación que utiliza principalmente es el motor de la Base de Datos Oracle 9i y MySQL 4.0.

No necesita actualización o cambios en su configuración actual. La ubicación del servidor se mantendrá en la zona de la LAN en el firewall.

4.1.1.2.2. Servidor de control de dominio

El servidor de control de dominio cuenta con sistema operativo Windows 2003 Server. Es un servidor con un procesador Intel Xeon de 3.0 Ghz de velocidad, con 512 MB de memoria RAM, 3 discos SCSI de 70 Gb, 2 tarjetas de red 10/100/1000.

Para la gestión de usuarios se encuentra configurado el Active Directory del Windows 2003. Se solicita el aumento de la capacidad de la memoria RAM del servidor de 512 a 1024 Mb, para una mejor operatibilidad del servidor, en el caso que los usuarios de la WLAN accedan al dominio de la institución.

La ubicación del servidor se mantendrá en la zona de la LAN en el firewall.

4.1.1.2.3. Servidor Antivirus

El servidor de control antivirus cuenta con sistema operativo Windows 2003 Server. Es un equipo CLON con procesador Intel Pentium IV de 3.0 Ghz de velocidad, con 1 GB de memoria RAM, 1 disco de 120 Gb, 1 tarjeta de red 10/100.

Se dedica de manera exclusiva al filtrado y control de antivirus, para lo cual cuenta con Symantec Antivirus Corporativo.

En la actualidad se encuentra ubicado en la zona de la LAN en el firewall, se cambia a la zona DMZ, puesto que el servidor de correo y Proxy, se instalarán en esta zona.

4.1.1.2.4. Servidor Web, Proxy y Mail

El servidor Web, Proxy y de Mail cuenta con sistema operativo Red Hat 9.0. Es un equipo IBM con 2 procesadores Intel Pentium III de 1.2 Ghz de velocidad, con 1 GB de memoria RAM, 3 disco de 30 Gb, 1 tarjeta de red 10/100.

En el se manejan los servicios de WebServer, Proxy y Mail. Tomando en cuenta que al implantar la red WLAN el número de usuarios se incrementarán, se solicita la adquisición de 2 servidores, los mismos que se manejarán los servicios mencionados por separado.

Las características mínimas de los servidores deben ser:

1 Procesador Intel Xeon 3.0, con capacidad para 2 procesadores
Memoria RAM de 1 Gb, capacidad de crecimiento hasta 4 Gb
4 discos de 60 Gb, con capacidad de RAID 5
1 tarjeta de red 10/100/1000
Hot swap de fuente de poder y discos
Sistema operativo Linux de uso gratuito

El servidor actual se dedicará para servir de Proxy Server con cache de páginas web.

Los dos servidores nuevos se destinarán para Servidor Web y Servidor de Mail. Los servidores estarán ubicados en la zona desmilitarizada DMZ

4.1.1.3.Puntos de acceso

Actualmente no se cuenta en la red con ningún punto de acceso, por lo que se hace necesaria la adquisición de todos los puntos de accesos especificados en el diseño de la WLAN del capítulo 3 de este documento.

En los pisos 2 al 9 se instalará un AP por piso y 2 puntos de acceso en los pisos 1, planta baja y subsuelo 1, logrando de esta manera cubrir todo el edificio.

4.1.1.4.Red de datos

El backbone vertical principal esta constituido de fibra óptica y además cuenta con un backbone de cobre que sirve de respaldo en caso que el backbone principal falle.

Las redes horizontales están constituidas por cable UTP Categoría 6. Se conectan al backbone de fibra con switch 3Com 3226 y 3250 de 24 y 48 puertos respectivamente.

Para la implementación de la WLAN propuesta no se necesita de equipos de conexión adicionales, los dispositivos actuales cuentan con la capacidad técnica y de puertos para conectar los puntos de acceso a ellos.

Cada switch de piso se conecta a través del backbone principal al switch central o core 3Com 4950, y a través de este a los servidores para acceder a los servicios de Internet, correo electrónico, antivirus, autenticación, etc.

Todos los dispositivos de conexión cuentan con la capacidad de manejar VLAN por puertos, por lo que a cada puerto que se conecte un punto de acceso se le asignará la VLAN creada para el efecto.

4.1.2. ADAPTABILIDAD DE LA WLAN CON LA RED CABLEADA

Un punto importante de la WLAN propuesta es su integración con la red cableada existente, manteniendo los niveles de seguridad, confiabilidad, operatividad y eficiencia.

4.1.2.1.VLAN

Actualmente la red se encuentra segmentada por VLANs La VLAN principal se encuentra en la red 10.1.1.0; y en ella se encuentran todos los servidores, los switch de conexión de redes locales, el firewall.

Las VLANs restantes están creadas de acuerdo a grupos de usuarios o área de terminada, por ejemplo se tiene la VLAN de el grupo de usuarios académicos o la VLAN de el área de biblioteca.

Para los usuarios o el grupo de usuarios de la WLAN se creará una VLAN, la cual solo tendrá comunicación exclusiva con la DMZ en donde se encontrarán los servicios de Internet, mail. Mediante esta se restringirá el tráfico con los usuarios de la LAN cableada.

4.1.2.2.Servidor DHCP

En la actualidad no se cuenta con un servidor de asignación de direcciones dinámicas DHCP.

Para la implementación del proyecto, será necesaria la activación del servidor DHCP, en el servidor que actúa como controlador de dominio. El rango de las direcciones asignadas por el servidor DHCP estará definido por la VLAN asignada para la WLAN.

4.1.2.3.Autenticación y autorización de los usuarios

Para el acceso a la WLAN, se debe adquirir, instalar y configurar un servidor AAA que utilice RADIUS, el cual se hará cargo de la autenticación y autorización de los usuarios.

Cuando un usuario se asocie con un punto de acceso, este acepta la asociación del usuario pero lo ubica en un área de espera sin estar autenticado; esto quiere decir que el usuario permanecerá bloqueado hasta que sea autenticado.

El cliente proporciona su nombre de usuario y contraseña a través de una página web común para todos los usuarios inalámbricos. El punto de acceso reenvía esta información a través del enlace cableado al servidor AAA con RADIUS. El servidor RADIUS buscará el ID del usuario en la base de datos del Active Directory de Windows 2003. Una vez que el usuario sea identificado por el servidor RADIUS y este determina que el cliente es legítimo, se abre la red virtual y el usuario puede acceder a la WLAN.

4.1.2.4.Servicios HTTP, SMTP

Una vez conectado el cliente a la WLAN, este podrá hacer uso de los servicios a los cuales le será permitido. Los servicios por el momento que se compartirán con los usuarios de la WLAN son Internet. El servicio de correo electrónico solo estará accesible vía HTTP.

Los usuarios de la WLAN podrán acceder al portal web de la institución y a través de él consultar toda la información que se encuentra publicada en el portal y los servicios que se ofertan; como son: Pagos en línea, biblioteca, educación virtual, correo electrónico, eventos en línea y próximamente el sistema de gestión docente tanto para estudiantes, profesores y coordinadores y autoridades de la institución.

4.1.3. PERSONAL TÉCNICO CAPACITADO

El personal que labora actualmente en el área de Tecnologías de información y comunicación es muy limitado en cuanto a cantidad, puesto que solo cuenta con 2 personas para toda la gestión tecnológica al interior de la organización.

En lo que concierne a la parte técnica, el personal maneja con suficiencia la gestión de la red local cableada, cuentan con la preparación adecuada y de base en lo que se refiere al conocimiento de redes. Se deduce que el personal esta apto para entender el funcionamiento de la WLAN, puesto que en resumen los servicios se mantienen, lo único que cambia es el medio con el cual se accede a la red.

El proveedor de los puntos de acceso deberá brindar una capacitación mínima en la operación y configuración de los equipos.

Se debe indicar que con la implantación de la WLAN, el número de usuarios aumentara y por ende la demanda de los servicios. El diseño propuesto tiene una capacidad de crecimiento de hasta 2 años, de acuerdo a la proyección de crecimiento del uso de los espacios físicos y de manera especial los espacios públicos (biblioteca, cafetería, auditorios, y más). El principal objetivo es brindar como valor agregado el acceso al Internet de manera ininterrumpida.

4.2 FACTIBILIDAD OPERATIVA

La factibilidad operativa se refiere a la viabilidad de la implementación del proyecto propuesto y el impacto de aceptación o no que puede provocar en los usuarios, tanto internos como externos de la institución.

En resumen, la factibilidad operativa se refiere a la evaluación del proyecto desde el punto de vista operativo y en el cual se considerarán los siguientes puntos:

4.2.1 USO DE LA WLAN

Para acceder a usar la WLAN, el acceso a los usuarios debe ser de manera completamente transparente, es decir el usuario simplemente deberá encender su dispositivo certificado Wi-Fi o con el estándar 802.11x y automáticamente luego de ingresar su login y password conectarse a la WLAN.

El login y password de los usuarios en el caso de los estudiantes, profesores y demás personal administrativo-financiero y de apoyo será el mismo que maneja para su acceso a la red cableada.

Para los usuarios del centro de convenciones se creará una única cuenta el momento que se realiza la reserva de un área determinada. Esta cuenta estará activa el momento y durante el periodo que dure el evento para la cual fue creada. El número máximo de conexiones concurrentes que puede acceder con la cuenta, corresponde al número especificado en el capítulo 3 en la sección de dimensionamiento de la WLAN.

Por ejemplo: Si la empresa XXXX alquila el auditorio para el día 5 de agosto de 2006 en el horario de 9:00 a 18:00. Se creará la cuenta XXXX con una clave especifica; el tiempo de duración de la cuenta será de 9:00 a 18:00 el día señalado y la cantidad de usuarios concurrentes que podrán acceder con esta cuenta será de 15% de la capacidad del auditorio.

Para los usuarios de biblioteca que no pertenezcan a la institución y visitantes de la institución en particular las cuentas para el acceso se lo realizará directamente al personal del área de Tecnologías de Información y el tiempo de vida de una cuenta visitante será de acuerdo al horario de atención de biblioteca u horario de atención de la institución.

Con esta política de asignación y uso de cuentas, se pretende mantener un control del uso de WLAN así como de los accesos de usuarios autenticados y autorizados. También mantener un registro de contabilidad de los usuarios que acceden a la red a través de la WLAN propuesta

4.2.2 OPERACIÓN DE LA WLAN POR PARTE DEL DEPARTAMENTO DE LAS TIC DE LA ORGANIZACIÓN.

El personal que labora en el área de las TIC, es muy limitado ya que actualmente solo trabajan 2 personas en el área. Este personal se encarga de la gestión, instalación y administración de todo lo relacionado a las tecnologías como son:

- Administración de servidores de BDD, de Proxy, Mail, Antivirus, Central telefónica, Controlador de dominio (Active Directory), Control de accesos con tarjeta de proximidad, CCTV, entre otros.
- Help desk
- Administración de Centros de cómputo
- Pagina WEB
- Respaldos de la información
- Mantenimiento preventivo de las estaciones de trabajo
- Soporte técnico en la plataforma de educación virtual
- Soporte técnico en la realización de video conferencias
- Soporte técnico en la realización de eventos
- Instalación y configuración de puntos de voz y datos
- Administración de los equipos de comunicación (Switch, Routers, Central telefónica, Racks de distribución)

- Administración de los sistemas de información (Sistema financiero, Sistema de Pagos en línea, Biblioteca virtual, Sistema de Gestión Docente)
- Administración y monitoreo del canal de acceso al Internet

De lo expuesto anteriormente, el 75% del tiempo se destina para soporte y apoyo a usuarios (Help Desk); y con la propuesta de la implementación del proyecto propuesto se incrementará el número de usuarios y por ende habrá mayor demanda de los servicio ofertados, provocando esto una mayor necesidad de control de acceso y seguridades en la red local, lo que implica una mayor carga de trabajo en el personal de las TIC actual. Por tal motivo se sugiere contratar a un técnico que se haga cargo del soporte a los usuarios, para de esta manera descongestionar al personal actual de estas tareas y de esta manera el personal de las TIC pueda dedicarse a la administración y configuración de la WLAN propuesta.

El personal de las TIC será el encargado de asignar las claves de acceso a las WLAN propuesta; así como, de crear y configurar las políticas de acceso a la red local y de uso de los recursos y servicios brindados.

4.2.3 IMPACTO DE LA WLAN EN LA ORGANIZACIÓN

El impacto del diseño propuesto en la red actual será de manera notoria en el incremento de los usuarios así como la demanda de uso de los servicios. Este incremento no afectará al performance de la red local puesto que la WLAN propuesta estará dentro de una VLAN y no generará tráfico con el resto de las VLANs de la red local, a excepción de la VLAN en la cual se encuentra el servidor de acceso a Internet.

Por lo expuesto anteriormente se deduce que el impacto que tendrá la WLAN propuesta se verá en el acceso al Internet, puesto que la demanda del ancho de banda será mayor por el aumento de usuarios.

Actualmente la institución mantiene un contrato con IMPSAT para la provisión del servicio de Internet con un canal clear channel de 1128 Kbps de ancho de banda. Cada año se revisa el contrato con el proveedor y tomando en cuenta que los costos de conexión al Internet cada año bajan, el proveedor en común acuerdo con la institución aumenta el ancho de banda en lugar de disminuir el costo por el mismo canal.

