ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE UNA RED INALÁMBRICA PARA EL BLOQUE DE LA CARRERA DE ACTIVIDAD FÍSICA DEPORTES Y RECREACIÓN, UTILIZANDO 802.1X COMO MECANISMO DE CONTROL DE ACCESO.

HÉCTOR IVÁN ANANGANÓ LEIME

CRISTIAN FERNANDO ARCE VERA

SANGOLQUÍ – ECUADOR

2010

CERTIFICACIÓN POR PARTE DEL DIRECTOR Y CODIRECTOR DE LA ELABORACION DEL PROYECTO DE GRADO BAJO SU DIRECCION Y PIE DE FIRMAS.

_____	_____
ING. CARLOS ROMERO	ING. DARWIN AGUILAR
DIRECTOR	CODIRECTOR

RESUMEN

En el presente proyecto, se realiza un análisis de la situación actual en la que se encuentra la red de datos del bloque "CAFDER", mediante mediciones de tráfico antes de la instalación de la nueva red inalámbrica y posterior a la implementación de la misma. El diseño de la red inalámbrica se realizó con el software 3COM WIRELESS SWITCH MANAGER; haciendo uso de sus respectivos parámetros, por medio de los cuales se ubicaron los distintos puntos de red en los lugares específicos del edificio.

Dentro de la red de datos del bloque CAFDER; se implementó el cableado estructurado necesario además del servidor de autenticación "RADIUS", basado en la tecnología de acceso 802.1x, bajo la plataforma de "Linux FEDORA 12", junto con el servidor de base de datos "MySQL" y la interfaz web de control de cuentas de usuarios "DALORADIUS", esto con el fin de brindar los respectivos servicios y seguridades a la nueva red implementada. Por otra parte permitirá administrar los usuarios de manera eficiente y versátil, además de los puntos de acceso que contenga la red.

Para verificar el servicio en la nueva red inalámbrica, se realizaron las pruebas y análisis respectivos del correcto funcionamiento de la misma.

DEDICATORIA

Dedico este esfuerzo, esmero y dedicación el cual está plasmado en el siguiente proyecto primero a Dios, el cual ha sido mi salvavidas en mis momentos difíciles; luego a mis Padres, los cuales han sido la parte importante e indispensable en mi vida ya que a ellos debo mis triunfos y mis éxitos; a mis hermanos Ramiro y Felipito, los cuales han sido un ejemplo de perseverancia, constancia y mi inspiración constante para seguir adelante.

A esa persona importante la que siempre estuvo a mi lado en mis momentos de tristezas y alegrías; a mis amig@s, compañeros inseparables de amaneceres que sin ellos nada de esto hubiese sido llevadero.

HÉCTOR IVÁN

AGRADECIMIENTO

Agradezco a Dios por haberme dado la vida y unos Padres dedicados al bienestar tanto de mis hermanos como del mío, sin ellos este logro nunca hubiese sido posible, son lo más importante en mi vida además de ser la columna vertebral en mi familia; a mis hermanos Ramiro y Felipito los que han sido una inyección emocional, anímica constante en todo momento; son mi fuerza y mi aliento para seguir adelante.

Agradezco a esa personita importante la que siempre soportó todos mis momentos buenos y malos; a su vez supo entenderme, comprenderme y ayudarme; gracias por todo tu apoyo y tu amor constante.

Agradezco a mis amig@s; alguien dijo que los compañeros son muchos pero los amigos y los verdaderos son pocos; por eso gracias amig@s, confidentes, además de ser mi familia en esta etapa de mi vida.

HÉCTOR IVÁN

DEDICATORIA

A Dios, que ha sido mi fuente de ánimo espiritual durante toda mi vida en especial durante esta complicada trayectoria.

A mis padres y hermanos que han sido el muro de contención sobre el cual me he edificado, mi motivo principal de vida.

Al deporte más hermoso sobre la tierra, el básquet, sin él nada de esto se hubiese conseguido.

A todos mis amigos que considero, son una de las partes más importante de este gran logro.

CRISTIAN ARCE

AGRADECIMIENTO

Primero, un agradecimiento enorme a mi Dios que siempre está conmigo brindándome fuerzas y permitiéndome levantar cada vez que caigo, aquel que siempre ha estado y estará protegiéndome durante el resto de mis días de vida.

A mis padres, Alberto y Celinda, por estar siempre en las buenas y en las malas conmigo, brindándome su cariño y apoyo incondicional, a ellos que nunca me abandonaron y supieron darme valor para seguir de pie en la lucha.

A mis hermanos, Luis y Gabriela, sin ustedes nada tendría sentido, han sido mi fuente de inspiración y alegría durante toda mi vida, gracias a ustedes por su cariño, aprecio y apoyo para conseguir este gran logro.

A un balón, una cancha y un cesto, quienes me lo han dado todo, mis estudios, amigos, chicas, absolutamente todo.

A la Facultad de Ingeniería Electrónica y a todos sus maestros, por enseñarme a enfrentar al mundo tan competitivo de hoy, no los voy a olvidar.

Al Crnl. Leonardo Higaldo, por haberme dado la oportunidad de pertenecer a esta noble Institución, La ESPE. Al Crnl. Marcelo Montalvo, por haber sido parte importante en la elaboración de éste proyecto. A todos mis amigos que han sido las personas con quienes he compartido durante todos estos años de sacrificio, experiencias inolvidables, siempre serán mis amigos. Al CICTE y a todo su personal por permitirme aplicar los conocimientos obtenidos durante mi etapa estudiantil y por ser mi fuente de aprendizaje diario.

CRISTIAN ARCE

PRÓLOGO

Siendo la ESPE una Institución que promueve el desarrollo intelectual y tecnológico de toda su comunidad politécnica, el bloque CAFDER no podía quedar exento de este avance; razón por la cual se observó la necesidad de implementar una red de datos inalámbrica para que los estudiantes tenga facilidad de acceso a la misma.

Debido a la gran demanda de ingreso de alumnos al bloque CAFDER y su necesidad de acceder a servicios de datos (Internet) que dispone la ESPE se realizó el análisis de tecnologías para ofrecer este servicio, considerando la tecnología inalámbrica como la más adecuada para las condiciones que presenta el bloque.

En base al análisis de tecnología considerado anteriormente; el diseño de la red se basó en la ubicación de varios puntos de acceso, los mismos que dotarán de servicio y cobertura a los diferentes departamentos y aulas que forman parte del bloque. Para la implementación de la nueva red inalámbrica se utilizó el método de acceso 802.1x (Servidor RADIUS), el mismo que permite la autorización, autentificación y registro de cuentas de usuarios.

En la implementación del cableado estructurado del bloque, se consideró entre otros aspectos la ubicación física de cada punto de red diseñado, mismos que brindan cobertura óptima a cada uno de los usuarios en cada piso.

Para la validación de servicio de la nueva red inalámbrica; se realizó análisis de troughput, pérdida de tramas, análisis de retardo, congestión de tráfico; antes y después de la implementación de la nueva red inalámbrica.

INDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

GLOSARIO

AAA: Autorización, Autenticación y Registro de Cuentas

ADSL: Línea de Abonado Digital Asimétrica

ADSL2+: Línea de Abonado Digital Asimétrica con capacidad aumentada

AES-CCMP: Advanced Encryption Standard, esquema de cifrado por bloques

AP: Punto de Acceso

ARIB: Asociación de Industrias de Radio y Negocios

ARQ: Solicitud Automática de Transmisión

ATM: Modo de Transferencia Asíncrono

BER: Rata de errores de bit

BERT: bit error rate/tester (probador de BER).-Procedimiento de diagnóstico o equipo que examina la calidad de un circuito mediante la medición del grado en el cual los bits son recibidos con error.

BPSK: Modulación por Desplazamiento de Fase Binaria

BSS: Grupo de Estación de Servicio

BWA: Acceso inalámbrico de Banda Ancha

CA: Autorización de Certificación

CAFDER: Carrera de la Actividad Física, Deportes y Recreación

CCA: Análisis de Correlación Canónica

CCK: Modulación de código Complementario

CHAP: Protocolo de autenticación por desafío mutuo

CNT: Corporación Nacional de Telecomunicaciones

CPE: Equipos de las instalaciones del cliente

CPU: Unidad Central de Proceso

CRC: Código de Corrección de Errores

CSMA: Acceso Múltiple con escucha de Portadora

CSMA/CA: Acceso Múltiple con escucha de Portadora, con Prevención de colisión

CSMA/CD: Acceso Múltiple con escucha de Portadora, con detección de colisión

DB2: Servidor de Base de Datos

DES: Estándar de Encriptación de Datos

DFS: Selección de Dinámica de Frecuencia

DHCP: Protocolo de Configuración Dinámica de Máquinas

DMZ: Red Local Desmilitarizada

DS: Secuencia Directa

DSL: Línea de suscripción digital

DSSS: Espectro Ensanchado por Secuencia Directa

EAP: Protocolo de Autenticación Extensible

EAPOL: EAP sobre LAN

EAP-TLS: EAP con seguridad a nivel de Transporte

EAP-TTLS: El sistema de autenticación se basa en una identificación de un usuario y contraseña que se transmiten cifrados mediante TLS, para evitar su transmisión en texto limpio. Es decir se crea un túnel mediante TLS para transmitir el nombre de usuario y la contraseña.

ESS: Grupo de servicio extendido

ETSI: Instituto Europeo de Normas de Telecomunicaciones

FDD: Duplexación por División de Frecuencia

FHSS: Espectro Ensanchado por Salto de Frecuencia

FSK: Modulación por desplazamiento de frecuencia

G_{AT}: Ganancia de la antena Transmisora

G_{AR}: Ganancia de la antena Receptora

GHz: Giga hertzios

GSM: Sistema Global para las Comunicaciones Móviles

GPL: Licencia Pública General

GPRS: Servicio General de Paquetes vía Radio

GPS: Sistema de posicionamiento global

HISWAN: Red Local inalámbrica de alta Velocidad

HIPERLAN2: LAN de radio del alto rendimiento

HTTP: Protocolo de Transferencia de Hipertexto

IBM: International Business Machines

ICV: Valor de Chequeo de Integridad

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos

IP: Protocolo de Internet

IP DST: IP Destino

IPX: Intercambio de Paquetes interred

ISM: Bandas de Frecuencias, Industriales, Científicas y Médicas

ISP: Proveedor de Servicios de Internet

IV: Vector de Inicialización

LAN: Red de Area Local

LAT: Protocolos de servidores de terminales

LDAP: Protocolo Ligero de Acceso a Directorios

LEAP: Protocolo ligero de autenticación extensible

Lo: Pérdidas en el Espacio Libre

LoS: Con Línea de Vista

L_T: Pérdida total

MAC: Control de Acceso al Medio

MAN: Red de área Metropolitana

MAPs: Puntos de Acceso Administrados

MBPS: Megabits por segundo

MD5: Algoritmo de Resumen del Mensaje 5

MHz: Mega hertzios

MPEG: Estándar de compresión y formato de archivos de video digital

MS-CHAP: Variante de CHAP creada por Microsoft

MTT: Caja de herramientas modular de pruebas

MySQL: Sistema de gestión de base de datos relacional, multihilo y multiusuario

NAS: Servidor de Acceso a la Red

NAT: Traducción de Dirección de Red

NAV: Vector de asignación de Red

NIC: Tarjeta de Interfaz de Red

NLOS: Sin Línea de Vista

NOC: Orientado a No Conexión

ODBC: Base de Datos con conectividad Abierta

OFDM: Multiplexación por División de Frecuencia Ortogonal

ORACLE: Es un sistema de gestión de base de datos relacional

OSI: Modelo de referencia de Interconexión de Sistemas Abiertos

PAN: Red inalámbrica de área personal

PAP: Protocolo de Autenticación de Contraseña

PCMCIA: Personal Computer Memory Card International Association

PDA: Asistente Digital Personal

PHP: Preprocesador de Hipertexto

PoE: Alimentación a través de Ethernet

PPP: Protocolo Punto a Punto

P_R: Potencia de Recepción.

P_T: Potencia de Transmisión.

QAM: Modulación de amplitud en cuadratura

QoS: Calidad de Servicio

QPSK: Modulación por Corrimiento de Fase en Cuadratura

RC4: Sistema de cifrado de flujo

RF: Radio Frecuencia

RFC: Request For Comment

RPM: Red Hat Package Manager

RSA: (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública

RSSI: Indicador de fuerza de señal de recepción

RTS: Respuesta al envío

RX: Rayos X

Rx: Recepción

SPEKE: Contraseña simple autenticado exponencial de intercambio de claves

SPI: Interfaz Periférica Serial

SQL: Lenguaje de Consulta Estructurado

SSID: Es un nombre incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos

ST: Set and Twist

TCP: Protocolo de Control de Transmisión

TDD: Duplexación por División de Tiempo

TDM: Multiplexación por División de Tiempo

TDMA: Acceso Múltiple por División de Tiempo

TKIP: Protocolo de Integridad de Clave Temporal

Tx: Transmisión

UMTS: Sistema Universal de Telecomunicaciones Móviles

UNIX: Sistema operativo portable, multitarea y multiusuario

USB: Bus Universal en Serie

UTICS: Unidad de Tecnologías de Información y Comunicación

UTP: Par trenzado no apantallado

VBR: Rata de bits de video

VLAN: Red de área Local Virtual

VoIP: Voz sobre IP

WEB: Red Global Mundial

WECA: Alianza de Compatibilidad Ethernet Inalámbrica

WEP: Privacidad equivalente a Cableado

WEP2: Privacidad equivalente a Cableado con mayor número de bits de cifrado (128bits)

WG: Grupo de Trabajo

WIFI: Wireless Fidelity

WIMAX: Interoperabilidad mundial para acceso por microondas

WLAN: Red de área Local inalámbrica

WPA: Acceso Protegido WI-FI

WPA2: Acceso Protegido WI-FI mejorado

XOR: Función OR exclusiva

2G: Segunda generación

CAPÍTULO I

MARCO TEÓRICO

1.1 REDES DE AREA LOCAL

Las redes en general, son creadas para "compartir recursos" y algunos de sus objetivos más importantes son:

- *Hacer que todos los programas, datos y equipos estén disponibles para cualquier usuario de la red* que así lo solicite, sin importar la localización física del recurso o del usuario. En otras palabras, el hecho de que el usuario se encuentre a una determinada distancia (sea esta distante o corta) de la red de datos, no debe evitar que éste pueda utilizar la información como si fueran originados localmente.

- *Brindar un alto grado de fiabilidad*, al contar con fuentes alternativas de suministro. Un ejemplo de esto se da cuando los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, en este caso se podría utilizar una de las otras copias; además la presencia de múltiples CPU's significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque esto provocaría que el rendimiento global disminuya.

- *Ahorro económico*. Las computadoras pequeñas brindan una mejor relación costo/rendimiento, comparada con la ofrecida por las máquinas grandes. Esto es, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es mayor. Este desequilibrio ha ocasionado que muchos diseñadores de

sistemas construyan sistemas constituidos por poderosos computadores personales, uno por cada usuario, con los datos guardados en una o más máquinas que funcionan como servidor de archivo compartido.

- *Capacidad de crecimiento/rendimiento de la red*; un punto muy importante a tener en cuenta en el diseño de una red, es la capacidad para aumentar el rendimiento del sistema en forma gradual a medida que crece la misma (usuarios y servicios), esto es añadiendo más procesadores. Con máquinas grandes, si el sistema se satura; deberá reemplazarse con uno más grande, operación que por lo normal genera un gran gasto y una perturbación inclusive mayor al trabajo de los usuarios.

Las redes de área local (LAN)[1] llevan mensajes a velocidades relativamente altas entre computadoras conectadas a un único medio de comunicación, que puede ser un cable de par trenzado, cable coaxial o una fibra óptica. Un segmento es una sección de cable que da servicio y que puede tener varias computadoras conectadas, el ancho de banda del mismo se reparte entre dichas computadoras.

Las redes de área local mayores están compuestas por varios segmentos interconectados por conmutadores (*Switch*) o concentradores (*Hubs*). El ancho de banda total del sistema es grande y la latencia pequeña, salvo cuando el tráfico es muy alto.

Desde los años 70s se han desarrollado varias tecnologías de redes de área local, destacándose *Ethernet* [2] como tecnología dominante para las redes de área amplia; estando esta carente de garantías necesarias sobre latencia y ancho de banda necesario para la aplicación multimedia. Como consecuencia de esta surge la tecnología ATM[3] para cubrir estas falencias, sin embargo, el costo de la misma impide su implementación en redes de área local.

En su lugar se implementan las redes Ethernet de alta velocidad que resuelven estas limitaciones, no superando la eficiencia de ATM. Aunque aparece desde 1983 la LAN ha continuado evolucionando hasta llegar a ser una parte integral de la conectividad de las computadoras. El proceso de incorporar una computadora a una LAN consiste en la instalación de una tarjeta de interfaz de red (NIC) en cada computadora. Las NIC de cada

[1] *Local Area Network*
[2] Estándar de redes de computadoras de área local
[3] Modo de transferencia Asíncrona tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones

computadora se conectan con un cable especial para red o aparatos receptor/emisor (módem). Por último la instalación de un *software* conocido como Sistema Operativo de Red.

1.2 REDES WLAN

1.2.1 INTRODUCCIÓN A LAS REDES WLAN

En los últimos años las redes de área local inalámbricas (WLAN)[4] están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar.

Con las WLANs, la red por sí misma es móvil, elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red; y lo más importante, incrementa la productividad y eficiencia en las empresas donde está instalada.

Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e incluso sobre áreas metropolitanas a velocidades de 11 Mbps o superiores. Pero no solamente encuentran aplicación en las empresas, si no que su extensión se ha hecho visible a ambientes públicos, en áreas metropolitanas como medio de acceso a Internet o para cubrir zonas de alta densidad de usuarios.

Muchos de los fabricantes de ordenadores y equipos de comunicaciones como los PDAs[5], módems, terminales de punto de venta y otros dispositivos están introduciendo aplicaciones soportadas en las comunicaciones inalámbricas.

Las nuevas posibilidades que ofrecen las WLANs son:

- Permitir una fácil incorporación de nuevos usuarios a la red
- Ofrecer una alternativa de bajo costo a los sistemas cableados
- Posibilidad para acceder a cualquier base de datos o cualquier aplicación localizada dentro de la red.

[4] *Wireless Local Area Network*
[5] *Personal Digital Assistants*

Al igual que las redes tradicionales cableadas, las redes inalámbricas se clasifican en tres categorías, que son: como se muestra en la figura 1.1:

- WAN/MAN[6]
- LAN
- PAN[7]

La Figura 1.1, muestra la clasificación de las redes inalámbricas.

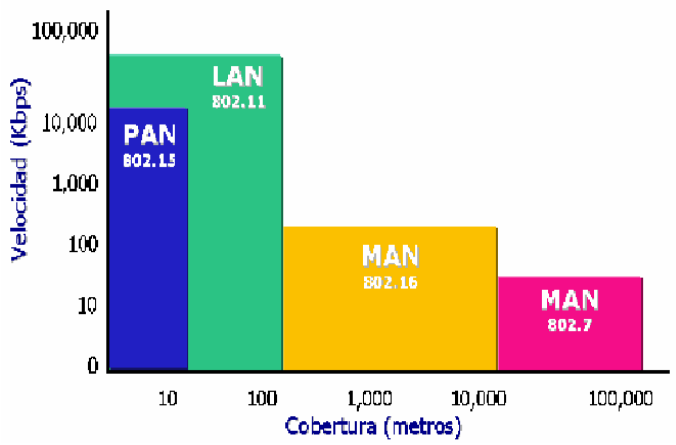


Figura. 1.1. Comparación de velocidades de transmisión entre los diferentes tipos de redes[8]

Figura. 1.2 Clasificación de las redes inalámbricas[9]

[6] *Wide Area Network/Metropolitan Area Network*
[7] *Personal Area Network*
[8] Ponce, Enrique, Redes Inalámbricas: IEEE 802.11, http://www.canal-ayuda.org/a-informatica/inalambrica.htm, Noviembre 2009
[9] Ponce, Enrique, Redes Inalámbricas: IEEE 802.11, http://www.canal-ayuda.org/a-informatica/inalambrica.htm, Noviembre 2009

- **Redes WAN/MAN**

En esta clasificación se encuentran las redes que cubren desde decenas hasta miles de kilómetros, cuya finalidad es la constitución de redes globales de comunicación móvil. Como ejemplo de estas redes se encuentran los siguientes sistemas:

- **GSM[10]:** Sistema global de comunicaciones móviles de 2ª generación (2G) que permite comunicaciones de hasta 9,6 Kbps.
- **GPRS[11]:** Estándar de comunicaciones móviles que permite velocidades de hasta 115 Kbps.
- **UMTS:** [12]Tecnología de comunicaciones móviles de 3º generación (3G) que ofrece velocidades desde 144 Kbps hasta 2 Mbps

- **Redes LAN**

En la segunda categoría LAN, pondremos las redes que comprenden de varios metros hasta decenas de metros. Permiten la creación de redes locales sin cables, realizando la comunicación por ondas de radio. La tecnología más conocida es el estándar 802.11[13] (o WiFi) que opera dentro de los 2.4 GHz (5 GHz 802.11a) y provee un ancho de banda de hasta 54 Mbps.

La norma *IEEE 802.11* estableció en junio de 1997 el estándar para redes inalámbricas, siendo su finalización definitiva para la introducción y desarrollo de los sistemas WLAN en el mercado[14]. Una red de área local inalámbrica puede definirse como una red de alcance local que tiene como medio de transmisión el aire.

El estándar 802.11 es muy similar al 802.3[15] (Ethernet) con la diferencia que tiene que adaptar todos sus métodos a un medio no guiado de transmisión. En este estándar se encuentran las especificaciones tanto físicas como a nivel de enlace MAC.

[11] *General Packet Radio Service*
[12] *Universal Mobile Telecommunications System*
[13] "Estándar que define el uso de los dos niveles inferiores de la arquitectura OSI (capas fisica y de enlace de datos)"
[14] IEEE 802.11, http://es.wikipedia.org/wiki/IEEE_802.11, Noviembre 2009.
[15] Estándar que define las redes con tecnología Ethernet

Por otro lado el foro global HiperLAN2[16] definió una especificación que opera en la banda de 5 GHz y que permite la transferencia de datos de hasta 54 Mbps que utiliza una técnica de modulación conocida como OFDM[17] para transmitir señales analógicas. *OFDM* es muy eficiente en ambientes dispersos en el tiempo, como oficinas, donde las señales de radio son reflejadas desde muchos puntos antes de que llegue al receptor. Debido a que HiperLAN es orientado a conexión posee características de Calidad de Servicio (QoS). El soporte de QoS en combinación con las altas velocidades de HiperLAN facilita la transmisión de diferentes tipos de ráfagas de datos como vídeo, voz y datos.

Tabla. 1.1. Cuadro comparativo de tecnologías WLAN

CARACTERISTICA	802.11	802.11b	802.11a	802.11g	HiperLAN2
ESPECTRO	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz	5 GHz
MAX. TASA DE TRANSMISION	2 Mbps	11 Mbps	54 Mbps	54 Mbps	54 Mbps
CONEXIÓN	NOC	NOC	NOC	NOC	NOC
ENCRIPTACIÓN	RC 4 de 40 bits	RC 4 de 40 bits	RC 4 de 40 bits		DES, 3DES
MULTICAST	Si	Si	Si	Si	Si
SOPORTE DE REDES FIJAS	Ethernet	Ethernet	Ethernet	Ethernet	Ethernet, IP, ATM, UMTS, FIREWIRE, PPP
SELECCIÓN DE FRECUENCIAS	FHSS o DSSS	DSSS	OFDM portadora única	DSSS y OFDM	Portadora única con selección dinámica de frecuencias

[16] "Estándar global para anchos de banda inalámbricos LAN que operan con un rango de datos de 54Mbps en la frecuencia de banda de 5GHz"

[17] *Orthogonal Frequency Digital Multiplexing*

FHSS: *Frequency Hopping Spread Spectrum*

DSSS: *Direct Sequence Spread Spectrum*

ATM: *Asynchronous Transfer Mode*

OFDM: *Orthogonal Frequency Division Multiplexing*

IP: *Internet Protocol*

DES: *Data Encryption Standard*

UMTS: *Universal Mobile Telephone Service*

PPP: *Point - Point Protocol*

- ***REDES PAN***

Por último, en la categoría PAN se encuentran las redes que comprenden desde muy poca distancia hasta 30 metros. Se trata de redes personales que tienen como principal fin eliminar los cables de comunicación con todos los dispositivos electrónicos (PC con periféricos o accesorios, teléfonos móviles, cámaras etc). Su principal exponente es la tecnología *Bluetooth*[18].

Bluetooth es una tecnología inalámbrica europea que permite la inter-conectividad de dispositivos inalámbricos con otras redes e Internet. *Bluetooth* trabaja en la banda de frecuencias de espectro extendido de 2.4 GHz. *Bluetooth* es capaz de transferir información entre un dispositivo a otro a velocidades de hasta 1 Mbps, permitiendo el intercambio de vídeo, voz y datos de manera inalámbrica.

El Estándar IEEE 802.15 se enfoca básicamente en el desarrollo de estándares para redes tipo PAN o redes inalámbricas de corta distancia. Al igual que *Bluetooth*, el 802.15 permite que dispositivos inalámbricos portátiles como PCs, PDAs y teléfonos, entre otros, puedan comunicarse e interoperar uno con el otro.

Así mismo se puede destacar la diferencia de velocidades de transmisión, respecto a las distancias de alcance entre las tres principales tecnologías: 802.11a, 802.11b y 802.11g, esto se puede verificar en la Figura 1.3.

[18] Especificación industrial para Redes Inalámbricas de Área Personal (WPANs)

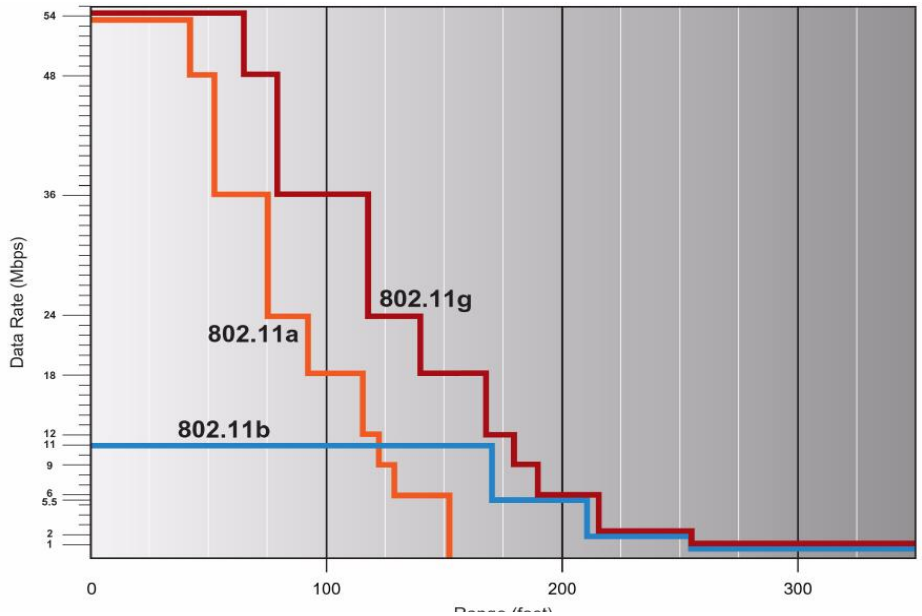


Figura. 1.3. Velocidad de transmisión respecto a la distancia[19]

1.2.1 Evolución histórica de las WLAN

La tecnología de las redes inalámbricas no es precisamente nueva, ha sido utilizada tanto en la industria como en centros de investigación desde hace más de 15 años.

El origen de las LAN inalámbricas se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica.

En mayo de 1985, y tras cuatro años de estudios, el FCC[20], la Agencia Federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas ISM (*Industrial, Scientific and Medical*) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en *spread spectrum*. ISM es una banda para uso comercial sin licencia.

[19] Gokul,Rajagopalan, 802.11n Client Throughput Performance, http://www.arubanetworks.com/pdf/technology/TB_11NPERF.pdf, Noviembre 2009
[20] *Federal Communications Commission*

- **1997.- Aparece 802.11, primer estándar mundial de redes inalámbricas**

Refiriéndonos al pasado más reciente, es concretamente en Junio de 1.997 cuando el IEEE (*Institute of Electrical and Electronics Engineers*) ratifica el estándar 802.11 como el primer estándar mundial WLAN (redes locales inalámbricas). Esa primera versión proporcionaba velocidades de 1 y 2 Mbps en las frecuencias de 2,4 GHz., así como un conjunto de métodos de señalización y otros servicios de red.

En estos primeros momentos y tras el desarrollo del primer estándar, la demanda seguía en niveles muy bajos. La limitada capacidad de estas primeras WLAN estandarizadas era muy baja y no podía satisfacer las necesidades de la mayoría de las empresas.

- **1999.-Aparece 802.11b – Wi-Fi se adopta como sello distintivo**

Consciente de la necesidad de conseguir mayores velocidades de transmisión de datos, IEEE ratificó en 1.999 el estándar 802.11b, también conocido como 802.11 High Rate, que opera a velocidades de hasta 11 Mbps. Este estándar dispone de un nuevo método de selección de frecuencias por secuencia directa (DS).

En Agosto de 1.999 los principales promotores de la tecnología DS formaron WECA[21], encargada de certificar la interoperatividad de productos IEEE 802.11b. Al mes siguiente la WECA adopta Wi-Fi (Wireless Fidelity) como sello distintivo. Wi-Fi es el certificado de interoperatividad que aparece como logotipo en los productos comprobados. Posteriormente se agregaron las letras a, b, g para especificar cuál de los estándares se cumple.

Figura. 1.4. Logotipo de certificación Wi-Fi

[21] *Wireless Ethernet Compatibility Alliance*

- **1999. Tras 802.11b, aparece 802.11ª**

Además del estándar 802.11b, en 1.999 se aprueba el 802.11ª. Este estándar opera en la frecuencia de 5 GHz y alcanza una velocidad máxima de 54 Mbps. La técnica de modulación de radio que utiliza 802.11ª es la clave de sus mayores velocidades y eficiencia en la prestación. Sin embargo, la frecuencia de 5 GHz tan sólo alcanza una distancia de 30 m, frente a los 100 m de la frecuencia de 2.4 GHz.

Otro inconveniente es la presencia de interferencias, sobre todo en EE.UU., ya que los sistemas militares de defensa ocupan esta misma frecuencia y saturan el espectro. A pesar de estos problemas, el llamado Wi-Fi5 (802.11ª) se impuso en su día al 802.11b en EE.UU.

- **Año 2002. 802.11 g**

Con la aprobación de la nueva versión 802.11g se ha conseguido que el actual índice de transmisión de datos de 11 Mbps empleado por la versión b, pase a ser de 54 Mbps, lo que permitirá dar servicio a 4 ó 5 veces más de usuarios, y extender el uso de las redes 802.11 a servicios bastante demandados como la transmisión inalámbrica de vídeo-multimedia y la difusión de MPEG.

Las unidades 802.11g podrán trabajar también a velocidades de 11 Mbps, de modo que los dispositivos 802.11b y 802.11g puedan coexistir bajo la misma red. Los dos estándares aplicarán la banda de frecuencia de 2.4 GHz.

- **802.11n Lo nuevo en tecnología Wi-Fi**

La tecnología 802.11n para Redes Inalámbricas WIFI, suministra velocidades superiores a 100 Mbps lo cual duplica la velocidad de 802.11g y 802.11ª, que es de 54 Mbps.

802.11n necesita ser capaz de usar el canal con 20Mhz de ancho, el mismo que 802.11b y 802.11g, a fin de que no siga los pasos del 802.11a, que se despoja de compatibilidad con estándares anteriores a cambio de velocidades mayores, pero la compatibilidad con 802.11b de 802.11g le dio el triunfo frente a 802.11a.

802.11n fue aprobada en septiembre del 2009, los estudios de este proyecto duraron 7 años; debido a la incompatibilidad que existía con las versiones anteriores de 802.11 tales como la 802.11a y la 802.11g. Con esta nueva tecnología podrían alcanzarse velocidades de hasta 300 Mbps o incluso más.

Otros estándares

- **802.11 c:** Define características de Punto de Acceso (*Access Point*) como puentes (*bridges*).
- **802.11 d**: (Múltiples dominios reguladores), permite el uso de 802.11 en países restringidos por el uso de frecuencias.
- **802.11 e**: Define el uso de Calidad de Servicio QoS (*Quality of Service*).
- **802.11 f:** Define el enlace entre estaciones y Puntos de Acceso en modo viajero (*roaming*).
- **802.11 h**: DFS (*Dynamic Frequency Selection*), permite la asignación dinámica de canales, habilita la coexistencia con HyperLAN, y regula la potencia de difusión en función de la distancia.
- **802.11 i**: (Seguridad). Estándar que define el cifrado y la autenticación para complementar, completar, y mejorar WEP[22]. Es un estándar que mejora la seguridad de las comunicaciones mediante el uso de WPA[23] con su técnica llamada *Temporal Key Integrity Protocol* (TKIP), aplicable a redes 802.11 a, 802.11 b, y 802.11 g.
- **802.11 j:** Permitirá la armonización entre IEEE 802.11, ETSI[24], HyperLAN2, ARIB[25] y HISWAN[26].

[22] *Wired Equivalent Privacy*
[23] *Wifi Protect Access*: Mecanismo de control de acceso a una red inalámbrica
[24] *European Telecommunications Standards Institute*
[25] *Association of Radio Industries and Businesses*
[26] *High-Speed Wireless Local Area Network*

- **802.11 k**: En proceso. Proporciona información como: *roaming*, conocimiento del canal RF, nodos ocultos, estadísticas de clientes, y transmisiones de control de energía, para hacer las redes inalámbricas más eficientes.

- **802.11 l**: Saltado porque asimila el 802.11 i.

- **802.11 m**: Trabajo en proceso, propuesto para mantenimiento de redes inalámbricas.

- **802.11 o**: Trabajo en proceso. Exclusivo para voz en redes inalámbricas. Un cambio de código "*handoff*" rápido, da la prioridad a tráfico de voz sobre datos.

- **802.11 p**: Trabajo en proceso, usa la banda de 5.9 GHz para largo alcance.

- **802.11 q**: Trabajo en proceso. Ayuda para la VLAN[27] (Virtual LAN).

- **802.11 r**: Trabajo en proceso. R de *roaming*, manejando un cambio de código "*handoff*" rápido cuando hay un viajero "*roaming*" entre Puntos de Acceso.

- **802.11 s**: Trabajo en proceso. Redes de auto ayuda y auto configuración.

- **802.11 w**: Mejoras a 802.11 i.

- **802.11 x**: Se utiliza para resumir todos los estándares dentro del grupo de funcionamiento pero no es un estándar.

- **WiMax (*Worldwide Interoperability for Microwave Access*)**

  Desde que entramos en el nuevo milenio, las redes inalámbricas no han hecho más que proliferar WiFi, el estándar creado por la IEEE, ha permitido a los usuarios moverse alrededor de muchos sitios sin necesidad de que los dispositivos portátiles o PDA tengan cables. Ahora es el turno de WiMax, que promete ampliar la banda ancha inalámbrica reduciendo costos.

  Contrariamente al acceso inalámbrico Wi-Fi, que sólo permite la conexión con la Web dentro de zonas muy restringidas, las estaciones base de Wi-MAX podrían extender el espectro de conectividad a 50 kilómetros, lo que supone un gran avance en comparación con los 91 metros de Wi-Fi, y ni qué decir sobre los 9 metros de Bluetooth.

[27] *Virtual LAN* (Red de área local virtual) es un método de crear redes lógicamente independientes dentro de una misma red física.

La mayor distancia de cobertura es clave para permitir que los proveedores de servicios sean capaces de ofrecer acceso a Internet de banda ancha directamente a los hogares, sin tener que tender un cable físico hasta el final; lo que se conoce como la "última milla", que conecta a cada uno de los hogares con la red principal de cada proveedor.

Por este motivo, Wi-MAX está considerada como una alternativa más barata a las líneas de suscripción digital y a los accesos de cable de banda ancha, ya que los costos de instalación de una infraestructura inalámbrica son mínimos si se comparan con las versiones cableadas. Wi-Max (que opera en la frecuencia de 10 a 66 GHz), es un reemplazo inalámbrico para la conexión de cableado de banda ancha, particularmente en zonas rurales gracias a su rápido despliegue con estaciones base de muy amplia cobertura. Además, puede transmitir y recibir datos a 70 Mbps, 35 veces la velocidad de ADSL[28] típica, o 3,5 veces la velocidad de ADSL2+, y por un precio equiparable a ésta.

1.3 CARACTERÍSTICAS DE LAS WLAN

Las redes locales inalámbricas más que una sustitución de las LANs convencionales son una extensión de las mismas, ya que permite el intercambio de información entre los distintos medios en una forma transparente al usuario, minimizando la necesidad de establecer una conexión física cableada y ofreciendo al usuario conexión de datos de banda ancha y movilidad.