De acuerdo a conversaciones mantenidas con el personal de administración del Centro de Convenciones y biblioteca, sus usuarios demandan el servicio de acceso a Internet inalámbrico. Uno de los objetivos de la dirección de la institución es la de proveer acceso al Internet de manera gratuita. Por lo que la WLAN propuesta cumple con este objetivo planteado por la dirección.

Con este servicio de Internet inalámbrico se espera que el número de visitantes y la demanda por el uso del Centro de convenciones y biblioteca aumente, lo que representaría un mayor prestigio para la institución, lo que significaría también una mayor promoción y difusión de la institución y de las actividades que al interior se realizan.

A continuación se presentan tres escenarios de crecimiento de usuarios del Internet.

De acuerdo a la Tabla 3.3, existen 177 usuarios fijos que se conecta a la red, y si se cuenta con un canal de acceso al Internet de 1128 Kbps, tenemos que a cada usuario de promedio se le esta asignando como
Espacio de ancho de banda = 1128 Kbps / 177 usuarios = 6,37 Kbps/usuario.

El ancho de banda provisto por usuario no satura el canal de acceso, llegando a usar entre el 80 y 90% de acuerdo al análisis de uso de canal (Anexo 4).

Primer caso

De acuerdo al dimensionamiento realizado en el capítulo 3, y suponiendo que todos los usuarios planificados por pisos o áreas se conecten de manera

concurrente a la WLAN y hagan uso del Internet, el número de usuarios es de 283, sumando los 177 usuarios fijos actuales, el numero de usuarios total es de 360. Entonces el

Espacio de ancho de banda = 1128 Kbps / 360 usuarios = 3,13 Kbps/usuario

por lo que de acuerdo a este análisis de deberá implementar el canal por lo menos al doble es decir a 2256 Kbps, con lo que el

Espacio de ancho de banda = 2256 Kbps / 360 usuarios = 6,26 Kbps/usuario.

Segundo caso

Si tomamos en cuenta y de acuerdo a la encuesta realizada (Anexo 3), el 82,5% de los usuarios de la red utilizan el Internet, por lo que de los 177 usuarios solamente 146 usuarios aproximadamente utilizarían el Internet de manera concurrente; adicionalmente en la actualidad el 20% de los encuestados disponen de un dispositivo inalámbrico y un 20% adquirirían uno en caso de implementar una red inalámbrica, por lo que, si se han dimensionado 283 usuarios inalámbricos el 20% que dispone un dispositivo WiFi, sumando el 20% de los usuarios que adquirirían uno, tendríamos que 113 usuarios de la WLAN aproximadamente, que sumandos a los 150 usuarios concurrentes de conexión por cable, el número total de usuarios es de 259. Entonces

Espacio de ancho de banda = 1128 Kbps / 259 usuarios = 4.36 Kbps/usuario

por lo que de acuerdo a este análisis de deberá implementar el canal a 1640 Kbps, con lo que el

Espacio de ancho de banda = 1640 Kbps / 259 usuarios = 6,33 Kbps/usuario.

Tercer caso

El caso más real, es tomando en cuenta el 82.5% de los usuarios de la red cableada que usan el Internet, y de acuerdo al informe suministrado por el departamento de relaciones públicas, el número de usuarios promedio del centro de convenciones en un mes es de 220 usuarios, a los cuales y de acuerdo al dimensionamiento del capitulo 3, solo se otorgará el 15% de la capacidad del centro, por lo que se estima que el centro de convenciones será

de 33 usuarios concurrentes. Adicionalmente el número de estudiantes actuales es de 167 y aplicando la misma regla del 15%, el número de estudiantes que utilizarían WLAN es de 25. Finalmente si aplicamos la misma regla a los usuarios de la red cableada, 27 de ellos utilizarían la WLAN, por lo que el número de usuarios total de la WLAN es de 231. Entonces el
Espacio de ancho de banda = 1128 Kbps / 231 usuarios = 4.88 Kbps/usuario
por lo que de acuerdo a este análisis de deberá implementar el canal a 1640 Kbps, con lo que el
Espacio de ancho de banda = 1512 Kbps / 231 usuarios = 6,55 Kbps/usuario.

4.3 FACTIBILIDAD ECONÓMICA

El análisis de la factibilidad económica se refiere al estudio de los costos de los recursos necesarios para desarrollar o llevar a cabo el proyecto propuesto. Fundamentalmente incluye el costo de los dispositivos, instalación, configuración y capacitación en la operación de los equipos.

En el análisis de factibilidad económica realizado, se plantea una opción óptima, en la cual se detalla todos los componentes necesarios para que el proyecto propuesto cubra las necesidades y objetivos planteados al inicio.

En la tabla 4.1 se presenta el detalle de los elementos necesarios y sus costos para la implementación propuesta.

Cant.	Detalle	P. Unitario	Subtotal
14 uni.	Puntos de acceso	450,00	6.300,00
1 uni.	Rollo de cable UTP cat.6	150,00	150,00
50 uni.	Conectores RJ45	0,45	22,50
1 uni.	Pequeño material (tornillos, tuercas, grapas, material de sujeción, cinta aislante)	30,00	30,00
1 uni.	Obra civil	50,00	50,00
1 uni.	Módulo de memoria RAM de 512	120,00	120,00

2 uni.	Servidores (Web Server y Mail)	3.000,00	6.000,00
1 uni.	Servidor AAA	4.500,00	4.500,00
1 uni.	Instalación, configuración y capacitación	500.00	500.00
8 uni.	Antenas externas	120,00	960,00
20 metros	Cables de antena	3,00	60,00
12 meses	Un operador técnico	350,00	4.200,00
		TOTAL	**USD 22.892,50**

Tabla 4.1: Detalle de elementos y costos para Wlan

La implementación total de la WLAN propuesta, garantiza que la infraestructura sea funcional por un lapso de 2 años, tomando en cuenta el crecimiento de usuarios y servicios. Paralelamente a ello se deberá pensar en la ampliación del ancho de banda que se tiene actualmente.

La tabla 4.2 muestra el detalle de los elementos mínimos necesarios para que la WLAN propuesta opere en el momento actual. Se garantiza su funcionamiento con las condiciones actuales de la red únicamente añadiendo los puntos de acceso y realizando las configuraciones e instalaciones necesarias para su operación.

Cant.	Detalle	P. Unitario	Subtotal
10 uni.	Puntos de acceso	450,00	4.500,00
1 uni.	Rollo de cable UTP cat.6	150,00	150,00
50 uni.	Conectores RJ45	0,45	22,50
1 uni.	Pequeño material (tornillos, tuercas, grapas, material de sujeción, cinta aislante)	30,00	30,00
1 uni.	Servidor AAA	4.500,00	4.500,00
1 uni.	Instalación, configuración y	500.00	500.00

	capacitación		
1 uni.	Obra civil	50,00	50,00
8 uni.	Antenas externas	120,00	960,00
20 metros	Cables de antena	3,00	60,00
		TOTAL	**USD 10.772,50**

Tabla 4.2: Propuesta mínima para la implementación de la Wlan

Se debe tomar en cuenta que de implementarse esta segunda opción, el rendimiento de la red puede disminuir al momento de contar con más usuarios conectados y la funcionalidad de la red podría no ser óptima.

Al intentar realizar el análisis costo/beneficio que representaría la implementación del proyecto propuesto, prácticamente se hace posible, toda vez que la dirección actual de la institución manifiesta su intención de no facturar por su uso, por lo que no contaría con una fuente de ingreso con la cual se pretenda medir el retorno de la inversión que se realizaría en el proyecto.

Los beneficios que se pretende obtener al implementar el proyecto propuesto y por el hecho de que no se va a cobrar ningún monto por el acceso y uso de la WLAN, son intangibles.

Decimos que son intangibles debido a que el beneficio no se va a poder cuantificar económicamente, puesto que lo que se busca como principal objetivo es la de brindar acceso a Internet a todos los usuarios y visitantes de la organización.

Ofrecer un centro de convenciones y biblioteca con acceso inalámbrico al Internet, posicionaría al centro de convenciones y a la institución como un centro de referencia de eventos culturales, políticos, sociales, académicos de gran magnitud. Permitirá al centro tener una mayor demanda de uso de sus instalaciones, dando como resultado mayor ingreso por concepto de alquiler y préstamo de las mismas.

Al desarrollarse eventos continuos en la institución, el número de visitantes también aumentaría, permitiendo que más personas conozcan a la institución y las actividades que realiza. Esto aumentaría la cantidad de posibles interesados en participar o vincularse con la organización ya sea como estudiantes, en proyectos de investigación o consultorías.

En definitiva no va a generar un beneficio directo por el uso de la WLAN propuesta, sino que producirá beneficios indirectos a varias actividades que se realizan en la institución.

CAPITULO 5: CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

1 El proyecto propuesto permitirá una fácil incorporación de nuevos usuarios a la red, con nueva tecnología, y sin necesidad de estar limitado a la conexión a través de cable.

2 La WLAN puede brindar flexibilidad a los profesores y estudiantes, para que en cualquier tiempo tengan acceso a los recursos que desean, por ejemplo, puede dar la facilidad de la impartición de clases tipo magistrales donde el profesor descarga las diapositivas de la clase y las proyecta, en tanto que los estudiantes desde sus ubicaciones pueden también seguir las clases con las diapositivas en sus computadores. También brinda flexibilidad a los estudiantes al poder conducir sus trabajos en sitios no convencionales, por ejemplo, en los pasillos del campus, áreas verdes, cafetería, biblioteca y otros sitios existentes en el campus. También existe la posibilidad de que los profesores puedan impartir lecciones fuera del aula de clases, tal como lo realizarían en ejercicios de laboratorios en condiciones de ambientes exteriores.

3 Los instructores pueden implementar con la WLAN un aprendizaje electrónico complementando sus instrucciones del aula de clase con actividades en línea y de conexión entre estudiantes para crear una experiencia de aprendizaje integrada y colaborativa.

4 Con la WLAN se puede dar conexión a varios usuarios en sitios donde tienen la mayor costumbre de permanecer (sitios que no pueden convertirse en laboratorios de computadoras, por ejemplo la cafetería) y sin la preocupación o necesidad de que exista una persona que administre la compartición de computadoras para que asigne un punto de red y cable para que puedan conectar sus equipos WiFi.

5 Los campus de educación superior se constituyen en un terreno fértil para las WLAN por que existe la tendencia a tener ambientes donde los estudiantes pueden hacer proyectos y trabajos en grupos más colaborativos y abiertos a un intercambio de ideas y experiencias. Además, este ambiente recibe apoyo por el hecho de que los estudiantes y profesores tienen una tendencia a la adquisición masiva de gran cantidad de aparatos y dispositivos móviles

6 La WLAN será beneficiosa para la institución por que la conexión inalámbrica entregará valor agregado a los estudiantes y usuarios, les hará parte de la red de la universidad, y dará valor a la institución en general.

7 La institución tendrá competitividad con otras universidades o centros donde se realizan eventos, puesto que los usuarios de hoy son más conocedores de la tecnología y el acceso inalámbrico a través de los campus y áreas de estancia. La institución se beneficiará de mucha innovación porque se fomentará un ambiente de aprendizaje más colaborativo y creativo. La WLAN colaborará con la institución para que soporte de mejor manera sus misión y visión institucional.

8 La solución inalámbrica es una solución de bajo costo, cablear para ethernet es una solución que consume costo y tiempo. En comparación, lo inalámbrico puede ser instalado mucho más rápidamente y a una fracción del costo. Más que eso, lo inalámbrico puede virtualmente eliminar la sobrecarga operacional asociada con adiciones, movimientos y cambios en la red del campus.

9 Con el servicio de Internet inalámbrico se espera que el número de visitantes y la demanda por el uso del Centro de convenciones y biblioteca aumente, lo que representaría un mayor prestigio a la institución, lo que significaría también una mayor promoción y difusión de la institución y de las actividades que al interior se realizan.

10 Cuando existen eventos contratados por terceros se tendrá mayor movilidad ya que podrán trasladarse de un lugar a otro sin perder el acceso a la información. Además existirá mayor demanda para el uso de las instalaciones para dichos eventos.

11 Se formará una red híbrida, que estará conformada por la red cableada existente con la WLAN propuesta, la misma que cubrirá todo el edificio, esto permitirá mejorar los servicios actuales que ofrece la institución, seguirá teniendo las ventajas que brinda la red cableada y proporcionará mayor disponibilidad, velocidad y movilidad a los usuarios dentro del edificio.

12 Se constituye un objetivo prioritario para las autoridades de la institución la dotación de una WLAN al interior del campus, por lo que el proyecto propuesto es viable desde el punto de vista ejecutivo y también desde el punto de vista financiero, puesto que no solo se plantea la instalación de una WLAN sino además de cubrir o solucionar ciertas debilidades encontradas en el análisis de la situación actual y que las autoridades han comprendido la necesidad de llevar a cabo el proyecto.

13 Para la implementación del proyecto se debe indicar que no se cuenta con ninguna imposición legal por el uso de la frecuencia en la que trabajan las WLAN, debido a que son de uso gratuito de acuerdo a la Resolución 417 vigente aprobada por el CONATEL en noviembre de 2005.

5.2 RECOMENDACIONES

1. Con el aumento de los usuarios de la red local, se debe prever que será necesaria la ampliación del canal de acceso al Internet. Al aumentar los usuarios, la demanda por el uso del Internet será mayor, lo que provocará que el acceso al Internet sea lento, de mantenerse el ancho de banda contratado. La institución tiene como política hacer ajustes anuales de su canal de acceso al Internet, tomando en cuenta que cada año disminuyen los costos de prestación de servicio del acceso, en lugar de bajar los costos

el proveedor en común acuerdo con la institución aumenta su ancho de banda al mismo precio o incluso un poco más pero sin que afecte de manera significativa al presupuesto de la institución.

2. Se recomienda establecer e implementar políticas y perfiles de acceso con el servidor RADIUS AAA, así como el tipo de servicio al que tendrán acceso los usuarios de la WLAN propuesta. Con el fin de proteger la red cableada se recomienda que únicamente el tráfico que pueden generar los usuarios de la WLAN sea HTTP para navegación por Internet. Los servicios de página Web, pagos en línea, biblioteca virtual, correo electrónico y sistema de gestión docente se podrán acceder a ellos a través de un browser (Internet Explorer, Mozilla, Netscape, entre otros).

3. Se recomienda implementar un servidor FTP y HTTP cifrados o seguros, con el fin de poder compartir archivos en la red y garantizar su confidencialidad e integridad en la información. Estos servicios deberían ser implementados en el servidor Web de la institución, para que los archivos estén disponibles y los usuarios puedan acceder a ellos desde el Internet.

4. Se recomienda la instalación de antenas externas en los puntos de acceso (AP), tanto en la planta baja como en el subsuelo 1, para brindar brindar una mayor cobertura en estas áreas, se hace esta recomendación ya que la mayor demanda de acceso inalámbrico por parte de los usuarios y las áreas más grandes de cobertura se encuentran allí.

5. Se recomienda realizar un monitoreo continuo del uso del canal de acceso al Internet y obtener reportes estadísticos con el objetivo de mantener un control permanente del uso del ancho de banda contratado, para verificar si es necesaria la ampliación del canal de acceso al Internet. Este monitoreo se lo puede realizar utilizando herramientas como son por ejemplo MRTG, que es una herramienta de uso gratuito, no necesita de licencia y se lo puede configurar en varias plataformas.

6. Se recomienda la ampliación de la memoria RAM a 1 Gb del servidor controlador de dominio que actualmente cuenta con 512 Mb. El incremento de usuarios demandará mayor procesamiento por parte del servidor y el aumento de la memoria RAM evitará que su rendimiento disminuya, atendiendo las peticiones con la misma calidad y velocidad que lo realiza actualmente.

7. Se cuenta actualmente con un firewall, el mismo que maneja las zonas WAN, LAN y DMZ. Se recomienda habilitar y usar la zona desmilitarizada DMZ, con el objetivo de tener un mayor control del acceso hacia la red interna. Así los usuarios que ingresen desde la WAN solo podrán acceder a los servidores que se encuentren en esta zona semipública o DMZ y por ende únicamente utilizarán los servicios disponibles allí. De esta manera se pretende aislar completamente todo tipo de comunicación entre las redes WAN y LAN.

8. Se recomienda la compra de 2 servidores adicionales. Actualmente un solo equipo cumple con las funciones de servidor WEB, MAIL y PROXY. Si este servidor llega a sufrir algún fallo, la institución perderá los 3 servicios simultáneamente. La adquisición de los 2 servidores permitirá la descentralización de los 3 servicios, uno en cada servidor; si uno llega a sufrir un daño, los otros 2 servicios seguirán disponibles.

   Al separar los servicios de Web, Proxy y correo electrónico en 3 servidores físicamente distintos, se garantizará la eficiencia y velocidad de procesamiento de los servidores en las peticiones que se les realice, tomando en cuenta el incremento de usuarios previstos al implementar la WLAN propuesta.

9. Con la implementación del proyecto propuesto se incrementará el número de usuarios y por ende habrá mayor demanda de los servicios ofertados, provocando esto una mayor necesidad de control de acceso y seguridades en la red local, lo que implica una mayor carga de trabajo en el personal de las TIC actual. Por tal motivo se sugiere contratar un técnico que se haga

cargo del soporte a los usuarios, para de esta manera descongestionar al personal actual de estas tareas y así el personal de las TIC pueda dedicarse a la administración, configuración y mantenimiento de la WLAN propuesta.

10. Se recomienda implementar AP de la misma marca de los equipos existentes para la conexión de la red local (switch de piso). La razón principal es, que cada fabricante incluye en sus productos herramientas que facilitan la integración y comunicación entre ellos. Además que el personal técnico existente esta ya familiarizado con las herramientas para la configuración y uso.

REFERENCIAS BIBLIOGRAFICAS

— REID, Neil & SEIDE, Ron. Manual de redes inalámbricas. Editorial Mc Graw Hill, primera edición, 2004

— ENGST, Adam & FLEISHMAN, Glenn. Introducción a las redes inalámbricas. Editorial Anaya Multimedia. España. 2003

— Norma para la implementación y creación de Sistemas de Espectro Ensanchado. CONSEJO NACIONAL DE TELECOMUNICACIONES

— CITA SÁNCHEZ Alberto. Tecnología de redes de área local inalámbricas: WLAN. CERN Datanet S.A. Grupo TELINDUS. http://www.kerndatanet.com. White paper.

— La situación de las Tecnologías WLAN basadas en el estándar IEEE 802.11 y sus variantes (“Wi-Fi”). Colegio Oficial de Ingenieros de Telecomunicación, http://www.coit.es.

— Advanced Design System 2002. WLAN DesignGuide. Agilent Technologies. Palo Alto, CA U.S.A. 2002

— IEEE Std 802.11a-1999(R2003). Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. High-speed Physical Layer in the 5 GHz Band. LAN/MAN Standards Committee of the IEEE Computer Society. 2003

— IEEE Std 802.11b-1999(R2003). Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band. LAN/MAN Standards Committee of the IEEE Computer Society. 2003.

— IEEE Std 802.11b-1999/Cor 1-2001. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 2: Higher-speed Physical Layer (PHY) extension in the 2.4 GHz band—Corrigendum 1. LAN/MAN Standards Committee. 2001.

— IEEE Std 802.11d-2001. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 3: Specification for operation in additional regulatory domains. LAN/MAN Standards Committee of the IEEE Computer Society. 2001.

— IEEE Std 802.11F™-2003. IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11™ Operation. LAN/MAN Standards Committee of the IEEE Computer Society. 2003.

— IEEE Std 802.11g™-2003. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band. LAN/MAN Standards Committee of the IEEE Computer Society. 2003

— IEEE Std 802.11h™-2003. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe. LAN/MAN Standards Committee of the IEEE Computer Society. 2003

— IEEE Std 802.11i™-2004. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. LAN/MAN Standards Committee of the IEEE Computer Society. 2004.

— IEEE Std 802.11j™-2004. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 7: 4.9 GHz–5 GHz

Operation in Japan. LAN/MAN Standards Committee of the IEEE Computer Society. 2004.

— SCHWARTZ, Sorin M. Frequency Hopping Spread Spectrum (FHSS) vs. Direct Sequence Spread Spectrum (DSSS) in the Broadband Wireless Access and WLAN Arenas. Alvarion Ltd. BreezeCOM and Floware unite. www.alvarion.com. 2001.

— Sistema Integrado de Legislación Ecuatoriana (SILEC Pro). Ver. 4.1 r5. Lexis S. A. 2005.

— http://www.tdx.cesca.es/TESIS_URL/AVAILABLE/TDX-1104104-101718/Tavb13de23.pdf

ANEXOS

ANEXO I

ESPECTRO ENSANCHADO

La mayor parte de los sistemas WLAN utilizan tecnología de Espectro Ensanchado o Expandido (Spread Spectrum). Esta tecnología inicialmente fue desarrollada para uso militar en sistemas de comunicaciones seguros en aplicaciones críticas. Con esta técnica se consume más ancho de banda que con los sistemas de Banda Estrecha.

Spread Spectrum es un tipo de modulación creada para incrementar la inmunidad en la comunicación vía radio a las interferencias y para dificultar su detección e intercepción. Existen dos tipos de sistemas de Espectro Expandido:

- Frecuency Hopping (salto de frecuencia). El emisor va cambiando continuamente de canal. Utiliza una portadora de banda estrecha que cambia de frecuencia (salta de una frecuencia a otra) según un patrón conocido por el transmisor y el receptor. Sincronizadas de manera adecuada las estaciones, de manera lógica parece ser que se mantiene un único canal. Para un receptor indeseado, una transmisión de FHSS aparece como impulsos de ruido de corta duración. FHSS proporciona una elevada tolerancia a las interferencias, pero la velocidad de transmisión es menor.

- Direct Sequence (secuencia directa). El emisor emplea un canal mas ancho. La potencia de emisión es similar a FHSS, pero al repartirse en una banda mas ancha da como resultado una señal de baja intensidad. Genera un patrón único de bits redundantes por cada bit que va a transmitir. Así, un único bit se convierte en varios "pedazos", siguiendo el patrón. Este mismo patrón usa el receptor para decodificar la información recibida. De esta forma se tiene que en DSSS cada bit es transmitido sobre múltiples frecuencias al mismo tiempo y si parte de la señal se pierde, el símbolo puede ser recuperado de las restantes frecuencias utilizadas. Utiliza mayor ancho de banda del espectro para una misma velocidad de transmisión, puesto que se transmiten 11 veces

el mismo bit, provocando que ocupe un ancho de banda de 22 Mhz. Presenta mejoras en las características de transmisión que FHSS, puesto que a igualdad de velocidades de transmisión DSSS proporciona el doble de distancia de cobertura que FHSS. Y a igualdad de coberturas DSSS consigue el doble de velocidad de transmisión que FHSS.