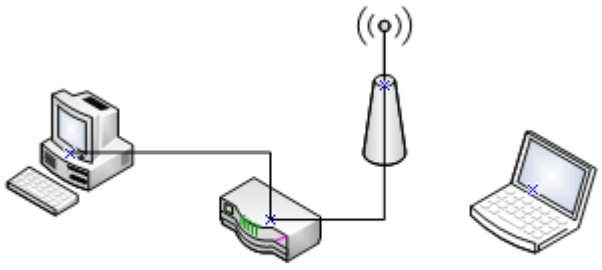


Figura. 1.5. Ejemplo de red inalámbrica sencilla[29]

[28] Línea de Abonado Asimétrica Digital
[29] Autor: Arce, Cristian, Diciembre 2009

En este sentido, el objetivo fundamental de las redes WLAN es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde coexistan los dos tipos de sistemas, enlazando los diferentes equipos o terminales móviles asociados a la red. Este hecho proporciona al usuario una gran movilidad sin perder conectividad.

El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado. Las redes inalámbricas son la alternativa ideal para hacer llegar una red tradicional a lugares donde el cableado no lo permite. En general las WLAN se utilizarán como complemento de las redes fijas.

1.3.1 Ámbito de aplicación

Entre los diferentes campos de aplicación tenemos:

- *Entornos difíciles de cablear*: Implementación de redes de área local en edificios históricos, de difícil acceso y en general en entornos donde la solución cableada no es viable
- *Configuración de topología*: Posibilidad de reconfiguración de la topología de la red sin añadir costes adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.
- *Redes locales* para situaciones de emergencia o congestión de la red cableada.
- *Varios entornos*: Entornos en los que se debe permitir el acceso a la información mientras el usuario se encuentra en movimiento y en tiempo real. Por ejemplo en hospitales, fábricas, almacenes, entre otros.
- *Generación de grupos de trabajo eventuales y reuniones ad-hoc*[30]: En estos casos no valdría la pena instalar una red cableada. Con la solución inalámbrica es viable implementar una red de área local aunque sea para un plazo corto de tiempo (exposiciones, acontecimientos deportivos, zonas catastróficas, etc.).
- *Entornos industriales*: En ambientes industriales con severas condiciones ambientales este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.
- *Interconexión de redes LAN*: Interconexión de redes de área local que se encuentran en lugares físicos distintos. Por ejemplo, se puede utilizar una red de área local

[30] Es una red inalámbrica descentralizada

inalámbrica para interconectar dos o más redes cableadas de área local situadas en dos edificios distintos.

- *Zonas IP*: Actualmente se están desplegando las denominadas Zonas IP, que son lugares públicos donde las WLAN ofrecen conexión a Internet: aeropuertos, estaciones de ferrocarril, auditorios de congresos, hoteles y otros lugares públicos.

1.3.2 Ventaja sobre las LAN cableadas

Enumeramos algunas de las ventajas que supone la utilización de redes inalámbricas:

- **Facilidad de instalación**

  Basta un dispositivo, un portátil o una agenda personal, equipado con tarjeta inalámbrica PCMCIA y un nodo de acceso de red para acceder al servicio de las redes cableadas LAN. Además las redes inalámbricas se han simplificado en los últimos tiempos tanto en lo referente a la configuración como al uso.

- **Movilidad**

  Sin cables, esta es la ventaja más clara. Además su reducida cobertura puede ampliarse a través de antenas hasta 50 Kilómetros o más. La movilidad se está extendiendo ahora a los TabletPC y a las computadoras PDA, o tipo agenda. Los usuarios tienen acceso a los datos en cualquier lugar y en cualquier momento lo que proporciona un aumento potencial de productividad y servicio sobre las LAN tradicionales.

- **Superior ancho de banda**

  El estándar 802.11b permite velocidades de 11 Mbps. Este hecho ha provocado que ISP's[31] de varios países comercialicen conexiones a Internet a través de este medio. Otros estándares de la misma familia, el 802.11a y el 802.11g alcanzan transferencias de 54 Mbps.

[31] Proveedores de Servicios de Internet

- **Libre utilización de la frecuencia de 2.4 Ghz**

Esta frecuencia, utilizada por el estándar 802.11 b, es de uso libre en Ecuador. Cualquiera puede crear su propia red sin necesidad de solicitar licencia alguna, tan sólo es necesaria una autorización C de la CNT[32] para proveer de servicios de Internet a través de WI-FI. Sin embargo en otros países europeos existen numerosas restricciones para la ocupación del espacio radioeléctrico.

- **Reducción de costos**

Evita el tendido de cables y costosas instalaciones; además los proveedores WI-FI pueden ofrecer acceso de banda ancha a un precio muy inferior al del acceso tradicional. Si se compara con el coste de implantación de UMTS, la ventaja competitiva de Wi-Fi resulta inmensa.

- **Velocidad simétrica**

A diferencia del ADSL, WI-FI es bidireccional, pudiendo recibir y enviar datos a la misma velocidad. Es por tanto útil para prestar una gran variedad de servicios que requieren idéntico ancho de banda para recepción y para envío de datos.

- **Complemento perfecto de redes tradicionales con cableado**

Con la colocación de puntos de acceso conectados a la red corporativa, cualquier empleado situado en el radio de acción (en un edificio más que suficiente) tiene acceso desde su portátil a los datos de la empresa sin necesidad de estar ligado a una conexión fija. Con ello se consigue la movilidad dentro de la oficina, lo que ahora mismo se considera fundamental en las empresas.

- **Cobertura en zonas sin infraestructuras de telecomunicaciones**

Wi-Fi posibilita el acceso a Internet de banda ancha a explotaciones, núcleos rurales, empresas o lugares que hasta la fecha por distintas razones han quedado al margen del despliegue de otras infraestructuras de telecomunicaciones (ADSL, Cable o incluso línea telefónica).

[32] Corporación Nacional de Telecomunicaciones

- **Funcionamiento sin errores**

En 802.11b y 802.11g, los dispositivos se comunican siempre a la mayor velocidad soportada que sea posible. Si la intensidad de la señal o las interferencias están degradando los datos, los dispositivos cambiarán su velocidad, disminuyendo a valores más bajos que no provoquen errores. Aunque esto pueda significar una reducción de la velocidad permite que la red siga funcionando.

- **Escalabilidad**

Puede aumentarse sin límite y de forma paulatina la cobertura de la red y su capacidad de transmisión

1.3.3 Inconvenientes

Entre los inconvenientes, se pueden destacar los siguientes:

- **Alcance limitado**

Las áreas que WI-FI puede cubrir en edificios pueden llegar a distancias comprendidas entre los 75 y 120 metros. Los forjados de los edificios representan un problema importante para la transmisión a través de WI-FI. En áreas abiertas el alcance puede llegar a 300 metros. Esta carencia en la cobertura puede paliarse mediante la interconexión a través de antenas.

- **Seguridad**

Sin duda su punto más débil. En primera instancia son inseguras en sí mismas dado que el medio de transporte es el aire. Además el sistema de cifrado que se utiliza en redes inalámbricas (cifrado WEP) está basado en algoritmos de cifrado de 40 bits. Actualmente están desarrollados sistemas de cifrado de 128 bits propios de las redes con hilos (WEP2). Existen otros sistemas de cifrado más seguros, aunque todavía no están suficientemente extendidos, ya sea por desconocimiento, como por incompatibilidad de dispositivos que no los soportan.

Por otra parte, muchos usuarios (tanto particulares como empresariales) están acostumbrados a su utilización sin sistema de seguridad alguno, lo que puede ocasionar

graves problemas, especialmente patentes en las intrusiones en intranets. Para llevar a cabo el ataque, tan sólo se necesitaría una pequeña antena.

- **Ancho de banda compartido**

Los usuarios conectados a través de un mismo punto, comparten el ancho de banda, por lo cual la velocidad teórica comentada, puede reducirse de forma considerable si no se ha realizado un correcto dimensionado de las conexiones. La velocidad obtenida está por tanto supeditada al número de usuarios conectados.

- **Posibles interferencias**

Wi-Fi en las versiones más extendidas (802.11b y 802.11g) trabaja en la frecuencia de 2.4 Ghz. Casi todos los productos WI-FI mencionan las posibles interferencias en el ámbito doméstico con los populares microondas, sin embargo en múltiples experimentos se ha comprobado que las interferencias con tales aparatos no se manifiestan.

Otro posible punto de interferencia podría surgir con los dispositivos conforme a otros estándares como Bluetooth, que operan en la misma frecuencia, aunque los respectivos consorcios de normalización aspiran a solucionar estos problemas.

- **Posibles repercusiones sobre la salud**

No existen conclusiones claras al respecto por la frecuencia utilizada, se dice que el uso de la banda de 2.4 GHz., podría tener consecuencias de calentamiento (similar a los microondas). Pero la potencia de emisión es considerablemente inferior a la de sistemas como el de la telefonía móvil. Mientras una tarjeta inalámbrica emite radiaciones de 30 milivatios de potencia, los móviles alcanzan radiaciones 20 veces superiores[33].

- **Confusión debida a la multiplicidad de estándares**

Si bien el futuro de WI-FI es muy prometedor, todavía no está disponible un chipset (conjunto de chips que realizan todas las funciones básicas de cualquier placa

[33] *The Guardian, Posibles efectos negativos de las redes WiFi sobre la salud, http://kernel666.wordpress.com/2007/04/26/posibles-efectos-negativos-de-las-redes-wifi-sobre-la-salud/, Abril 26, 2007, Diciembre 2009*

base), que integre los estándares existentes. Los fabricantes están trabajando en este sentido y es muy probable la integración en breve tiempo.

- **Difícil uso simultáneo en múltiples países**

  En Europa se presenta esta dificultad por la existencia de roaming entre proveedores.

1.3.4 Topología y configuraciones

La versatilidad y flexibilidad de las redes inalámbricas es el motivo por el cual la complejidad de una LAN implementada con esta tecnología sea tremendamente variable. Esta gran variedad de configuraciones ayuda a que este tipo de redes se adapte a casi cualquier necesidad. Estas configuraciones se pueden dividir en dos grandes grupos, las redes *Peer to Peer* y las que utilizan Puntos de Acceso.

- **Configuración *Peer-to-Peer* (*Ad-Hoc*)**

  También conocidas como redes ad-hoc, es la configuración más sencilla ya que en ella los únicos elementos necesarios son terminales móviles equipados con los correspondientes adaptadores para comunicaciones inalámbricas.

  En este tipo de redes, el único requisito deriva del rango de cobertura de la señal, ya que es necesario que los terminales móviles estén dentro de este rango para que la comunicación sea posible.

  Por otro lado, estas configuraciones son muy sencillas de implementar y no es necesario ningún tipo de gestión administrativa de la red.

  Un ejemplo sencillo de esta configuración se muestra en la Figura 1.6.

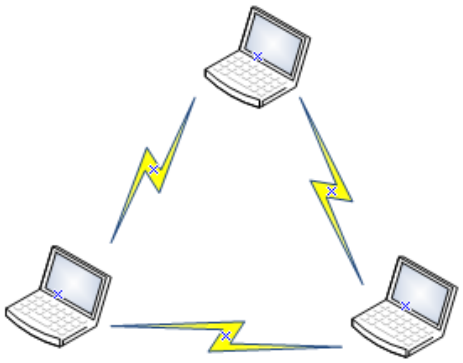


Figura. 1.6. Arquitectura *Peer to Peer* (*ad-hoc*)[34]

- **Configuración en modo Punto de Acceso**

También conocidas como configuraciones en Modo Infraestructura, utilizan el concepto de celda, ya utilizado en otros sistemas de comunicación inalámbrica como la telefonía móvil. Una celda podría entenderse como el área en el que una señal radioeléctrica es efectiva.

En el caso de las redes inalámbricas esta celda suele tener un tamaño reducido, mediante el uso de varias fuentes de emisión, es posible combinar celdas para cubrir de forma casi total un área más extensa. La estrategia empleada para aumentar el número de celdas, y por lo tanto el área cubierta por la red, es la utilización de los llamados AP[35], que funcionan como repetidores, y por tanto son capaces de doblar el alcance de una red inalámbrica, ya que ahora la distancia máxima permitida no es entre estaciones, sino entre una estación y un punto de acceso.

Los Puntos de Acceso son colocados normalmente en alto, pero solo es necesario que estén situados estratégicamente para que dispongan de la cobertura necesaria para dar servicio a los terminales que soportan. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un radio de al menos treinta metros y hasta varios cientos de metros.

La Figura 1.7., muestra el uso de puntos de acceso.

[34] Autor: Arce, Cristian, Diciembre 2009
[35] Access Point

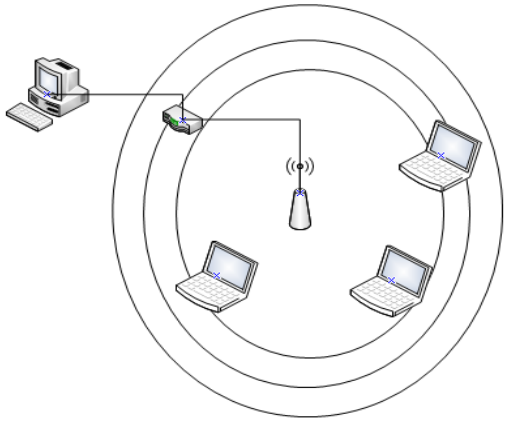


Figura. 1.7. Arquitectura basada en puntos de acceso[36]

La configuración de Punto de Acceso es capaz de dotar a una red inalámbrica de muchas más posibilidades; además del evidente aumento del alcance de la red, permite lo que se conoce como *roaming*, es decir que los terminales puedan moverse sin perder la cobertura y sin sufrir cortes en la comunicación como lo muestra la Figura 1.8. Esto representa una de las características más interesantes de las redes inalámbricas.

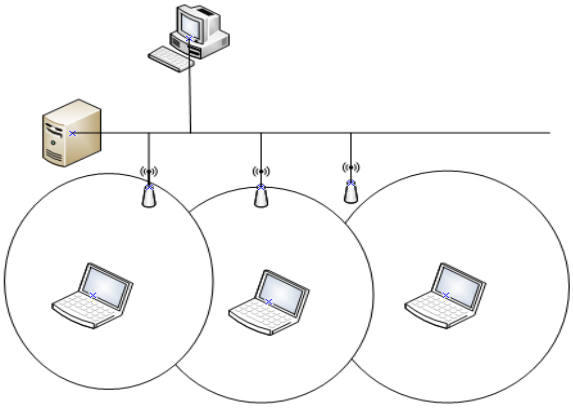


Figura. 1.8. Utilización de varios puntos de acceso: Terminales con capacidad de *roaming*

- **Otras configuraciones: Interconexión de redes**

Las posibilidades de las redes inalámbricas pueden verse ampliadas gracias a la interconexión con otras redes, sobre todo con redes no inalámbricas; esto mediante el uso de antenas (direccionales u omnidireccionales) ya que es posible conectar dos redes separadas por varios cientos de metros, como por ejemplo dos redes locales situadas en dos edificios distintos.

[36] Autor: Arce, Cristian, Diciembre 2009

De esta forma, una LAN no inalámbrica se beneficia de la tecnología inalámbrica para realizar interconexiones con otras redes, que de otra forma serian más costosas, o simplemente imposibles, como lo muestra la Figura 1.9.

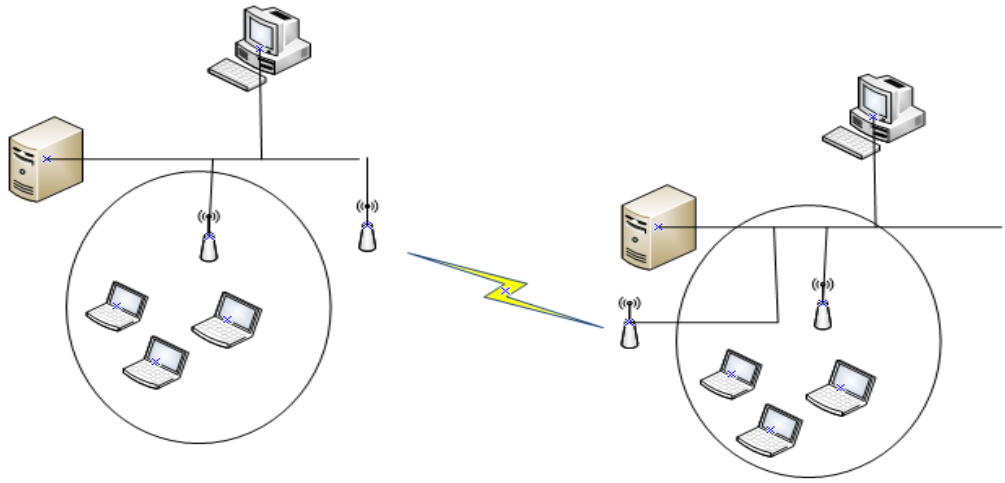


Figura. 1.9. Interconexión de LAN's mediante antenas direccionales [37]

1.4 TECNOLOGIAS INALÁMBRICAS

Dentro la gama de tecnologías inalámbricas que existen en el mercado se tienen: 802.11 WiFi y 802.16 WiMax.

1.4.1 802.11 y sus variantes

Existen muchas variantes de 802.11, en esta sección se realiza un análisis de cada una de ellas.

- ***Introducción a la 802.11***

En Junio de 1997 el IEEE (*Institute of Electrical and Electronic Engineers*) finalizó el estándar inicial para redes inalámbricas, IEEE 802.11[38]. Este estándar especifica una frecuencia de operación de 2.4 GHz con velocidades de transmisión de 1 y 2 Mbps. Desde esta versión inicial, el IEEE 802.11 WG (*Working Group*) ha llevado a cabo diferentes revisiones a través de diferentes grupos de trabajo especializados en distintas áreas. Reconociendo la necesidad crítica de soportar velocidades de

[37] Autor: Arce, Cristian, Diciembre 2009
[38] IEEE_802.11, http://es.wikipedia.org/wiki/IEEE_802.11, Noviembre 2009

transmisión más altas, el grupo de trabajo B dentro del IEEE 802.11 WG ratificó en 1999 el estándar 802.11b para velocidades de hasta 11 Mbps. Con el 802.11b las WLANs proporcionan un rendimiento comparable a una LAN *Ethernet* tradicional de la época.

La mayoría de las WLAN instaladas actualmente funcionan con arreglo a este estándar el cual es la base para la certificación WiFi proporcionada por la WECA. Los productos con certificación WiFi, pueden usarse conjuntamente aunque sean de distintos fabricantes. Aprobado junto al 802.11b, el IEEE 802.11a significará para el mercado de las redes inalámbricas lo que en su día representó la aparición de *Gigabit* Ethernet[39] para las redes de cableado.

Su mayor ventaja radica en que proporciona una velocidad en la transmisión de datos que oscila entre 6 y 54 Mbps. Para conseguir este salto en la velocidad se recurre a la denominada Multiplexación por División en Frecuencia Ortogonal (OFDM), una modalidad de la tecnología de Espectro Extendido.

El ***estándar 802.11a***, utiliza la banda de los 5 GHz, una frecuencia distinta a los 2,4 GHz a los que recurre el 802.11b, lo que lo convierte en incompatible con las redes WiFi; si bien hay que añadir que pueden coexistir sin que surjan riesgos de interferencias. Sin embargo, un escenario compartido entre ambas tecnologías requiere la instalación de infraestructuras diferentes, lo que sin duda aumenta los inconvenientes y los costes, en buena medida derivados de la necesidad de un mayor número de puntos de acceso de 802.11a para disponer de una cobertura óptima.

El nuevo estándar ofrece mayor potencial de absorción de señal y atenuación, además de una menor resistencia multicanal en comparación con las redes basadas en los 2,4 GHz, en las que disminuye de forma considerable la señal según los entornos en que se produzca la comunicación. El consumo eléctrico es otro factor que diferencia a ambos estándares. La mayor capacidad de transmisión de datos y el incremento de los requerimientos de la señal del 802.11a hace necesario un mayor consumo, lo que redunda a su vez en mayores costes procedentes de las baterías de los ordenadores portátiles.

[39] Ampliación del estándar Ethernet (concretamente la versión 802.3ab y 802.3z del IEEE) que consigue una capacidad de transmisión de 1 *gigabit* por segundo.

Pero, sin duda, el mayor logro del 802.11a reside en el salto de velocidad hasta los 54 Mbps, desde los 11 Mbps. De hecho, diversas pruebas han demostrado la mayor eficiencia en la transmisión del nuevo protocolo con respecto a los anteriores. Cuando se comparó el 802.11b a 11 Mbps con el 802.11a a una velocidad limitada de 6 Mbps, se observó que la capacidad de transmisión fue casi similar.

El ***estándar 802.11g***, aprobado en junio de 2002, ofrece la ventaja de que se le considera la continuación natural del 802.11b, en cuanto a que puede operar con este tipo de redes sin ningún contratiempo, ya que también utiliza la banda de 2,4 GHz; lo que le convierte en el siguiente paso de las redes WiFi. Al utilizar la tecnología OFDM, las redes locales inalámbricas basadas en el estándar 802.11g pueden alcanzar una velocidad máxima de 54 Mbps. Los equipos compatibles con 802.11g, así como los puntos de acceso inalámbricos compatibles, pueden proporcionar conectividad de red local inalámbrica para equipos basados en el estándar 802.11g y 802.11b.

Para establecer una conexión se necesitan 2 elementos básicos:

- Un adaptador para cada uno de los terminales a conectar.
- Una Estación Base o Punto de Acceso.

- **Adaptador de red**

Los adaptadores de red mostrados en la Figura 1.10 (uno por puesto de trabajo), adoptan el formato adecuado a cada terminal, (PCI, PCMCIA, PC Card, USB, embebidas en portátiles, en PDA, etc.). Implementan las funciones de estación, normalmente con antena integrada, permitiendo configuraciones ad-hoc o en modo infraestructura.

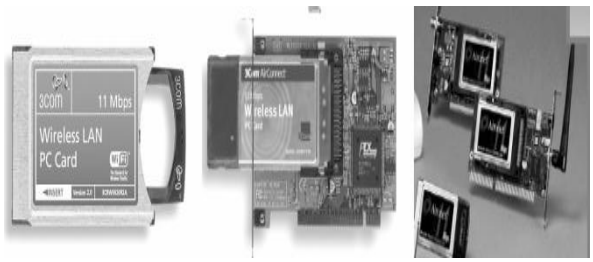


Figura. 1.10. Adaptadores de red inalámbricos[40]

[40] Pcone, www.pcone.com.mx/images/TARJETA_DE_RED, Noviembre 2009

- **Estación base**

La estación base cumple, además de la función de estación, dos funciones: la de ***concentrador*** o hub de una red convencional al que se conectan todos los terminales (sólo que en este caso la conexión se realiza sin cables), implementando funciones de control; y la de ***conexión a la infraestructura*** cableada llevando a cabo el puente con otras redes, como puede ser Internet.

Por esta razòn, la estación base cuenta habitualmente con al menos una conexión Ethernet 10/100 con posibilidad de funcionamiento en modo *bridge* transparente o en modo *Gateway*[41] (con *router*[42] + DHCP[43] + NAT). Ver Figura 1.11

Figura. 1.11. Puntos de acceso[44]

Al igual que el resto de estándar IEEE 802, el 802.11 se centra en las 2 capas inferiores del modelo OSI, la capa física y la capa de enlace. Por tanto, cualquier aplicación LAN, sistema operativo o protocolo, incluido TCP/IP y Novell NetWare, serán compatibles por igual en una WLAN 802.11 como lo son en una LAN Ethernet.

- **Capa Física:** Espectro Ensanchado por secuencia directa (DSSS)
- **Capa de Enlace (MAC):** Adaptación de trama Ethernet + *CSMA/CA* (con *Acknowledge*)

[41] Dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación
[42] Dispositivo que permite conectar uno o varios equipos o incluso una red de área local
[43] ("*Dynamic Host Configuration Protocol*"), especifica un método para configurar dinámicamente los parámetros de red necesarios para que un sistema pueda comunicarse efectivamente
[44] Autor: Arce, Cristian, Diciembre 2009

El 802.11 original define la arquitectura básica, características y servicios de 802.11b. La especificación 802.11b afecta solo a la capa física, aumentando la velocidad de transmisión y proporcionado mecanismos para hacer la conexión más robusta.

- **Arquitectura**

El 802.11 está basado en una arquitectura celular donde el sistema se divide en celdas. Cada celda se denomina BSS[45] y está controlada por una estación base o AP. La mayor parte de las instalaciones están compuestas por un conjunto de celdas formando una red con los AP's conectados a un *backbone*[46]. Este conjunto se denomina DS *(Distribution System).*

El *backbone* de red puede ser una LAN cableada o incluso una WLAN. El conjunto completo de elementos descritos conforma una red única 802.11 para los niveles superiores del modelo de referencia OSI[47] y se denomina ESS[48]

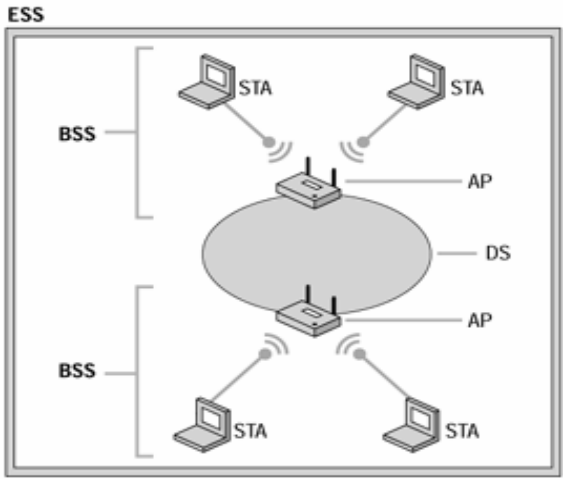


Figura. 1.12. Arquitectura 802.11[49]

[45] (*Basic Service Set*)
[46] Se refiere a las principales conexiones troncales de Internet
[47] El modelo de referencia de Interconexión de Sistemas Abierto
[48] *Extended Service Se*
[49] Arquitectura 802.11, http://bcognizance.iiita.ac.in/jan-mar07/t5_files/image003.jpg, 18-Feb-2009, Noviembre 2009

1.4.2 Capas del IEEE 802.11

Como todos los estándar 802.x, el 802.11 cubre la capa física y la capa de enlace o MAC, por tanto el estándar define tres capas físicas diferentes: espectro ensanchado por secuencia directa (DSSS), espectro ensanchado por salto en frecuencia (FHSS) e infrarrojos. La capa de enlace o MAC es común para las 3 capas físicas, proporcionando una interface única a los protocolos de capas superiores. MAC soporta funciones como la Fragmentación, Retransmisión y Aceptación de paquetes.

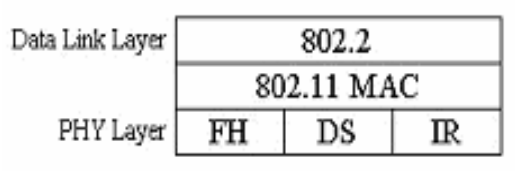


Figura. 1.13. Capas del IEEE 802.11[50]

- **IEEE 802.11: Capa Física**

  La Capa Física de cualquier red define la modulación y la señalización características de la transmisión de datos. Como se ha mencionado anteriormente, los métodos de RF operan en la banda de frecuencia de 2.4 GHz, ocupando aproximadamente 83 MHz de ancho de banda entre los 2,400 y 2,483 GHz.

  El nivel de potencia máximo permitido en este rango de frecuencias varía de un país a otro según sus normas regulatorias. IEEE 802.11 define dos posibles opciones para la elección de la capa física para la transmisión y recepción de tramas 802.11:

  - Espectro expandido por secuencia directa o DSSS
  - Espectro expandido por salto de frecuencias

  En cualquier caso, la definición de tres capas físicas distintas se debe a las sugerencias realizadas por los distintos miembros del comité de normalización, que han manifestado la necesidad de dar a los usuarios la posibilidad de elegir en función de la relación entre costes y complejidad de implementación por un lado, y prestaciones y fiabilidad por otra.

[50] Arquitectura 802.11, http://bcognizance.iiita.ac.in/jan-mar07/t5_files/image003.jpg, 18-Feb-2009, Noviembre 2009

- **Espectro Ensanchado por Salto de Frecuencia (FHSS)**

La tecnología de espectro ensanchado por salto en frecuencia (FHSS) consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamado *dwell* time inferior a 400 ms. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia, de esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo, como muestra la Figura 1.14.

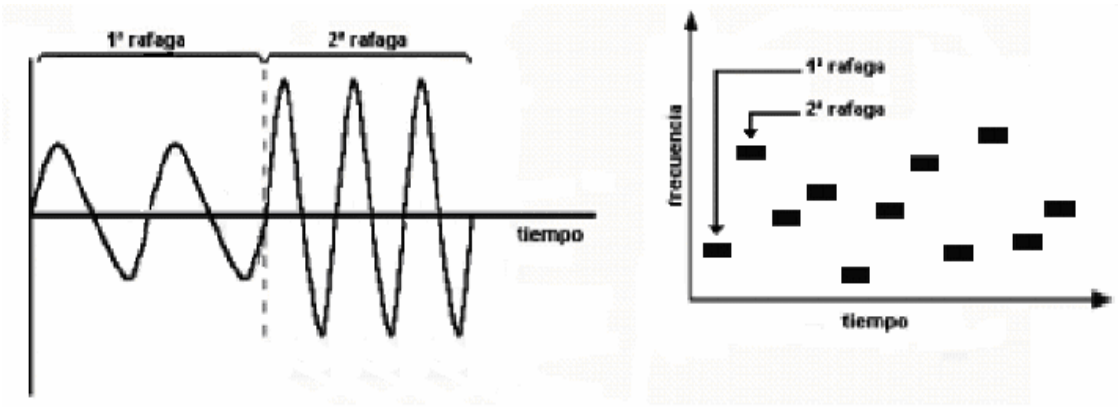


Figura. 1.14. Gráfica de codificación con salto en frecuencia[51]

El orden en los saltos en frecuencia se determina según una secuencia pseudoaleatoria almacenada en unas tablas, que tanto el emisor y el receptor deben conocer.

Si se mantiene la sincronización en los saltos de frecuencias se consigue que, aunque en el tiempo se cambie de canal físico, a nivel lógico se mantiene un solo canal por el que se realiza la comunicación.

Esta técnica utiliza la zona de los 2.4 GHz, la cual se organiza en 79 canales con un ancho de banda de 1MHz cada uno. No obstante el número real de canales que son usados se regula por las autoridades competentes de cada país, el número de saltos por segundo está también regulado en cada país.

[51] Ponce, Enrique, Redes Inalámbricas: IEEE 802.11,http:// www.canal-ayuda.org/a-informatica/inalambrica.htm, Noviembre 2009

Se utiliza la modulación en frecuencia FSK[52] con una velocidad de 1 Mbps ampliable a 2 Mbps. En la revisión 802.11b del estándar, la velocidad también ha aumentado a 11Mbps.

- **Espectro Ensanchado por Secuencia Directa (DSSS)**

DSSS es el segundo nivel físico soportado por el 802.11 y el único especificado en el 802.11b, soportando velocidades de transmisión de 5.5 y 11Mbps.

En el caso de Estados Unidos y Europa la tecnología DSSS utiliza un rango de frecuencias que va desde los 2,4 GHz hasta los 2,4835 GHz, lo que permite tener un ancho de banda total de 83,5 MHz. Este ancho de banda se subdivide en canales de 5 MHz, lo que hace un total de 14 canales independientes. Cada país está autorizado a utilizar un subconjunto de estos canales; en Europa existen 13 canales disponibles (excepto en Francia) aunque tan solo 3 están no solapados.

De acuerdo al estándar 802.11 debe existir una separación de 30 MHz entre las frecuencias centrales de los canales, esto con el objeto de que si las celdas se solapan y/o son adyacentes no cause interferencias. En 802.11b la separación se reduce a 25 MHz, esto significa que pueden existir 3 celdas con zonas solapadas y/o adyacentes sin causar interferencias entre ellas, tal y como se muestra en la Figura 1.15.

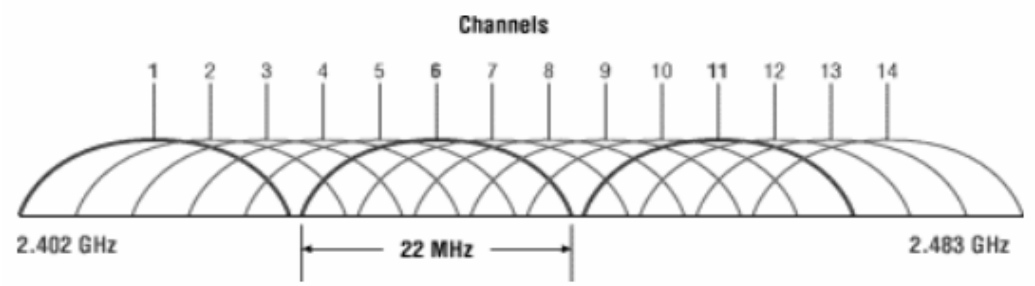


Figura. 1.15. Canales DSSS[53]

En configuraciones donde existan más de una celda; éstas pueden operar simultáneamente y sin interferencias, siempre y cuando la diferencia entre las frecuencias centrales de las distintas celdas sea de al menos 30 MHz, lo que reduce a

[52] (Frequency Shift Keying),Tipo de modulación de frecuencia

[53] Ponce, Enrique, Redes Inalámbricas: IEEE 802.11,www.canal-ayuda.org/a-informatica/inalambrica.htm, Noviembre 2009

tres el número de canales independientes y funcionando simultáneamente en el ancho de banda total de 83,5 MHz.

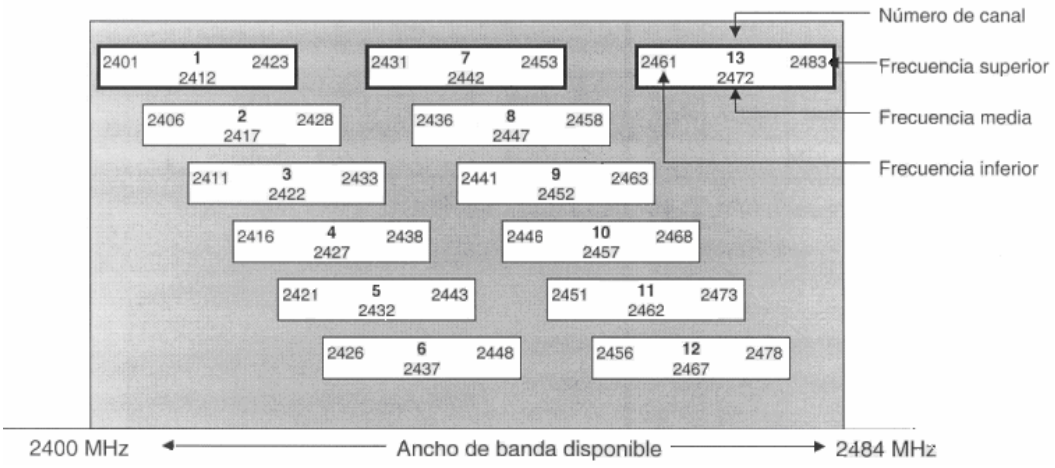


Figura. 1.16. Tabla de frecuencias DSSS[54]

El estándar 802.11b utiliza DSSS en la banda de 2.40 GHz y la estructura de canales diseñada en el estándar 802.11. La principal diferencia entre los dos estándares estriba en que 802.11b utiliza modulación CCK (Complimentary Code Keying) para las velocidades de 5.5 Mbps y 11 Mbps, mientras que el estándar 802.11b soporta también las velocidades de 1Mbps y 2 Mbps, por lo que tiene compatibilidad con dispositivos 802.11, como se ve en la Figura 1.16

- **Modulación por división ortogonal de frecuencias (OFD*M*)**

Esta tecnología sólo está presente en 802.11a y en 802.11g como principal variación respecto a 802.11 y 802.11b.

Se observa que la modulación pasa a ser OFDM (*Orthogonal Frequency Division Multiplexing*), en vez de la clásica y más fiable hasta entonces CCK (*Complimentary Code Keying*); aunque esta norma pueda coexistir en los puntos de acceso 802.11g, conservando a su vez la banda de los 2.4Ghz (precedido de un CCK RTS). Ver Figura 1.17.

[54] Ponce, Enrique, Redes Inalámbricas: IEEE 802.11, www.canal-ayuda.org/a-informatica/inalambrica.htm, Noviembre 2009

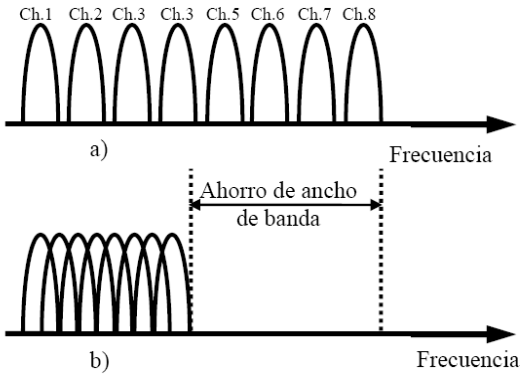


Figura. 1.17. OFDM. Orthogonal Frequency Division Multiplexing[55]
a) Técnica multiportadora original.
b) Modulación de portadoras ortogonales.