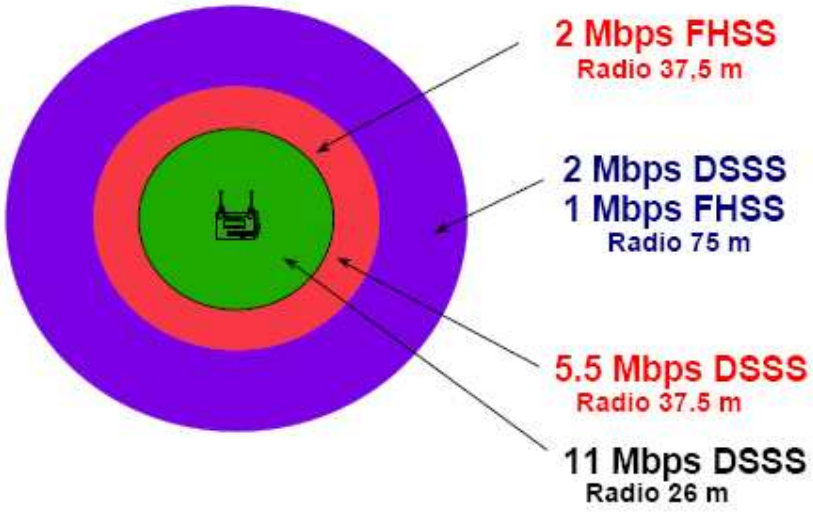
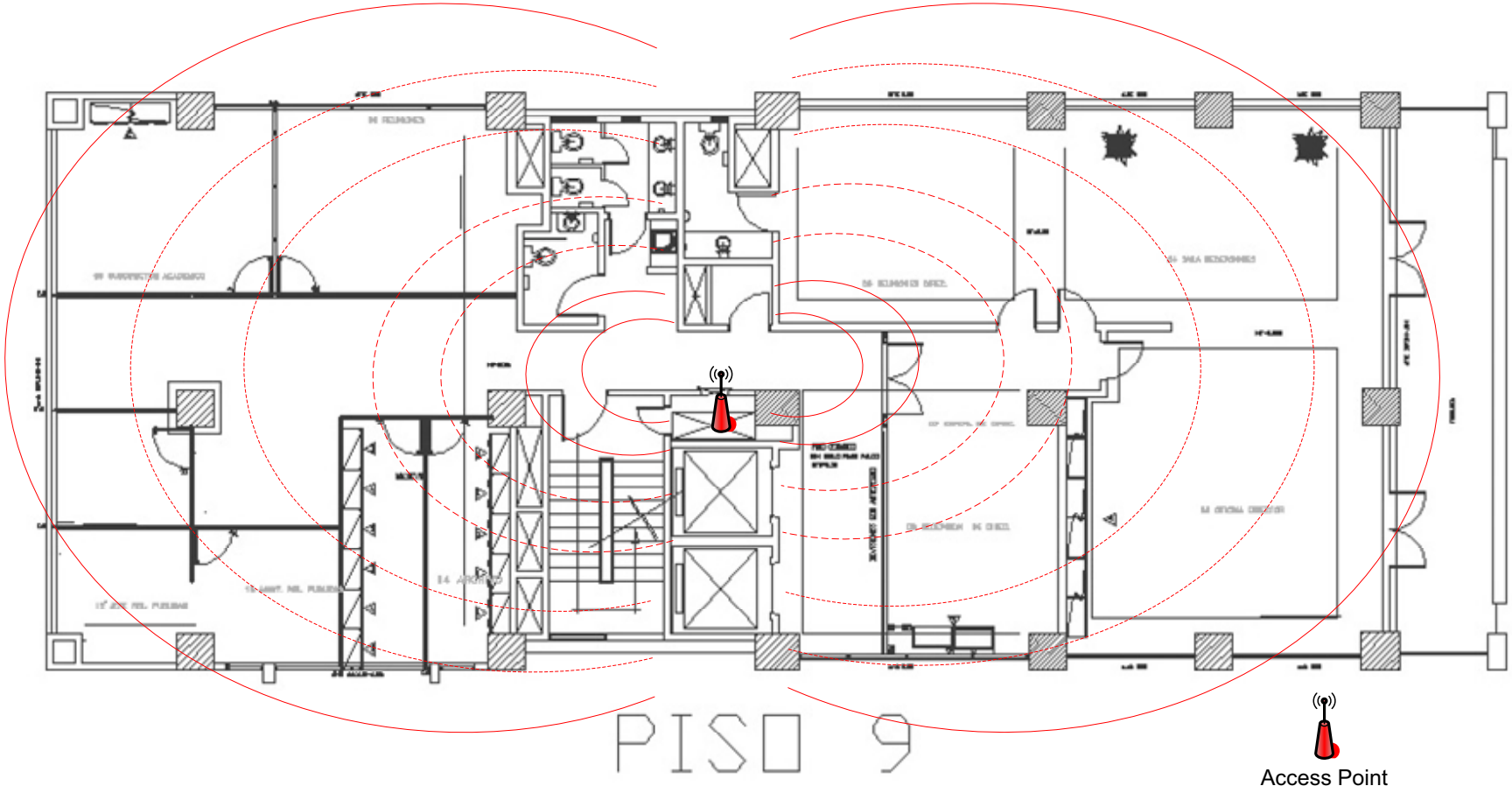
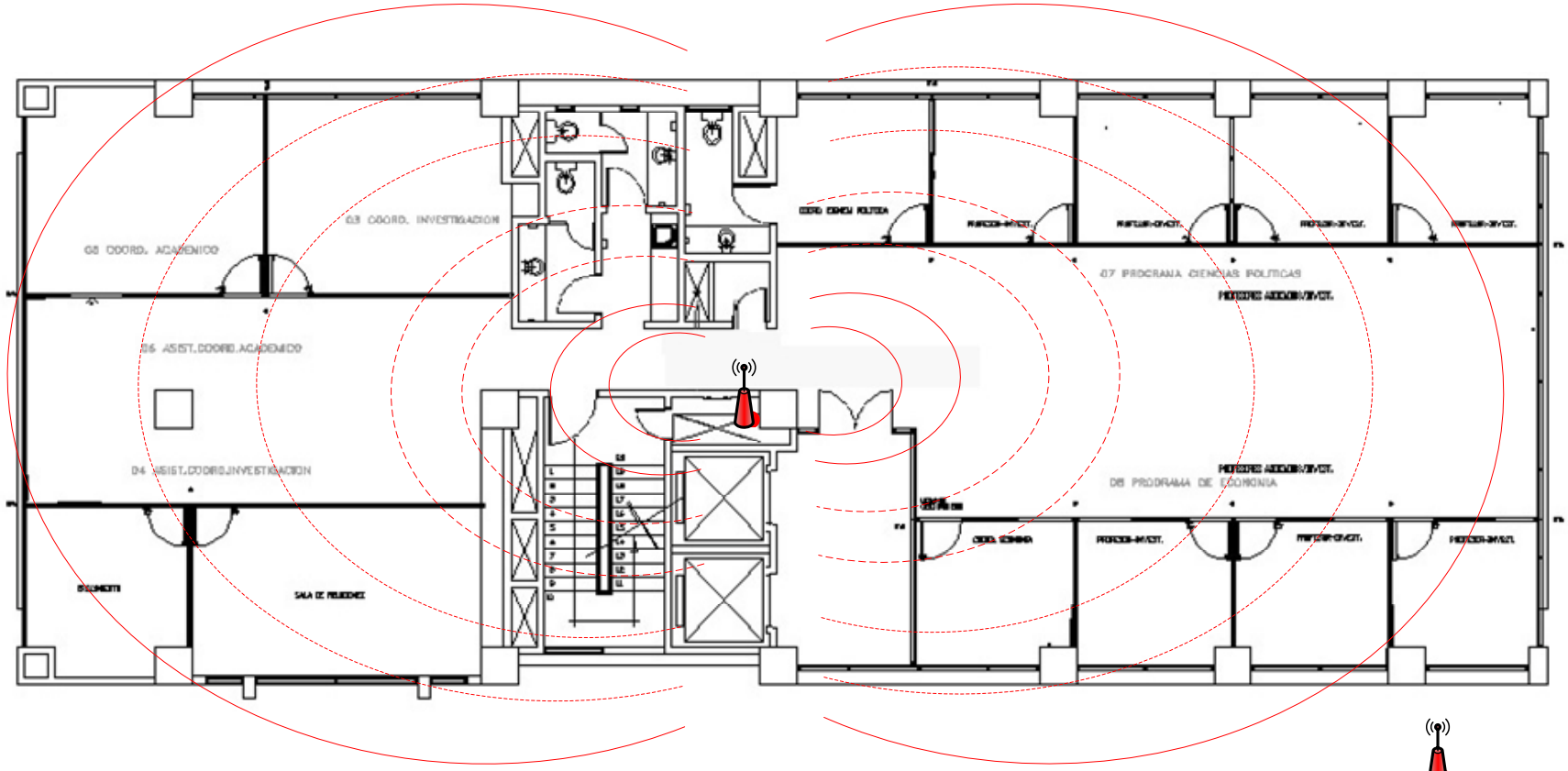


Figura 1: Comparación entre FHSS y DSSS

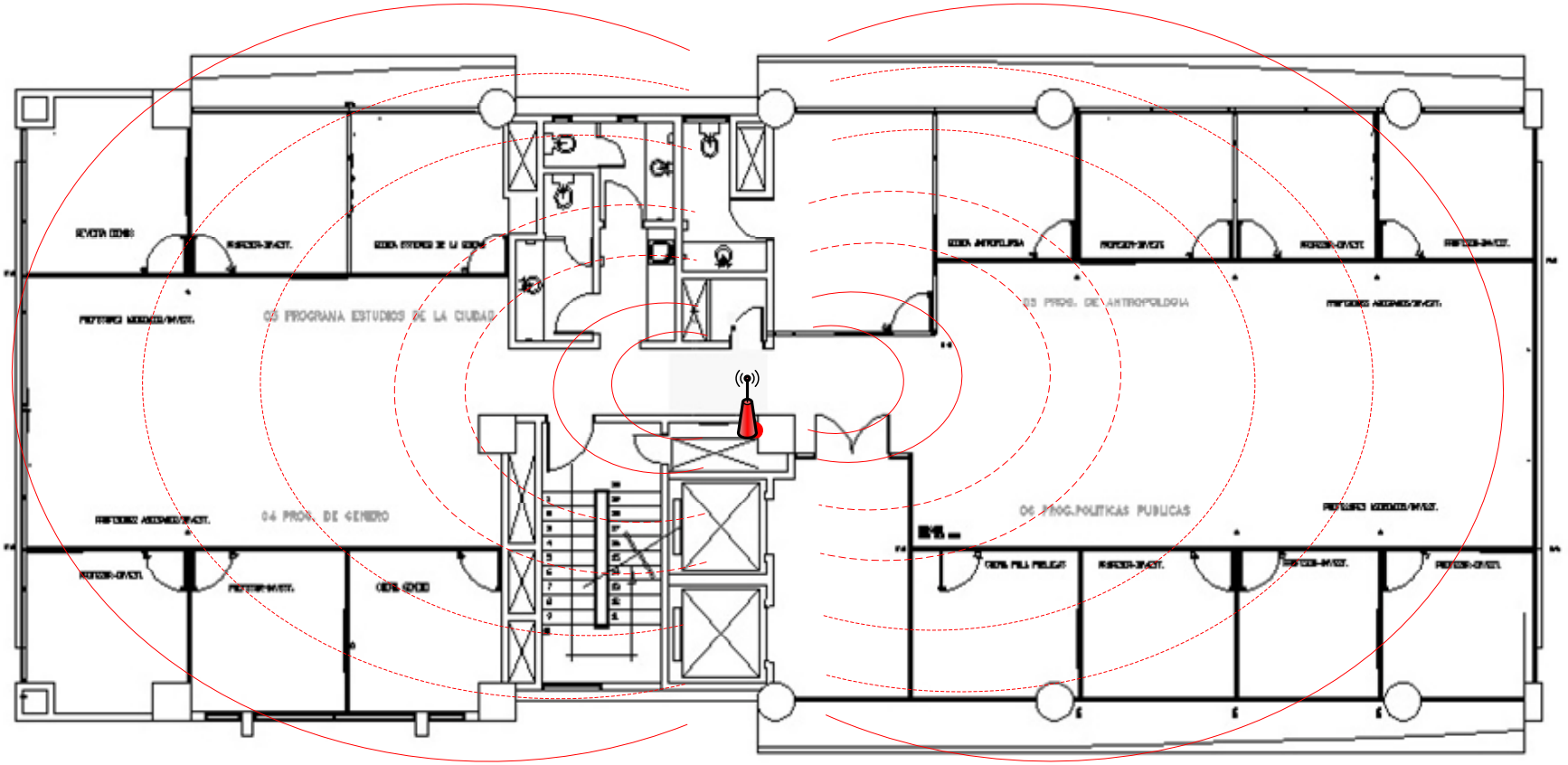
ANEXO II

AREAS DE COBERTURA DE LA WLAN EN EL EDIFICIO FLACSO

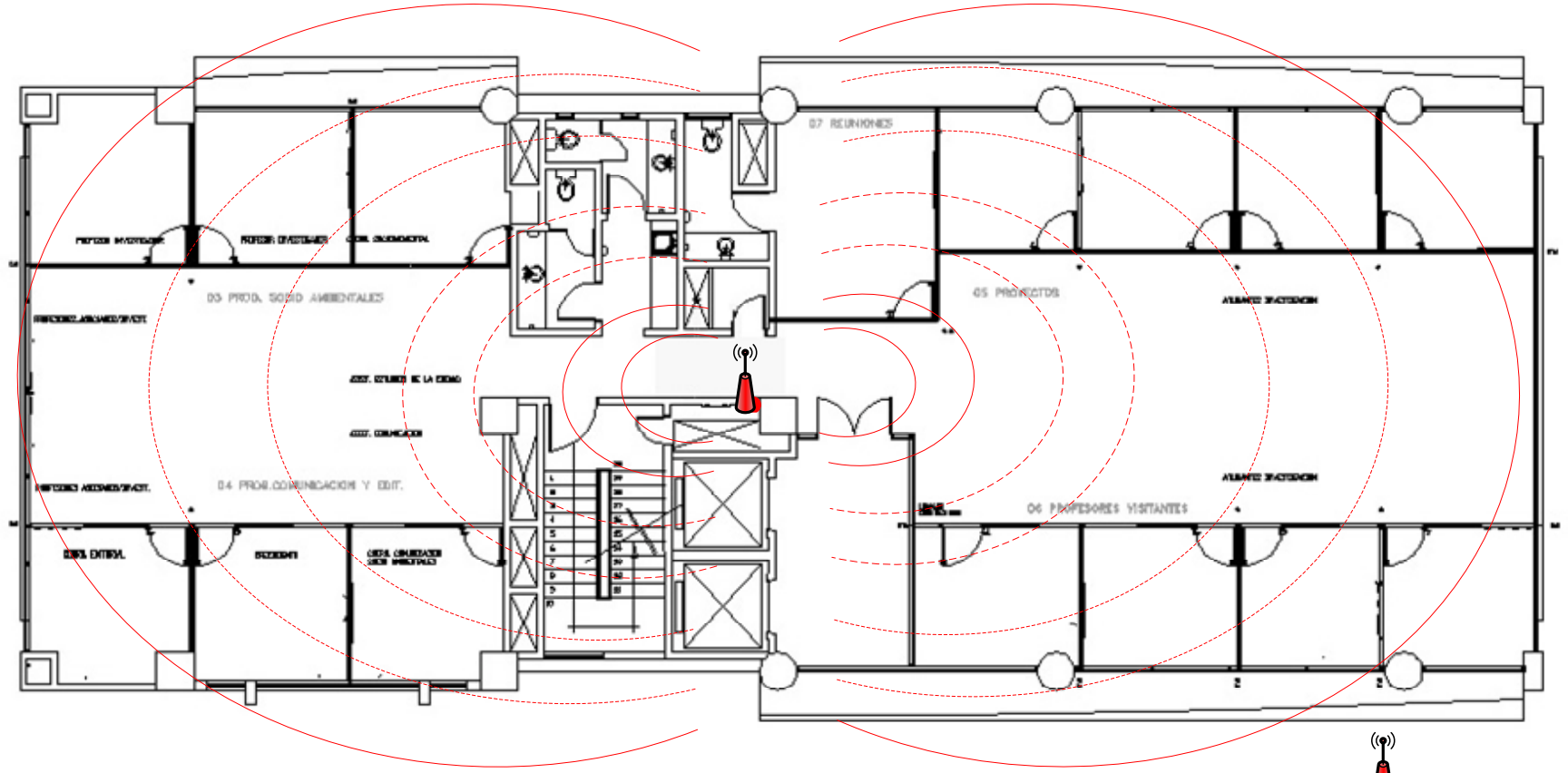



02 COORD. ACADEMICO
03 COORD. INVESTIGACION
04 ASIST.COORD.ACADEMICO
07 PROGRAMA CIENCIAS POLITICAS
08 PROGRAMA DE ECONOMIA
SALA DE PROFESORES
Access Point