Durante los últimos años, se ha aceptado OFDM como tecnología de base para el 802.16a, que es un estándar de IEEE para redes de área metropolitana inalámbrica; y que puede proveer extensión inalámbrica para acceso de última milla de banda ancha en instalaciones de cable y DSL.

El mismo cubre el rango de frecuencias de 2 a 11 GHz y alcanza hasta 50 kilómetros lineales, brindando conectividad de banda ancha inalámbrica sin necesidad de que exista una línea directa de visión a la estación de base. La velocidad de transmisión de datos puede llegar a 70 Mbps, una estación de base típica puede albergar hasta seis sectores. La calidad de servicio está integrada dentro del MAC, permitiendo la diferenciación de los niveles de servicio.

La transmisión sin línea de visión ocurre cuando entre el receptor y el transmisor existen reflexiones o absorciones de la señal, lo que resulta en una degradación de la señal recibida, que se manifiesta por medio de los siguientes efectos: atenuación plana, atenuación selectiva en frecuencia o interferencia inter-símbolo.

Actualmente se ha introducido al mercado la tercera generación de equipos OFDM siendo el único proveedor mundial con una sólida experiencia en esta tecnología probada a través de la excelencia de sus productos.

Las tecnologías 802.11a y 802.11b definen una capa física diferente. Los emisores 802.11b transmiten a 2.4 GHz y envían datos a tasas tan altas como 11 Mbps

[55] Ponce, Enrique, Redes Inalámbricas: IEEE 802.11, www.canal-ayuda.org/a-informatica/inalambrica.htm, Noviembre 2009

usando modulación DSSS; mientras que los emisores 802.11a y 802.11g transmiten a 5 y 2,4 GHz respectivamente y envían datos a tasas de hasta 54 Mbps usando OFDM (*Orthogonal Frequency Division Multiplexing* o en español Multiplexación de División de Frecuencia Ortogonal). OFDM es una tecnología de modulación digital, una forma especial de modulación multi-portadora (*multicarrier*) considerada la piedra angular de la próxima generación de productos y servicios de radio frecuencia de alta velocidad, para uso tanto personal como corporativo.

La técnica de espectro disperso de OFDM distribuye los datos en un gran número de portadoras (*carriers*) que están espaciados entre sí en distintas frecuencias precisas, ese espaciado evita que los demoduladores vean frecuencias distintas a las suyas propias. OFDM tiene una alta eficiencia de espectro y menor distorsión multi-ruta.

Actualmente OFDM no sólo se usa en las redes inalámbricas LAN 802.11a y 802.11g, sino también en comunicaciones de alta velocidad por vía telefónica como las ADSL y en difusión de señales de televisión digital terrestre en Europa, Japón y Australia. (Ver Figura 1.18)

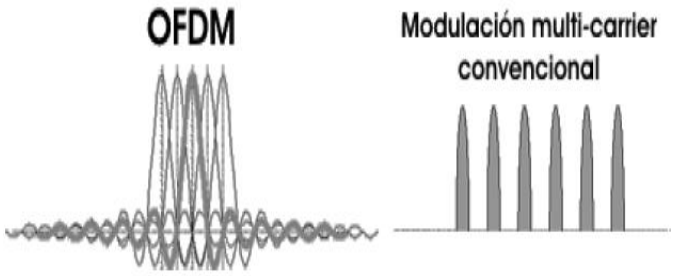


Figura. 1.18. Espectro de OFDM Solapado[56]

- **IEEE 802.11: Capa de Enlace (MAC)**

Diseñar un protocolo de acceso al medio para las redes inalámbricas es mucho más complejo que hacerlo para redes cableadas, ya que deben tenerse en cuenta las dos topologías de una red inalámbrica (modo independiente o infraestructura). Además se deben de tener en cuenta otros factores como:

- Perturbaciones ambientales (interferencias).

[56] Ponce, Enrique, Redes Inalámbricas: IEEE 802.11,www.canal-ayuda.org/a-informatica/inalambrica.htm, Noviembre 2009

- Variaciones en la potencia de la señal.
- Conexiones y desconexiones repentinas en la red.
- *Roaming* o itinerancia, nodos móviles que van pasando de celda en celda.

A pesar de todo ello la norma IEEE 802.11 define una única capa MAC (divida en dos subcapas) para todas las redes físicas, facilitando de este modo la fabricación en serie de chips. La principal función de esta capa es el control de acceso al medio, realizando igualmente funciones como fragmentación, encriptación, gestión de alimentación eléctrica, sincronización y soporte de roaming entre múltiples APs.

- **Mecanismos de Acceso básico CSMA/CA**

El estándar 802.11 utiliza como mecanismo de acceso básico el método CSMA (*Carrier Sense Multiple Access*) que trabaja del siguiente modo; la estación que desea transmitir "escucha" el medio de transmisión; si el medio está ocupado significa que otra estación está transmitiendo y por lo tanto debe retrasar su transmisión.

Si el medio está libre durante un tiempo especifico, llamado DIFS (*Distributed Inter Frame Space*) en el estándar, la estación está habilitada para transmitir. Esta clase de métodos de acceso, denominados protocolos de acceso por contienda, son muy efectivos si la carga de uso del medio no es muy alta, ya que esto permitirá a las estaciones transmitir con un retardo mínimo.

Hay que tener en cuenta además que pueden producirse colisiones debido a la posibilidad de que 2 estaciones "escuchen" el medio simultáneamente, detectando que esté libre e iniciando su transmisión al mismo tiempo.

El método de acceso más popular en redes cableadas es el CSMA/CD (*Collision Detection*) utilizado por el estándar IEEE 802.3 (Ethernet). Este método no puede aplicarse a redes inalámbricas debido a dos razones:

- Para implementar un mecanismo de detección de colisiones, se necesitarían dispositivos de radio full dúplex capaces de transmitir y recibir simultáneamente, lo cual incrementaría significativamente el coste de los equipos.

- En una red cableada cualquier estación pueden “escuchar” al resto, mientras que en redes inalámbricas esto puede no cumplirse (nodo escondido).

El método que más se utiliza en redes inalámbricas es el CSMA/CA (Carrier-Sense, Multiple Access, Collision Avoidance), este protocolo evita colisiones en lugar de descubrir una colisión, como el algoritmo usado en la 802.3. En una red inalámbrica es difícil descubrir colisiones; es por ello que se utiliza el CSMA/CA y no el CSMA/CD debido a que entre el final y el principio de una transmisión suelen provocarse colisiones en el medio.

En CSMA/CA, cuando una estación identifica el fin de una transmisión espera un tiempo aleatorio antes de transmitir su información, disminuyendo así la posibilidad de colisiones, como lo muestra la Figura 1.19.

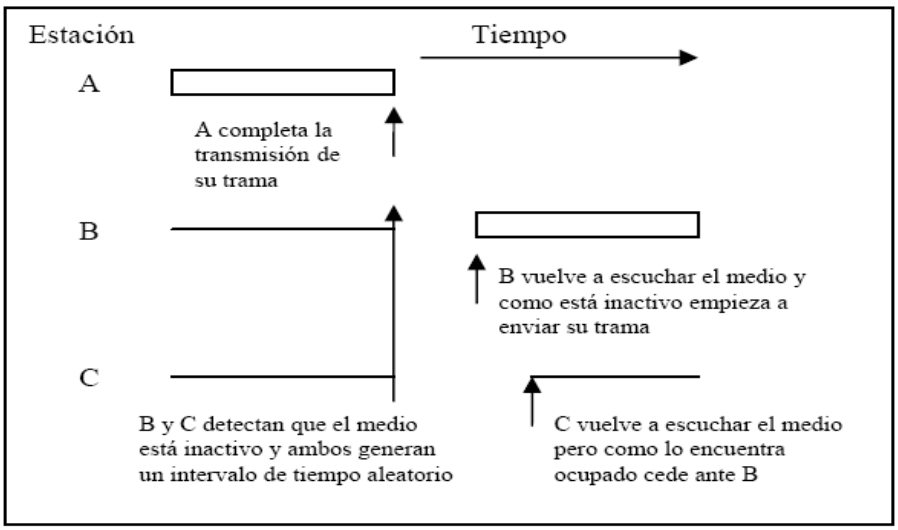


Figura. 1.19. Método CSMA/CA[57]

La capa MAC opera junto con la capa física probando la energía sobre el medio de transmisión de datos, la capa física utiliza un algoritmo de estimación de desocupación de canales (CCA) para determinar si el canal está vacío; esto se cumple midiendo la energía RF de la antena y determinando la fuerza de la señal recibida.

Esta señal medida es normalmente conocida como RSSI; si la fuerza de la señal recibida está por debajo de un umbral especificado, el canal se considera vacío, y a la

[57] Peña, Inés de Carrillo,http://gavilan.uis.edu.co/~clarenes/docencia/informatica_educativa/pdfs/seminario-redes-ceis.pdf, Diciembre de 1998, Enero 2010

capa MAC se le da el estado del canal vacío para la transmisión de los datos. Si la energía RF está por debajo del umbral, las transmisiones de los datos son retrasadas de acuerdo con las reglas protocolares.

El estándar proporciona otra opción CCA que puede comprobarse independientemente o con la medida RSSI. El sentido de la portadora puede usarse para determinar si el canal está disponible; esta técnica es más selectiva ya que verifica que la señal es del mismo tipo de portadora que los transmisores del 802.11. En comunicaciones inalámbricas, este modelo presenta todavía una deficiencia debida al problema conocido como terminal oculta (o nodo escondido). Ver Figura 1.20.

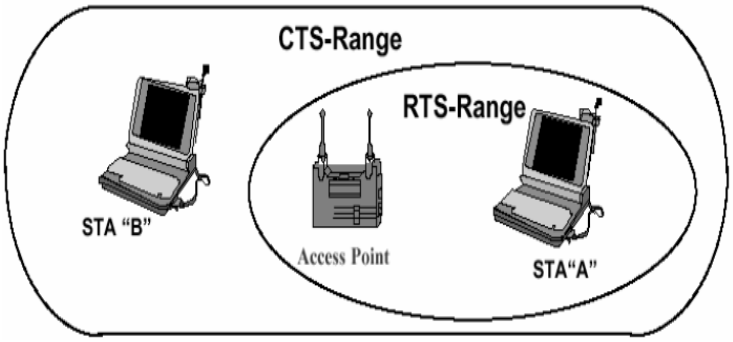


Figura. 1.20. Ejemplo de Nodo escondido[58]

Un dispositivo inalámbrico puede transmitir con la potencia suficiente para que sea escuchado por un nodo receptor, pero no por otra estación que también desea transmitir y que por tanto no detecta la transmisión. Para resolver este problema, la norma 802.11 ha añadido al protocolo de acceso CSMA/CA un mecanismo de intercambio de mensajes con reconocimiento positivo, al que denomina *Reservation-Based Protocol*, que es la 2ª subcapa MAC.

Cuando una estación está lista para transmitir, primero envía una solicitud (destino y longitud del mensaje) al punto de acceso (RTS - "*request to send*") quien difunde el NAV (*Network Allocation Vector*) -un tiempo de retardo basado en el tamaño de la trama contenido en la trama RTS de solicitud- a todos los demás nodos

[58] Ponce, Enrique, Redes inalámbricas: IEEE 802.11 http://multingles.net/docs/Manual%20- %20Redes%20WiFi%20inalambricas.Pdf, Noviembre 2009

para que queden informados de que se va a transmitir (y que por lo tanto no transmitan); y cuál va a ser la duración de la transmisión.

Estos nodos dejarán de transmitir durante el tiempo indicado por el NAV más un intervalo extra de *backoff* (tiempo de retroceso) aleatorio. Si no encuentra problemas, responde con una autorización (CTS - "*clear to send*") que permite al solicitante enviar su trama (datos). Si no se recibe la trama CTS, se supone que ocurrió una colisión y los procesos RTS empiezan de nuevo.

Después de que se reciba la trama de los datos, se devuelve una trama de reconocimiento (ACK - AC*Knowledged*) notificando al transmisor que se ha recibido correctamente la información (sin colisiones). Aún así permanece el problema de que las tramas RTS sean enviadas por varias estaciones a la vez, sin embargo estas colisiones son menos dañinas ya que el tiempo de duración de estas tramas es relativamente corto. Este mismo protocolo también puede utilizarse si no existen dispositivos auxiliares en las redes ad-hoc, en este caso no aparecería la trama NAV.

1.4.3 Tecnología WiMax – 802.16

La tendencia actual en telecomunicaciones es la convergencia de servicios, tecnologías, estándares; los cuales deben estar soportados por accesos de banda ancha, en la actualidad este tipo de acceso está limitado a las grandes ciudades y a los sectores con recursos económicos para utilizar estos servicios.

WiMax es un sistema de comunicaciones digitales inalámbricas, también conocida como IEEE 802.16, que se destina para la telefonía celular "redes de área metropolitana". WiMax puede proporcionar acceso inalámbrico de banda ancha (BWA) de hasta 30 millas (50 km) para estaciones fijas, y de 5 - 15 km para las estaciones móviles.

Con WiMax y WiFi las tasas de datos son fácilmente compatibles, pero la cuestión de la interferencia se reduce. WiMax opera en ambos con licencia y sin licencia de frecuencias, proporcionando un entorno regulado y un modelo económico viable para los operadores inalámbricos. WiMax puede ser utilizada para las redes inalámbricas en la misma forma como el protocolo Wi-Fi.

WiMax es un protocolo de segunda generación que permite un uso más eficiente de ancho de banda, para evitar interferencias, y está destinado a permitir mayores velocidades de datos a largas distancias.

WiMax (*Worldwide Interoperability for Microwave Access*), una tecnología reciente basada en el estándar IEEE 802.16 promete ser la tecnología que proveerá servicios de banda ancha en todo tipo de ambientes urbanos y rurales; zonas donde los operadores pueden suministrar diferentes servicios con inversiones bajas y despliegue rápido de tecnología, además, el servicio puede ser prestado en bandas no licenciadas, lo que aún más bajará los costos de operación.

- **Versiones de WiMax**

La Tabla 1.2., muestra una clasificación de las versiones de WIMAX.

Tabla. 1.2. Versiones de WiMax[59]

COMENTARIOS	MOTIVACION	COBERTURA MAX.	RANGO DE FRECUENCIA	APROBADO	VERSION
Portadoras simples (Single Carriers)	Primera Versión.	5 Km	10-66 GHz	2001/2002	802.16
Incluye 3 interfaces aire: Portadora Simple, OFDM-256 y OFDMA 2048	Incluye a los enlaces sin línea de Vista	50 Km	2-11 GHz	2003	802.16a
Se concentra en QoS para Aplicaciones de audio y video en tiempo real. Se lo llama también Wireless HUMAN.	Permite trabajar con aplicaciones en bandas de frecuencias no licenciadas.	No definido	5-6 GHz	2001/2002	802.16b

[59] Descripción de las Tecnologías WiMax y Wi-Fi, http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/532/8/T10464CAP2.pdf, Enero 2010

Versión creada para actualizar y expandir el estándar IEEE 802.16-2001	Crea perfiles de sistemas con línea de vista LoS en el rango de 10-66 GHz	50 Km	10-66 GHz	Final del 2002	802.16c
Reemplazó a todos los Estándares anteriores.	Mejoras varias al IEEE 802.16a	50 Km	2-11GHz	Jun-04	802.16d
Máxima velocidad móvil de hasta 250 Km/h	Incluye movilidad dentro del estándar.	5 Km	2-6GHz (bandas licenciadas)	Sep-2004	802.16e
Permite la creación de redes Ad-Hoc. Define la base de información para la administración de la capa MAC y física.	Incluye funcionalidades de Multisalto - MultiHop	50 Km	2-6GHz	Ago-2004	802.16f
Mejoramiento del QoS.	Incluye un manejo eficiente del handover.	50 Km		Ago-2004	802.16g

1.4.4 Capas del IEEE 802.16

- **Capa Física WiMax**

La capa física fue revisada en el anexo IEEE 802.16d, en el cual se incluía 3 nuevas especificaciones: Portadora Simple, OFDM 256 puntos y OFDMA-2048 puntos. El fórum de WiMax ha recomendado utilizar la segunda, OFDM 256-puntos.

OFDM se ha convertido en el factor determinante para tecnologías de banda ancha, especialmente en casos sin línea de vista (NLOS). Sin embargo, los SCI no son la única aplicación donde OFDM puede ser utilizado. OFDM también ha sido utilizado

en aplicaciones de sistemas alambrados como xDSL y en cable módems, inclusive, dentro de la industria de video digital, especialmente en Europa. En la Tabla 1.3., se muestran las características de la capa física.

Tabla. 1.3. Características de la Capa Física WiMax[60]

CARACTERISTICA	BENEFICIO
256-FFT OFDM	Soporta direccionamiento multicamino en ambientes con y sin línea de vista (LoS y NLoS)
Modulación Adaptable y corrección codificada de error de variable por ráfaga de radiofrecuencia RF.	Asegura un enlace robusto de RF a la vez que maximiza el número de bits/segundo para cada unidad de suscriptor.
Soporta TDD, FDD dúplex y también half-dúplex FDD, esto es, H-FDD.	Se adapta a las diferentes variantes regulatorias a nivel mundial.
Flexible tamaño de los canales. (3.5Mhz, 5Mhz, 10Mhz, etc.)	Provee la flexibilidad necesaria para operar en diferentes bandas de frecuencia con diferentes variantes y requerimientos del canal alrededor del mundo

En la capa física, WiMax especifica canales entre 1.75MHz y 20 MHz, con varios opciones intermedias, mientras que los productos WiFi requieren al menos de 20MHz por canal (22MHz en la banda de 2.5GHz para 802.11b).

- **Capa De Enlace WiMax**

En la capa de enlace (MAC), WiMax presenta muchas ventajas sobre previos estándares. En la Tabla 1.4., se detallan las características de la capa de enlace WIMAX.

[60] Descripción de las Tecnologías WiMax y Wi-Fi. http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/532/8/T10464CAP2.pdf, Enero 2010

Tabla. 1.4. Características de la capa de enlace WiMax[61]

CARACTERISTICA	BENEFICIO
TDM/TDMA tramas programadas para enlaces de subida y bajada.	Uso eficiente del ancho de banda.
Escalable de uno a cientos de suscriptores.	Permite desarrollos costo-efectivo conveniente.
Orientado a Conexión.	QoS por conexión. Envío y Ruteo rápido de paquetes.
QoS Soporta tasa de bit variable continua en tiempo real y en tiempo no real de mejor esfuerzo.	Baja latencia para servicios que son sensibles al retardo (TDM Voz, VoIP). Transporte óptimo para tráfico VBR (como por ejemplo, video) con soporte de prioridad de información.
Solicitud Automática de Transmisión (ARQ)	Rendimiento mejorado de extremo a extremo ocultando errores inducidos en la capa de RF de los protocolos de capas superiores.
Soporte de modulación adaptable	Permite alcanzar altas tasas de información permitidas por las condiciones del canal, mejoran la capacidad del sistema.
Seguridad y Encriptación (Triple DES)	Protege la privacidad del usuario.
Control automático de potencia.	Permite el desarrollo celular minimizando la propia interferencia.

En la capa MAC, WiFi utiliza CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), lo cual de estudios iniciales (Ethernet usa CSMA/CD collision

[61] Descripción de las Tecnologías WiMax y Wi-Fi. http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/532/8/T10464CAP2.pdf, Enero 2010

detection) se conoce que no es un protocolo eficiente. Es decir CSMA/CA es la versión inalámbrica de CSMA/CD.

1.5 COMPARACIÓN ENTRE WIMAX Y WIFI

En la Tabla 1.5 se realiza una comparación entre las dos tecnologías posibles a utilizar, cabe resaltar que dentro de la elección se debe considerar el aspecto de costos.

Tabla. 1.5. Comparación entre WiFi y WiMax[62]

	WIFI	**WIMAX**
Cobertura Aproximada	Inferior a 100m	15-30Km(LOS), 3-5Km(NLOS)
Optimización	Para cortos rangos de espacios de inferiores	Para ambientes en NLOS (bandas de 2-11 GHz), soporta técnicas avanzadas de antena, modulación adaptativa, técnicas de detección de error
Escalabilidad	Aplicación LAN. El número de usuarios puede variar con un subscriptor por CPE.	Soporte eficiente de cientos de estaciones de suscriptores con un número limitado de usuarios por estación. Canales flexibles de ancho de banda, en el rango de 1.5 – 20 MHz
Tasa de Bit	Máx. eficiencia espectral de 2,7 bps/Hz. 54 Mb/s en canales de 20 MHz	Máx. Eficiencia. espectral de 5 bps/Hz 75-100 Mbps en canales de 20 MHz
QoS	Sin soporte de QoS	Soporte nativo de QoS en la MAC Niveles de diferenciación de servicios

[62] Descripción de las Tecnologías WiMax y Wi-Fi, http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/532/8/T10464CAP2.pdf, Enero 2010

CAPÍTULO II

ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED

2.1 ANTECEDENTES DEL SECTOR A IMPLEMENTAR

El Departamento de Actividad Física, Deportes y Recreación, recibe este nombre en marzo del 2006, y su inicio fue en noviembre de 1989 como el Instituto de Educación Física.

Este departamento se encuentra aprovisionado con un sistema de red alámbrico, el mismo que desde UTICS se interconecta con fibra óptica, así conectando al Departamento con la red general de la ESPE; los equipos se encuentran ubicados en el tercer piso del bloque en el rack numero 15, el mismo que distribuye el servicio de acceso a la red a las oficinas del Departamento Administrativo (tercer piso).

2.2 LEVANTAMIENTO DE INFORMACION ACTUAL DEL BLOQUE

2.2.1 Análisis de la estructura existente en el Bloque

El bloque se encuentra dividido en varios pisos que se detallan a continuación:

- **Planta baja**
  - ♦ Edificio CAFDER
    - o Tercer Nivel
  - ♦ Gimnasio
    - o Vestidor Hombres
    - o Vestidor Mujeres
  - ♦ Coliseo
    - o Bastidores
    - o Vestidores1
    - o Camerinos
    - o Escenario
    - o Cancha de uso múltiple
    - o Vestidores Hombres y Mujeres
    - o Hall de ingreso
    - o Baño de Hombres
    - o Baño de Mujeres
    - o Bodega1
    - o Bodega2
  - ♦ Área de Relajación
    - o Sauna
    - o Turco
    - o Duchas
    - o Caldero
    - o Vestidores Hombres y Mujeres
    - o Área de descanso
    - o Piscina
    - o Hall de Ingreso
  - ♦ Fisioterapia y RX
    - o Fisioterapia

- Vestidores Hombres y Mujeres
- Camerinos
- Baño
- Sala de Rayos X rodante
- Laboratorio
- Traumatología y Medicina Deportiva
- Baño
- Emergencias Observación
- Medicina General
- Baño1
- Baño2
- Odontología

- **Primer piso**

  - Edificio CAFDER

    - Sexto Nivel
    - Primer Nivel
    - Segundo Nivel
    - Quinto Nivel
    - Biblioteca
    - Sala de Dibujo y Audiovisuales
    - Corredor
    - Baños

- **Segundo piso**

  - Edificio CAFDER

    - Hall de ingreso
    - Séptimo Nivel
    - Octavo Nivel
    - Cuarto Nivel

  - Oficinas Administrativas

- Sala de Reuniones
- Ofic. docente Msc. Vaca
- Ofic. docente Lic. A. Obando
- Ofic. DT. Basketball Msc. P. Ponce
- Secretaria
- Departamento de Clubes
- Ofic. Director TCRN. E.M Franklin Pico
- Ofic. Subdirector Dr. Enrique Chávez
- Coordinador Estudiantil

En el ANEXO1, se muestran los planos con la distribución detallada de cada uno de los pisos existentes en el bloque.

2.2.2 Descripción de la red existente

La topología utilizada en el diagrama de red es ESTRELLA EXTENDIDA, teniendo como punto central el rack de distribución ubicado en la Unidad de Tecnologías (UTICS), como se muestra en la Figura 2.1.

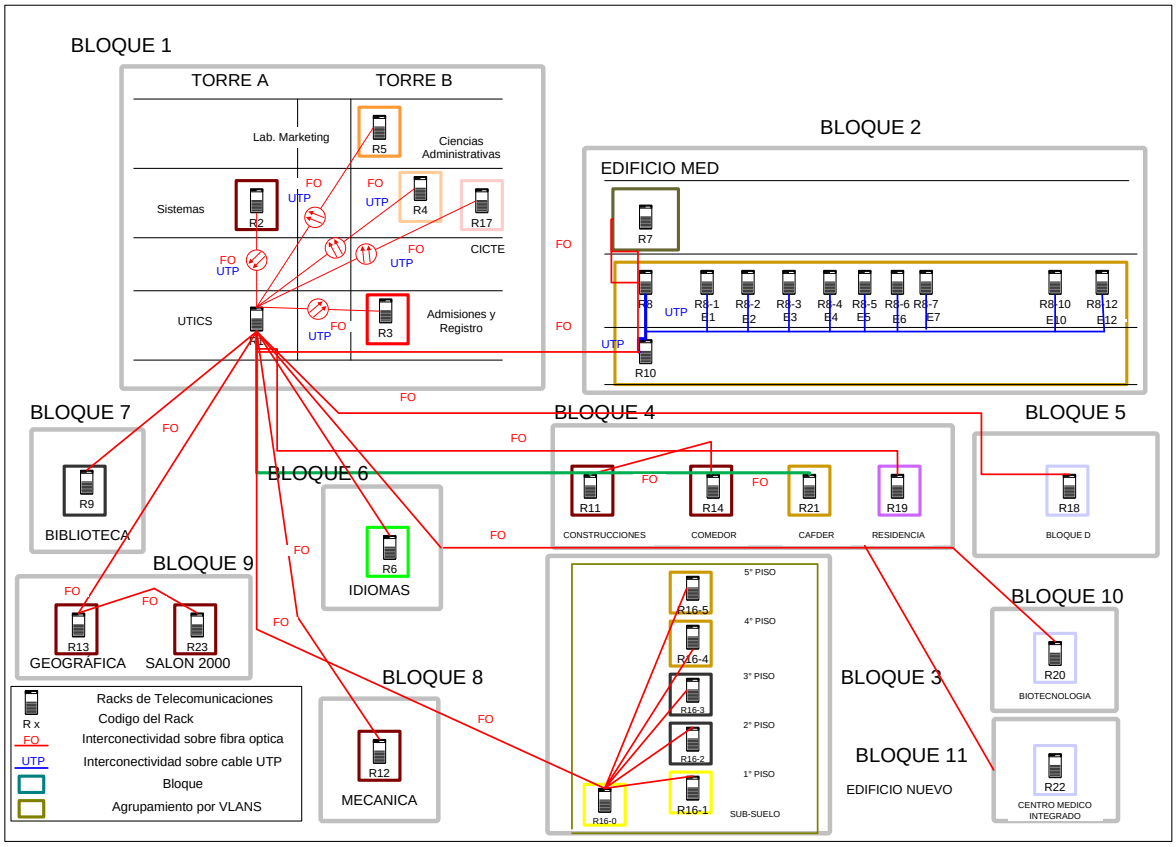


Figura. 2.1. Diagrama General de la Red ESPE

Desde el departamento de UTICS, BLOQUE 1, rack N° 1, se provee de conectividad sobre fibra óptica al departamento de construcciones ubicado en el BLOQUE 4, rack N° 11, el mismo que distribuye interconexión sobre fibra óptica, a los siguientes lugares:

- Comedor (Bloque 4, rack N°14)
- Departamento de Actividad Física Deportes y Recreación (Bloque 4, rack N°21)
- Residencia estudiantil (Bloque 4, rack N°19)

Desde el departamento de UTICS se extienden 8 hilos de fibra óptica divididos en:

- 4 hilos para Transmisión

- 4 hilos para Recepción

Estos a su vez se encuentran utilizados; 1par (Tx-Rx) los mismos que son R11 R21 1-R11 R21 2 y 1par (Tx-Rx) para Bodega 01, quedando libres R11 R21 3-R11 R21 4 y Bodega 02.

La fibra óptica llega de R11-R21-1; R11-R21-2 a un convertidor de fibra a RJ45, el mismo que va hacia el Switch de 50 puertos Ethernet 10/100 Base-Tx modelo 3COM 4500, el cual se encarga de distribuir el servicio a los siguientes puntos de red mostrados en la Tabla 2.1., los puertos que se encuentran de color azul son los que se encuentran conectados mientras que los de color rojo no están conectados.

Tabla. 2.1. Descripción de puntos ubicados en el Rack 21 del Bloque CAFDER

PUERTO	UBICACIÓN	DESCRIPCIÓN DEL PUNTO	NOMENCLATURA
1	2do piso, Cubículo	El punto de red se encuentra libre	R21-P1-01
2	2do piso, Ofic. MSC. M. Vaca	Se encuentra conectado del punto de red al tel IP y de este a su vez al computador	R21-P1-02
3	2do piso, Ofic. Lic. A.Obando	El punto de red se encuentra libre	R21-P1-03
4	2do piso, Ofic. DT. Basketball MSC. P. Ponce	El punto de red se encuentra libre	R21-P1-04
5	2do piso, Ofic. Coordinador Estudiantil	El punto de red se encuentra libre	R21-P1-05
6	2do piso, Ofic. Subdirector Dr. Enrique Chávez	El punto de red se encuentra libre	R21-P1-06
7	2do piso, Ofic. Director	Se encuentra conectado del	R21-P1-07

	TCRN.E.M. F. Pico	punto de red al tel IP y de este a su vez al computador	
8	2do piso, Secretaria General	Se encuentra conectado del punto de red al tel IP y de este a su vez al computador	R21-P1-08
9	2do piso, sala reuniones	El punto de red se encuentra libre	R21-P1-09
10	2do piso, sala reuniones	El punto de red se encuentra libre	R21-P1-10
11	Oficinas Coliseo	El punto de red se encuentra libre	R21-P1-11
12	2do piso, secretaria general	Se conecta del punto de red a un Switch NEXXT 10/100M de 8 puertos	R21-P1-12
13	2do piso, Ofic. Lic. A. Obando	Se conecta del punto de red al computador	R21-P1-13
14	2do piso, Ofic. DT. Basketball MSC. P. Ponce	Se conecta del punto de red al computador	R21-P1-14
15	2do piso, Ofic. Coordinador Estudiantil	Se conecta del punto de red al computador	R21-P1-15
16	2do piso, Ofic. Subdirector Dr. Enrique Chávez	Se conecta a un computador portátil	R21-P1-16
17	2do piso, Ofic. Director TCRN.E.M. F. Pico	El punto de red se encuentra libre	R21-P1-17

18	2do piso, Departamento de Clubes	El punto de red se encuentra libre	R21-P1-18
19	Coliseo	El punto de red se encuentra libre	R21-P2-1
20	Coliseo	El punto de red se encuentra libre	R21-P2-2
21	Coliseo	El punto de red se encuentra libre	R21-P2-3
23	Sala de Dibujo y Audiovisuales	Se conecta a un computador	R21-P2-4
24	Biblioteca	Se conecta a un computador	R21-P2-5
26	Coliseo	El punto de red se encuentra libre	R21-P2-6
27	Desconocido	El punto de red se encuentra libre	R21-P2-7
28	Desconocido	El punto de red se encuentra libre	R21-P2-8
29	Desconocido	El punto de red se encuentra libre	R21-P2-9
45	Tx Fibra Óptica	La fibra llega al convertidor de fibra a RJ45 y va al switch	
46	Rx Fibra Óptica	El cable de red va hacia el convertidor de fibra	

Los puntos de red asignados a cada computador de las oficinas administrativas se conectan a un teléfono IP el mismo que sirve de Switch de 2 puertos, tomándose el otro para conexión de la tarjeta Ethernet de cada computador.

En la Secretaría General el punto de red R21-P1-12 se conecta a un Switch NEXXT 10/100M de 8 puertos de los cuales 3 están conectados; del punto de red R21-P1-12 va hacia el puerto 2, del puerto 3 va hacia el teléfono IP 3COM y el último puerto va hacia el computador, en el puerto 5 se conecta el computador que se encuentra en la oficina 5, los demás puertos del Switch NEXXT se encuentran libres, como muestra la Figura 2.2.

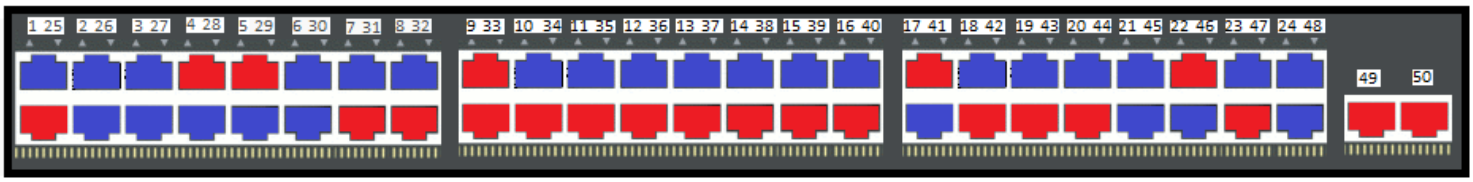


Figura. 2.2. Descripción de puertos utilizados y libres en el Switch ubicado en el Bloque CAFDER.

La Figura 2.3, muestra el diagrama estructural donde se indica la ubicación física de los puntos de red y de los equipos con los que cuenta cada subdivisión de las oficinas administrativas:

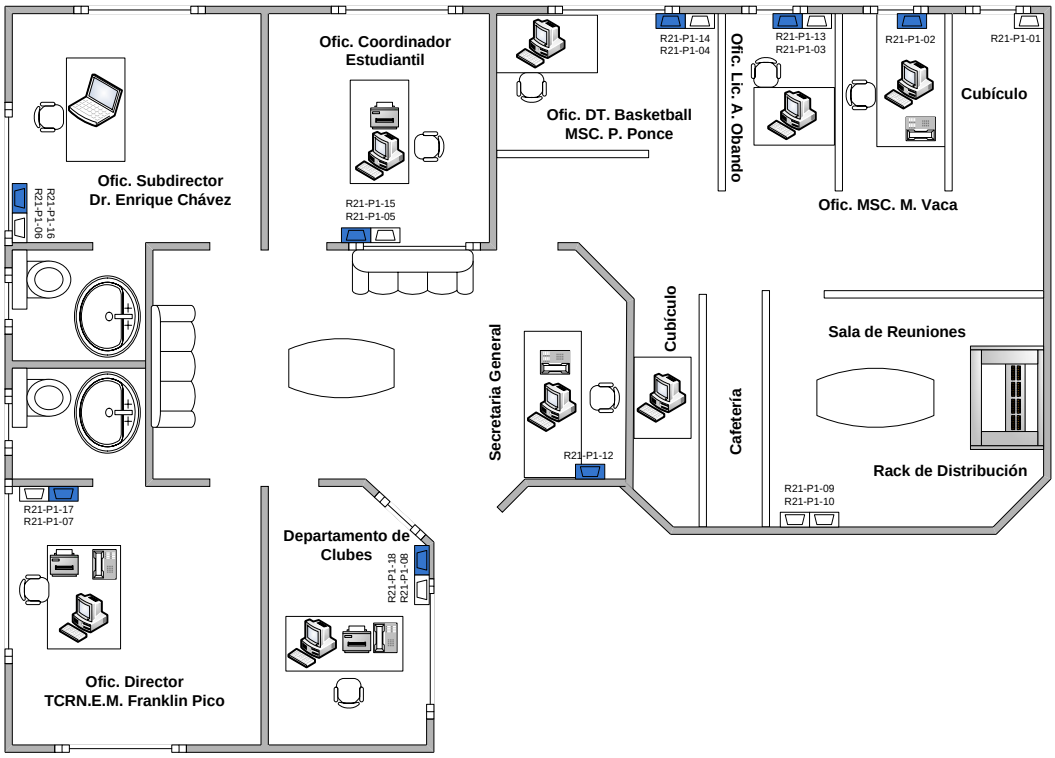


Figura. 2.3. Diagrama estructural y ubicación física de los puntos existentes en el Bloque CAFDER.

2.2.3 Análisis de los equipos existentes

- **Rack N°21**

Se encuentra equipado con:

- 1 Switch 3COM 10/100 Base-Tx 4500 50port
- 2 Convertidores de fibra óptica d-link DMC-300SL
- 1 Bandeja de fibra óptica
- 2 fatch panel de 24 puertos c/u

Figura. 2.4. Ubicación del Rack Nº21 en el Bloque CAFDER

- **Switch 3com 10/100 base-Tx 4500 50port**

El *Switch 3COM 4500* de las características gestionados, apilables y agrupable *switches* 10/100 Ethernet proporciona conectividad de LAN segura y flexible de servicios avanzados de voz optimizados tales como *PoE* y *Auto-Voice VLAN* y QoS.