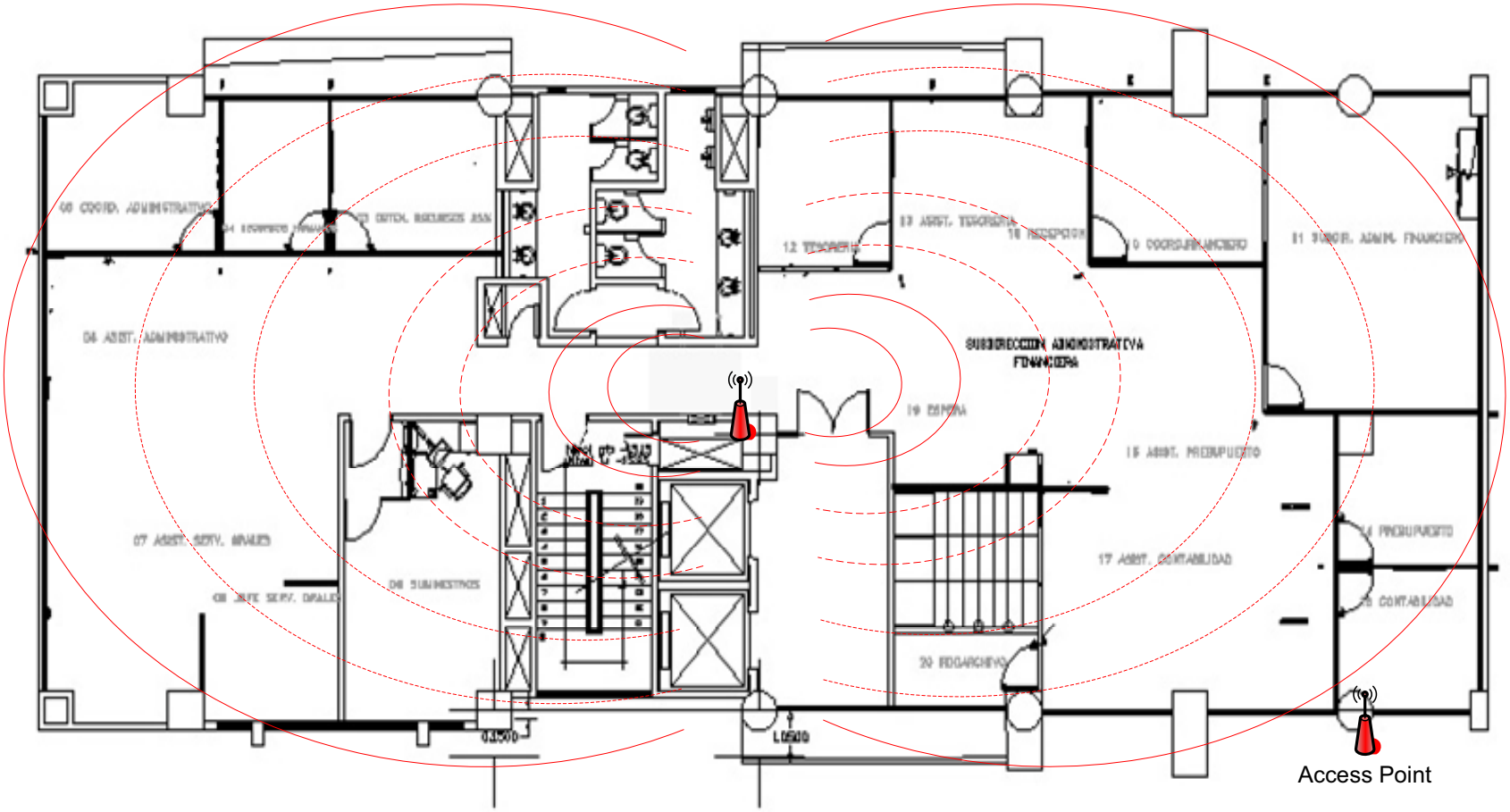
PISO 8


05 PROGRAMA ESTUDIOS DE LA CIUDAD
04 PROG. DE GENERO
06 PROG.POLITICAS PUBLICAS
Access Point

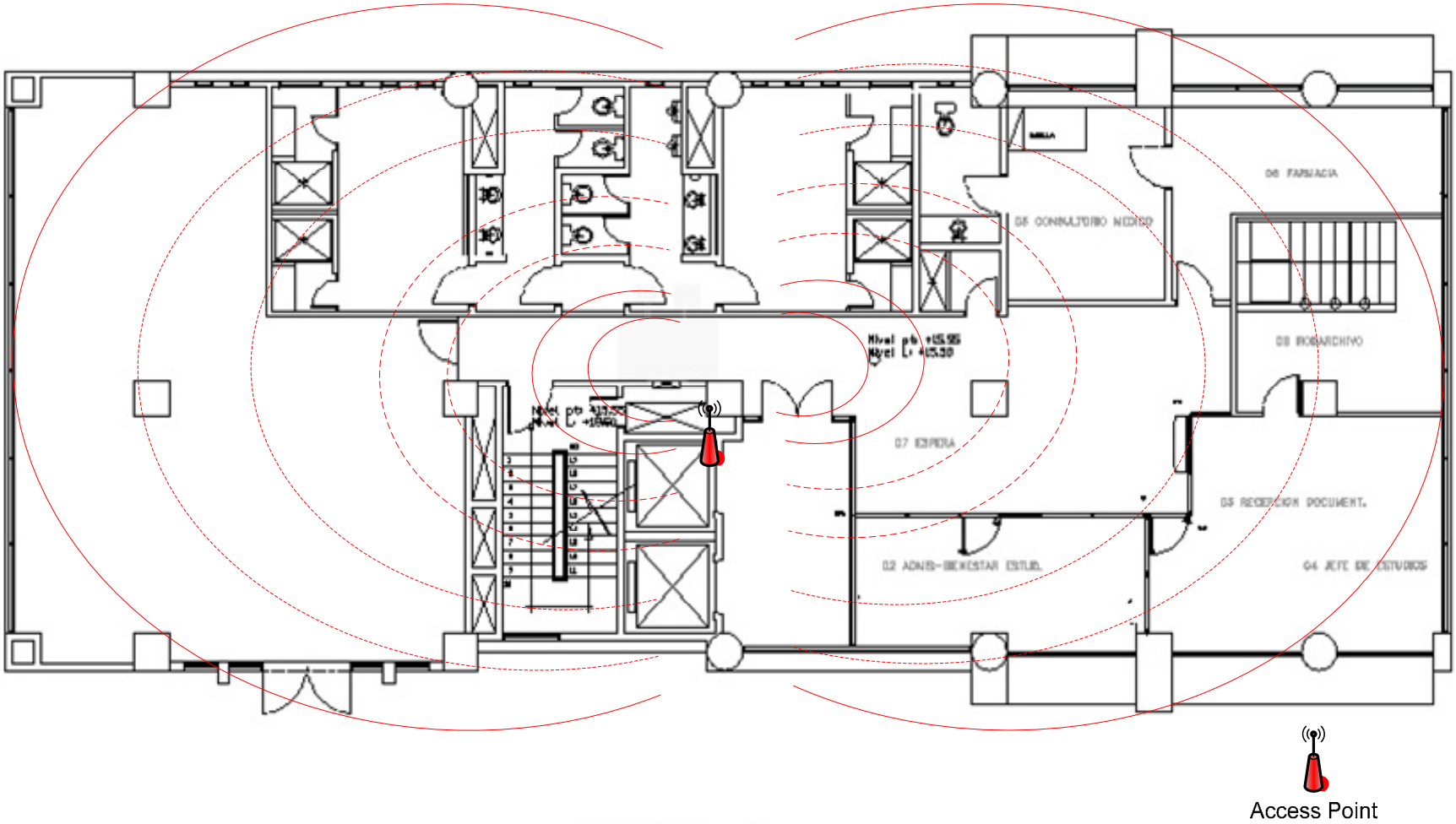
PISO 7


07 REUNIONES
05 PROYECTOS
03 PROD. SOCIO AMBIENTALES
04 PROD.COMUNICACION Y EDIT.
06 EMPRESORES VISITANTES
Access Point

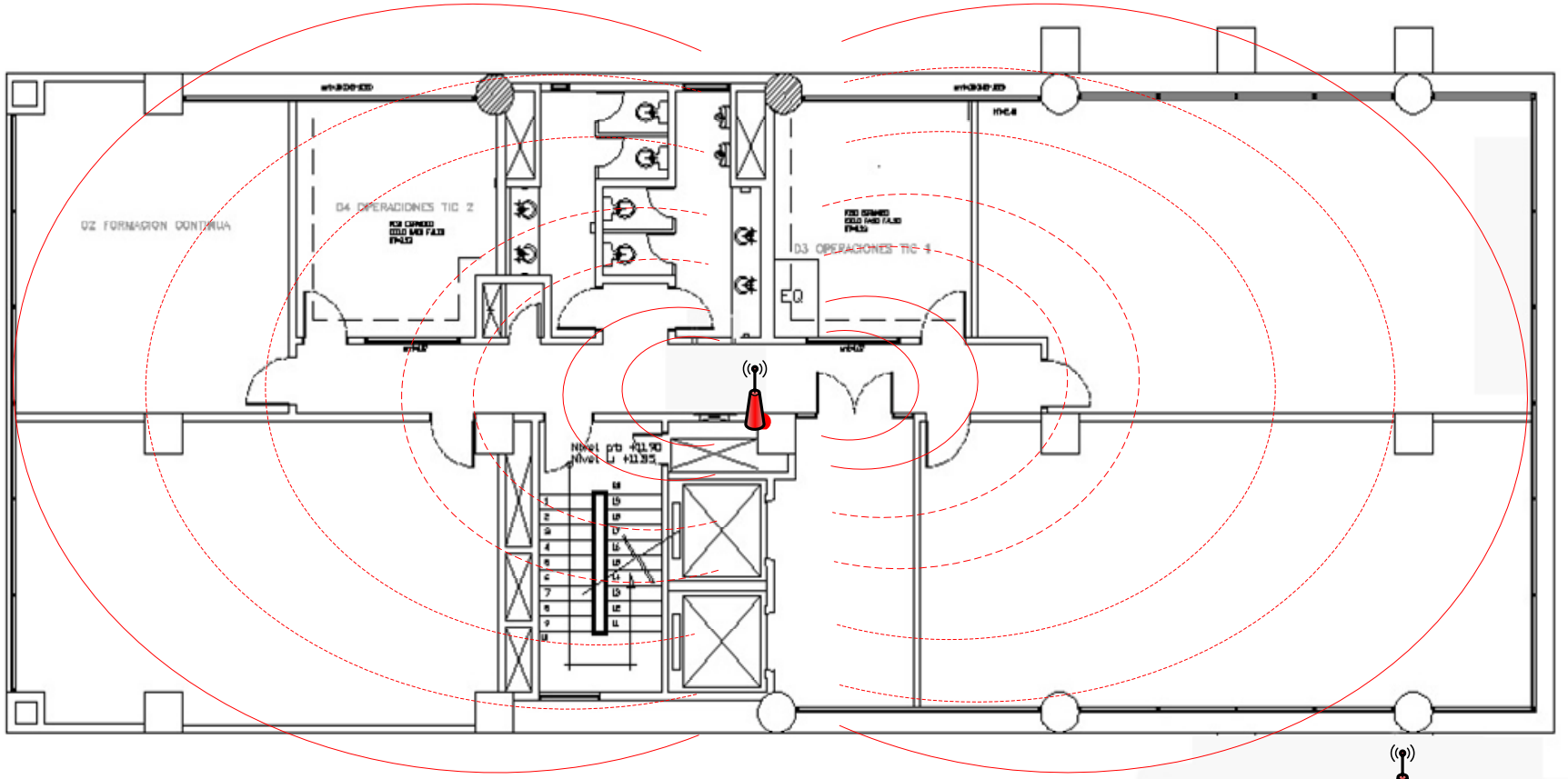
PISO 6



PISOS 5

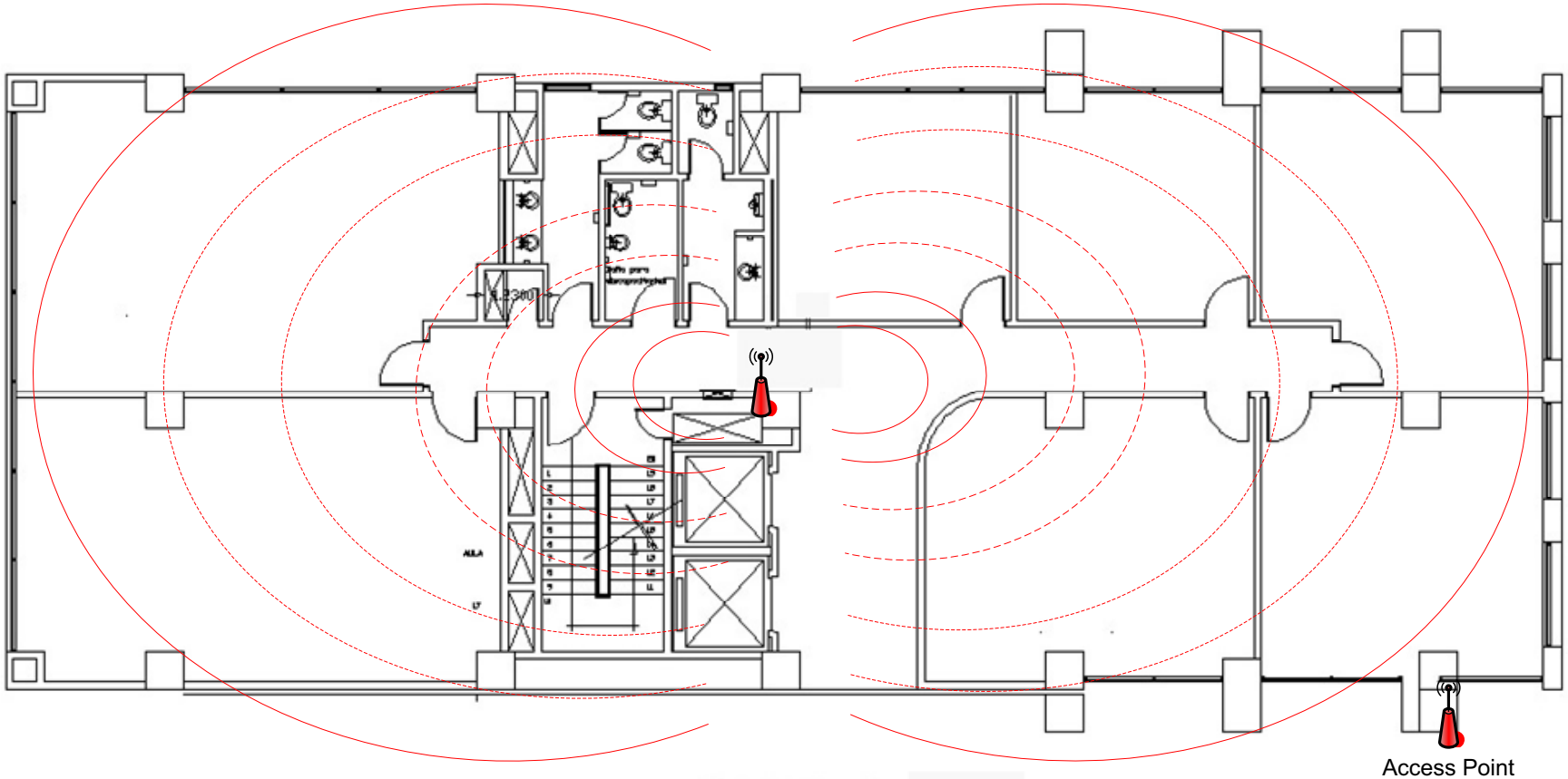

06 FARMACIA
05 CONSULTORIO MEDICO
08 ARCHIVO
07 ESPERA
03 RECEPCION DOCUMENT.
02 ADMIS-BIENESTAR ESTUD.
04 JEFE DE ESTUDIOS
Access Point