Ofrece conmutación *Layer 2* y *Layer 3* de enrutamiento dinámico, así como una seguridad robusta, Calidad de Servicio *(QoS)* y gestión para ofrecer conectividad de extremo inteligente para las aplicaciones empresariales esenciales.

El 3Com *Switch* 4500 50-Port dispone de 48 puertos 10/100 y dos puertos *Gigabit* de doble personalidad. Cada puerto *Gigabit* ofrece una selección de cobre o de fibra de medios: 1000BASE-T (mediante RJ45) o 1000BASE-X (a través de facultativos "SFP", factor de forma pequeño conectable transceptores). Además, el 3Com *Switch* 4500 50-Port es el encargado de la distribución de los diferentes puertos del *fatch panel*.

Las diferentes VLANS del *Switch* se describen a continuación:

- [4500] *display* VLAN
  - *The following* VLANs *exist*:
  - 1(*default*), 5, 7-9, 50, 415

- Puertos del 1 al 46, son puertos híbridos
  - híbrido VLAN 50 *tagged*
  - híbrido VLAN 1 415 *untagged*

- híbrido pvid VLAN 415

♦ Puerto 48 Enlace a Construcciones

- Puerto Trunk
- Permite VLAN 1 7 50 415

♦ Puerto 49

- Puerto Trunk
- Permite vlan 1 7 50 415

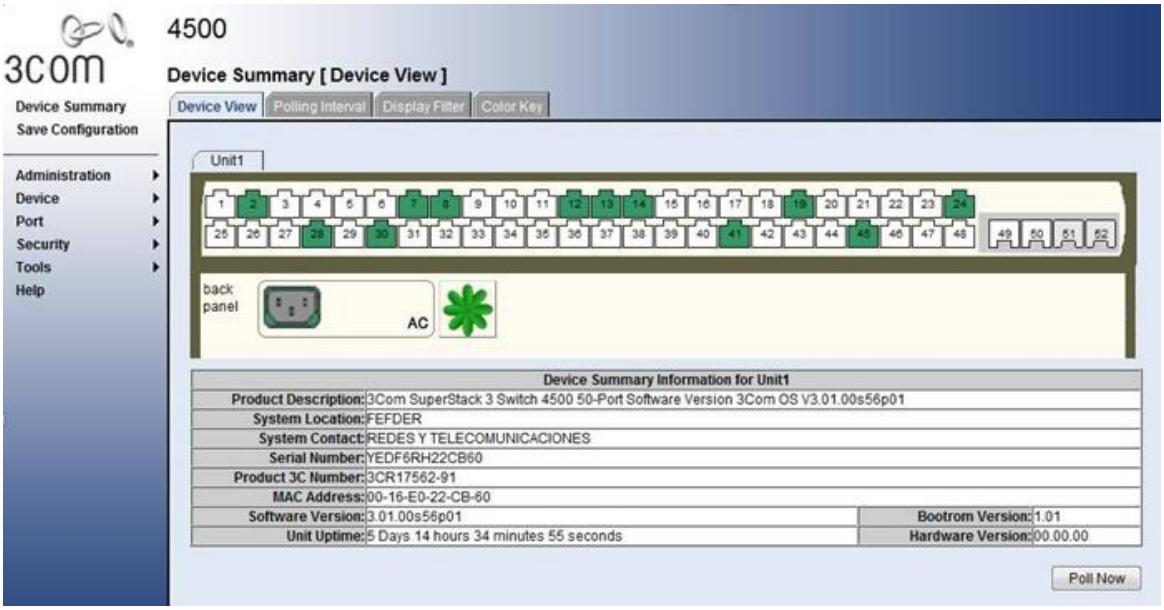


Figura. 2.5. Configuración del Switch de la marca 3COM ubicado en el Bloque CAFDER

➢ Convertidores de fibra óptica d-link dmc-300sl

Dispositivos especialmente diseñados para proveer una conversión de medios de comunicación para el estándar Fast Ethernet; desde un cable de cobre UTP 100BASE-TX a cable de fibra óptica 100BASE-FX multimodo, la distancia máxima para el cable de fibra óptica es de 2Km.

Estos conversores posibilitan la conexión de dispositivos 100BASE-TX sobre diferentes estaciones departamentales o en edificios separados, de tal manera de poder extender los cables UTP (dada la limitación de éstos, de 100mts de distancia).

De la fibra óptica que llega a la bandeja de fibra con un cable de red de fibra se realiza el bridge hacia los convertidores, y del puerto *Ethernet* va hacia el *Switch;* el mismo que es el encargado de distribuir hacia el *fatch panel* y este a su vez a los puntos de red.

- **Bandeja de fibra óptica**

La bandeja está provista por conectores ST, en la cual se encuentran ponchados los 8 hilos de fibra que llegan al rack.

- ***Fatch panel* de 24 puertos**

A cada uno de estos se encuentra ponchado cables UTP, los mismos que tienen ponchados Jacks para ser puntos de red ya descritos anteriormente.

Todos los equipos mencionados, tanto el convertidor como el *Switch,* se encuentran ubicados en el *rack* N° 21

2.3 ESTUDIO DEL TRÁFICO ACTUAL

2.3.1 Herramientas a utilizar. Descripción

El equipo a utilizar en el análisis es el *SUNSET MTT BASIC COLOR SA942 de Sunrise Telecom.*

- ***Sunset MTT (Modular Test Toolkit) (datasheets).***

"La computadora de mano Sunset MTT proporciona a los técnicos de campo selecciones más amplias de sector, con opciones de prueba necesarias para instalar, comprobar y solucionar problemas de una gran variedad de tecnologías de servicios" [1]

[1] Sunset MTT, http://www.sunrisetelecom.com/products/mtt.php, Enero 2010

*"*La familia SunSet MTT se compone de varias configuraciones de chasis que le permite adaptar a sus necesidades de pruebas y de presupuesto. El SunSet MTT ACM (Advanced Cable de mantenimiento) ofrece una poderosa combinación de mantenimiento de cable y las pruebas de verificación de servicios, junto con una pantalla a color de alta resolución.*"*[2]

"Un mayor despliegue de banda ancha a hogares y empresas, junto con las tecnologías más rápidas y básicas, están impulsando la demanda de Metropolitan Ethernet y servicios de almacenamiento. Hay una gran necesidad de implementar y optimizar las redes metro, rápida y económica. Sunset MTT satisface esta necesidad, con los módulos de prueba para Ethernet, Gigabit Ethernet y Fiber Channel, el Sunset MTT proporciona una plataforma rentable para la realización de cualquier tipo de pruebas. "[3]

"La amplia gama de plug-in de módulos de interfaz permite a un ingeniero con una unidad de MTT hacer frente a una amplia gama de aplicaciones de pruebas, y solucionar los problemas en múltiples niveles."[4]

La Figura 2.6, muestra los equipos SunSet MTT, con diferentes módulos

Figura. 2.6. Equipo SunSet MTTcon sus diferentes módulos

[2]Sunset MTT, http://www.sunrisetelecom.com/products/mtt.php, Enero 2010
[3] Sunset MTT, http://www.sunrisetelecom.com/products/mtt.php, Enero 2010
[4]Sunset MTT, http://www.sunrisetelecom.com/products/mtt.php, Enero 2010

"El módulo Ethernet MTT es una poderosa herramienta para la instalación de servicios y mantenimiento; ofreciendo a los puertos duales monitoreo en vivo, bidireccional de rendimiento de la red y la conformidad con los Acuerdos de Nivel de Servicio. Además, BERT simultánea y pruebas de bucle invertido en un solo módulo permite la calificación eficiente de los dispositivos de red; IP BER / rendimiento, ping, y rastrear las pruebas de ruta son ideales para la capa de control de redes enrutadas".

10/100BASE-T puertos dual con puerto 100BASE-FX opcional Capa de 1 / 2 / REC / rendimiento de los ensayos a plena velocidad de cable con el tráfico y la configuración de longitud de image definidos por el usuario MAC / IP / VLAN, para hasta cuatro *streams* simultáneos.

Característica de bucle invertido automática a través del modo de bidireccional, en el servicio de vigilancia de RFC 2544, VLAN de exploración, barrido de ancho de banda, y las pruebas de retardo de ida y vuelta."[5]

2.3.2 Pruebas a realizar

- **Terminología según RFC 1242 y RFC 2544**

La RFC 2544 discute y define un número de pruebas que pueden ser utilizadas para describir y comparar las características de performance de dispositivos de interconexión de redes. Asimismo describe los formatos para el reporte de los resultados de las pruebas.

Las pruebas a realizarse dentro de la red actual del bloque son:

- Throughput
- Latency
- Frame loss rate
- Back-to-back frames

Antes de realizar las respectivas pruebas, surge la necesidad de aclarar ciertos conceptos acerca de cada una de las mediciones que se realizarán dentro de la red.

[5]Sunset MTT, http://www.sunrisetelecom.com/products/mtt.php, Enero 2010

2.3.3 Mediciones de retardo

- **Latency (Latencia) definición (RFC 1242 ítem 3.8)**

Se define a la latencia, como el intervalo de tiempo comenzando cuando el final del primer bit de la trama entrante alcanza el puerto de entrada y terminando cuando el comienzo del primer bit de la misma trama es visto en el puerto de salida.

La variabilidad de la latencia cambia para algunos protocolos (por ejemplo, LAT y IPX) puesto que estos son dependientes de ciertas medidas de tiempo. Este retraso en los dispositivos puede reducir el ancho de banda útil de la red. Se desea eliminar el efecto de la velocidad de datos sobre la medición de la latencia; esta medida sólo debe reflejar la actual latencia del dispositivo y las mediciones deben ser tomadas por un espectro de tamaños de tramas sin cambiar la configuración del dispositivo.

Idealmente, las mediciones para todos los dispositivos serían desde el primer bit actual de la trama después del preámbulo.

- **Unidades de medida**

Tiempo en unidades suficientemente buenas para distinguir entre 2 eventos, apropiadamente milisegundos. Para redes *Ethernet* los tiempos de la latencia tienen que ser menores a 100 ms para que exista un correcto desempeño y funcionamiento de la red.

2.3.4 Mediciones de *Troughput*

- **Throughput (Rendimiento). Definición (RFC 1242 ítem 3.17)**

Se llama *throughput* al volumen de trabajo o de información que fluye a través de un sistema. Así también, se le llama al volumen de información que fluye en las redes de datos.

En las redes de comunicación, tales como *Ethernet* o de radio por paquetes, el rendimiento o el rendimiento de la red es la tasa promedio de éxito de la entrega de mensajes en un canal de comunicación. Estos datos pueden ser prestados a través de un enlace físico o lógico, o pasar a través de un nodo de red segura. El rendimiento suele medirse en bits por segundo (bit / s o bps).

El rendimiento del sistema o en el rendimiento global es la suma de los tipos de datos que se entregan a todas las terminales de una red. El rendimiento es esencialmente sinónimo de consumo de ancho de banda digital.

La cifra de rendimiento o *Throughput* permite a los proveedores un informe de único valor que ha demostrado tener uso en él, puesto que incluso la pérdida de una trama en un flujo de datos puede causar retrasos significativos. Es útil conocer la tasa máxima de datos reales que un dispositivo puede soportar, las mediciones deben realizarse con diferentes tamaños de trama.

- **Unidades de medida**

Las unidades de medida son:

- N-octetos de tramas de entrada por segundo
- Bits de entrada por segundo
- Porcentaje (%)

2.3.5 Medición de tráfico y tramas

♦ **Frame Loss Rate (tasa de tramas perdidas) Definición (RFC 1242 ítem 3.6)**

Porcentaje de tramas que deberían ser enviadas (*forwarded*) por un dispositivo de red bajo estado estacionario de carga (constante) pero no son enviadas (*forwarded*) por la falta de recursos.

Esta medición puede ser utilizada en la presentación de informes de rendimiento de un dispositivo de red en un estado de sobrecargas. Esto puede ser una indicación útil de cómo un dispositivo funcionaría dentro de la red en condiciones patológicas tales como las tormentas de difusión.

Las unidades de medición para las tramas de paquetes perdidas son en porcentaje de acuerdo a la tasa de transmisión.

♦ **Back-to-back frames Definición (RFC 1242 ítem 3.1)**

Tramas de un mismo largo; enviadas a una tasa para la cual hay una separación legalmente mínima entre tramas, para un medio dado, durante un período de tiempo, comenzando desde el estado inactivo (*idle time*).

Un creciente número de dispositivos dentro de una red puede producir ráfagas de *back-to-back frames*, esto se traduce en que existirán muchos fragmentos para ser transmitidos. La pérdida de un solo fragmento debido a la incapacidad de algunos dispositivos intermediarios de red para procesar suficientes tramas continuas puede provocar un bucle sin fin, puesto que el remitente realizará repetitivamente intentos de enviar sus datos en un bloque de gran tamaño.

Con el aumento de tamaño de la red de Internet, el enrutamiento de tramas se ha actualizado en los *routers* modernos, que ahora son capaces de transmitir grandes cantidades de información con gran rapidez. La falta de información de ruteo puede producir falsas indicaciones de inaccesibilidad.

- **Unidades de medida**

Número de N-octetos de tramas en ráfagas.

2.3.6 Análisis de resultados obtenidos

Para realizar el análisis de tráfico de la red se procedió a la captura de tráfico de datos dentro de la red actual de la CAFDER mediante la utilización del equipo *Sunset* MTT (*Modular Test Toolkit*) el cual mediante un *loopback* permite medir varios parámetros como son: el *Throughput*, latencia, *Frame loss Rate* y *back –to- back frames*.

Para realizar esta medición, se escogieron varios puntos de red para realizar los mismas, puesto que con esto se podría analizar por completo la red, y ciertos días específicos los cuales nos ayudarán a obtener un resultado claro acerca del estado actual de la red.

Cabe resaltar que entre los días escogidos para las mediciones se eligió uno de los días (primer día) de la semana de matrículas puesto que en estos días el tráfico de la red es mayor, y con estas mediciones se lograría realizar un mejor análisis.

Se realizó el análisis de 5 días; debido a la gran cantidad de información capturada y analizada se presenta a continuación el análisis de la captura de tráfico de un día, cabe resaltar que el análisis de los demás resultados obtenidos se encuentra en el ANEXO 2.

2.3.6.1 Throughput

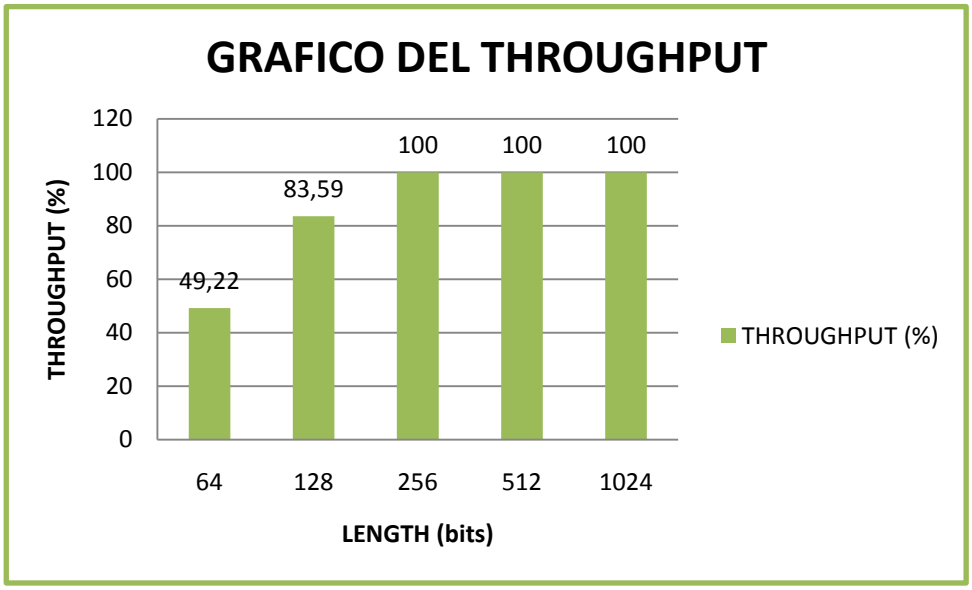


Figura. 2.7. Gráfica de medición de *Throughput* Vrs la Longitud de paquetes para el quinto día de medición

De igual manera, se realizaron las mediciones de *Throughput* en un día fuera de matrículas encontrando buenos resultados como lo muestran la Figura 2.7, se observa datos obtenidos para tramas de 1024 bits en donde el *Throughput* es el máximo alcanzado del 100%, el cual representa el buen desempeño de la red.

2.3.6.2 Latencia

Tabla. 2.2. Resultados de medición de Latencia para longitudes de 64, 128, 256, 512 y 1024 bits para el quinto día de medición

LENGTH	RATE (%)	LATENCY (msec)
64	49.22	21,475
128	83.59	21,475
256	100.00	21,475

512	100.00	21,475
1024	100.00	21,475

La Tabla 2.2., muestra los resultados de latencia los cuales indican que las tramas están siendo enviadas en los tiempos adecuados.

2.3.6.3 Pérdida de tramas

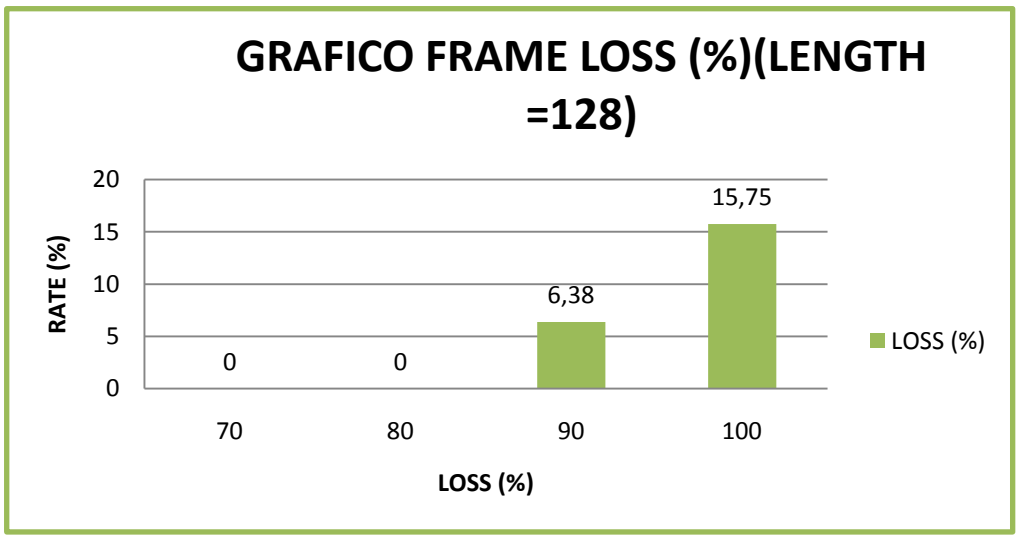


Figura. 2.8. Gráfica de medición de Pérdidas de tramas para longitudes de paquetes de 128 bits para el quinto día de medición

Los datos que se obtuvieron indican que existen mínimas pérdidas de paquetes para las diferentes longitudes de tramas, como es el caso de la medición realizada para una longitud de trama de 1024 bits en donde existen 0% de pérdidas, lo cual ratifica que la red está totalmente descongestionada y con un correcto funcionamiento.

2.3.6.4 Back to back frames

Tabla 2.3. Resultados de medición de *back to back frames* para longitudes de 64, 128, 256, 512 y 1024 bits para el quinto día de medición

LENGTH	64	128	256	512	1024
MIN	1488095	84459	452898	234962	119731
MAX	1488095	84459	452898	234962	119731

AVG	1488095	84459	452898	234962	119731

Como se puede observar en los resultados obtenidos en la Tabla 2.3 se puede concluir que los valores de número de ráfagas que se obtuvieron se encuentran dentro del rango permitido para el tipo de tráfico que se está analizando en la red, puesto que todo el porcentaje de tráfico se está recibiendo al 100% de las ráfagas transmitidas para las diferentes longitudes de tramas.

Después de todos los datos obtenidos se observa que sobre la red cableada se puede implementar una solución inalámbrica para el CAFDER.

CAPÍTULO III

SEGURIDAD EN REDES INALÁMBRICAS

3.1 INTRODUCCIÓN A LA SEGURIDAD EN REDES INALÁMBRICAS

La falta de seguridad en las redes inalámbricas es un problema que, a pesar de su gravedad, no ha recibido la atención debida por parte de los administradores de redes y los responsables de la información.

Lo que se pretende en este estudio, es presentar las diferentes tecnologías existentes para mejorar el nivel de seguridad en las redes inalámbricas 802.11, con sus ventajas, desventajas y los respectivos ámbitos de aplicación. El acceso sin necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere.

Cualquier equipo que se encuentre a 100 metros o menos de un punto de acceso, podría tener acceso a la red inalámbrica. Un ejemplo simple, si suponemos que varias empresas tienen sede en un mismo edificio, y todas ellas poseen red inalámbrica, el equipo de un empleado podría encontrarse en cierto momento en el área de influencia de dos o más redes diferentes, y dicho empleado podría conectarse (intencionalmente o no) a la red de una compañía que no es la suya, en la Figura 3.1 se puede apreciar el ejemplo planteado.

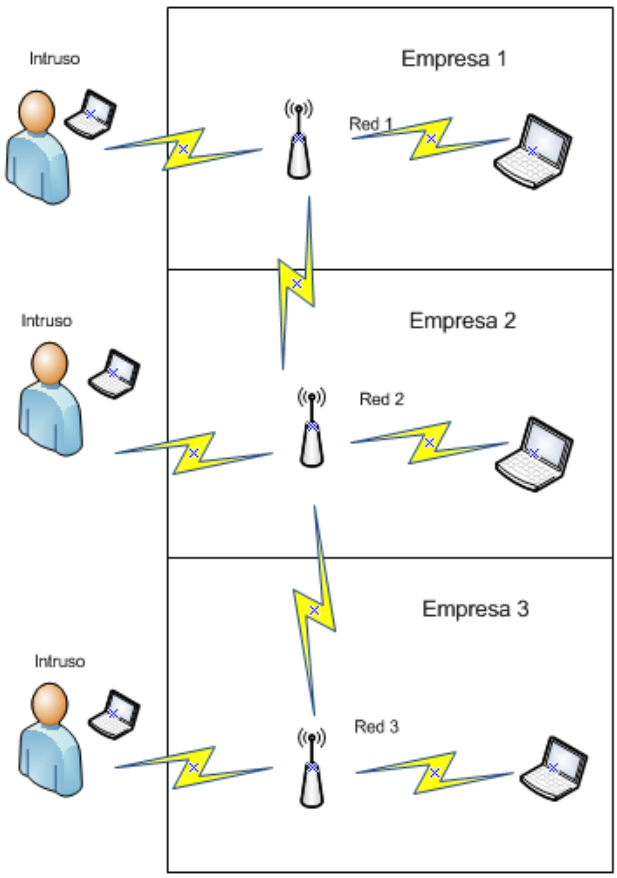


Figura. 3.1. Acceso no autorizado a red inalámbrica

Aún peor, como las ondas de radio pueden salir del edificio, cualquier persona que posea un equipo móvil y entre en el área de influencia de la red, podría conectarse a la red de la empresa, y esto si sería un gran problema, por estas razones se han desarrollado tecnologías de seguridad para este tipo de redes.

3.2 ASPECTORS REALTIVOS A LA SEGURIDAD

Por las características de la tecnología inalámbrica, sabemos que ésta posee una serie de puntos débiles y ataques característicos a nivel de seguridad que es importante conocer.

Por un lado; se encuentra la característica de facilitar la rápida generalización de este tipo de tecnología entre los usuarios y evitar en lo posible la carga del soporte, se implantan soluciones con configuraciones de arranque en el que prácticamente todas las medidas de seguridad están deshabilitadas: dispositivos cliente que se activan de manera automática, una WLAN (*Wireless* LAN) operativa, software que el cliente detecta y conecta de manera automática con una WLAN, etc.; y por otra parte, los límites del medio

de transmisión resultan difusos y que se extienden más allá de lo que puede, en muchos casos, ser controlado

3.2.1 WIFI sin proteger

Existen una serie de ideas generalizadas respecto a la seguridad de los sistemas en general, y perfectamente aplicable a las redes WIFI, que suelen resultar fatales a corto o mediano plazo, tales como: "nadie conoce el sistema", o "nadie tiene interés en el sistema", así pues ¿para qué gastar recursos y tiempo en protegerlo?.

Por desgracia, la experiencia demuestra que ninguno de los dos razonamientos resulta cierto, y que efectivamente hay más personas de las que en un principio parece que conocen de la existencia de ese sistema, y además, tienen intereses en él. Las consecuencias más comunes de ataques a redes WIFI son:

- *Consumo de ancho de banda*: Resulta sorprendentemente sencillo conseguir una conexión a una de las muchas redes inalámbricas desprotegidas, y sólo un poco más difícil a alguna de las protegidas con algún tipo de medida mínima; como consecuencia de este tipo de acceso no autorizado, el ancho de banda de las correspondientes redes WIFI se ve claramente mermado, más aún si éstas son utilizadas como medio de acceso a conexiones de tipo ADSL, cable módem, etc.

- *Acceso no autorizado a equipos*: En general, las protecciones frente a equipos externos a la red local suelen ser más fuertes que aquellas que se aplican frente a equipos que pertenecen a la misma red local.

  De ahí, que en el momento que un equipo no autorizado se conecta a la red inalámbrica, los equipos que se encuentran conectados a dicha red y los que se encuentran en la misma LAN, suelen ser muy vulnerables. Las consecuencias de un acceso no autorizado a un equipo, puede provocar: robo o destrucción de datos almacenados en dicho equipo, el robo de claves y contraseñas de acceso a cuentas bancarias, certificados personales, etc.

- *Responsabilidades legales*: Como se ha comentado anteriormente, la intrusión en la red inalámbrica suele ser mucho más vulnerables a los equipos de esa misma LAN, lo que facilita el acceso no autorizado. A partir de aquí, un equipo atacado puede servir como

equipo atacante de sistemas remotos, esto podría dar lugar a responsabilidades legales si se considera que el propietario de la red WIFI o la persona que la ha instalado lo ha hecho de manera descontrolada y sin tener en cuenta ningún tipo de medida de seguridad preventiva.

3.2.2 Problemas de seguridad

Es muy común encontrar redes en las que el acceso a internet se protege adecuadamente con un firewall bien configurado, pero al interior de la red existen puntos de acceso inalámbrico totalmente desprotegidos e irradiando señal hacia el exterior del edificio.

Cualquier persona 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 el internet, emplear la red de la compañía como punto de ataque hacia otras redes y luego desconectarse para no ser detectado, robar software y/o información, introducir virus o software maligno, entre muchas otras cosas.

Un punto de acceso inalámbrico mal configurado se convierte en una puerta trasera que vulnera por completo la seguridad informática de la compañía. La mala configuración de un acceso inalámbrico es, desgraciadamente, una cosa muy común. Existen dos prácticas bien conocidas para localizar redes inalámbricas, como son:

- ***Warchalking***[1]

Este método consiste en caminar por la calle con un computador portátil dotado de una tarjeta WLAN, buscando la señal de puntos de acceso. Cuando se encuentra uno, se pinta con tiza un símbolo especial en la acera o en un muro, indicando la presencia del punto de acceso y si tiene configurado algún tipo de seguridad o no. De este modo, otras personas pueden conocer la localización de la red.

La Figura 3.2., muestra varios de los símbolos aplicados con este método de detección de señales de redes inalámbricas.

[1] Es el dibujo de símbolos en espacios públicos para advertir acerca de redes inalámbricas Wi-Fi

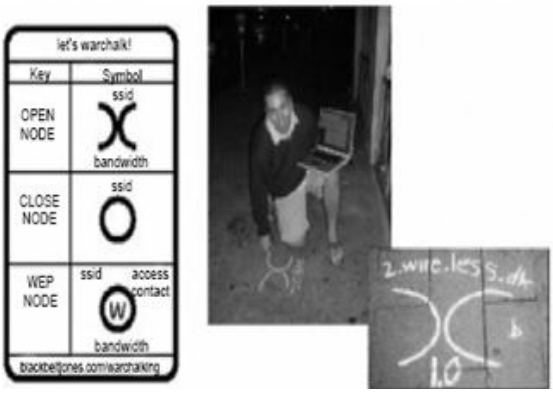


Figura. 3.2. Warchalking y su simbología[2]

- ***Wardriving*** [3]

Este método es el mejor para localizar puntos de acceso inalámbrico desde un automóvil. Para este fin se necesita de un computador portátil con una tarjeta WLAN, una antena adecuada (que se puede elaborar fácilmente con una lata de conservas o de papas fritas), un GPS para localizar los puntos de acceso en un mapa, y software para detección de redes inalámbricas, que se consigue libremente en internet. La Figura 3.3a y 3.3 b muestra claros ejemplos de *Wardriving.*

a) b)

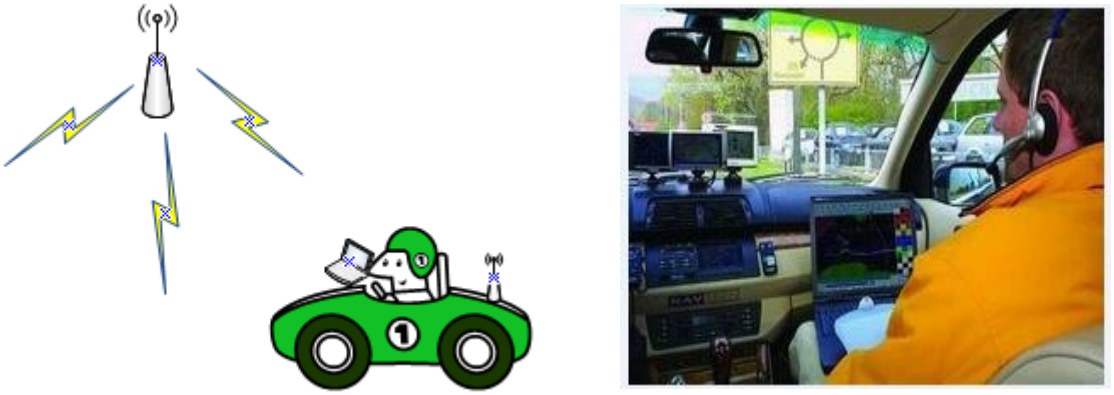


Figura. 3.3. a) Wardriving b) Accesorios utilizados en la detección

[2] Andrew A. Vladimir Konstantin V. Gavrilenko. "Hacking Wireless – Seguridad de Redes Inalámbricas". Anaya Multimedia (2005). ISBN:84-415-1789-4, Febrero 2010

[3] Se le llama así a la búsqueda de redes inalámbricas Wi-Fi desde un vehículo en movimiento

Una vez localizada una red inalámbrica, una persona podría llevar a cabo dos tipos de ataques:

- Ingresar a la red y hacer uso ilegítimo de sus recursos.
- Configurar un punto de acceso propio, orientando la antena de tal modo que los computadores que son clientes legítimos de la red atacada, se conecten a la red del atacante.

Una vez hecho esto, el atacante podría robar la información de dichos computadores, instalarles software maligno o dañar la información.

3.3 MECANISMOS DE SEGURIDAD

Para poder considerar una red inalámbrica como segura, ésta debe cumplir los siguientes requisitos:

- Las ondas de radio deben confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.

- Debe existir algún mecanismo de autenticación[4] en doble vía; que permita al cliente verificar que se está conectando a la red correcta, y a la red, constatar que el cliente está autorizado para acceder a ella.

- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

Existen varios métodos para lograr la configuración segura de una red inalámbrica; cada método logra un nivel diferente de seguridad y presenta ciertas ventajas y desventajas, a continuación una explicación de cada uno de ellos.

[4] Hace referencia a la identificación del usuario de la red

3.3.1 Filtrado de direcciones MAC [5]

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica.

La tabla contiene las direcciones MAC (*Media Access Control*) de las tarjetas de red inalámbrica que se conectan al punto de acceso, como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo. Este método tiene como ventaja su sencillez, por lo que se puede usar en redes caseras o pequeñas, sin embargo, posee muchas desventajas que lo hacen poco práctico para uso en redes medianas o grandes; como son:

- No escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso.
- Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.
- El formato de una dirección MAC no es amigable (normalmente se escriben como 6 bytes en hexadecimal), lo que puede llevar a cometer errores en la manipulación de las listas.
- Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un *sniffer*[6], y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, empleando programas tales como *AirJack*[7] o *WellenReiter*[8], entre otros. De este modo, el atacante puede hacerse pasar por un cliente válido.
- 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, porque el punto de acceso contiene toda la tabla de direcciones válidas en su memoria de configuración.

Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida, ya que no prevé ningún mecanismo de cifrado.

[5] Control de acceso de medios

[6] Es un programa de captura de las tramas de de red
[7] *AirJack*: http://802.11ninja.net/airjack/, Febrero 2010
[8] *Wellenreiter* – WLAN Hacking. http://www.wellenreiter.net/, Febrero 2010

3.3.2 Wired Equivalent Privacy (WEP)

El algoritmo WEP[9] 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.

El cifrado que realiza el algoritmo WEP, se realiza como lo muestra la Figura 3.4

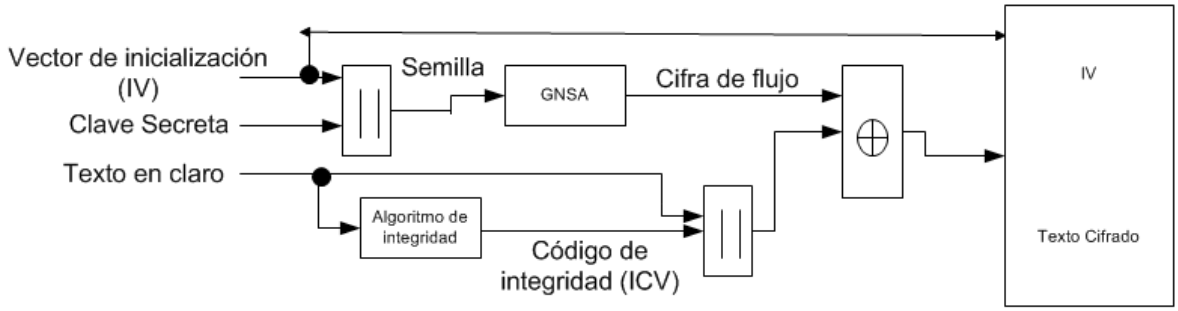


Figura. 3.4. Funcionamiento del algoritmo WEP en modalidad de cifrado[10]

A la trama en claro; se le computa un código de integridad ICV (*Integrity Check Value*) mediante el algoritmo CRC-32[11], dicho ICV se concatena con la trama, y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.

Se escoge una clave secreta compartida entre emisor y receptor, esta clave puede poseer 40 ó 128 bits. Si se empleará siempre la misma clave secreta para cifrar todas las tramas, dos tramas en claro iguales producirían tramas cifradas similares; para evitar esta eventualidad, se concatena la clave secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits. El IV cambia con cada trama.

La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4 de números pseudo-aleatorios. El generador RC4 es capaz de generar una secuencia pseudo aleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.

---

[9] WEPCrack Project Info, http://sourceforge.net/projects/wepcrack, Febrero 2010

[10] Authentication and Privacy En ANSI / IEEE Standard 802.11, 1999 Edition, http://standards.ieee.org/getieee802/download/802.11-1999pdf 59- 68 pp, Febrero 2010

[11] Comprobación de redundancia cíclica, tipo de función que recibe flujo de datos como entrada y devuelve un valor de longitud fija como salida

El generador RC4 genera una 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 hace un XOR bit por bit de la trama con la secuencia de clave, obteniéndose como resultado la trama cifrada. El IV y la trama se transmiten juntos.

En el receptor se lleva a cabo el proceso de descifrado, la Figura 3.5., muestra el funcionamiento del algoritmo WEP de descifrado.

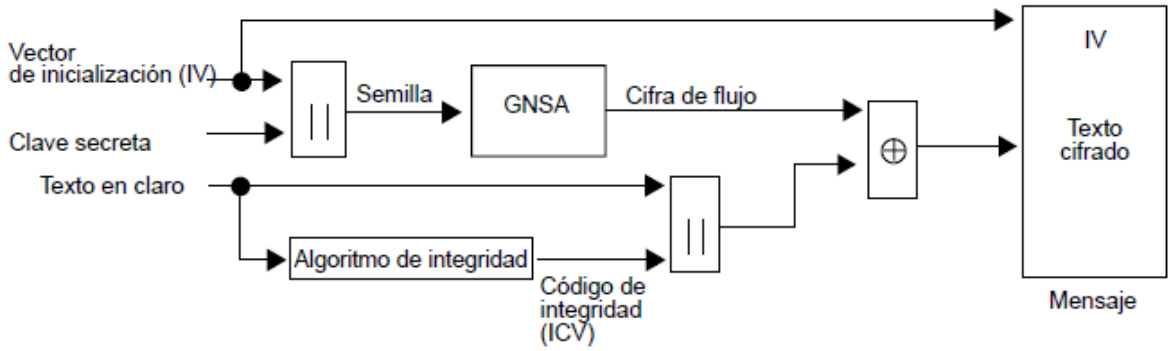


Figura. 3.5. Funcionamiento del Algoritmo WEP en modo de descifrado[12]

Para la realizar la función de descifrado, este algoritmo realiza es lo siguiente:

Se emplean el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor. Un generador RC4 produce la cifra de flujo a partir de la semilla; si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será idéntica a la usada en la transmisión. Se efectúa un XOR bit por bit de la cifra de flujo y la trama cifrado, obteniéndose de esta manera la trama en claro y el ICV. A la trama en claro se le aplica el algoritmo CRC-32 para obtener un segundo ICV, que se compara con el recibido; si los dos ICV son iguales, la trama se acepta; caso contrario se rechaza.

El algoritmo WEP resuelve aparentemente el problema del cifrado de datos entre emisor y receptor. Sin embargo, existen dos situaciones que hacen que WEP no sea seguro en la manera que es empleado en la mayoría de aplicaciones; dichas situaciones se indican a continuación:

- Primero; en la mayoría de instalaciones se emplea WEP con claves de cifrado estáticas (se configura una clave en el punto de acceso y no se la cambia nunca, o muy de vez en

[12] *Authentication and Privacy*, En ANSI/IEEE *Standard* 802.11,1999 *Edition*, http://standards.ieee.org/getieee802/download/802.11-1999.pdf, 59- 68 pp, Febrero 2010.

cuando), esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque por fuerza bruta.

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 224 IV distintos.

Esto no es problemático en una red casera 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.

- La segunda; es que WEP no ofrece servicio de autenticación es decir, el cliente no puede autenticar a la red, ni al contrario; basta con que el equipo móvil y el punto de acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo.

  Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP.

3.3.3 VPN

Una red privada virtual (*Virtual Private Network*, VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público.

Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP, para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir 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 adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea *switching*;

dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN.

Además; deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado. La Figura 3.6., se muestra la estructura de una VPN para acceso inalámbrico seguro.

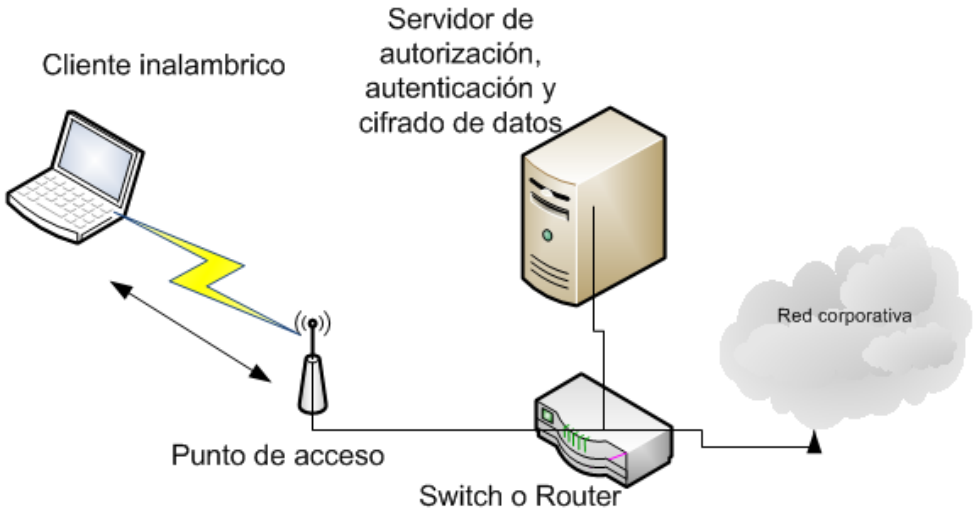


Figura. 3.6. Estructura de una VPN para acceso inalámbrico seguro[13]

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP en este esquema.

3.3.4 802.1x[14]

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red. El protocolo fue inicialmente creado por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x, el protocolo 802.1x involucra tres participantes; como se puede observar en la Figura 3.7.

[13] Autor, Arce, Cristian, Febrero 2010
[14] Norma de la IEEE para control de acceso a red basado en puertos

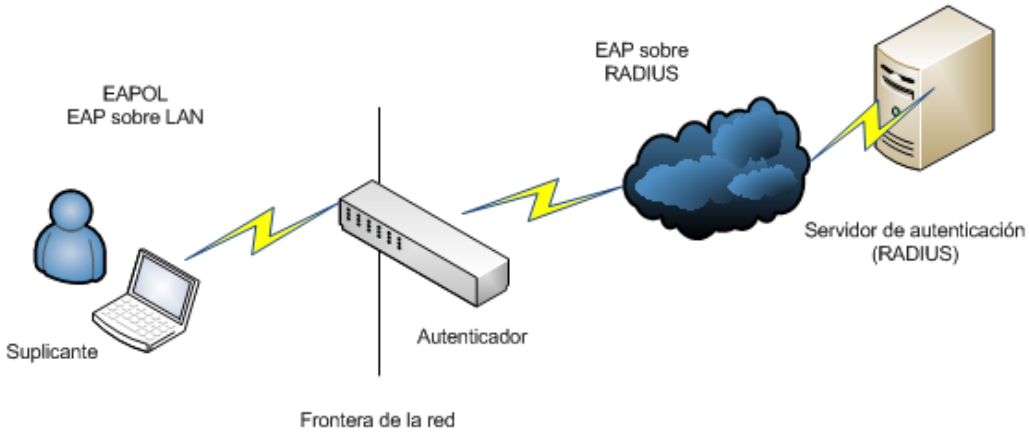


Figura. 3.7. Arquitectura de un sistema de autenticación 802.1x[15]

El servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios se encuentran autorizados para acceder a la red. En un principio 802.1x fue diseñado para emplear servidores RADIUS[16], cuya especificación se puede consultar en la RFC 2058[17].

Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autenticación en las LAN. El autenticador, que es el equipo de red (*switch*, enrutador, servidor de acceso remoto...) recibe la conexión del suplicante.

El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza. La autenticación del cliente se lleva a cabo mediante el protocolo EAP[18] (*Extensible Authentication Protocol*) y el servicio RADIUS, de la siguiente manera:

El proceso inicia cuando la estación de trabajo se enciende y activa su interfaz de red (en el caso alámbrico) o logra enlazarse o asociarse con un punto de acceso (en el caso inalámbrico). En ese momento, la interfaz de red tiene el acceso bloqueado para tráfico

[15] Congdon, Paul, IEEE 802.1x Overview Port Based Network Access Control, http://www.ieee802.org/1/files/public/docs2000/P8021XOverview.PDF, Marzo de 2000, Febrero 2010
[16] Remote Authentication Dial-In User Server
[17] Remote Authentication Dial in User Service (RADIUS), http://www.faqs.org/rfcs/rfc2058.html, Febrero 2010
[15] IEC EAP Methods for 802.11 Wireless LAN Security, http:// www.iec.org/online/tutorials/ acrobat/eap_methods.pdf, Febrero 2010

normal, y lo único que admite es el tráfico EAPOL (EAP *over* LAN)[19], que es el requerido para efectuar la autenticación.

La estación de trabajo envía un mensaje EAPOL-*Start*[20] al autenticador, indicando que desea iniciar el proceso de autenticación, el autenticador solicita a la estación que se identifique, mediante un mensaje EAP-*Request/ Identity*[21]. La estación se identifica mediante un mensaje EAP-*Response/ Identity*.

Una vez recibida la información de identidad, el autenticador envía un mensaje RADIUS-*Access- Request*[22] al servidor de autenticación, y le pasa los datos básicos de identificación del cliente, el servidor de autenticación responde con un mensaje RADIUS-*Access- Challenge*[23], en el cual envía información de un desafío que debe ser correctamente resuelto por el cliente para lograr el acceso, dicho desafío puede ser tan sencillo como una contraseña, o involucrar una función criptográfica más elaborada. El autenticador envía el desafío al cliente en un mensaje EAP-*Reques*[24]*t*.

El cliente da respuesta al desafío mediante un mensaje EAP-Response (*Credentials*)[25] dirigido al autenticador. Este último reenvía el desafío al servidor en un mensaje RADIUS-*Access-Response*[26].

Si toda la información de autenticación es correcta, el servidor envía al autenticador un mensaje RADIUS-*Access-Accep*[27]*t*, que autoriza al autenticador otorgar acceso completo al cliente sobre el puerto, además de brindar la información inicial necesaria para efectuar la conexión a la red. El autenticador envía un mensaje EAP-*Success*[28] al cliente, y abre el puerto de acuerdo con las instrucciones del servidor RADIUS. En la Figura 3.8 se muestra el dialogo EAPOL-RADIUS utilizado para la tecnología 802.1x.

[19] Remote Authentication Dial in User Service (RADIUS), http://www.faqs.org/rfcs/rfc2058.html, Febrero 2010
[20] Remote Authentication Dial in User Service (RADIUS), http://www.faqs.org/rfcs/rfc2058.html, Febrero 2010
[21] Remote Authentication Dial in User Service (RADIUS), http://www.faqs.org/rfcs/rfc2058.html, Febrero 2010
[22] Remote Authentication Dial in User Service (RADIUS), http://www.faqs.org/rfcs/rfc2058.html, Febrero 2010
[23] Remote Authentication Dial in User Service (RADIUS), http://www.faqs.org/rfcs/rfc2058.html, Febrero 2010
[20] Remote Authentication Dial in User Service (RADIUS), http://www.faqs.org/rfcs/rfc2058.html, Febrero 2010
[25] Remote Authentication Dial in User Service (RADIUS), http://www.faqs.org/rfcs/rfc2058.html, Febrero 2010
[26] Remote Authentication Dial in User Service (RADIUS), http://www.faqs.org/rfcs/rfc2058.html, Febrero 2010
[27] Remote Authentication Dial in User Service (RADIUS), http://www.faqs.org/rfcs/rfc2058.html, Febrero 2010
[28] Remote Authentication Dial in User Service (RADIUS), http://www.faqs.org/rfcs/rfc2058.html, Febrero 2010

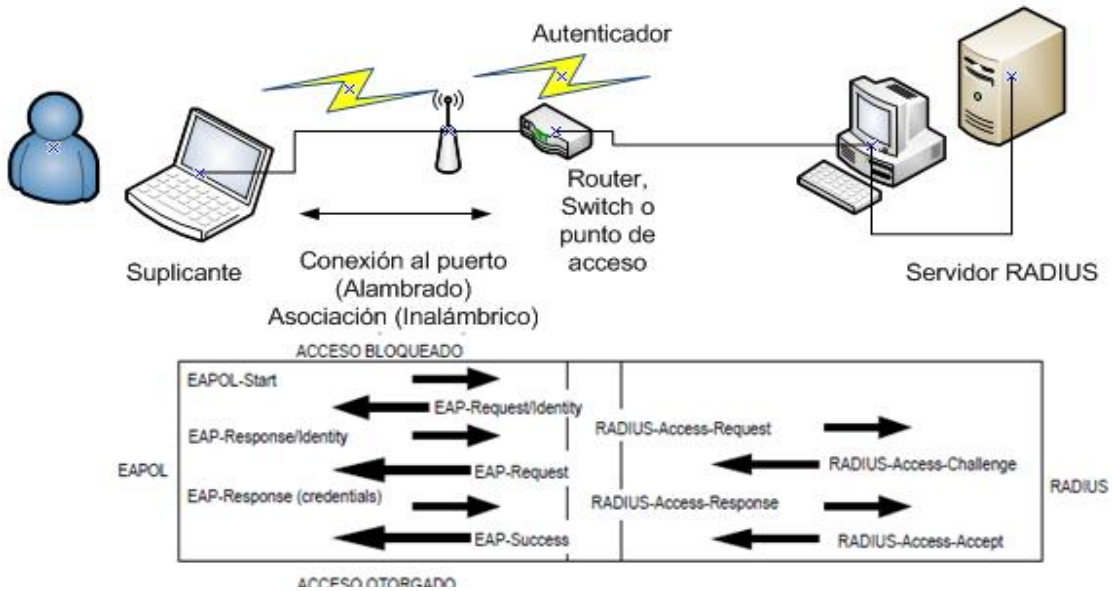


Figura. 3.8. Dialogo EAOPOL-RADIUS[29]

En el caso del acceso inalámbrico, el servidor RADIUS despacha en el mensaje RADIUS-*Access-Accept* un juego de claves WEP dinámicas, que se usarán para cifrar la conexión entre el cliente y el punto de acceso.

El servidor RADIUS se encarga de cambiar esta clave dinámica periódicamente (por ejemplo, cada cinco minutos), para evitar el ataque de rompimiento de la clave descrito en la sección referente a WEP.

Se puede hablar de dos grupos de variantes: las que emplean certificados de seguridad, y las que utilizan contraseñas.

- **Variantes de EAP - Certificadas**

Las variantes de EAP que emplean certificados de seguridad son las siguientes:

- **EAP-TLS**

Requiere de instalación de certificados en los clientes y en el servidor. Proporciona autenticación mutua fuerte (es decir, el servidor autentica al cliente y viceversa) y soporta el uso de claves dinámicas para WEP. La sesión de autenticación

[29] Eduardo Tabacman. Seguridad en Redes Wireless. En las memorias de la I Jornada de Telemática , "Comunicaciones Inalámbricas, Computación Móvil". ACIS, Bogotá (Colombia), Noviembre 13 y 14 2003

entre el cliente y el autenticador se cifra empleando el protocolo TLS (*Transparent Layer Substrate).*

- **EAP-TTLS**

Desarrollada por *Funk Software* y *Certicom*. Proporciona servicios similares a EAP-TLS, con la diferencia de que requiere solamente la instalación de un certificado en el servidor.

Esto garantiza la autenticación fuerte del servidor por parte del cliente; la autenticación del cliente por parte del servidor se efectúa una vez que se establece la sesión TLS, utilizando otro método tal como *PAP, CHAP, MS-CHAP ó MS-CHAP v2.*

- **PEAP**

Desarrollado por Microsoft, Cisco[30] y RSA *Security*[31], funciona de manera parecida a EAP'TTLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador. El empleo de certificados permite una autenticación fuerte entre cliente y servidor, sin embargo posee también varias desventajas, como:

- *La administración de los certificados de seguridad puede ser costosa y complicada*; especialmente en los esquemas donde se necesitan certificados en los clientes y en el servidor. Es necesario comprar los certificados a una autoridad de certificación (CA) conocida, o montar una CA propia.

- *El diálogo de autenticación es largo;* esto ocasiona que el proceso sea algo demorado, siendo especialmente molesto para usuarios que tienen que re-autenticarse con mucha frecuencia (por ejemplo, usuarios en movimiento que cambien de un punto de acceso a otro).

- *La manipulación del certificado* puede ser engorrosa para el usuario.

[30] PEAP, www.cisco.com, Noviembre 2009
[31] RSA, www.rsa.com, Enero 2010

En muchos casos se elige instalar el certificado en la terminal del usuario, con lo cual, si la terminal es robada y el certificado es el único nivel de seguridad que se posee, la seguridad de la red estaría en riesgo. Otra solución sería llevar el certificado en una tarjeta inteligente (*smart card*), lo que obligaría a instalar hardware adicional en las terminales para leer dichas tarjetas.

- **Variantes de EAP - Contraseñas**

Las variantes de EAP que utilizan contraseñas son las siguientes:

- **EAP-MD5**

Emplea un nombre de usuario y una contraseña para la autenticación. La contraseña se transmite cifrada con el algoritmo MD5. Su gran inconveniente consiste en el bajo nivel de seguridad que maneja, ya que es susceptible a ataques de diccionario (un atacante puede ensayar a cifrar múltiples contraseñas con MD5 hasta que encuentre una cuyo texto cifrado coincida con la contraseña cifrada capturada anteriormente).

Además, el cliente no tiene manera de autenticar al servidor (no se podría garantizar que el cliente se está conectando a la red adecuada), y el esquema no es capaz de generar claves WEP dinámicas. Por estos problemas, EAP-MD5 ha caído en desuso.

- **LEAP**

Esta variante es propietaria de Cisco. Emplea un esquema de nombre de usuario y contraseña, y soporta claves dinámicas WEP.

Al ser una tecnología propietaria, exige que todos los puntos de acceso sean marca Cisco, y que el servidor RADIUS sea compatible con LEAP.

- **EAP-SPEKE**

Esta variante emplea el método SPEKE (*Simple Password-authenticated Exponential Key Exchange*), que permite verificar que tanto cliente como servidor comparten una información secreta (en este caso una contraseña) a través de un medio inseguro.

Se ha comprobado que el método es muy seguro, aun con contraseñas cortas, ofrece protección contra ataques de diccionario, así como el servicio de autenticación mutua sin necesidad de certificados. Muchos proveedores lo implementan por ser un método de autenticación robusto y sencillo.

3.3.5 WPA (WiFi protected access) [32-33]

WPA es un estándar propuesto por los miembros de la Wi-Fi *Alliance* (que reúne a los grandes fabricantes de dispositivos para WLAN) en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.

Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (*Temporary Key Integrity Protocol*). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IVs, con respecto a WEP.

El mecanismo de autenticación usado en WPA emplea 802.1x y EAP, que fueron discutidos en la sección anterior. Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

- **Modalidad de red empresarial:**

  Para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El punto de acceso emplea entonces 802.1x y EAP para la autenticación, y 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 entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles.

[32] Wi-Fi Alliance Overview: Wi-Fi Protected Access.. http://www.weca.net/ Open Section/Pdf/Wi- i_Protected_Access_Overview.pdf, Octubre 31 de 2002, Febrero 2010
[33] WPA's Little Secret.. http:// www.stargeek.com/item/ 20270.html, Noviembre 4 de 2003, Febrero 2010

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. La norma WPA data de abril de 2003, y es de obligatorio cumplimiento para todos los miembros de la Wi-Fi Alliance a partir de finales de 2003.

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.

3.3.6 IEEE 802.11i – WPA2

El estándar WPA2 de la *WIFI Alliance* consiste en una mejora del WPA, cambiando el esquema de encriptación a *AES-CCMP*[34]. El algoritmo de encriptación AES[35] resulta muy interesante, ya que ha sido adoptado como estándar de privacidad por el *National Institute of Standards and Technology (NIST),* para el gobierno de EEUU.

En este caso la WIFI Alliance vuelve a adelantarse al IEEE sacando un estándar muy parecido al tan esperado 802.11i, en previsión de que se alargue la aprobación de éste. En aspectos relativos a la seguridad son prácticamente idénticos.

3.4 DIAGRAMA DE SOLUCION PARA UNA RED INLAMBRICA SEGURA

Una vez definido todos los protocolos y sistemas a usar, podemos presentar el modelo de trabajo a implementar. Este sistema se presenta como un método seguro para una red inalámbrica, mediante el cual sólo las personas autorizadas podrán acceder a la Red y hacer uso de sus recursos.

El proceso de autenticación de usuarios se realiza mediante un servidor *FreeRADIUS* versión 2.2, el cual realiza las peticiones a los suplicantes, a través de los clientes NAS. El método de autenticación usado será el EAP-PEAP/802.1x, el cual hace uso de la identidad del usuario y una contraseña para poder acceder a la red. El servidor *FreeRADIUS* hará uso

[34] Estándar de codificación avanzada, ofrece método de codificación más robusto que TKIP
[35] Advanced Encryption Standard, esquema de cifrado por bloques

de una base de datos creada en *MySQL* para almacenar la información de todos los usuarios autorizados a acceder a la Red inalámbrica.

A su vez, se contará con una interfaz gráfica denominada *DALORADIUS*, la cual es de sencillo uso, donde se podrá crear las cuentas de usuario y contraseñas directamente en la base de datos, así como poder realizar pruebas de testeo sobre el servidor de autenticación, también facturación de uso de servicios de cada usuario. Este modelo sistema de seguridad se encuentra esquematizado en la Figura 3.5:

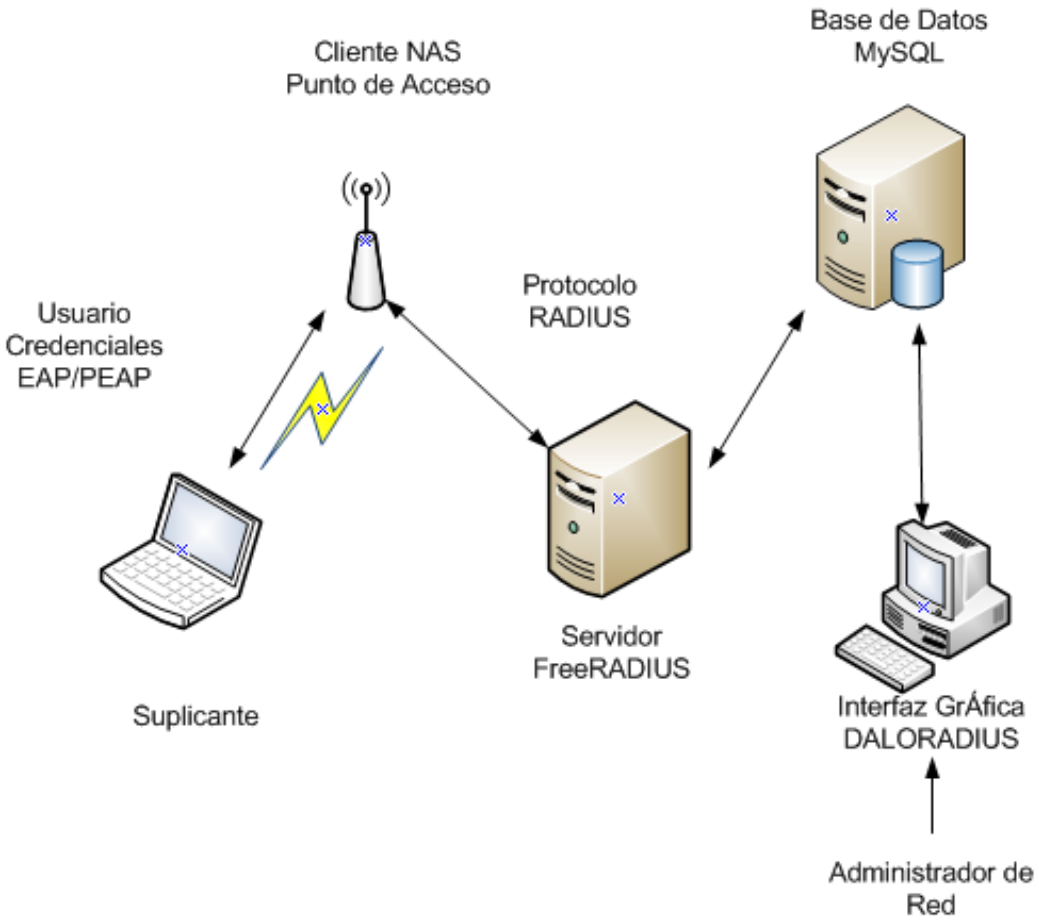


Figura. 3.9. Diagrama de Sistema para red inalámbrica Segura

3.4.1 Servidor Free-RADIUS

FreeRADIUS es una plataforma modular, de gran potencialidad, con diversas y completas características que lo convierte en uno de los más utilizados y potentes servidores RADIUS de clase AAA. FreeRADIUS incluye servidor, clientes y desarrollo de múltiples librerías útiles para el desarrollo de un excelente servicio; puede manejar miles de cuentas de usuarios y millones de peticiones de autenticación al día.

Esta plataforma consiste en un software libre, el cual es compatible con numerosos sistemas operativos, pudiendo trabajar en conjunto con bases de datos o directorios, donde se puede almacenar la información de cada usuario miembro de la red inalámbrica.

- **Autenticación:**

Consiste en el proceso de validar la petición de un usuario, el cual quiere hacer uso de los recursos de la red inalámbrica. El proceso de autenticación se realiza mediante la presentación de identidad y credenciales por parte del usuario.

La identidad del usuario viene a ser el nombre o alias con el cual está registrado en la base de datos del servidor de autenticación, mientras que las credenciales se implementarán mediante contraseñas, aunque también podría incluirse el uso de certificados digitales. El protocolo de autenticación usado será EAP-PEAP, este protocolo es usado entre el servidor FreeRADIUS y el Punto de Acceso para el proceso de autenticación de los usuarios.

Existen varios métodos de autenticación que son soportados por el servidor FreeRADIUS, algunos de los cuales se detallan a continuación:

- EAP-MD5
- EAP-TLS
- EAP-PEAP MSCHAPv2
- EAP-TTLS
- LEAP
- KERBEROS

- **Autorización**

El proceso de autorización es el siguiente paso luego de la autenticación. Este proceso consiste en determinar si un usuario se encuentra autorizado para hacer uso de ciertas tareas, operaciones o recursos de la red. Usualmente el proceso de autorización se realiza en conjunto con el de autenticación, de esta manera una vez que el usuario es autenticado como válido, este podrá hacer uso de ciertos recursos de la red.

Así mismo, los usuarios autorizados serán registrados en la base de datos MySQL, a la cual el servidor FreeRADIUS se conecta para saber que usuarios pertenecen a la red inalámbrica

- **Contabilidad**

La contabilidad es la última característica de un servidor AAA, y consiste en el proceso de medición y almacenamiento de consumo de recursos de red. Esto permite el monitoreo y reporte de eventos y uso de la red inalámbrica para varios propósitos, entre los cuales se encuentran: tarifación de usuarios, análisis de recursos de red, capacidad de la red.

Este proceso también hace uso de la base de datos para poder registrar el comportamiento de los usuarios en la red inalámbrica

3.4.2 Base de Datos de usuarios de la Red

Una base de datos es un sistema relacional que está compuesta por conjunto de datos pertenecientes a un mismo contexto, ordenados sistemáticamente para su posterior uso. Los datos son almacenados en tablas, cada tabla contiene características en común, por ejemplo tabla de nombre de usuarios, tabla de contraseñas, reporte de los usuarios, entre otros.

La plataforma FreeRADIUS puede soportar las siguientes bases de datos:

- MySQL
- Oracle
- PostgreSQL

Para la aplicación de la red inalámbrica se utilizó MySQL como base de datos del servidor FreeRADIUS.

Base Datos MySQL

MySQL está considerado un sistema de gestión de base de datos relacional, multitarea y multiusuario, que provee una solución robusta, rápida y de fácil uso. MySQL se basa en un Lenguaje de Consulta estructurado (SQL), el cual es un lenguaje estándar de computadora para el acceso y la manipulación de base de datos.

Las tablas creadas en MySQL se detallan a continuación:

- ***Badusers:*** Contiene la información de los usuarios que no pudieron conectarse a la red inalámbrica, por proveer una incorrecta credencial.

- ***Nas:*** Consiste en el cliente o clientes NAS o puntos de acceso los cuales realizan la autenticación hacia el servidor FreeRADIUS.

- ***Radcheck:*** Contiene todas las contraseñas de cada uno de los usuarios autorizados a hacer uso de la red inalámbrica.

- ***Radgroupcheck:*** Muestra los grupos de usuarios que contienen un método de autenticación, como por ejemplo EAP-PEAP.

- ***Radgroupreply:*** Muestra todos los grupos de usuarios creados con sus protocolos y características de cada uno de ellos. Cabe mencionar que los usuarios pertenecientes a un grupo, adoptarán las características del grupo al que forman parte.

- ***Radpostauth:*** Contiene un reporte sobre los procesos de autenticación realizados satisfactoriamente, cada proceso es almacenado en el día y la hora exacta.

- ***Usergroup:*** Contiene la tabla de todos los usuarios, indicando los grupos a los que pertenecen.

- ***Userinfo***: Contiene todas las características de los usuarios, como por ejemplo: número telefónico de casa o trabajo, teléfono móvil, departamento y correo electrónico.

3.4.3 Clientes Free-RADIUS

- **NAS - Network Access Server**

Cuando un usuario quiere acceder a la Red Inalámbrica, lo realiza mediante los clientes del servidor FreeRADIUS, los llamados Network Access Server (NAS), los cuales realizan una petición de usuario y contraseña a cada usuario que quiera autenticarse. Los clientes NAS se comunican directamente con el servidor FreeRADIUS a través del protocolo RADIUS, para realizar la entrega de la identificación y credenciales de cada uno de los usuarios.

En caso de que un usuario sea autenticado como autorizado, el NAS respectivo propone al usuario colocarse en el Protocolo Punto-Punto (PPP) y le asigna una dirección IP y una máscara de red para que pueda acceder a Internet a través de él.

- **Aplicación Gráfica Cliente de FreeRADIUS**

Una aplicación gráfica puede trabajar como un cliente de FreeRADIUS, facilitando la creación de cuentas de usuario, así como poder realizar pruebas de autenticación de los mismos y llevar estadísticas de acceso a la red inalámbrica. El uso de una interfaz gráfica permite la administración y modificación de nuestro servidor de una manera sencilla y rápida.

La interfaz gráfica se encuentra realizada en un programa basado en PHP4, el cual es ejecutado en un servidor Apache, especializado en páginas web.

- **Servidor HTTP Apache**

El servidor HTTP Apache es un software libre utilizado en plataformas UNIX o Windows que soporta el protocolo HTTP y es considerado el servidor de páginas HTTP más aceptado a nivel mundial. La razón de la amplia difusión del servidor Apache es porque consiste en un software modular, de código abierto, multiplataforma, extensible, popular y gratuito.

El servidor apache puede soportar páginas web escritas en lenguaje PHP.

- **PHP "PHP Hypertext Pre-processor"**

PHP es un acrónico recursivo que significa ***Personal Home Page Tools Hypertext Preprocesor***; es un lenguaje de programación utilizado para la creación de contenido dinámico de sitios Web, compatible con sistemas operativos *UNIX* y Windows, donde se puede programar páginas tipo *html*; así como la creación de aplicaciones para servidores. Este programa es de fácil uso y utiliza la programación estructurada como forma de programación, permitiendo la creación de aplicaciones complejas e interfaces gráficas para el usuario.

PHP permite la conexión a diferentes tipos de servidores de bases de datos tales como *MySQL*, *PostgreSQL*, *Oracle*, *ODBC*, *DB2*, entre otros; donde los primeros tres sistemas de bases de datos garantizan una compatibilidad con el servidor FreeRADIUS.

La interpretación y ejecución de las páginas web se realizan mediante la ejecución de un programa denominado "script", el usuario sólo recibe el resultado de su ejecución en la pantalla del computador. Cuando el usuario realiza una petición al servidor para mostrar una página web, generada por un "script" PHP, el servidor Apache ejecuta el intérprete de PHP, el cual procesa el "script", generando el contenido de manera dinámica.

3.4.4 Interface de administración "Dalo-RADIUS"

DaloRADIUS es una avanzada aplicación de gestión de radio web destinadas a la gestión de puntos críticos y para fines generales ISP despliegues. Ofrece gestión de usuarios, informes gráficos, contabilidad, facturación y un motor, y se integra con Google Maps para la localización geográfica. Licencia: GNU *General Public License* (GPL)

La interface DaloRADIUS consiste en un programa de código abierto basado en PHP4, que permite la administración del servidor FreeRADIUS vía página web.

Permite realizar la configuración de nuevos operadores como se muestra en la figura 3 permitiéndose ingresar datos de cuentas para los diferentes operadores de la interface.

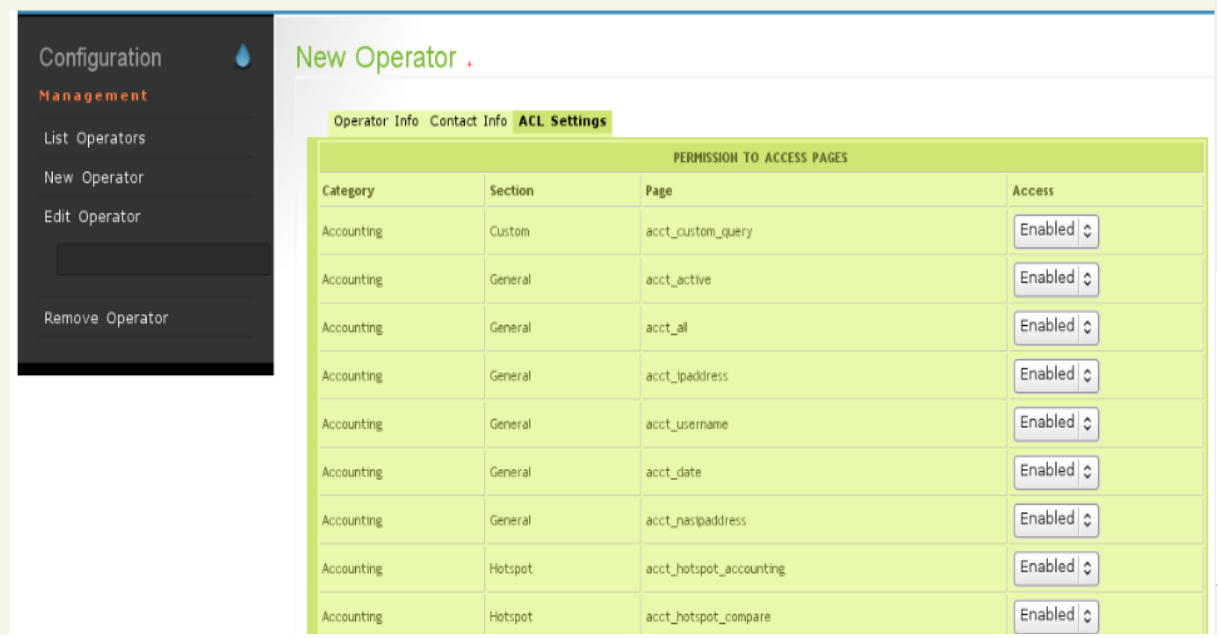


Figura. 3.10. Configuración de Nuevos Operadores

- **Cambios en el portal de Usuarios**

La vieja manera de los usuarios para autenticar a los usuarios del portal para que los comparen con su clave de acceso establecido en la tabla *radcheck* es obsoleta. Lo nuevo es que se ha establecido para el usuario una contraseña que verifica si el usuario está autorizado a ingresar o no (y posiblemente también para actualizar sus configuraciones de contacto), como se muestra en la Figura 3.11., donde se presentan varias configuraciones de los usuarios.