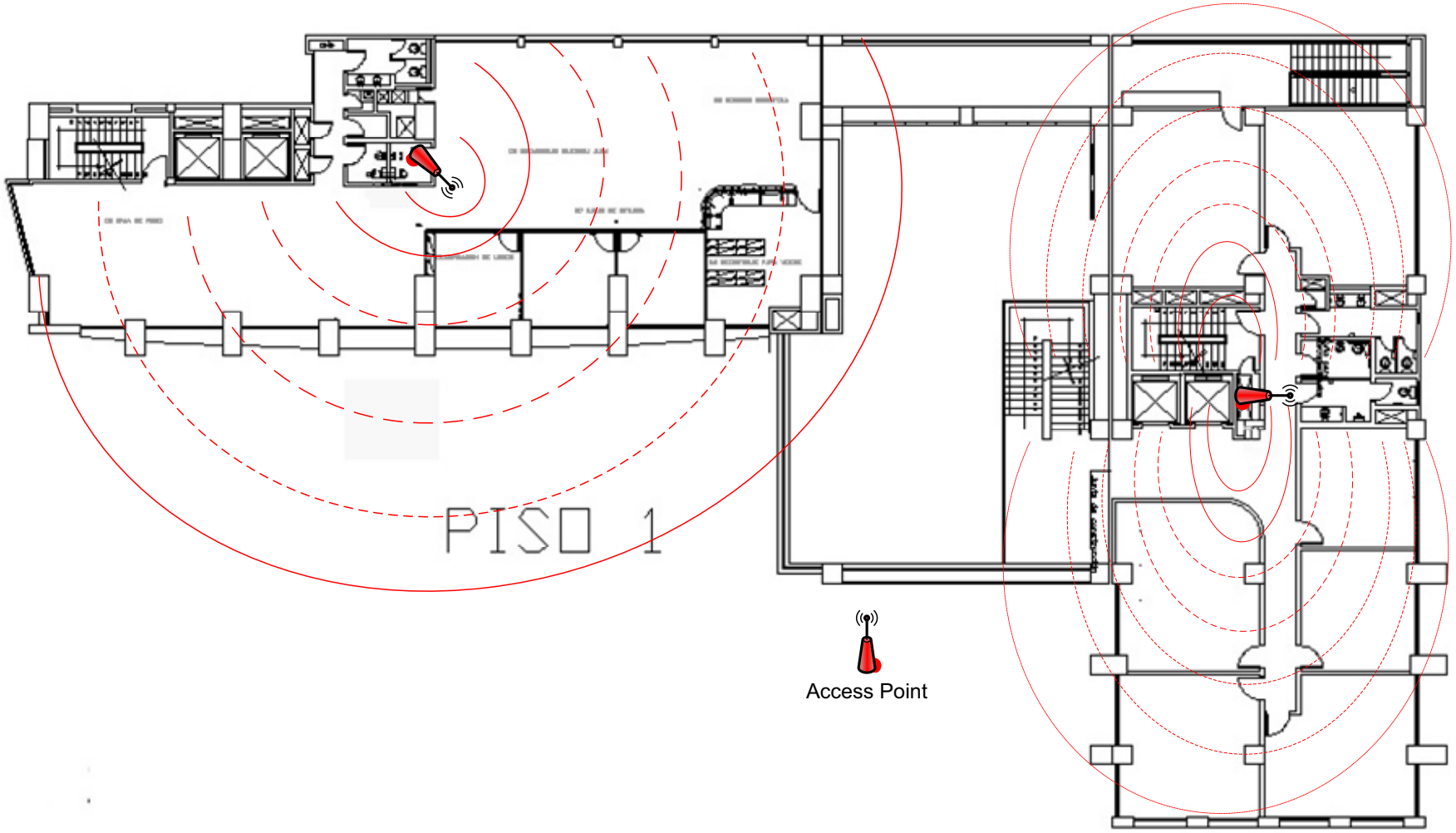
PISO 4

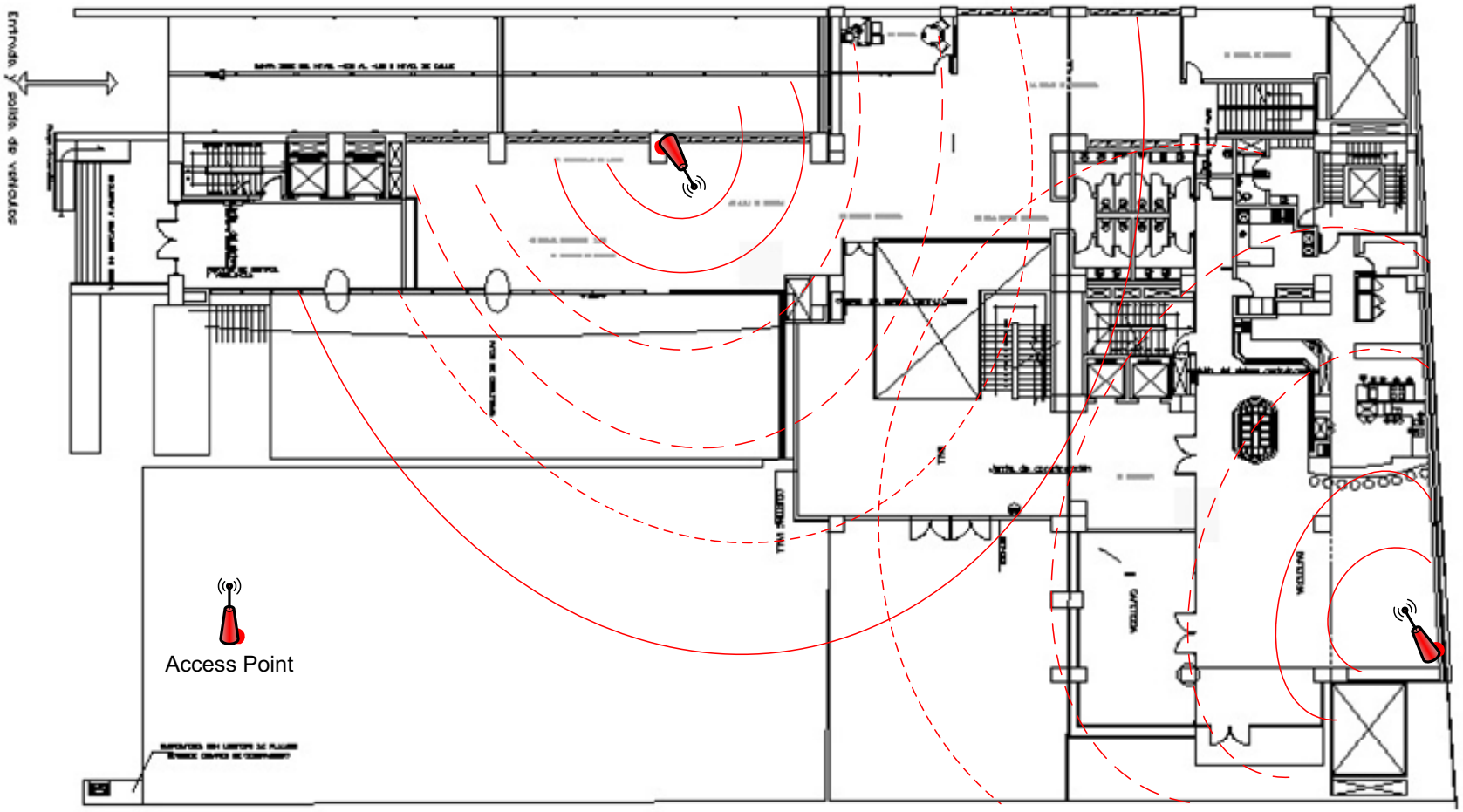


PISO 3

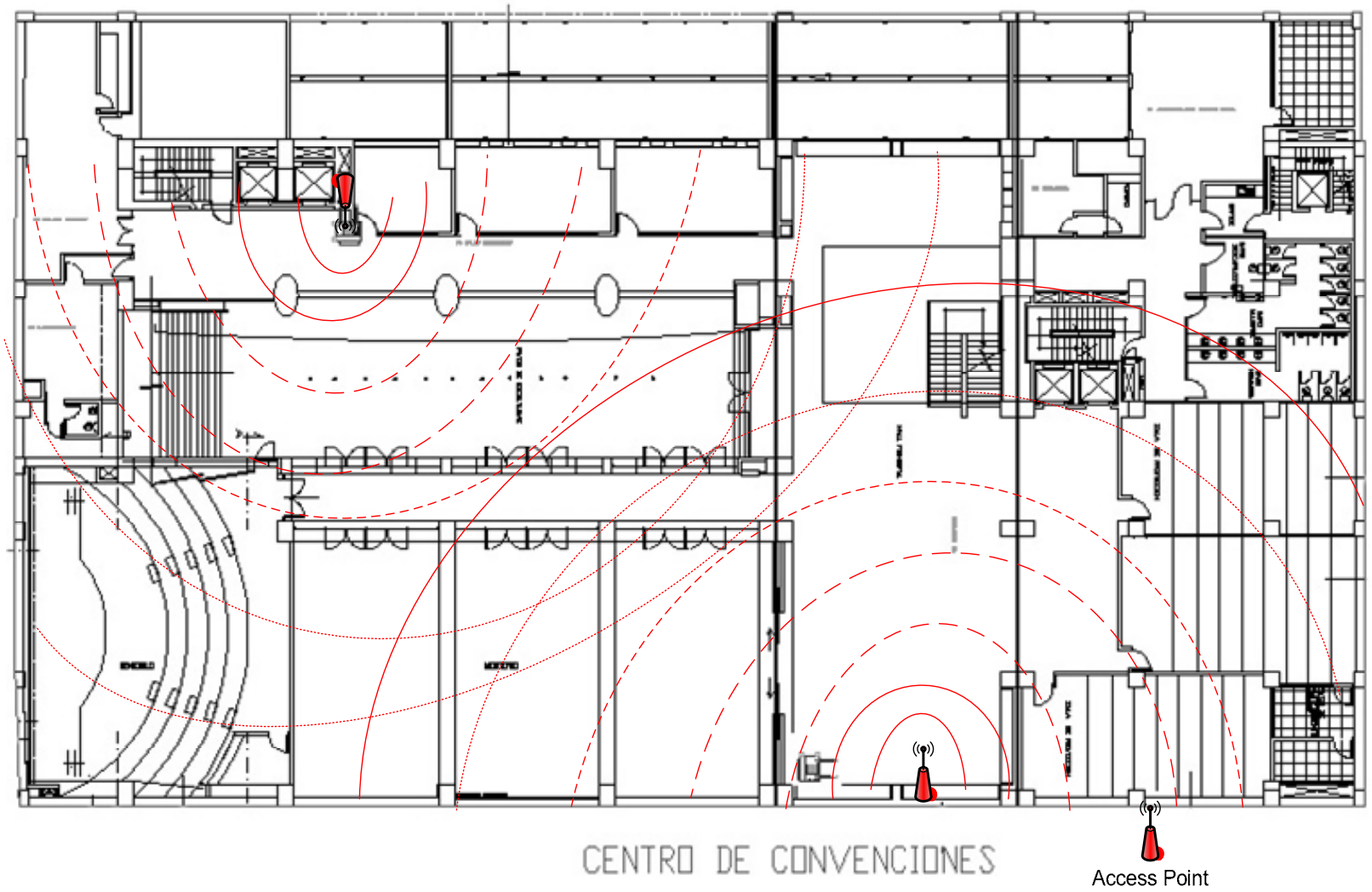
Access Point


Access Point
PISO 2


PISO 1
Access Point



PLANTA ARQUITECTONICA NIVEL 0.00


CENTRO DE CONVENCIONES
Access Point

ANEXO III

ENCUESTA DE LA RED DE DATOS DE FLACSO

Utiliza la red de datos de FLACSO — Si ☐ No ☐

Cuál es el uso que le da a la red de FLACSO
- Internet ☐
- Correo electrónico ☐
- Chat ☐
- Compartir archivos ☐
- Impresión ☐
- Uso de aplicaciones en red ☐
- Ninguno ☐
- Otros ☐ Cuál? ……

Que problemas ha tenido con la red
- Acceso lento ☐
- Caiga del sistema ☐
- Restricciones de uso ☐
- Virus ☐
- Ninguno ☐
- Otros ☐ Cuál? ……

Como calificaría el acceso al Internet
- Muy Bueno ☐
- Bueno ☐
- Regular ☐
- Malo ☐

Visita la página web institucional — Si ☐ No ☐

Que servicios de la página web institucional utiliza

Buscar información de:
- Oferta académica ☐
- Eventos ☐
- Sistema docente ☐

Pagos en línea
- Compra de libros ☐
- Inscripciones y matriculas ☐
- Pagos de colegiaturas ☐

Servicios
- Biblioteca en línea ☐
- Eventos en línea ☐

Correo electrónico ☐

Dispone de un dispositivo inalámbrico para conectarse a la red	Si ☐ No ☐
Le gustaría que la institución implemente una red inalámbrica	Si ☐ No ☐
Si se implementa una red inalámbrica, adquiriría un dispositivos inalámbrico para acceder a la red	Si ☐ No ☐

FACULTAD LATINOAMERICANA DE CIENCIAS SOCIALES
SEDE ECUADOR
CUADRO RESUMEN DE ENCUESTAS

PREGUNTA	OPCIONES	# RESPUESTAS	PORCENTAJE
Utiliza la red de datos de FLACSO	Si	35	87,5%
	No	5	12,5%
Cuál es el uso que le da a la red de FLACSO	Internet	33	82,5%
	Correo electrónico	33	82,5%
	Chat	28	70,0%
	Compartir archivos	5	12,5%
	Impresión	25	62,5%
	Uso de aplicaciones en red	8	20,0%
	Ninguno	5	12,5%
	Otros	0	0,0%
Que problemas ha tenido con la red	Acceso lento	10	25,0%
	Caiga del sistema	2	5,0%
	Restricciones de uso	8	20,0%
	Virus	10	25,0%
	Ninguno	19	47,5%
	Otros	4	10,0%

Como calificaría el acceso al Internet	Muy Bueno	6	15,0%
	Bueno	24	60,0%
	Regular	4	10,0%
	Malo	1	2,5%
Visita la página web institucional	Si	28	70,0%
	No	12	30,0%
Que servicios de la página web institucional utiliza			
Buscar información de:	Oferta académica	25	62,5%
	Eventos	22	55,0%
	Sistema docente	5	12,5%
Pagos en línea	Compra de libros	1	2,5%
	Inscripciones y matriculas	1	2,5%
	Pagos de colegiaturas	0	0,0%
Servicios	Biblioteca en línea	22	55,0%
	Eventos en línea	6	15,0%