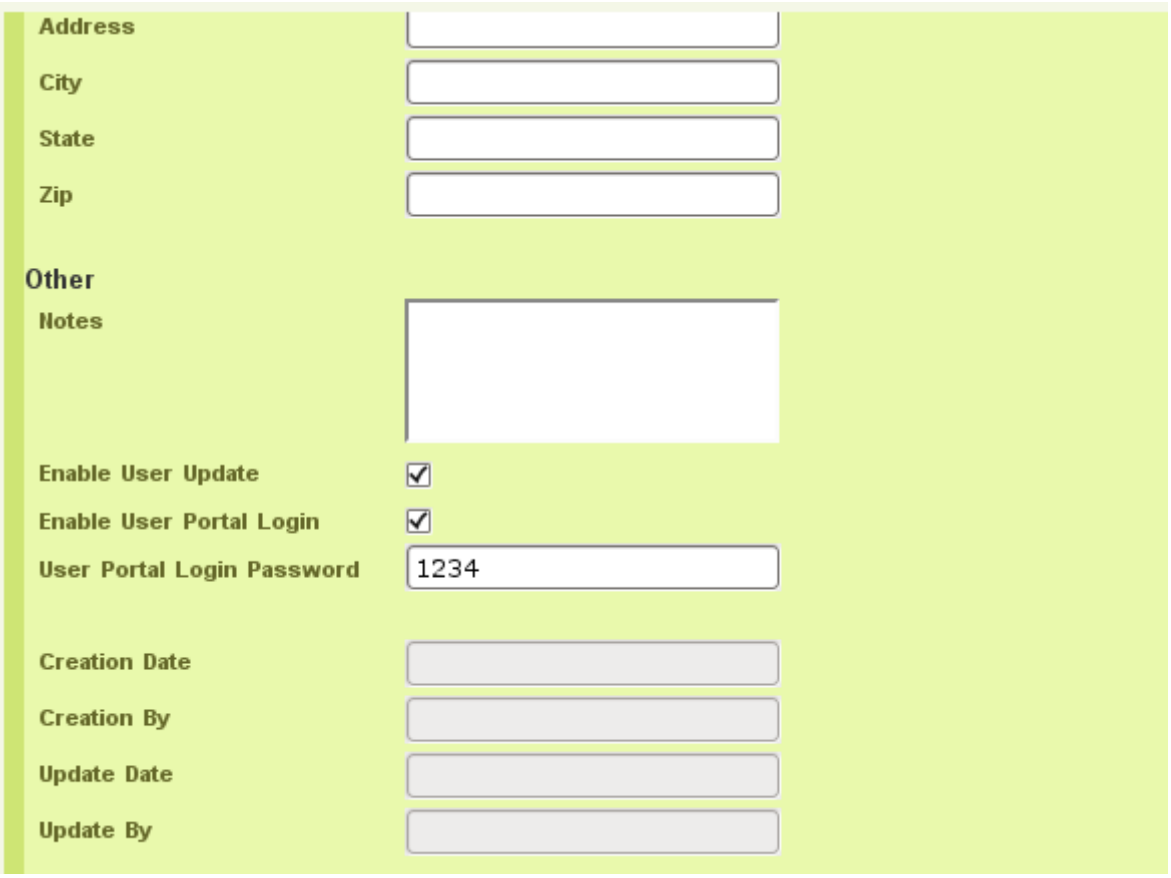
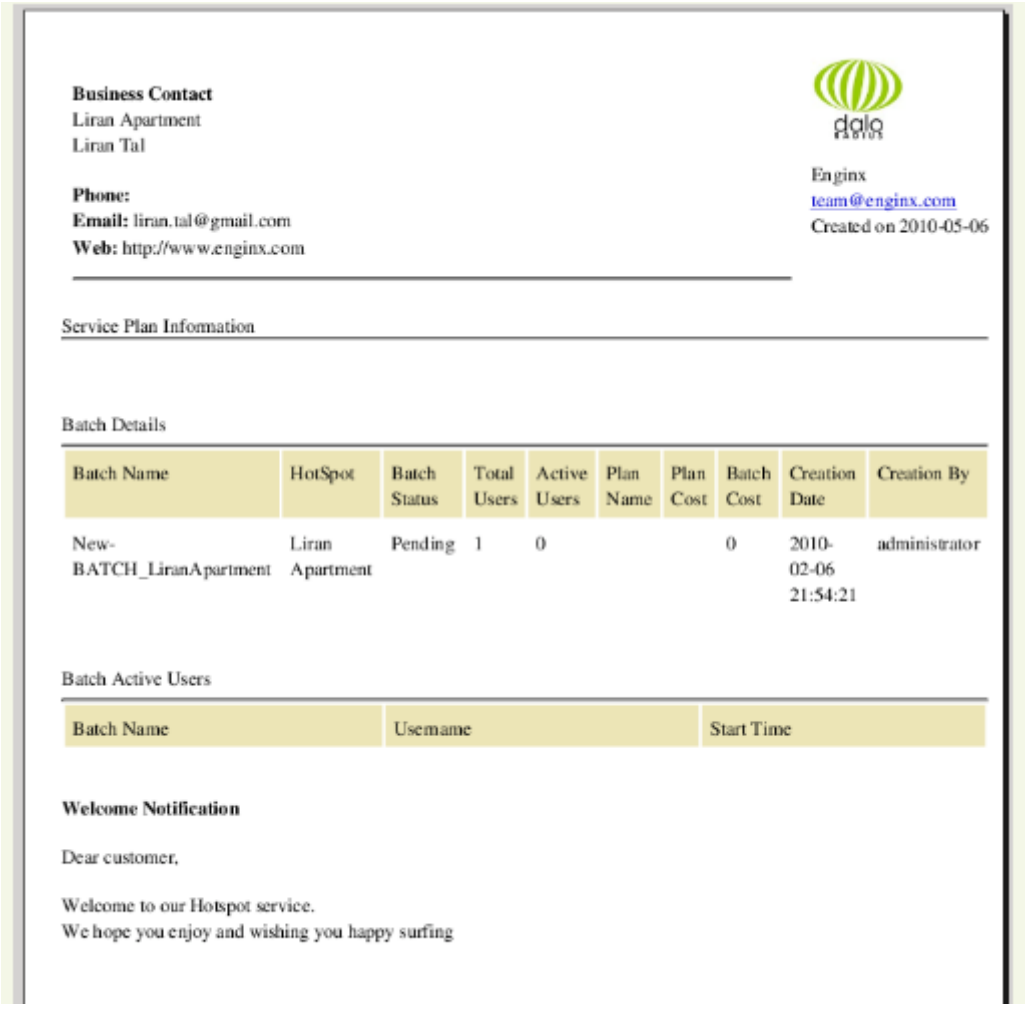


Figura. 3.11. Ventana de configuración de Usuarios

- **Facturas Pdf**

DaloRADIUS también permite realizar facturación y enviar resultados en formato PDF. Si bien es cierto esto es realmente sólo el principio; permite realizar dos tipos de notificaciones:

- ✓ **Notificación de Bienvenida-PDF**: Esta se realiza por correo electrónico y se envía la notificación al usuario, previa creación.
- ✓ **Factura / Informe**: Sólo se aplican actualmente para las creaciones de lote. Esta factura se puede verificar en la Figura 3.12.



Business Contact
Liran Apartment
Liran Tal

Phone:
Email: liran.tal@gmail.com
Web: http://www.enginx.com

Enginx
team@enginx.com
Created on 2010-05-06

Service Plan Infomation

Batch Details

Batch Name	HotSpot	Batch Status	Total Users	Active Users	Plan Name	Plan Cost	Batch Cost	Creation Date	Creation By
New-BATCH_LiranApartment	Liran Apartment	Pending	1	0			0	2010-02-06 21:54:21	administrator

Batch Active Users

Batch Name	Username	Start Time

Welcome Notification

Dear customer,

Welcome to our Hotspot service.
We hope you enjoy and wishing you happy surfing

Figura. 3.12. Factura/Informe creado por DaloRADIUS

Para ello se está haciendo uso de la biblioteca pdf, fuente abierta llamada *dompdf* que también permite un fácil manejo de las plantillas de estos documentos PDF generados.

- **Gestión de Usuarios por Grupos**

Una nueva adición genial en el sistema de gestión de grupos DaloRADIUS es la capacidad de rastrear el historial del grupo y de los usuarios asociados, que se crea con una sesión de proceso por grupos específicos y punto de acceso.

Además de permitir un mayor control sobre estos usuarios y datos de él; los informes están basados en las sesiones de ingreso por grupos, los usuarios activos de un grupo etc. En la figura 3.13., se muestra la ventana de gestión de usuarios por grupo.

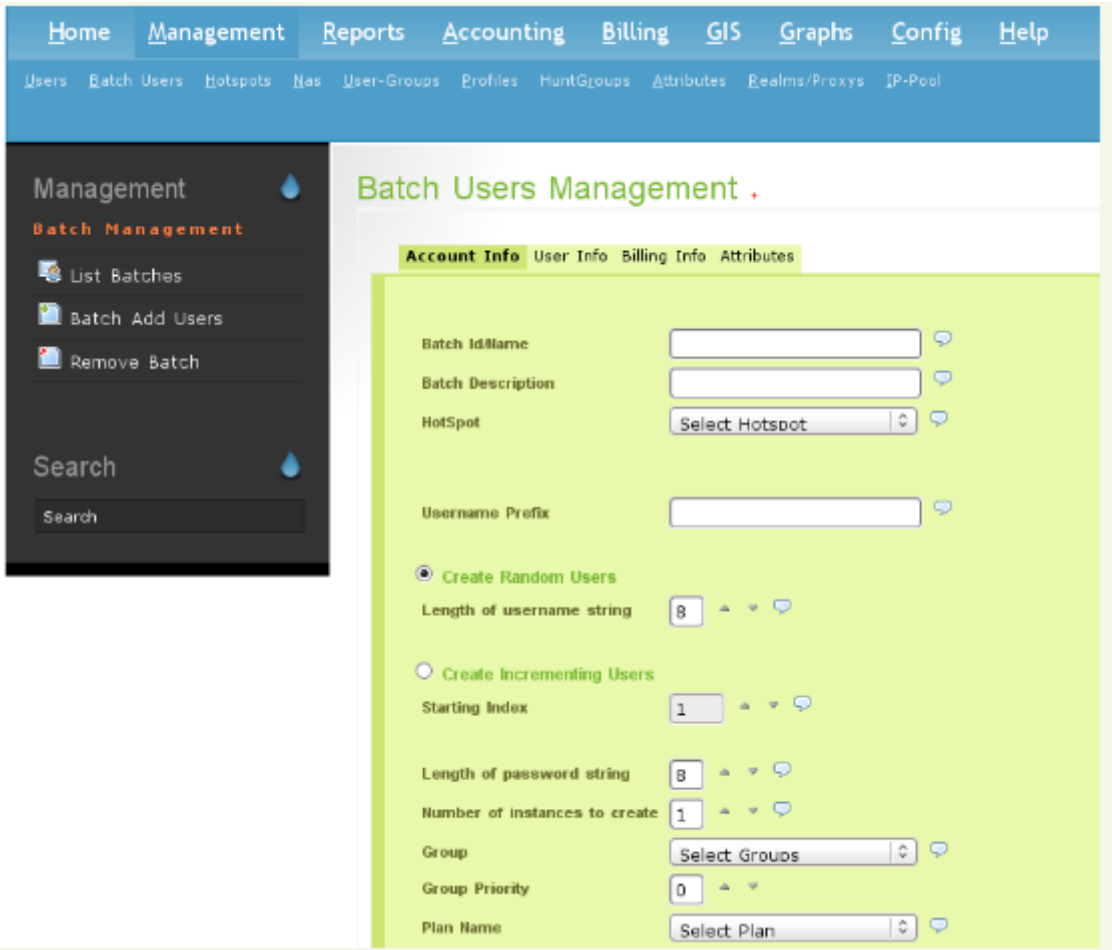


Figura. 3.13. Ventana de Gestión de Usuarios por Grupo en DaloRADIUS

El usuario de grupo ingresa en su propia página llamada “Usuario de Grupo”. Ahora debe especificar un ID de grupo/nombre que es solo un nombre para identificar el grupo así como algunos otros datos, como una descripción y también la asociación de estos usuarios de los grupos con un punto de acceso, esto es ideal para luego sacar los reportes.

La Figura 3.14., muestra la ventana de Usuario de Grupo.

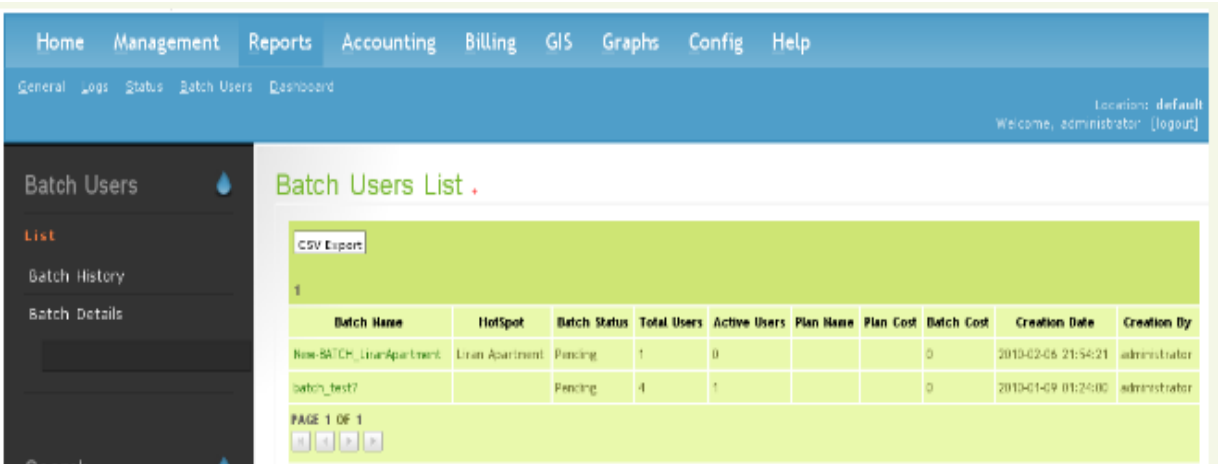


Figura. 3.14. Ventana de Lista de Usuario de Grupo

DaloRADIUS también permite realizar transacciones de facturación mediante su nueva característica de PayPal, varias de las funcionalidades de facturación de DaloRADIUS se muestran en la figura 3.15.

Figura. 3.15. Página de Transacción PAYPAL

CAPÍTULO IV

DISEÑO DE LA RED INALÁMBRICA

4.1 DISEÑO FÍSICO

4.1.1 Equipos

Para realizar el diseño de la red inalámbrica se utilizarán los AP2750 de 3com y para las pruebas respectivas el Access Point Linksys Wireless WAP54GS, los mismos que tienen características similares entre sí las cuales son:

4.1.1.1 Linksys Wireless WRT 54GS

"El Wireless-G Broadband Router con SpeedBooster es en realidad tres dispositivos en uno. En primer lugar, está el punto de acceso inalámbrico, que permite conectar dispositivos Wireless-G, Wireless-B, y otros dispositivos con mejora de rendimiento SpeedBooster a la red. También hay un built-in 4 puertos full-duplex 10/100 Switch para conectar sus dispositivos Ethernet. Por último, la función de ruteador une todos los elementos y permite a toda la red que compartan con un cable de alta velocidad o conexión DSL Internet."[1]

"SpeedBooster es plenamente compatible con 802,11 para otros dispositivos de tecnologías inalámbricas, utilizando solo 2.4GHz como canal que especifica el estándar inalámbrico oficial. A diferencia de otros tecnologías, con SpeedBooster apreciará una

[1] Linksys Wireless WRT54GS, www.linksysbycisco.com/EU/es/products/WRT54G, Febrero 2010

mejora en la velocidad global, aun cuando cuenten con una red mixta de dispositivos SpeedBooster y dispositivos Wireless-G."[2]

"La encriptación de grado industrial ayuda a proteger la confidencialidad y seguridad de sus comunicaciones. El filtro de acceso permite controlar quién accede a su red. Wi-Fi Protected Access ™ 2 (WPA2) protege los datos y la privacidad con 128-bits de potencia industrial de cifrado, la autenticación y autorización 802.1x. El ruteador puede funcionar como servidor DHCP, dispone de un potente firewall SPI para proteger sus PCs contra intrusos y ataques más conocidos de Internet, y soporta VPN pass-through. La configuración es sencilla con la utilidad de configuración web basada en navegador."[3]. En la Tabla 4.1., se detallan las características más importantes del WRT54GS.

Tabla. 4.1. Características del WRT54GS

WRT54GS	
Model	WRT54GS
Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u
Ports/Buttons	Internet: One 10/100 RJ-45 Port LAN:Four 10/100 RJ-45 switched ports
Cabling Type	Category 5 (with RJ-45 connectors)
LEDs	Power, DMZ, WLAN, LAN (1,2,3,4), Internet
RF Power Output	18 dBm
Security features	WPA, Linksys Wireless Guard (available in US and Canada only), WEP Encryption, MAC Filtering, SSID Broadcast Enable/Disable
Channels	11 Channels (US, Canada) 13 Channels (Europe and Japan)

[2] Linksys Wireless WRT54GS, www.linksysbycisco.com/EU/es/products/WRT54G, Febrero2010
[3] Linksys Wireless WRT54GS, www.linksysbycisco.com/EU/es/products/WRT54G, Febrero2010

Tabla. 4.2. Características de sensibilidad de receptor del WRT54GS

SENSIBILIDAD DE RECEPTOR	
802.11b	802.11g
1 Mbps: ≤-95 dBm	6 Mbps: ≤-89 dBm
2 Mbps: ≤-92 dBm	9 Mbps: ≤-89 dBm
5.5 Mbps: ≤-91dBm	12 Mbps: ≤-88 dBm
11 Mbps: ≤-88 dBm	18 Mbps: ≤-89 dBm
	24 Mbps: ≤-85 dBm
	36 Mbps: ≤-81 dBm
	48 Mbps: ≤-77 dBm
	54 Mbps: ≤-73 dBm

4.1.2 Herramientas de diseño

Para realizar el diseño de la red se utilizará el software **3com Wireless Switch Manager** versión 4.2.3.2.0 el mismo que presta facilidades de diseño como se detallan a continuación.

4.1.2.1 3COM Wireless Switch Manager

"Este paquete de software de administración de red inalámbrica contiene todas las características que se necesita para planificar, configurar, desplegar y administrar con éxito una LAN inalámbrica de clase empresarial. Como parte integrante del Sistema de Movilidad para LAN Inalámbrica de 3Com®, el software 3Com Wireless Switch Manager funciona con controladores y switches para LAN inalámbrica de 3Com para administrar de forma centralizada y controlar puntos de acceso administrados (MAPs) de 3Com para aquellas redes que requieren despliegues complejos, con múltiples oficinas o requisitos de LAN de alta seguridad. La parte de planificación de esta potente aplicación permite importar planos de planta de emplazamiento en diversos formatos y configurar automáticamente la capacidad y la cobertura de su sitio usando la funcionalidad integrada de replanteo virtual (Virtual Site Survey), que tiene en cuenta una gran variedad de

obstáculos habituales para la RF. Durante el despliegue de red inalámbrica, se duplican y verifican rápidamente las plantillas de configuración. "[4]

"Una vez completada la instalación, el Wireless LAN Switch Manager permite una operación sencilla y precisa de toda su LAN inalámbrica, permitiéndole estar al corriente de todas las actividades del espacio aéreo, incluyendo la detección y localización de puntos de acceso no autorizados, redes ad-hoc u otras señales interferentes de RF. Además, el administrador puede ajustar automáticamente la potencia de MAP para eliminar vacíos de cobertura y optimizar aún más el rendimiento de RF. Al estar construido sobre las sólidas características de seguridad inalámbrica de 3Com, el 3Com Wireless Switch Manager puede completamente administrar, asegurar y realizar el seguimiento de todos los servicios en la red inalámbrica sobre una base por usuario o por grupo. Con esta capacidad de Identity-Based Networking, los responsables informáticos pueden confiar en la seguridad mejorada de sus redes LAN inalámbricas mediante un control de acceso autenticado de grupos de usuarios, unas políticas de itinerancia coherentemente aplicadas y un uso de ancho de banda monitorizado mejorado."[5] A continuación en la Figura 4.1., se muestra el área de trabajo del 3com Wireless Switch Manager.

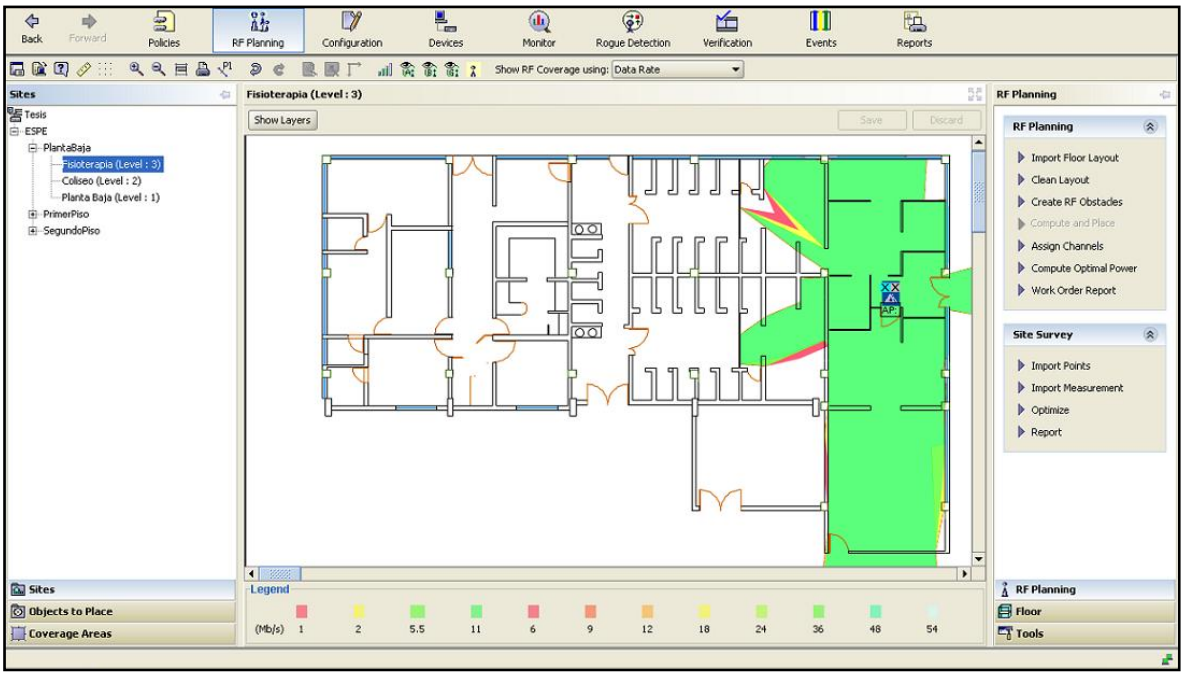


Figura. 4.1. Área de Trabajo del 3com Wireless Switch Manager

[4]3com Wireless Switch Manager, www.3com.com/prod/es_LA_AMER/detail.jsp?tab=features&sku=3CWXM10A, Febrero 2010
[5]3com Wireless Switch Manager, www.3com.com/prod/es_LA_AMER/detail.jsp?tab=features&sku=3CWXM10A, Febrero 2010

4.2 RED INALAMBRICA

Para la ubicación de los AP's en el software de diseño se procedió a separar las distintas áreas a las cuales se procederá a dar cobertura inalámbrica, las cuales se muestra en los diagramas de coberturas; la potencia de salida y ganancia de antenas del AP se obtuvieron de las características del equipo.

- Dos antenas de banda dual de 2,4-2,48/5,15-5,85 GHz, omnidireccionales de 2 dBi.
- Potencia de Transmisión 54 Mbps: ≥+17 dBm (para condiciones mínimas).

4.2.1 Diagramas de cobertura

4.2.1.1 Diseño de Planta Baja

Para cubrir la cobertura de la planta baja se utilizará un AP, como se observa en la Figura 4.2. Cobertura Planta Baja, se desea tener cobertura en una sola aula (Tercer Nivel), el SSID utilizado será CAFDER_PLANTABAJA.

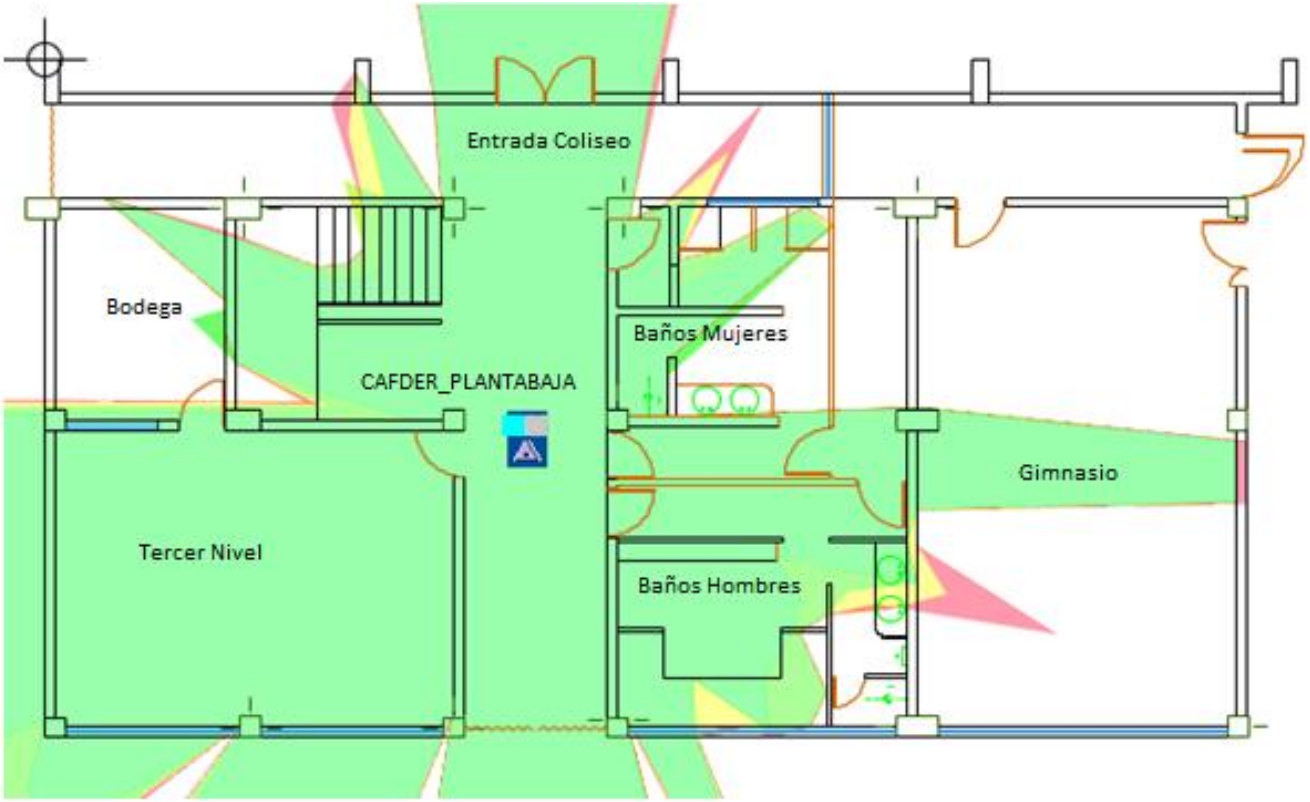


Figura. 4.2. Cobertura Planta Baja (CAFDER_PLANTABAJA)

4.2.1.2 Diseño Primer Piso

Se utilizarán dos AP´s los mismos que se ubicarán según el diseño mostrado en la Figura 4.3. Cobertura Primer Piso, los mismos que se ubicarán de la manera mostrada para obtener una cobertura óptima en todo el piso, ya que en el mismo se encuentran la mayoría de aulas y se vuelve necesaria una cobertura óptima, los SSID utilizados serán CAFDER_PISO1a y CAFDER_PISO1b.

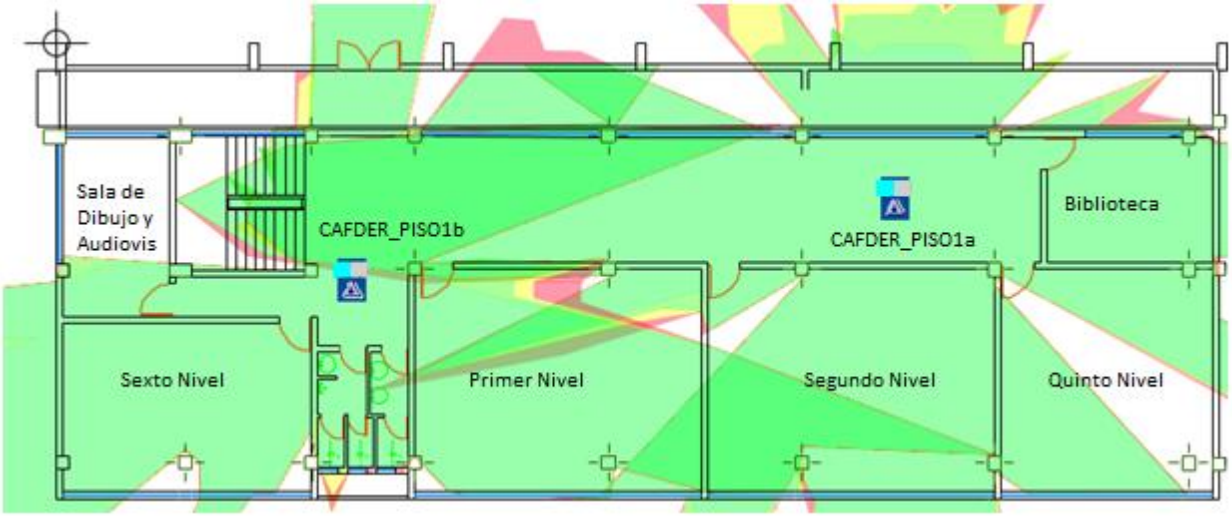


Figura. 4.3. Cobertura Primer Piso (CAFDER_PISO1a, b)

4.2.1.3 Diseño Segundo Piso

En el segundo piso se encuentran las oficinas administrativas de la carrera, así como las oficinas asignadas al personal docente del mismo, razón por la cual se utilizarán dos AP´s. El primer AP con SSID CAFDER_PISO2, cubrirá las aulas 7mo nivel, 8vo nivel y 4to nivel; el segundo AP con SSID CAFDER_ADMIN, cubrirá el área administrativa. La asignación de los respectivos AP`s se muestran en la Figura 4.4.

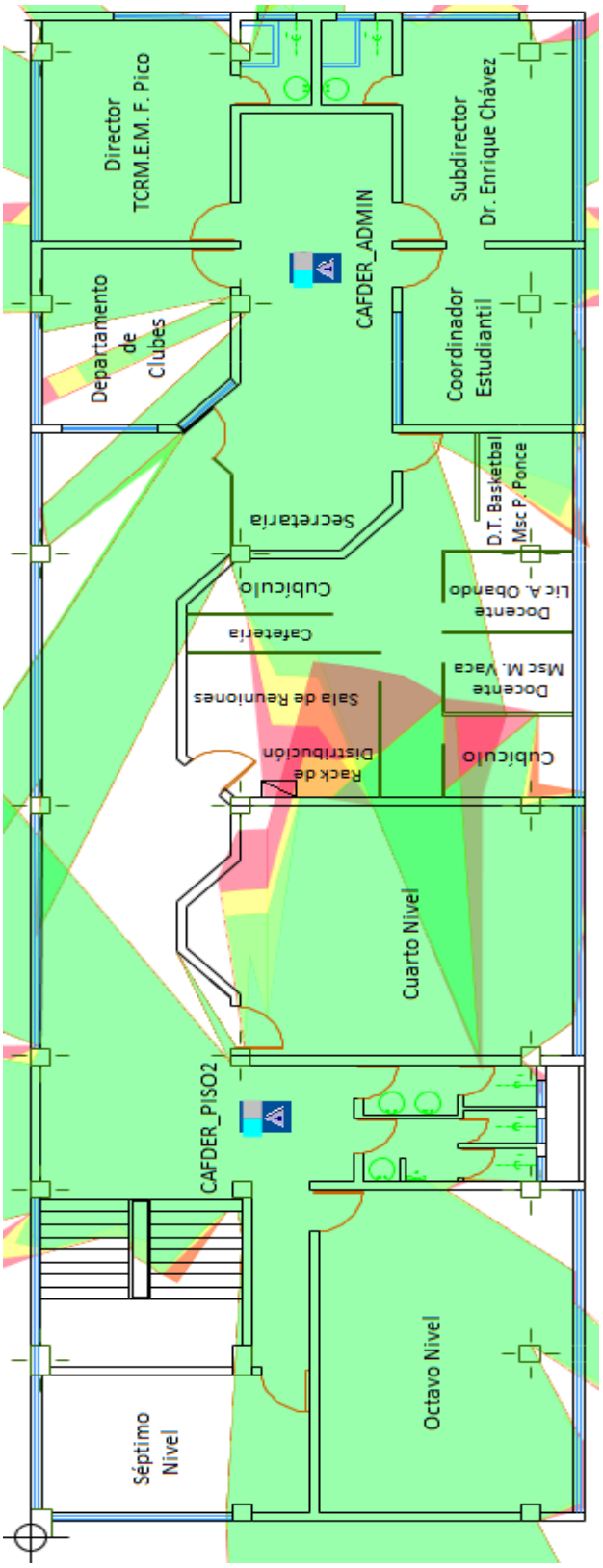


Figura. 4.4. Cobertura Segundo Piso (CAFDER_PISO2)

4.2.1.4 Diseño Coliseo

Tomando en cuenta que las matriculas de todo el alumnado se llevan a cabo en el coliseo se realiza el diseño de la red, colocando un solo AP con dos antenas de 5dbi, la cobertura será en línea de vista. El SSID colocado será CAFDER_COLISEO. La ubicación del AP se muestra en la Figura 4.5.

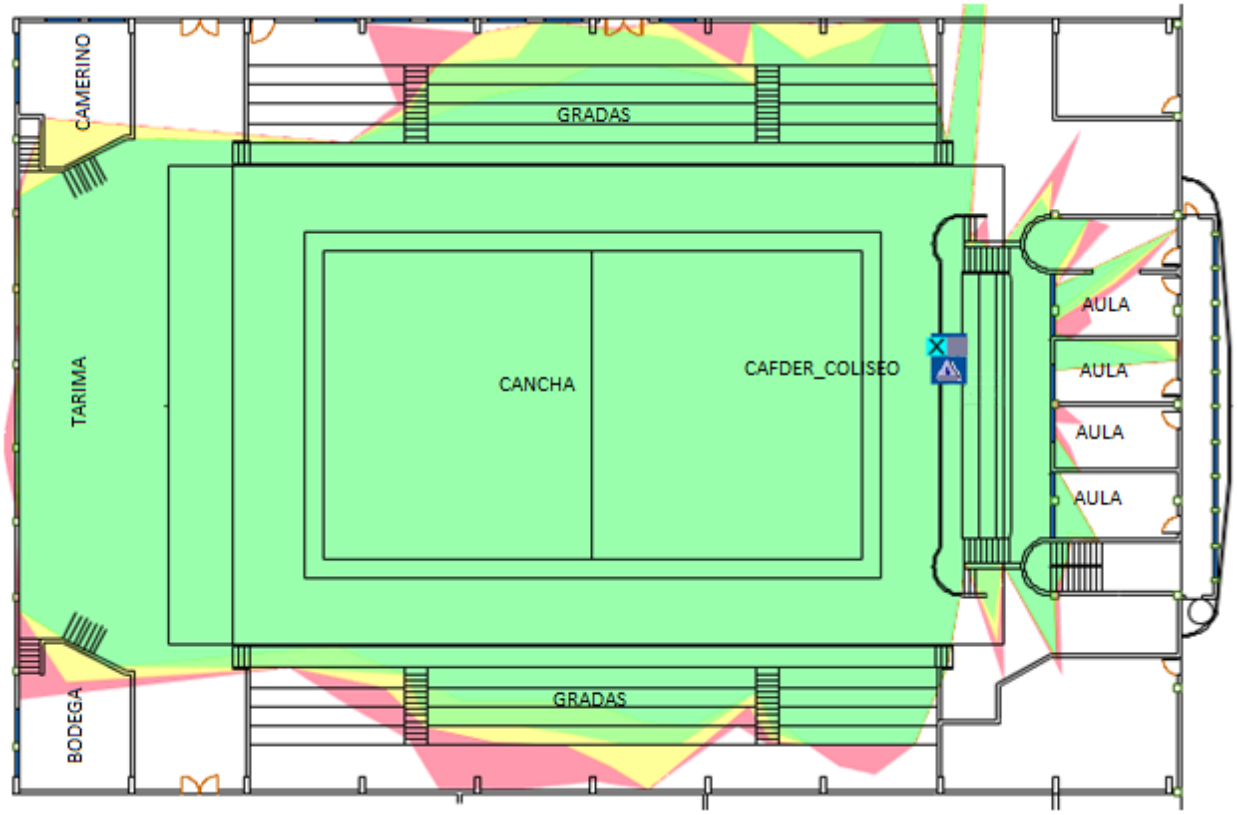


Figura. 4.5. Cobertura Coliseo (CAFDER_COLISEO)

4.2.1.5 Diseño Cobertura Fisioterapia

Con la implementación de nuevas aulas en esta área se observa la necesidad de colocar un AP para lograr una buena cobertura en el lugar, el SSID utilizado será CAFDER_AULAS. La Figura 4.6., muestra la ubicación de este AP.

Figura. 4.6. Cobertura Fisioterapia (CAFDER_AULAS)

Para la cobertura deseada se necesitarán 7 WAP54G los mismos que serán ubicados según el diseño realizado, sin embargo, si en la implementación el AP se coloca en otro lugar y se obtuviera mayor cobertura se procederá a realizar los cambios respectivos; los colores de los diagramas se interpretan según la siguiente leyenda mostrados en la Figura 4.7.

Figura. 4.7. Leyenda de Coberturas

Para el diseño de cada cobertura se utilizó las siguientes atenuaciones de cada una de las estructuras existentes en cada área separada.

Tabla. 4.3. Atenuación de los Materiales

ELEMENTOS		ATENUACIÓN 802.11 [dB]	
Estructuras	**Material**	**a**	**b,g**
Columnas	Concreto	30	18
Paredes	Concreto	10	10
Ventanas	Vidrio	2	3
Puertas	Madera	7	4
Div. Cubículo	Cubículo	4	6

Además de se utilizará los siguientes canales de frecuencia, mostrados en la Tabla 4.4, para cada AP:

Tabla. 4.4. Canal para cada SSID

SSID	CANAL	FRECUENCIA
CAFDER_ADMIN	1	2,412
CAFDER_PISO2	3	2,422
CAFDER_PISO1a	5	2,432
CAFDER_PISO1b	7	2,442
CAFDER_PLANTABAJA	9	2,452
CAFDER_COLISEO	11	2,462
CAFDER_AULAS	2	2,417

4.2.2 Cálculo de alcance máximo de la conexión inalámbrica

Para realizar el cálculo máximo de cobertura que se obtendría con la red inalámbrica se necesita:

- **Equipo inalámbrico (Tx):** las características del equipo, mostrados anteriormente en la Tabla. 4.1.; indican que las antenas con las que funciona el mismo (ganancias y diagramas de coberturas), desprecia las pérdidas en los conectores y guías de onda.
- **Tarjeta inalámbrica (Rx):** características.
- **Pérdida de propagación:** es la cantidad de señal necesaria para llegar de un extremo de la conexión wireless, al otro.

- **Atenuación debida a obstáculos:** en este caso, como es cobertura inalámbrica se debe tomar en cuenta la atenuación ocasionada debido a paredes, pisos, ventanas, etc.