	Correo electrónico	27	67,5%
Dispone de un dispositivo inalámbrico para conectarse a la red	Si	8	20,0%
	No	32	80,0%
Le gustaría que la institución implemente una red inalámbrica	Si	30	75,0%
	No	10	25,0%
Si se implementa una red inalámbrica, adquiriría un dispositivos inalámbrico para acceder a la red	Si	8	20,0%
	No	32	80,0%

ANEXO IV

MONITOREO DE LA RED ACTUAL

Sniffer Pro captura paquetes que circulan en la red, creando una base de datos de los objetos de red y presentando las anomalías que se encuentran en la red. Sniffer Pro analiza y categoriza los problemas, los analiza y muestra las posibles soluciones para corregirlo. Aprovecha el sistema de análisis Expert de Sniffer Technologies para ofrecer una automatización reforzada de la administración, información más completa sobre la solución de problemas y mayor visibilidad de la red.

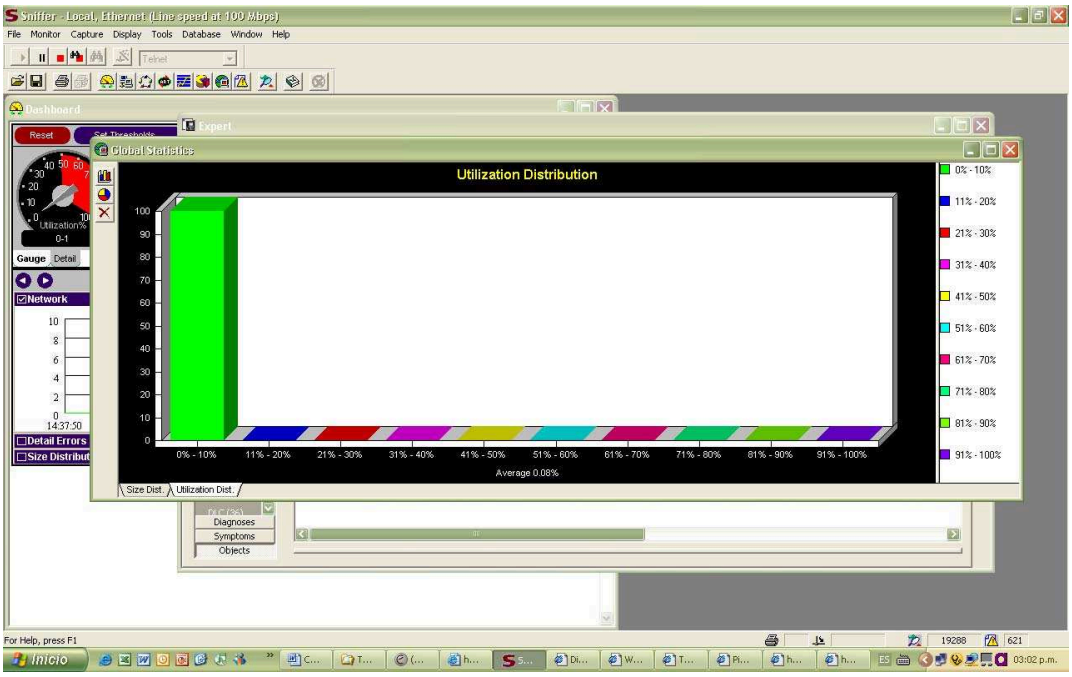
Identifica los problemas de la red en el momento en que se producen y los localiza para acelerar su resolución. Permite monitorear el consumo del ancho de banda de la red. Brinda una herramienta para obtener informes estadísticos globales así como filtros y así poder supervisar las aplicaciones y servicios que brinda la red.

Permite la captura y monitoreo de la red en línea, lo que permite al administrador detectar y corregir los problemas detectados en la red.

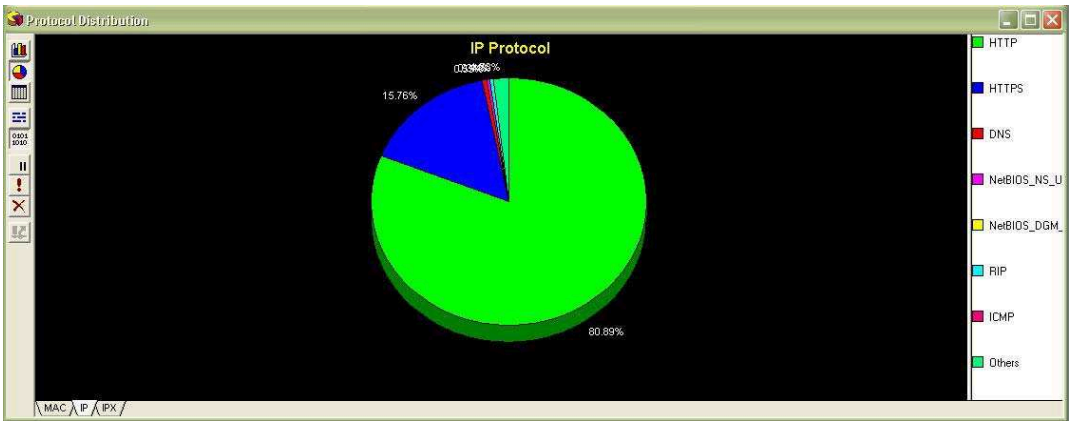
Análisis de la red de datos de FLACSO.

Luego de realizar por un día completo la captura del tráfico de la red de datos de la institución se han obtenido los siguientes resultados:

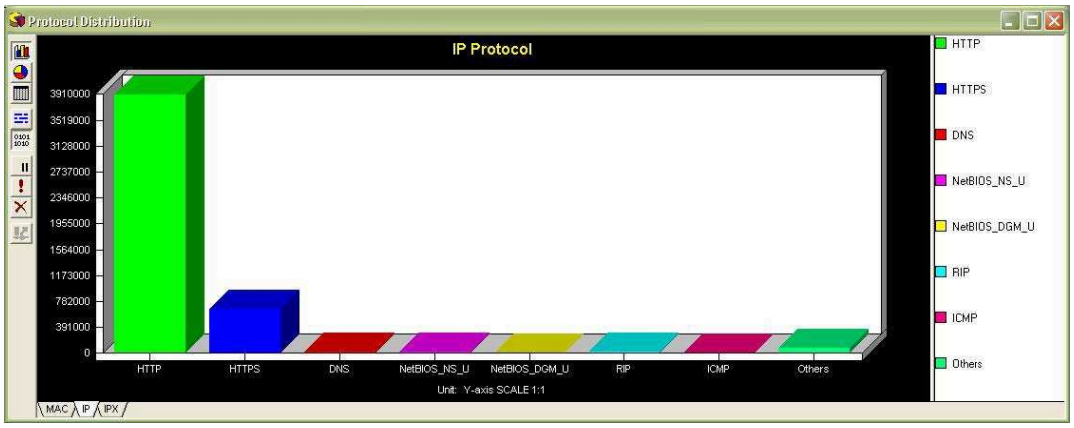
Se puede observar que la utilización del ancho de banda de la red de datos esta prácticamente subutilizada, la figura siguiente muestra que el uso del ancho de banda de la red de datos esta por debajo del 10% de su capacidad. Si tomamos en cuenta que el backbone de la red de fibra es de 1Gbps y la velocidad de las redes locales de piso es de 100 Mbps el uso es muy bajo, esto se debe especialmente que no existen aplicaciones que puedan producir una carga fuerte al tráfico al interior de la red, básicamente se utiliza para la navegación en Internet y chequear el correo electrónico.



El protocolo de mayor uso en la red corresponde al protocolo http, por lo que se define que la aplicación que más se utiliza en la red de datos es Internet. El protocolo http corresponde al 80% del tráfico de la red.



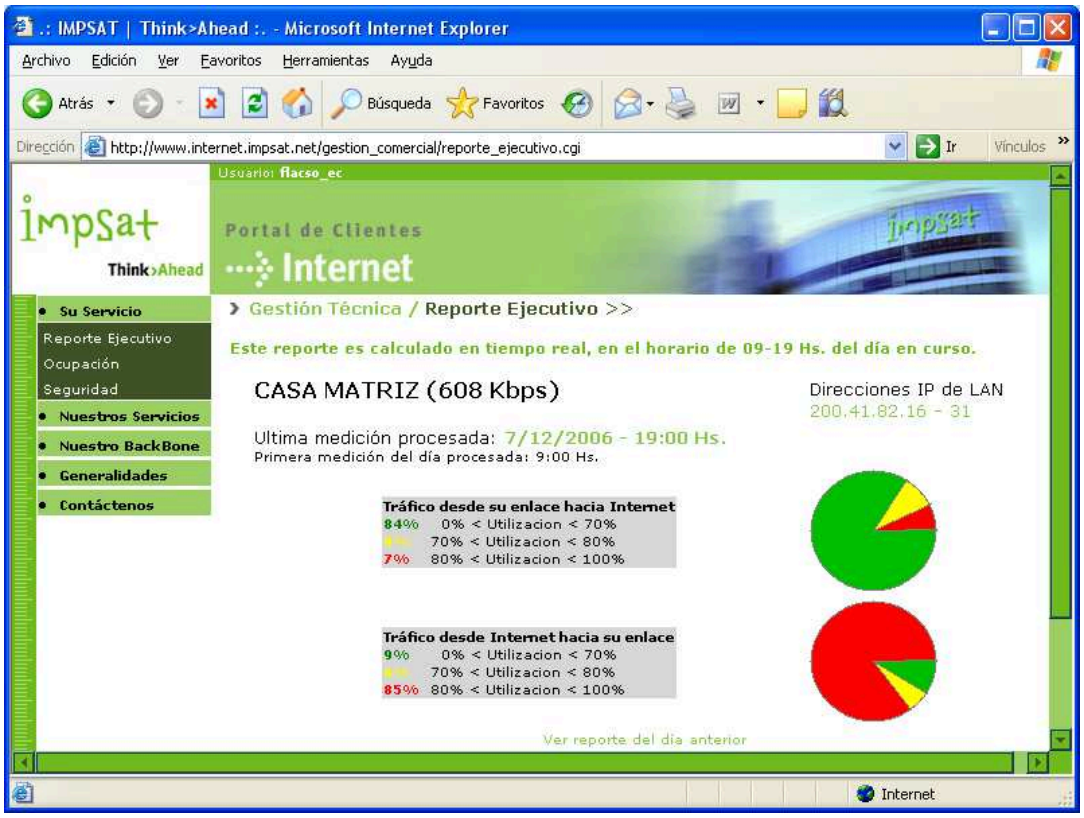
El protocolo https también es utilizado mayoritariamente, corresponde al 15% de tráfico de la red. https es un protocolo de Internet pero seguro, y se refiere en su gran mayoría al acceso a páginas web seguras, especialmente las correspondientes a instituciones financieras o servidores de correo gratuito como son Hotmail y netscape mail.



Otros protocolos de uso corresponden a DNS y NetBios, comprensibles por que se encuentra configurado un servidor de dominios Win2003 server.

Análisis del uso ancho de banda de conexión a Internet de FLACSO.

Para realizar el monitoreo del uso del canal de acceso al Internet, cuyo proveedor es la empresa IMPSAT; se utiliza la herramienta MRTG, y que es provista por el ISP. Se debe indicar que el canal es un Clear Channel de 1.128 Mbps.

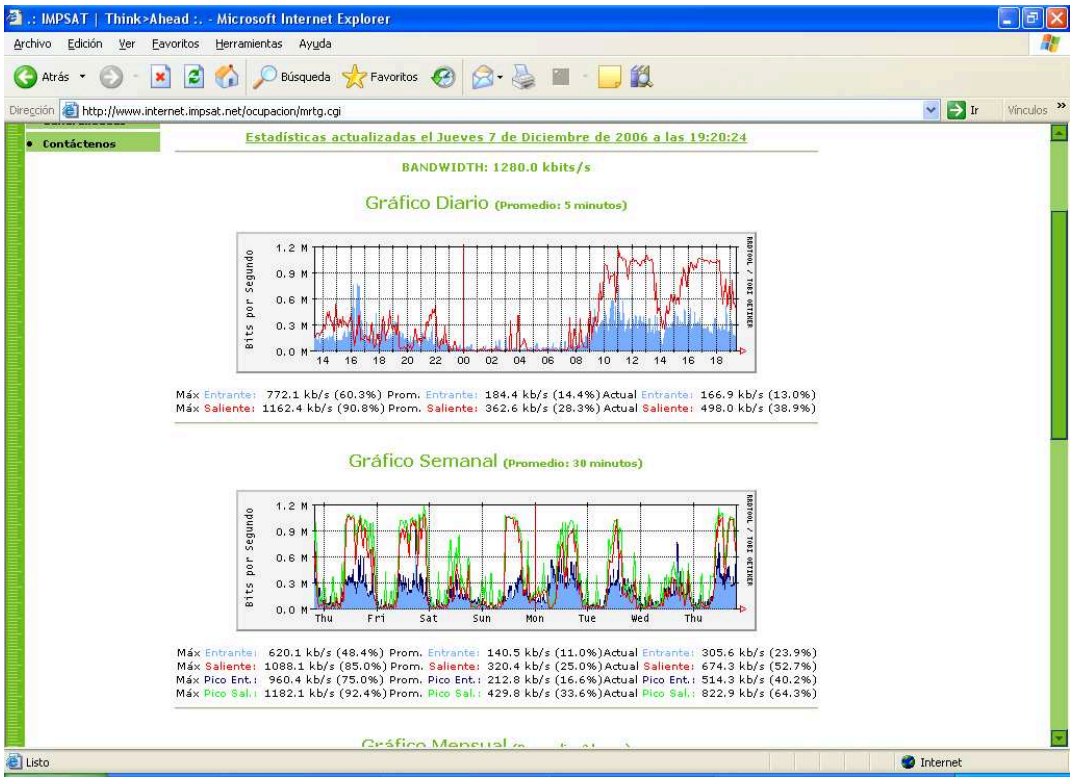


Reporte ejecutivo

De acuerdo a la figura que corresponde al informe ejecutivo, se observa que el uso del canal de acceso al Internet, el tráfico que se genera desde la red local hacia el Internet es muy bajo, el 84% del tráfico se encuentra entre el 0 y 70% de su capacidad; solamente el 7% esta entre el 80% y 100%.

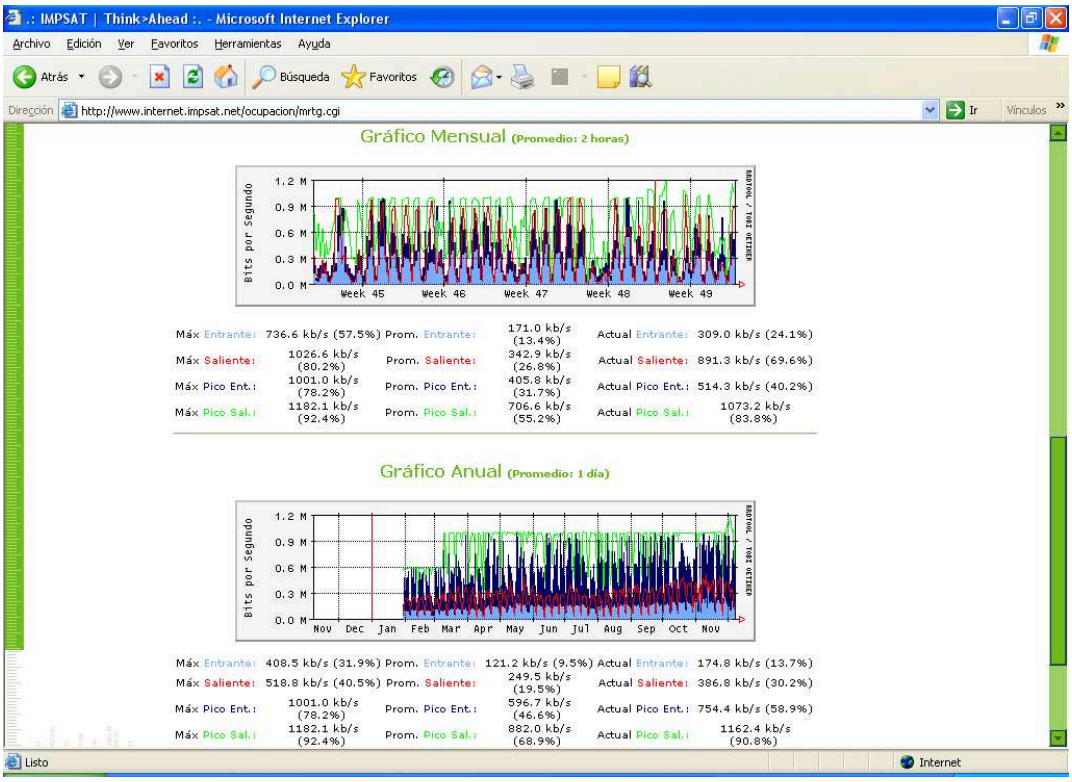
En lo que se refiere al tráfico generado desde el Internet hacia la red local de la institución, se observa que existe mucho tráfico por lo que se puede deducir que el canal se encuentra ocupado en toda su capacidad, el 85% del uso del canal se encuentra entre el 80 y 100%.

En las figuras siguientes se presenta la utilización del canal de acceso al Internet diario, semanal, mensual y anual.



De acuerdo al gráfico se observa que el canal no llega a saturarse en un 100%. Las horas picos son a las 10:00 a 13:00 y de 15:00 a 18:00 aproximadamente. Mantiene un uso constante del canal en especial el tráfico saliente de la red local hacia el Internet..

En los gráficos semanal, mensual y anual se observa que en ningún caso el canal llega a su tope. En las semanas anteriores se mantiene la constante de un uso del canal pero sin llegar al tope de los 1128 Mbps.



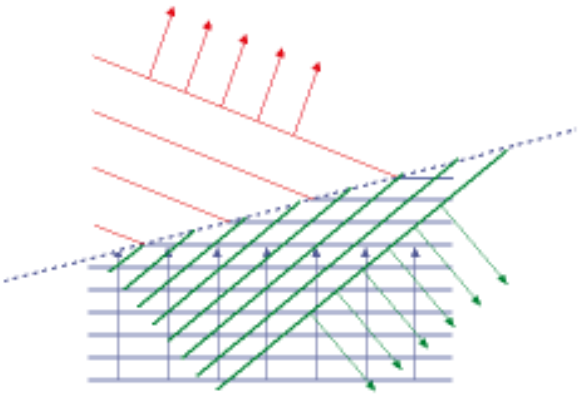
En el supuesto caso que no se incremente el numero de usuarios o de servicios que demanden el uso de Internet, se puede asumir que no es necesario en este momento la ampliación del canal; sin embargo, se debe pensar en incrementar el canal de acceso al Internet tomando en cuenta que en un poco tiempo se implementará el servicio de acceso inalámbrico al Internet en la institución.

ANEXO V

Reflexión, Refracción y Difracción

Cuando una onda llega a la superficie de separación de dos medios de distinta naturaleza se producen por lo general dos nuevas ondas, una que retrocede hacia el medio de partida (onda reflejada) y otra que atraviesa la superficie limite y se propaga o se transmite en el segundo medio (onda refractada o difractada).

La reflexión puede ser parcial o total. Además puede producirse con cambio de fase o no dependiendo de la rigidez de la superficie de separación.

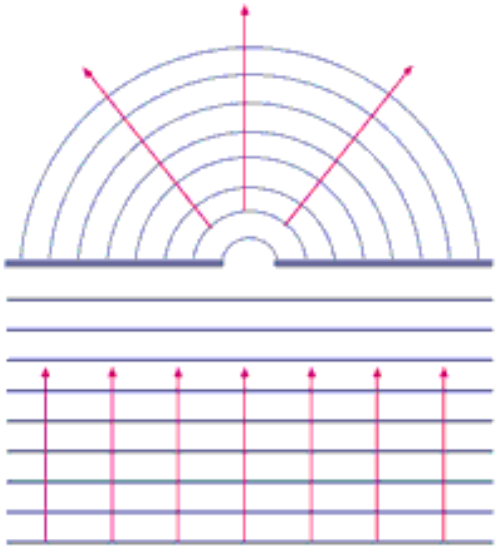


Una onda llega a una superficie de separación de dos medios una parte se refleja y otra se refracta.

Las ondas transmitidas pueden ser refractadas o difractadas:

Refracción: se da cuando la onda pasa de un medio a otro y se producen cambios en la velocidad y en la dirección de propagación.

Difracción: se produce cuando la onda "choca" contra un obstáculo o penetra por un agujero. La mayor difracción se produce cuando el tamaño del agujero o de los obstáculos son parecidos a la longitud de onda de la onda incidente.



Difracción de ondas