4.2.2.1 Procedimiento

♦ **Pérdidas en espacio libre [Lo]:**

$$\boldsymbol{Lo = 20\log(d[Km]) + 20\log(f[MHz]) + 32.5} \qquad \textbf{(1)}$$

Con:

d:distancia de la cobertura.

f: frecuencia a la que se configure el equipo.

Relación de frecuencias y canales 802.11 b/g

Tabla. 4.5. Relación Frecuencias y Canales 802.11 b/g

Canal	Frecuencia[MHz]	Canal	Frecuencia[MHz]
1	2,412	8	2,447
2	2,417	9	2,452
3	2,422	10	2,457
4	2,427	11	2,462
5	2,432	12	2,467
6	2,437	13	2,472
7	2,442	14	2,484

Distancia máxima 100mts

$Lo = 20log(0.1) + 20log(2400) + 32.5$

$\boldsymbol{Lo = 80.10\ dB = L_T}$

$$\boldsymbol{P_R = P_T + G_{AT} + G_{AR} - L_T}$$

Con:

P_R: Potencia de Recepción.

P_T: Potencia de Transmisión.

G_{AT}: Ganancia de la antena Transmisora

G_{AR}: Ganancia de la antena Receptora

L_T: Pérdida total

P_T=20dBm

G_{AT}=2*2=4dBm

La tarjeta inalámbrica Intel PRO/Wireless 3945ABG se utilizó como ejemplo general, esta tarjeta tiene las características mostradas en la Tabla. 4.6.

Tabla. 4.6. Características Intel PRO/Wireless 3945ABG

INTEL PRO/WIRELESS 3945ABG NETWORK CONNECTION		
Form Factor	PCI Express (TM) Mini Card	
Dimensions	Height 200 in x 1.18 in x 0.18 in (50.95 mm x 30 mm x 4.5 mm)	
Antenna Interface Connector	Hirose U.FL-R-SMT mates with cable connector U.FL-LP-066	
Dual Diversity Antenna	On-board dual diversity switching	
Connector Interface	53-pin Mini Card edge connector	
Voltage	3.3 V	
Operating Temperature	0 to +80 degrees Celsius	
Humidity	50 to 92% non-condensing (at temperatures of 25 ºC to 55 ºC)	
Frequency Modulation	5 GHz (802.11a)	2.4 GHz (802.11b/g)
Frequency band	5.15 GHz - 5.85 GHz	2.400 - 2.4835 GHz
Modulation	BPSK, QPSK, 16 QAM, 64QAM	CCK, DQPSK, DBPSK
Wireless Medium	5 GHz UNII: Orthogonal	2.4 GHz ISM: Orthogonal
	Frequency Division	Frequency Division
	Multiplexing (OFDM)	Multiplexing (OFDM)
Channels	4 to 12 non-overlapping,	Channel 1-11 (US only)Channel 1-13 (Japan, Europe)
Data Rates	54, 48, 36, 24, 18, 12, 9,6 Mbps	11, 5.5, 2, 1 Mbps
GENERAL		
Operating Systems	Microsoft Windows XP, Microsoft Windows 2000	
Wi-Fi(R) Alliance certification	Wi-Fi(R) certification for 802.11b, 802.11g, 802.11a,WPA, WPA2, WMM, EAP-SIM, LEAP, PEAP, TKIP, EAPFAST,EAP-TLS, EAP-TTLS, MD5	
Cisco Compatible Extensions certification	Cisco Compatible Extensions, v4.0	
WLAN Standard	IEEE 802.11g, 802.11b, 802.11a	
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes	
Security	WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, AES-CCMP 128-bit, WEP 128-bit and 64-bit;802.1x:EAP-TTLS, MD5 EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAPTLS,	
Product Safety	UL, C-UL, CB (IEC 60590)	

Dadas las características se obtiene lo siguiente:

$$G_{AR}=2*5=10dBm$$

Entonces,

$$P_R = 20 + 4 + 10 - 80.10$$

$$\boldsymbol{P_R = -46.1dB}$$

La tarjeta del portátil tiene una sensibilidad de **-88 dBm**, es decir una diferencia de:

-46.1dB - (-88 dBm) = 41.9 dB

Este resultado es mayor de lo que se necesita para mantener la conexión, cabe recalcar que al valor P_R se debería restar la atenuación que presentan los obstáculos dependiendo de donde se encuentre el equipo receptor (P_{RT} =P_R-Atenuación), obteniendo así los valores siguientes:

Tabla. 4.7. Cobertura después de Obstáculos

ELEMENTOS	ATENUACIÓN 802.11 [DB]		P_{RT}		RANGO PARA MANTENER CONEXIÓN	
Estructuras	**a**	**b,g**	**P_R-Atenuación [db]**		**P_{RT} -Sensibilidad [db]**	
Columnas	30	18	-71,6	-59,6	16,4	28,4
Paredes	10	10	-51,6	-51,6	36,4	36,4
Ventanas	2	3	-43,6	-44,6	44,4	43,4
Puertas	7	4	-48,6	-45,6	39,4	42,4
Div Cubículos	4	6	-45,6	-47,6	42,4	40,4

Como se observa, se sigue manteniendo un buen rango de cobertura incluso después de la atenuación por los obstáculos.

4.3 DISEÑO LÓGICO

4.3.1 Segmentación VLAN`s

Para la implementación de la red, se necesita la creación de una VLAN para la red inalámbrica la misma que segmentará al switch de la red del CAFDER y así no generar demasiado tráfico en dicha red, la ESPE cuenta con una VLAN exclusiva para la red inalámbrica la misma que será creada en el switch del CAFDER.

A continuación, las Figuras 4.8., 4.9., y 4.10., muestra la creación de dicha VLAN en los puertos 33, 34, 35, 36, 37, 38, 39,40.

SW CAFDER 3com 3250

IP: 10.1.100.34

Paso para crear VLANS.

Bridge →VLAN

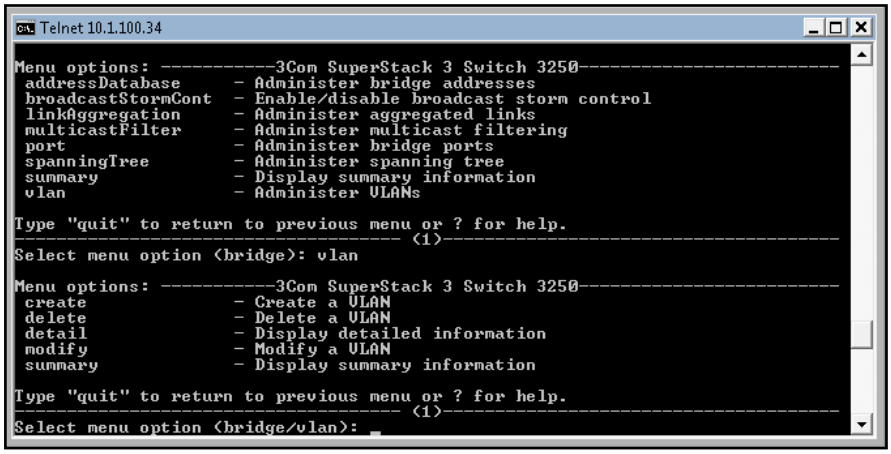


Figura. 4.8. Menú switch CAFDER

Creación de la VLAN

Bridge → VLAN → create

VLAN 2001 tagged

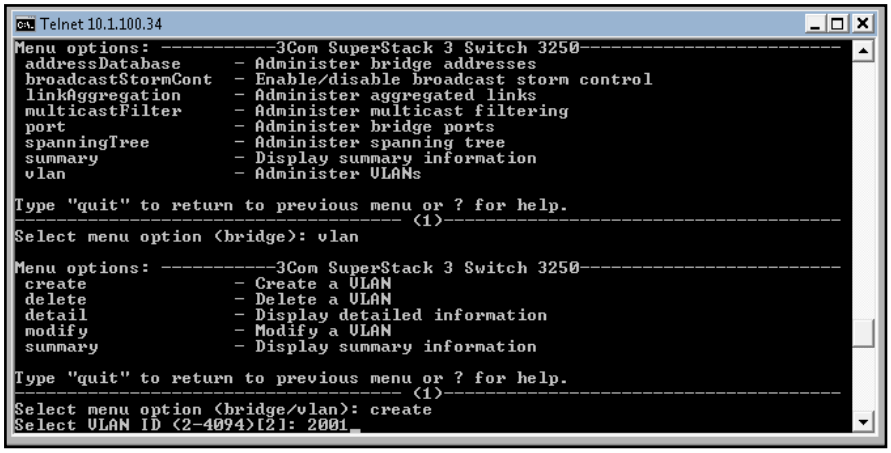


Figura. 4.9. Selección y creación VLAN

Selección de puertos a utilizar en VLAN 2001

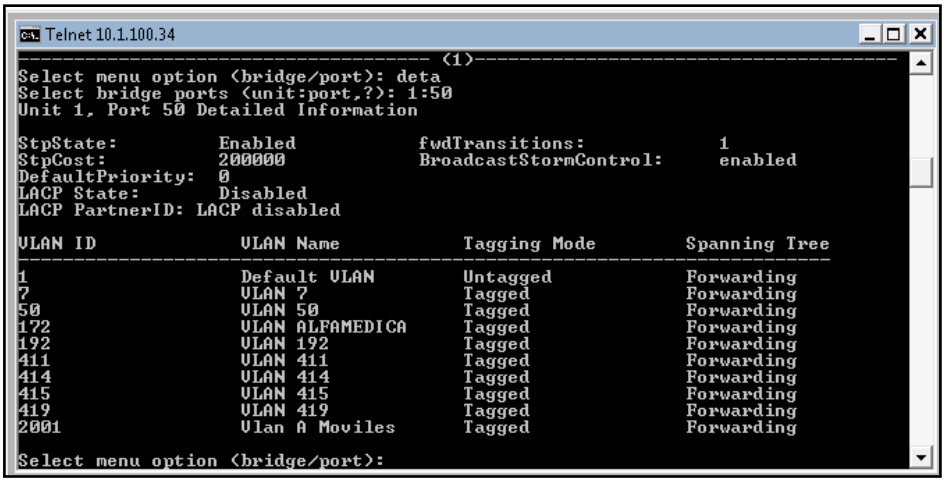


Figura. 4.10. Selección de puertos de VLAN

Con la creación de la VLAN 2001 en los puertos ya antes mencionados, se puede así realizar el direccionamiento IP de cada uno de los equipos de la red como lo son: servidor RADIUS, AP.

4.3.2 Direccionamiento IP

Para el direccionamiento se reservará la IP mediante las diferentes mac's de los equipos, tanto del servidor Radius como de los AP's, en el servidor DHCP general de la ESPE; como lo indica la Tabla 4.8.

Tabla. 4.8. Direccionamiento IP

EQUIPO	MAC	IP
Servidor RADIUS	00:0C:29:91:70:E7	10.1.204.97
CAFDER_ADMIN	00:1E:E5:2F:5F:13	10.1.204.94
CAFDER_PISO2	00:1D:7E:0A:45:66	10.1.204.98
CAFDER_PISO1a	00:18:F8:33:2A:C1	10.1.204.100
CAFDER_PISO1b	00:1E:E5:2F:5F:12	10.1.204.95
CAFDER_PLANTABAJA	00:21:29:A0:22:4A	10.1.204.101
CAFDER_COLISEO	00:21:29:A0:3F:D2	10.1.204.105
CAFDER_AULAS	00:22:B0:05:F5:C5	10.1.204.91

4.3.3 Implementación del servidor Radius

"FreeRADIUS es un paquete de software de código abierto y libre distribución que implementa diversos elementos relacionados con RADIUS, tales como una biblioteca BSD para clientes, módulos para soporte en apache, y un servidor de RADIUS. El servidor FreeRADIUS es modular, para facilitar su extensión, y es muy escalable; además, tiene casi todas las opciones que un usuario puede necesitar; como son:

- Realizar tareas de AAA, que puede almacenar y acceder a la información por medio de múltiples bases de datos: LDAP (AD, OpenLDAP,…), SQL (MySQL, PostgreSQL, Oracle,…) y ficheros de texto (fichero local de usuarios, mediante acceso a otros Realms, fichero de sistema /etc/passwd,…).

- Soporta prácticamente toda clase de clientes Radius (extensiones php de RADIUS, etc).

- Se puede ejecutar en múltiples sistemas operativos: Linux e incluso MS Windows por medio de cygwin.

- Soporta el uso de proxies y la replicación de servidores."[6]

[6] Radius Fin, Instalación y Configuración de un Servidor Radius, Marzo 2010

4.3.3.1 Instalación de FreeRADIUS

La versión de FreeRADIUS que se va a instalar es la 2.1.8, la misma que se puede descargar directamente de http://freeradius.org/download.html, se descarga los fuentes de FreeRADIUS (fichero .tar.gz) localmente en la máquina Fedora y luego se descomprime ó descarga los archivos ya compilados RPM.

Antes de poder compilar e instalar el servidor, necesitaremos una serie de paquetes adicionales de Fedora, dichos paquetes son: "gcc", "build_essential", "libssl-dev" y "libpq-dev". Para poder instalarlos necesitamos abrir una consola y pasar a ser superusuario (mediante la orden "su"), y usar la orden "yum install xxx" (donde xxx es el paquete a instalar), en general se necesita actualizar el sistema operativo Fedora mediante "**yum update**". La instalación está configurada para que la descarga se realice automáticamente por medio de ftp.

Una vez preparada la máquina para la compilación, podremos ir al directorio en el que se ha descomprimido toda la información necesaria ("cd freeradius-server-2.1.1"). El proceso básico de la instalación se encuentra descrito en el fichero de texto INSTALL.

Primero, debemos hacer una operación de configuración mediante el comando **"./configure "** podemos ver las opciones disponibles, nosotros usaremos las opciones por defecto. Una vez configurado el proceso, realizaremos la compilación mediante **"make"**, y posteriormente, si no ha ocurrido ningún error, instalaremos el software en el sistema mediante **"make install"**.

Si el proceso es correcto, se podrá ejecutar el servidor. Sin embargo, la primera vez que se ejecute el servidor se crearán los certificados necesarios para operar con EAP, antes de esta primera ejecución es conveniente configurar los certificados con los atributos que más se ajusten a nuestra instalación.

La configuración de los certificados se puede realizar editando los ficheros de configuración que se encuentran en /usr/local/etc/raddb/certs. Aquí podremos editar la configuración de los certificados de la autoridad certificadora (fichero ca.cnf), los usados como servidor (server.cnf), y los de cliente (client.cnf). Los atributos a configurar son: el país, provincia, localidad, organización, dirección de correo electrónico y nombre común.

Para su correcto funcionamiento, el servidor y la autoridad certificadora deben coincidir en país, estado y organización.

Una vez configurados los certificados, ya se puede ejecutar el servidor, mediante la orden “radiusd –X”, la X se utiliza para funcionar en modo debug, y así recibir información sobre los eventos que se suceden en el servidor). La primera vez que se ejecute el servidor se crearán los certificados necesarios. Si todo se instaló y configuró correctamente, el servidor debe quedarse escuchando en los puertos asociados a los servicios que ofrece. La configuración se muestra en la Figura 4.11.

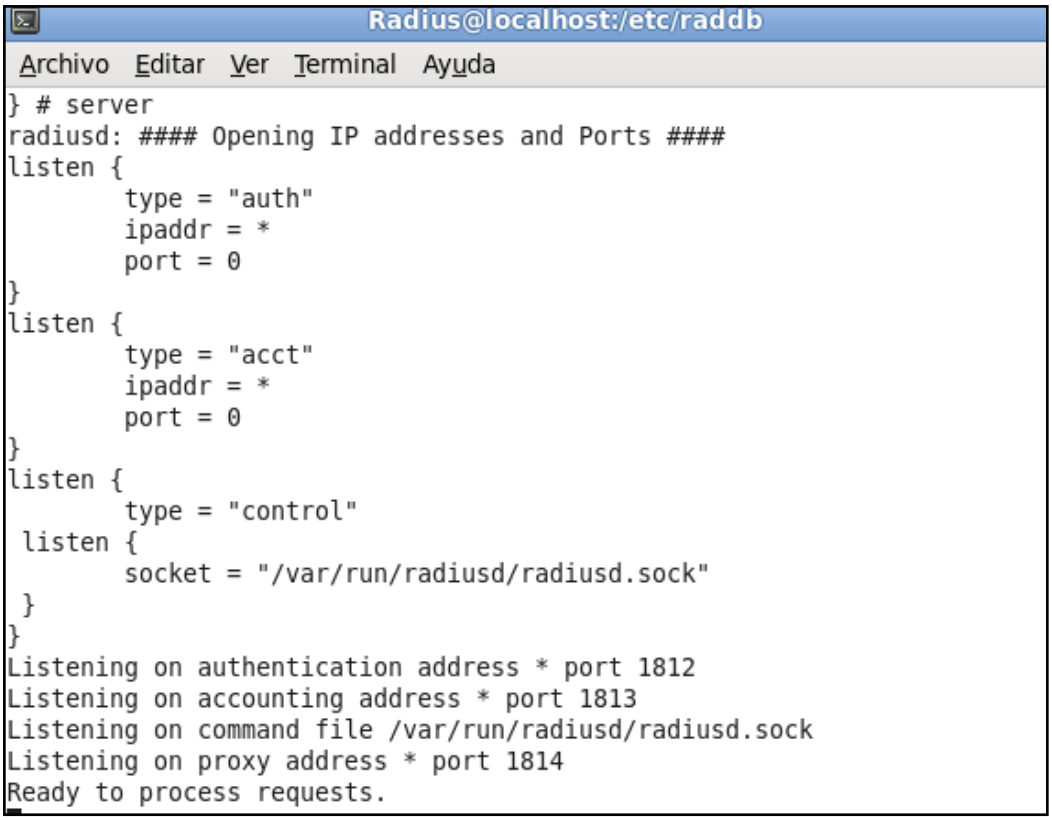


Figura. 4.11. Ejecución del Servidor Radius (radiusd –X)

Para comprobar que el servidor está funcionando correctamente, se puede hacer uso de la herramienta “radtest”, de la siguiente manera:

 # radtest usuario contraseña localhost 10 testing123

Donde “usuario” y “contraseña” son las credenciales de un usuario local de la máquina, “tesing123” es lo que se denomina un secreto mismo que viene creado por defecto, este permite asociar de manera segura un cliente al servidor, si todo es correcto la respuesta debe ser “Access-Accept”.

También se visualiza los mensajes en la pantalla que el servidor emite cuando éste recibe una solicitud en el modo debug (radiusd -X). Si se quiere ver una solicitud rechazada, podemos volver a realizar una solicitud de servicio, pero cambiando el secreto por otro cualquiera.

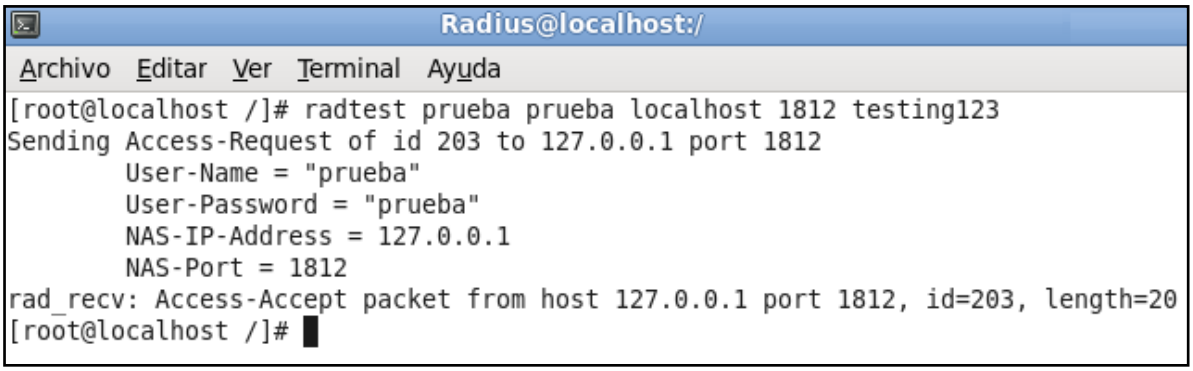


Figura. 4.12. Comprobación del servidor Radius con un usuario de prueba

4.3.3.2 Configuración del servidor Radius

Para la configuración del servidor Radius (freeradius) es necesario modificar los siguientes archivos:

- Radius.conf
- Users
- Clients.conf
- Eap.conf

Todos estos ubicados en el directorio /usr/local/etc/raddb si se realizó la instalación con los archivos .tar.gz, de lo contrario con los archivos RPM que se encuentran en /etc/raddb.

4.3.3.2.1. Radius.conf.

"Aquí podemos seleccionar aspectos relacionados con el servidor (ficheros de log, parámetros de uso máximo, usuarios, grupos, …), bases de datos a utilizar para autenticar y autorizar (ficheros, SQL, LDAP, …), métodos de AAA, etc. Para evitar una excesiva longitud de este fichero y por cuestiones de organización, "radiusd.conf" se subdivide en varios ficheros mediante la directiva "$INCLUDE":"[7]

- **eap.conf:** Se utiliza para configurar el tipo de EAP a emplear.
- **clients.conf**: Tiene la lista de clientes que están autorizados para usar los servicios de AAA proporcionados.
- **proxy.conf:** Este fichero configura directivas relacionadas con el funcionamiento en modo proxy y la lista de **realms**.
- Otros ficheros como **sql.conf** (para configurar el acceso a bases de datos SQL), policy.conf, etc.
- Además, el fichero "**users**" contiene información sobre la autenticación de suplicantes, de forma que incluso podemos añadir credenciales en forma de usuario y contraseña para permitir una configuración sencilla de usuarios (se debe tener en cuenta que estos usuarios serán realmente clientes del NAS, y no directamente del servidor RADIUS), sin embargo como se mostrará más adelante el ingreso de usuario se lo realizara mediante MySQL.

4.3.3.2.2. Eap.conf.

Se va a necesitar soporte de PEAP y mschapv2, para esto editamos el fichero eap.conf, y cambiamos el atributo "default_eap_type" general, de "md5" a "**peap**" (en minúsculas), y en el apartado de peap asegurarse de que "default_eap_type" esté a "mschapv2". En principio, si usamos la versión 2.1.8 de Radius no deberíamos necesitar cambiar nada más en este fichero, ya que la parte de "peap" está descomentada por defecto.

[7] Radius Fin, Instalación y Configuración de un Servidor Radius, Marzo 2010

4.3.3.2.3. Clients.conf.

A continuación, se informa al servidor RADIUS de que va a tener como cliente un punto de acceso. Para ello, se edita el fichero clients.conf, como se muestra en la Figura 4.13.,, y añadimos las siguientes líneas:

```
client 192.168.1.1 {
        secret        = ESPE
        shortname = CAFDER
}
```

```
#AP CAFDER
client 10.1.0.0/8{
        secret = ESPE
        shortname = CAFDER_ADMIN
}
```

Figura. 4.13. Configuración Client.conf

Como se observa, en el punto de acceso se configura toda una subred como es la 10.1.0.0/8, por la configuración del propio punto de acceso que vamos a emplear, y como secreto para la configuración posterior de NAS en el punto de acceso usaremos "ESPE".

4.3.3.2.4. Users.

Por último, se va a añadir un usuario que será utilizado por el suplicante cuando solicite acceso a la red inalámbrica. Para esto editamos el fichero users, y añadimos el siguiente usuario y contraseña es decir usuario: prueba y contraseña: *prueba*,

"prueba" *Cleartext-Password := "prueba"*
Reply-Message = "Bienvenido"

Para que la nueva configuración del servidor tenga efecto, se reinicia el servidor con el siguiente comando "*service radiusd restart*".

4.3.3.2.5. Certificados.

La creación de los certificados es la parte que proveerá de conectividad al usuario que intente conectarse a cualquier AP mismo que se encuentre conectado al servidor RADIUS; es decir el certificado es el que valida el usuario en cualquier computador.

Si el certificado no existe en el computador el usuario nunca podrá validarse dentro de la red a utilizar, para generar el certificado deseado editamos el archivo *ca.cnf* ubicado en *"#cd etc/raddb/cert"*, el mismo puede ser editado de cualquier manera sin embargo la configuración elegida es la que se muestra en la Figura 4.14.,:

```
[certificate_authority]
countryName             = FR
stateOrProvinceName     = Sangolqui-ESPE
localityName            = CAFDER-RADIUS
organizationName        = HECTOR ANANGANO CRISTIAN ARCE
emailAddress            = hectorzrs@hotmail.com
commonName              = "CERTIFICADO RADIUS-AUTHORITY"
```

Figura. 4.14. Configuración *ca.conf*

Los certificados generados tienen un tiempo de caducidad de 6 meses, con lo que se garantiza que al inicio del nuevo semestre nuevos alumnos no puedan conectarse a la red inalámbrica o a su vez la sigan utilizando alumnos que no se encuentren matriculados en el departamento.

Después de la configuración realizada, se guarda el archivo y se ejecuta los siguientes comandos:

#make ca.pem

#make ca.der

Con esto tenemos generado el certificado el mismo que se le otorga permisos *("#chmod 777 ca.pem")* para poder distribuirlo en los diferentes usuarios de la red.

4.3.3.2.6. Instalación y Configuración de daloRADIUS.

Para la utilización de daloRADIUS se debe crear y configurar MySQL para así poder utilizar la base de datos, descargamos la versión más reciente y estable de daloRADIUS de la siguiente dirección: http://softlayer.dl.sourceforge.net/project/daloradius/daloradius/daloradius-0.9-8/daloradius-0.9-8.tar.gz, para descomprimirlo se utiliza "*#tar xvzf daloradius-0.9-8.tar.gz"* dependiendo de donde se encuentre descargado el archivo. Luego, se copia el archivo descomprimido en el directorio WEB de fedora:

#cp daloradius-0.9-8 /var/www/html/daloradius -R

Después se instalan algunas librerías para el correcto funcionamiento de MySQL.

#yum install php-mysql
#yum install php-gd
#yum install php-pear
#yum install php-pear-DB

Creamos la base de datos de daloRADIUS en MySQL, accesamos a la administración de MySQL, *"#mysql –u root -p"* con contraseña *"admin"*, luego creamos la base de datos, *"CREATE DATABASE dalo",* creamos un usuario "*dalo"* y contraseña *"dalo"* para la base de datos dalo con la siguiente sentencia *"GRANT ALL ON dalo.* TO dalo@localhost IDENTIFIED by ´´dalo´´ ",* salimos de la base con *"exit"*.

En la configuración de radiusd.conf ubicado en /etc/raddb/radiusd.conf y descomentamos la línea "*$INCLUDE sql.conf*", también se configura el fichero *"sql.conf"* como se muestra en la Figura 4.15.:

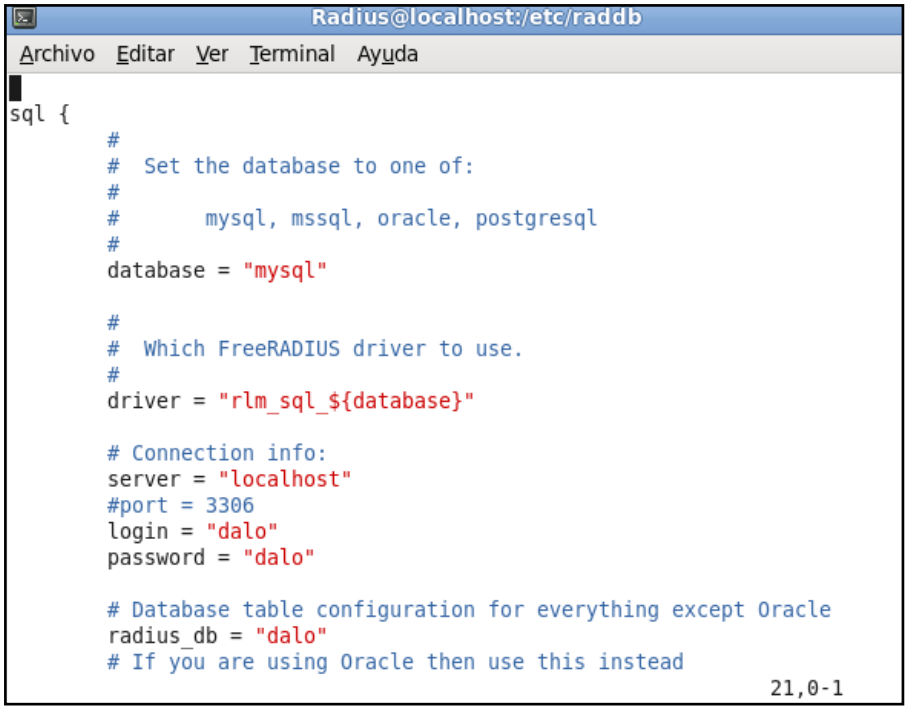


Figura. 4.15. Configuración fichero sql.conf

Después se cambia los permisos y propietarios del directorio daloRADIUS para que sea el propietario apache y tenga además todos los permisos de dicho directorio; con los siguientes comandos:

#chow apache.apache /var/www/html/daloradius

#chmod 777 /var/www/html/daloradius

Luego se crean las tablas de daloRADIUS para MySQL, utilizamos el siguiente comando:

#mysql -u root -p dalo < /var/www/html/daloradius/contrib/db/fr2-mysql-daloradius-and-freeradius.sql

Para observar las tablas creadas se ingresa al mysql *"#mysql –u root –p"* con contraseña *"admin"* , digitamos:

mysql>use dalo;

mysql>show tables;

Y se observará lo indicado en la Figura 4.16:

```
+-----------------+
| Tables_in_dalo  |
+-----------------+
| billing_history |
| billing_paypal  |
| billing_plans   |
| billing_rates   |
| dictionary      |
| hotspots        |
| nas             |
| operators       |
| proxys          |
| radacct         |
| radcheck        |
| radgroupcheck   |
| radgroupreply   |
| radippool       |
| radpostauth     |
| radreply        |
| radusergroup    |
| realms          |
| userbillinfo    |
| userinfo        |
| wimax           |
+-----------------+
21 rows in set (0.00 sec)
```

Figura. 4.16. Tablas daloRADIUS en MySQL

Para salir de MySQL se digita *"exit;"*, se realiza los siguientes cambios en el fichero: *"daloradius.conf.php"* ubicado en *"#cd var/www/html/daloradius/library";* como lo muestra la Figura 4.17:

```
$configValues['DALORADIUS_VERSION'] = '0.9-8';
$configValues['FREERADIUS_VERSION'] = '1';
$configValues['CONFIG_DB_ENGINE'] = 'mysql';
$configValues['CONFIG_DB_HOST'] = '127.0.0.1';
$configValues['CONFIG_DB_USER'] = 'dalo';
$configValues['CONFIG_DB_PASS'] = 'dalo';
$configValues['CONFIG_DB_NAME'] = 'dalo';
$configValues['CONFIG_DB_TBL_RADCHECK'] = 'radcheck';
$configValues['CONFIG_DB_TBL_RADREPLY'] = 'radreply';
$configValues['CONFIG_DB_TBL_RADGROUPREPLY'] = 'radgroupreply';
$configValues['CONFIG_DB_TBL_RADGROUPCHECK'] = 'radgroupcheck';
$configValues['CONFIG_DB_TBL_RADUSERGROUP'] = 'radusergroup';
```

```
$configValues['CONFIG_DB_TBL_RADNAS'] = 'nas';
$configValues['CONFIG_DB_TBL_RADPOSTAUTH'] = 'radpostauth';
$configValues['CONFIG_DB_TBL_RADACCT'] = 'radacct';
$configValues['CONFIG_DB_TBL_RADIPPOOL'] = 'radippool';
$configValues['CONFIG_DB_TBL_DALOOPERATOR'] = 'operators';
$configValues['CONFIG_DB_TBL_DALORATES'] = 'rates';
$configValues['CONFIG_DB_TBL_DALOHOTSPOTS'] = 'hotspots';
$configValues['CONFIG_DB_TBL_DALOUSERINFO'] = 'userinfo';
$configValues['CONFIG_DB_TBL_DALOUSERBILLINFO'] = 'userbillinfo';
$configValues['CONFIG_DB_TBL_DALODICTIONARY'] = 'dictionary';
$configValues['CONFIG_DB_TBL_DALOREALMS'] = 'realms';
$configValues['CONFIG_DB_TBL_DALOPROXYS'] = 'proxys';
$configValues['CONFIG_DB_TBL_DALOBILLINGPAYPAL'] = 'billing_paypal';
$configValues['CONFIG_DB_TBL_DALOBILLINGPLANS'] = 'billing_plans';
$configValues['CONFIG_DB_TBL_DALOBILLINGRATES'] = 'billing_rates';
$configValues['CONFIG_DB_TBL_DALOBILLINGHISTORY'] = 'billing_history';
$configValues['CONFIG_FILE_RADIUS_PROXY'] = '/etc/raddb/proxy.conf';
$configValues['CONFIG_PATH_RADIUS_DICT'] = '';
$configValues['CONFIG_PATH_DALO_VARIABLE_DATA'] = '/var/www/html/daloradius/var';
$configValues['CONFIG_DB_PASSWORD_ENCRYPTION'] = 'cleartext';
$configValues['CONFIG_LANG'] = 'en';
$configValues['CONFIG_LOG_PAGES'] = 'no';
$configValues['CONFIG_LOG_ACTIONS'] = 'no';
$configValues['CONFIG_LOG_QUERIES'] = 'no';
$configValues['CONFIG_DEBUG_SQL'] = 'no';
$configValues['CONFIG_DEBUG_SQL_ONPAGE'] = 'no';
$configValues['CONFIG_LOG_FILE'] = '/tmp/daloradius.log';
$configValues['CONFIG_IFACE_PASSWORD_HIDDEN'] = 'no';
$configValues['CONFIG_IFACE_TABLES_LISTING'] = '25';
$configValues['CONFIG_IFACE_TABLES_LISTING_NUM'] = 'yes';
```

Figura. 4.17. Configuración daloradius.conf.php

Terminamos editando el archivo *"default"*, ubicado en *"#cd etc/raddb/sites-available"*, se agrega la variable *sql* en las secciones de *autorize{....}* y *accounting {....}*. Luego para que se inicien todos los servicios al momento de arrancar el servidor se realiza lo siguiente.

#chkconfig mysqld on

#chkconfig httpd on

#chkconfig radiusd on

Para probar que todo funciona correctamente, se inicia un explorador en la que se ingresa *http://localhost/daloradius* y deberá lo indicado en la Figura 4.18:

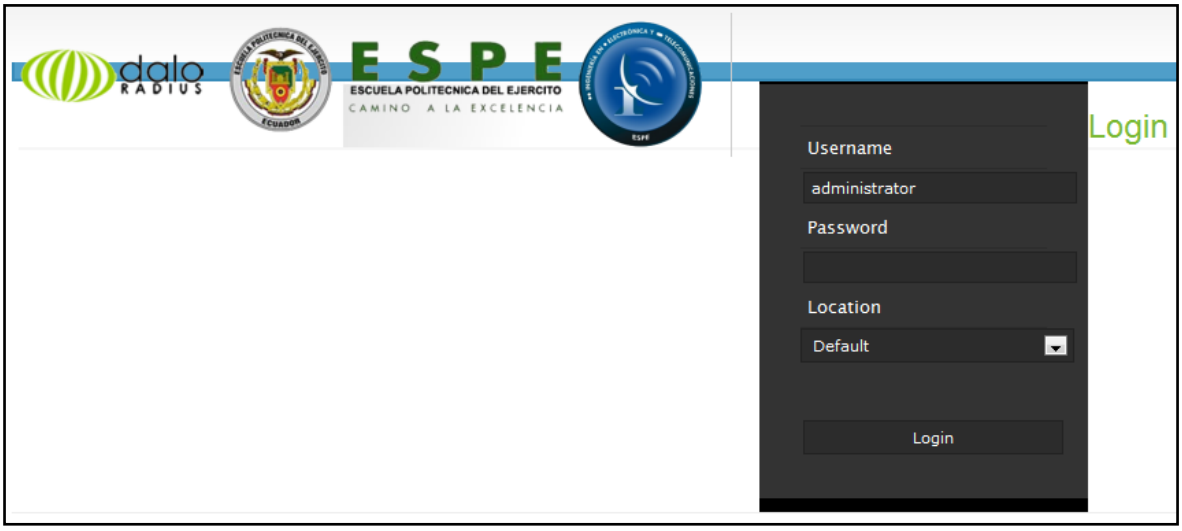


Figura. 4.18. Login daloRADIUS

El Username es ***administrator*** y el Password es ***radiusespe***, luego agregamos un usuario para realizar las pruebas respectivas; en nuestro caso agregamos *test* con password *test*, como se muestra en la Figura 4.19:

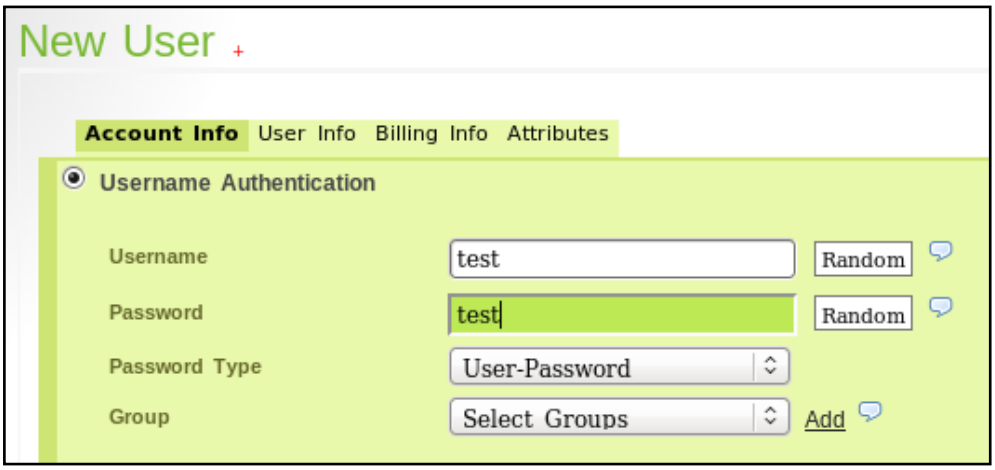


Figura. 4.19. Usuarios en daloRADIUS

DaloRADIUS presenta una herramienta para realizar pruebas con el usuario agregado Test User Connectivity, como se puede observar en la Figura 4.20.

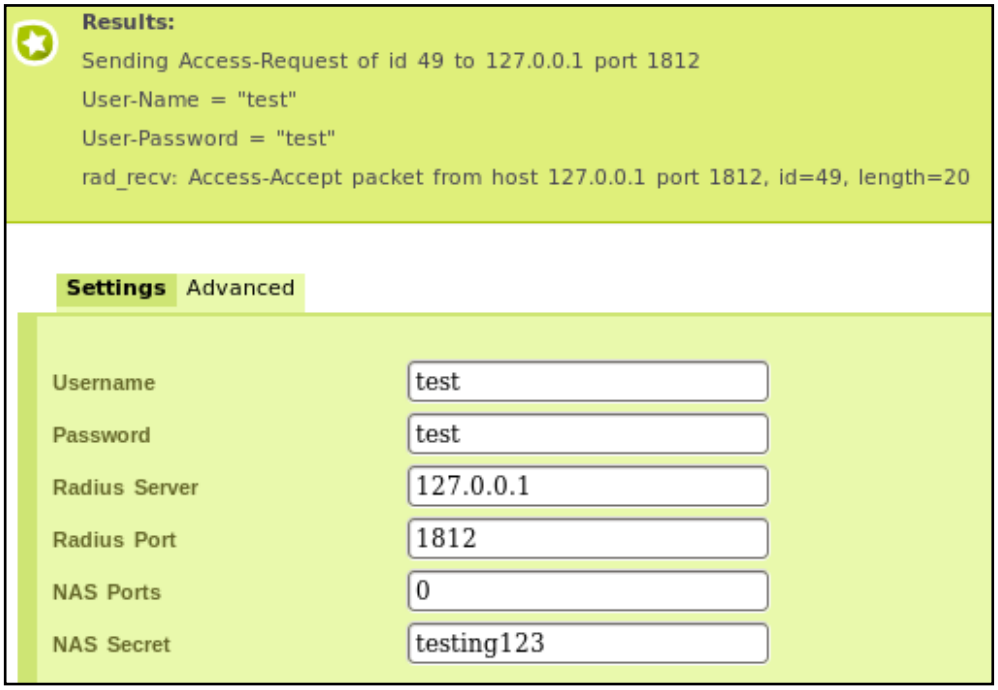


Figura. 4.20. Test de conectividad con user: test

4.3.3.3 Configuración de un punto de acceso para autenticar con Radius

Se configura el uso de RADIUS en un punto de acceso, que además tendrá funciones de router y asignación de direcciones privadas con NAT ó a su vez puede ser un Acces Point.

La configuración del punto de acceso (router ó acces point), suele hacerse mediante interfaz de Web. Además, el punto de acceso debe encontrarse en la misma red que el servidor RADIUS.

Accederemos a la pantalla de configuración (Figura 4.21) del punto de acceso mediante Web, usando el usuario y contraseña requeridos para la administración. Primero se configura el SSID del punto de acceso en el ejemplo se lo configurara como CAFDER_ADMIN, también se configura el canal en el que operara dicho router inalámbrico.

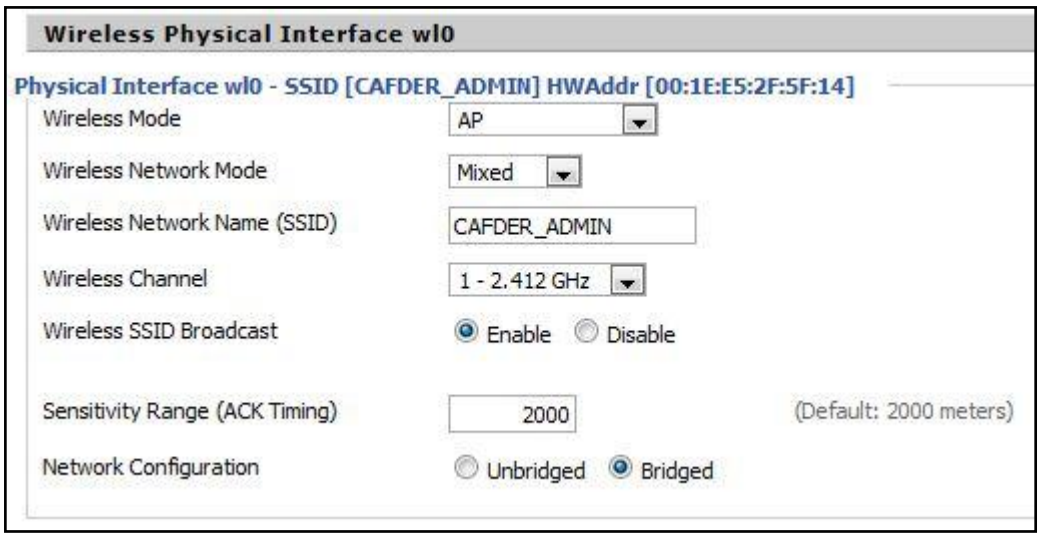


Figura. 4.21. Configuración de SSID

Por último, para indicar que estamos usando un servidor RADIUS, se accede a la parte de seguridad y configurarlo como RADIUS e introducimos la dirección IP de la máquina que ejecuta el servidor y la palabra secreta (en nuestro caso, "tesis"). Se guarda esta configuración y habremos terminado, como e indica en la Figura 4.22.

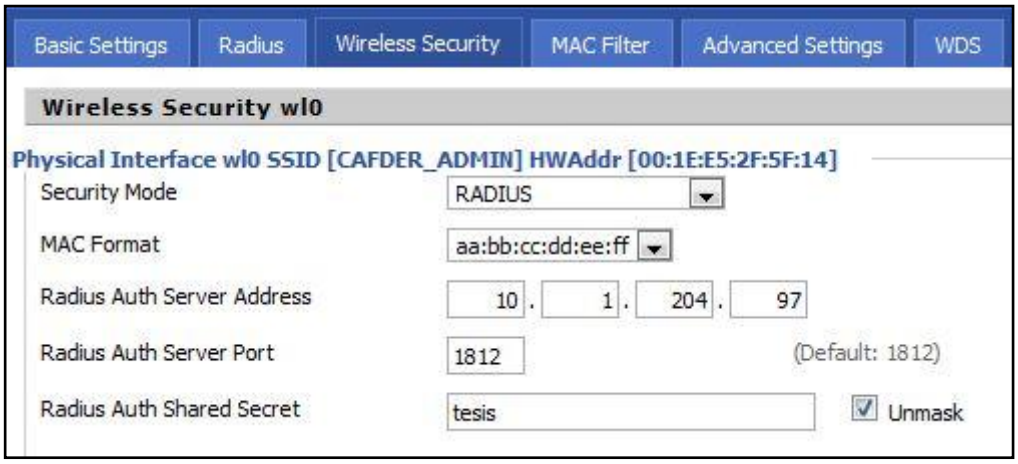


Figura. 4.22. Configuración de Seguridad

4.3.3.4 Configuración del suplicante (usuario del AP)

Se configura el computador que se utilizará para la autenticación con el servidor RADIUS. Primero se agrega el certificado generado en el servidor RADIUS (ca.pem), se inicia un explorador y se dirige a:

Herramientas >> Opciones de Internet >> Pestaña Contenido >> Certificados >> Pestaña Entidades de certificación raíz de confianza.

Una vez agregado el certificado agregamos la red inalámbrica a la que deseemos conectarnos:

Inicio >> Panel de Control >> Centro de redes y recursos compartidos >> Administrar redes inalámbricas >> Agregar >> Crear un perfil de red manualmente.

Luego configuramos como muestra en la Figura 4.23:

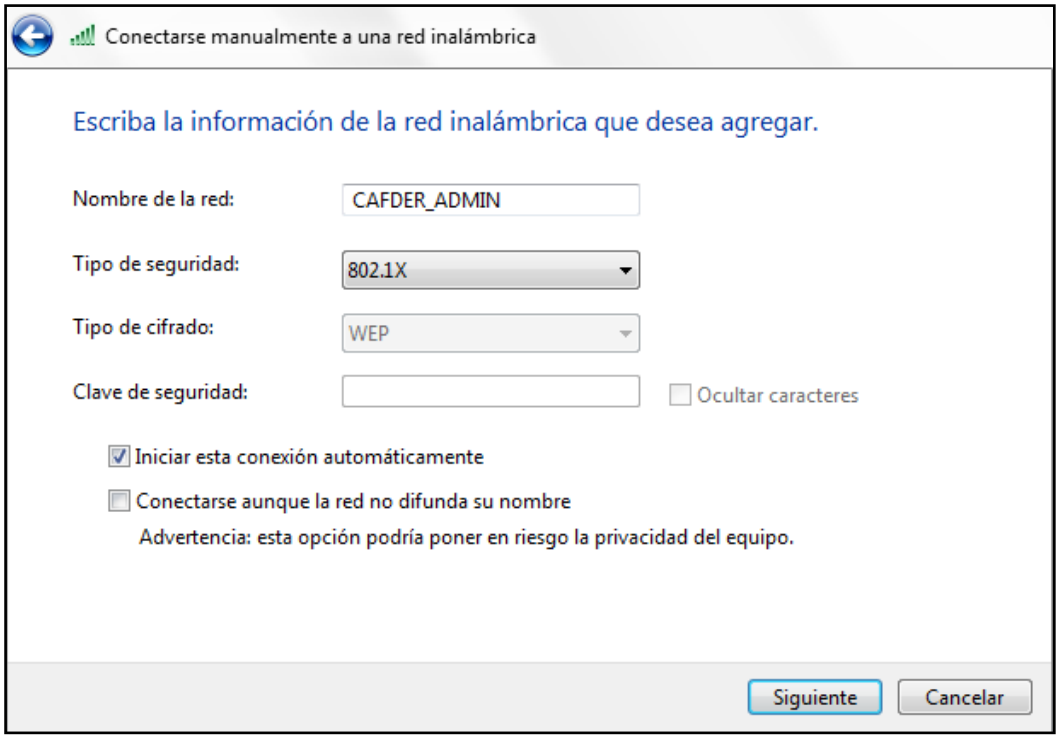


Figura. 4.23. Configuración manual de red inalámbrica

Luego presionamos, Siguiente >> Cambiar la configuración de conexión; y configuramos como se muestra en la Figura 4.24:

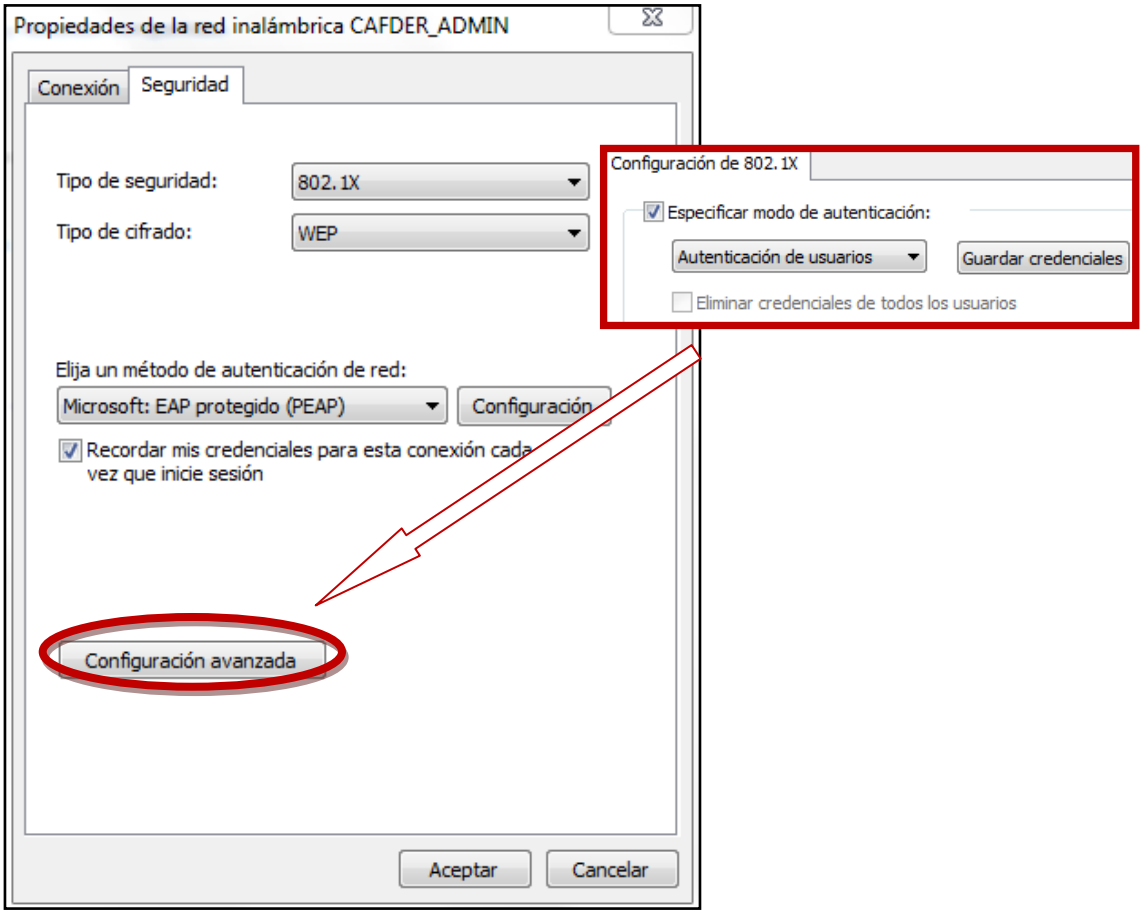


Figura. 4.24. Configuración de conexión

Con eso el computador del usuario estará listo para validarse con el servidor RADIUS.

4.4 ANÁLISIS DE COSTOS

Para realizar el análisis de costos se toma en cuenta que un servidor mediano tiene las siguientes características:

Tabla. 4.9. Características del Servidor Mediano

Procesador	SERVIDOR x3650 M2 (Rack 2U), 1 x Intel Xeon E5530 /2, Quad Core 2.4GHz / 1066MHz / 8MB L3, 2 x 2GB /128GB (64GB por Procesador), HS 0GB / 3600GB (SAS Controller) ==> 8, hasta 12 discos con 46D2516, IBM ServeRAID™ (RAID 0, 1 & 1E) CD-RW/DVD Combo / NO Floppy, Dual Gigabit, 2 x 675W (Hot Swap) / 2, 4 USB, 1serial, NO paralelo, (3-3-3)
RAM	8 GB
Discos Duros	2 discos de 300Gb c/u

Sin embargo todos los valores mencionados en la Tabla 4.10., pueden variar dependiendo tanto del proveedor como de la marca a utilizar, además de agregar los respectivos impuestos (IVA) a cada valor mencionado.

Tabla. 4.10. Análisis de costos

REFERENCIA	DESCRIPCION	CANT	V. UNITARIO	V.TOTAL
DWRT54GS	Linksys Wireless Router	7	320	2240
HP	Servidor Mediano(8GB RAM 600GB DD)	1	5800	5800
PANDUIT	Patch Panel cat 5e 24 ports modular	1	38	38
QPCOM	Rollo de cable UTP cat 5e solido gris	1	88	88,00
DEXSON	Canaleta lisa 20*12 blanco	15	1,3	19,50
DEXSON	Caja sobre puesta 40mm blanco	9	1,7	15,30
INTELLINET	Jack minicom cat 5e azules	9	2,95	26,55
NEXXT	Face plates 1 posc. Blanco	9	1,45	13,05
INTELLINET	Jack minicom cat 5e azules	9	2,95	26,55
VARIOS	Cinta espuma blanca doble faz 5mx18	1	5,19	5,19
VARIOS	Cinta doble Faz, cinta taype, amarras			10,00
VARIOS	Amarras, tornillos, tacos, broca			4,00
			TOTAL	**8286,14**

CAPÍTULO V

IMPLEMENTACIÓN DE LA RED INALÁMBRICA

5.1 DIAGRAMAS DE RED

En la VLAN creada en el switch del CAFDER se adicionará el servidor Radius, el mismo que contendrá a su vez la base de datos (MySQL-Server) y el servidor de autenticación; como la VLAN 2001 es la configurada en dicho switch trabajaremos en la red 10.1.204.0 / 8, como se muestra en la Figura 5.1.

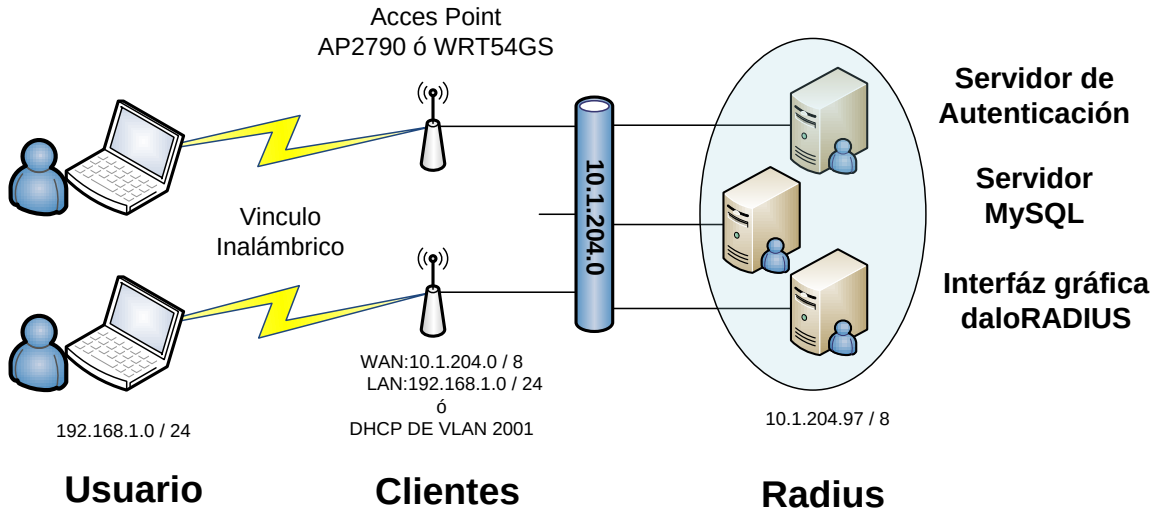


Figura. 5.1. Diagrama de Red

Como los AP's de prueba a utilizar son los WRT54GS, entonces en el puerto ethernet WAN se coloca la subred asignada por la VLAN (10.1.204.0 / 8) y en los puertos ethernet LAN (red inalámbrica) se utilizará el DHCP del propio equipo que está

configurado con la subred 192.168.1.0 / 24 con la finalidad de no saturar al DHCP de la VLAN asignada.

Tanto el servidor RADIUS como el puerto ethernet WAN de cada AP se encontrarán en la subred 10.1.204.0 / 8, mientras que los usuarios y el puerto ethernet LAN (red inalámbrica) de cada AP se encontrarán en la subred 192.168.1.0 / 24.

5.2 IMPLEMENTACION Y PRUEBAS DE LA RED INALAMBRICA

Para la implementación de la red inalámbrica, se necesita puntos de red los mismos que serán colocados según el diseño de la red inalámbrica descrito en el Capítulo: *4.2. Diseño de la red inalámbrica*, sin embargo, y luego de varias pruebas realizadas se observó la necesidad de mover dichos puntos hasta lograr una cobertura más óptima.

5.2.1 Cableado estructurado

Para realizar el cableado estructurado para la red inalámbrica, se siguió las siguientes rutas para cada uno de los puntos; optimizando la cobertura de cada una de ellas, tomando como referencia las observaciones realizadas en el diseño descrito anteriormente.

Todos los AP se colocarán a 20cm del punto de red (Figura 5.2), y la dirección de las antenas serán hacia fuera siguiendo la misma línea de referencia del punto de red; mientras que el resto del cableado se realizara con cable UTP Cat. 5e; ya que el edificio no presenta problemas de atenuaciones considerables.

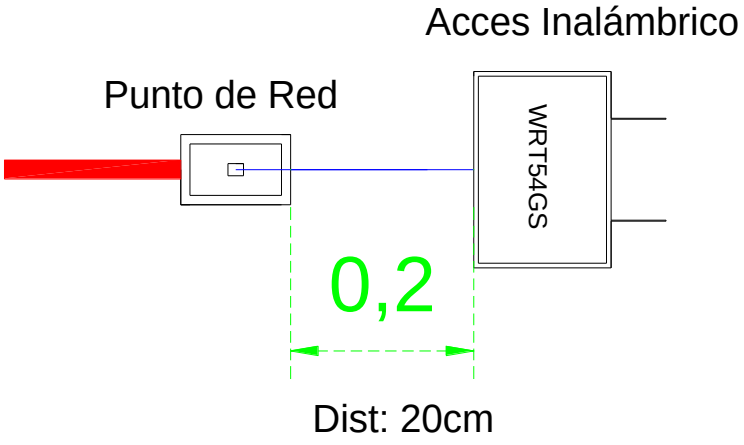


Figura. 5.2. Distancia punto de red-acces.

A continuación se muestra la trayectoria del cable para los diferentes puntos de red implementados, tomando en cuenta que cada piso se encuentra a 2.50 mtrs del siguiente solo se mostrarán las rutas de cada piso en el cual se instaló el punto de red.

5.2.1.1 Planta baja (CAFDER_PLANTA BAJA)

Como se observa en la Figura 5.3., se tiene una distancia considerable en la planta baja de 4.8 metros; mientras que la distancia total desde el rack hasta el punto de red es 24.2 metros.

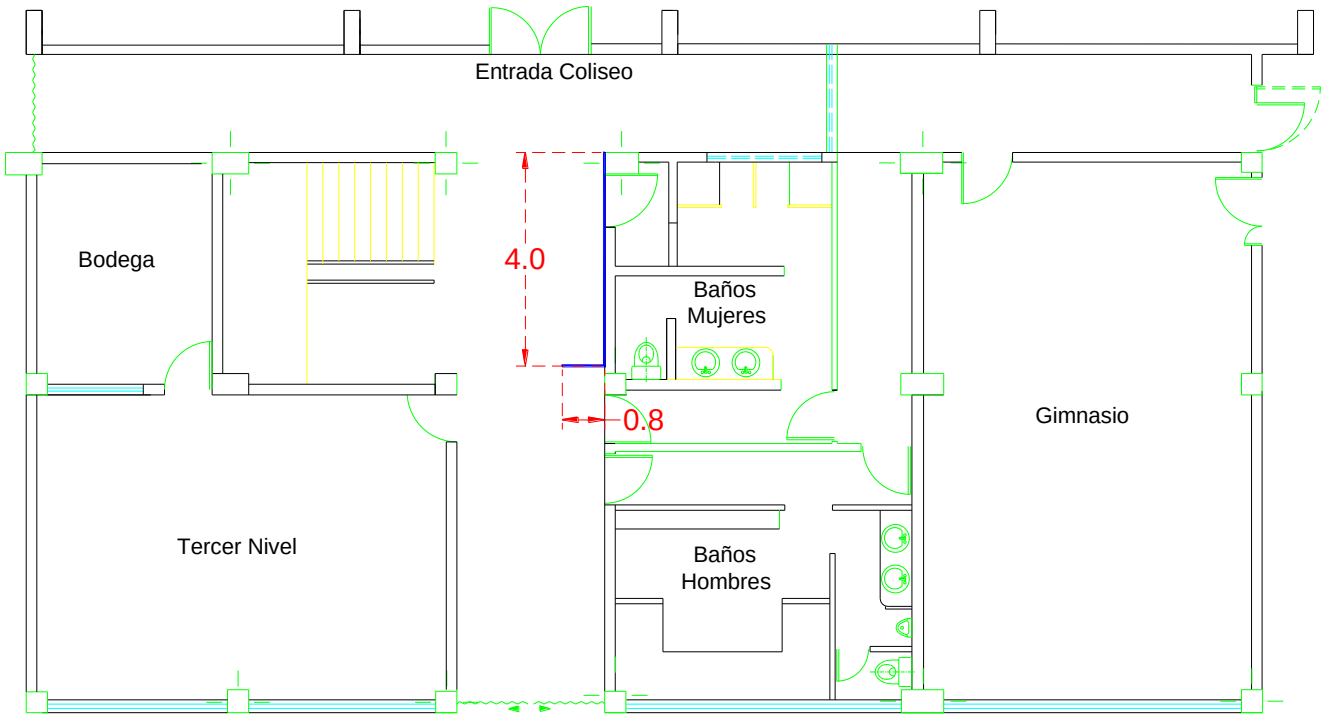


Figura. 5.3. Trayectoria y Distancias de CAFDER_PLANTABAJA

5.2.1.2 Primer piso (CAFDER_PISO 1a)

Como se observa en la Figura 5.4., la trayectoria descrita en color rojo es la correspondiente a CAFDER_PISO1a, mientras que la trayectoria en azul es CAFDER_PISO1b.

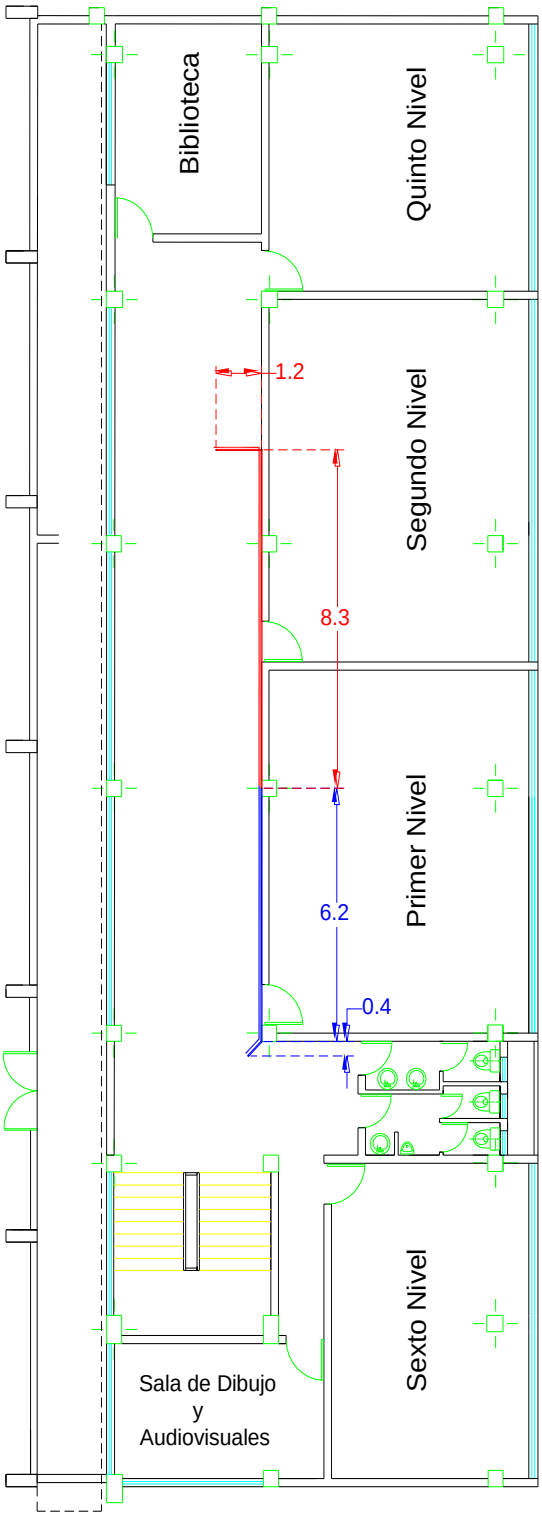


Figura. 5.4. Trayectoria y Distancia de CAFDER_PISO1a,b

La trayectoria de CAFDER_PISO1a tiene una distancia de 9.5 metros en el primer piso, mientras que la distancia total de todo el recorrido desde el rack de distribución hasta el punto de red es de 16.1 metros; la trayectoria de CAFDER_PISO1b en el primer piso es de 6.6 metros y el recorrido total del cable es de 13 metros.

5.2.1.3 Segundo piso (CAFDER_PISO 2 / CAFDER_ADMIN)

En la Figura 5.5., muestra la trayectoria de CAFDER_PISO2 (color rojo), mientras que la trayectoria de CAFDER_ADMIN se muestra con azul.

La trayectoria total de CAFDER_PISO2 es de 11.8 metros y la trayectoria total de CAFDER_ADMIN es de 19.2 metros.

Cabe recalcar que el rack de distribución se encuentra en el segundo piso, razón por la cual la distancia de CAFDER_PISO2 es mucho menor que las distancias anteriores; sin embargo la distancia de CAFDER_ADMIN es de 19.2 metros debido a la trayectoria que debe pasar por el edificio, además se debe tomar en cuenta las trayectorias verticales de cada uno de los puntos, tanto para el ingreso al rack de distribución como para su colocación en el patch panel y para la ponchada del mismo.

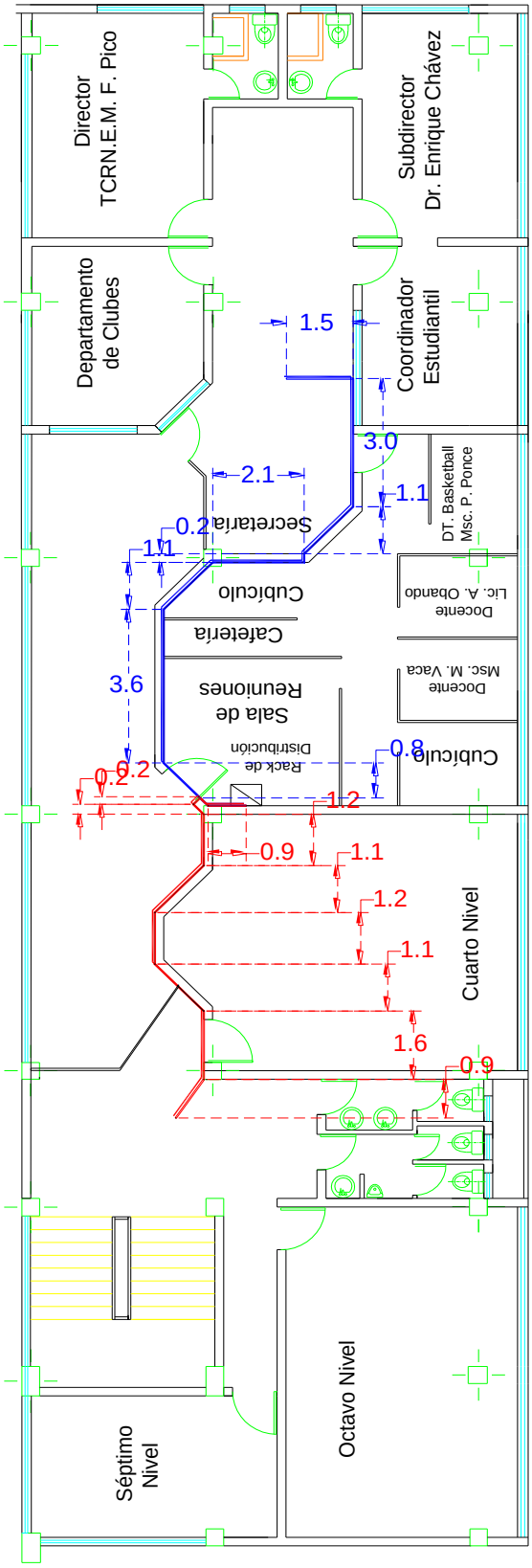


Figura. 5.5. Trayectoria, Distancia de CAFDER_PISO2 y CAFDER_ADMIN

5.2.1.4 Coliseo (CAFDER_COLISEO)

Para la implementación de CAFDER_COLISEO se reubico el punto de red R21-P1-11, él mismo que se lo ubico en el lugar deseado para el AP; por lo que la distancia que tiene el punto de red es de 99.7 metros; como se observar, la ubicación del punto de red se encuentra dentro de las normas de cableado estructurado. Ver Figura 5.6

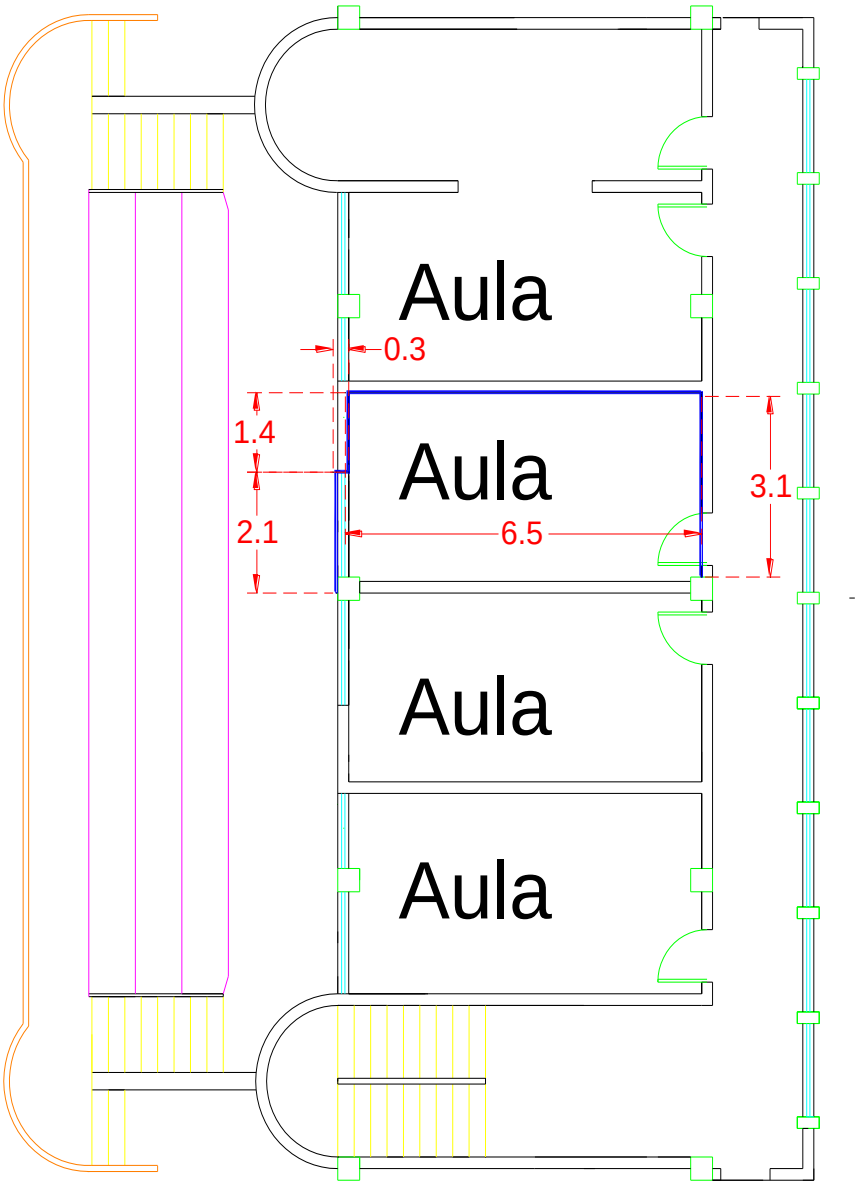


Figura. 5.6. Trayectoria y Distancia de CAFDER_COLISEO

5.2.1.5 Fisioterapia (CAFDER_AULAS)

Para la implementación de CAFDER_AULAS se tomó en cuenta que UTICS implementará un nuevo rack en las instalaciones, razón por la cual este punto de red no va al rack principal, en el cual se encuentran conectados los demás puntos, ya que la distancia para llegar a dicho rack sobrepasa los 100 metros y se tendrá una conexión defectuosa con pérdidas de paquetes; la ubicación exacta del nuevo rack es desconocida, razón por la cual se procedió a dejar un excedente superior al normal en el cable, la distancia que tiene el mismo es de 13.4 metros. Ver Figura 5.7

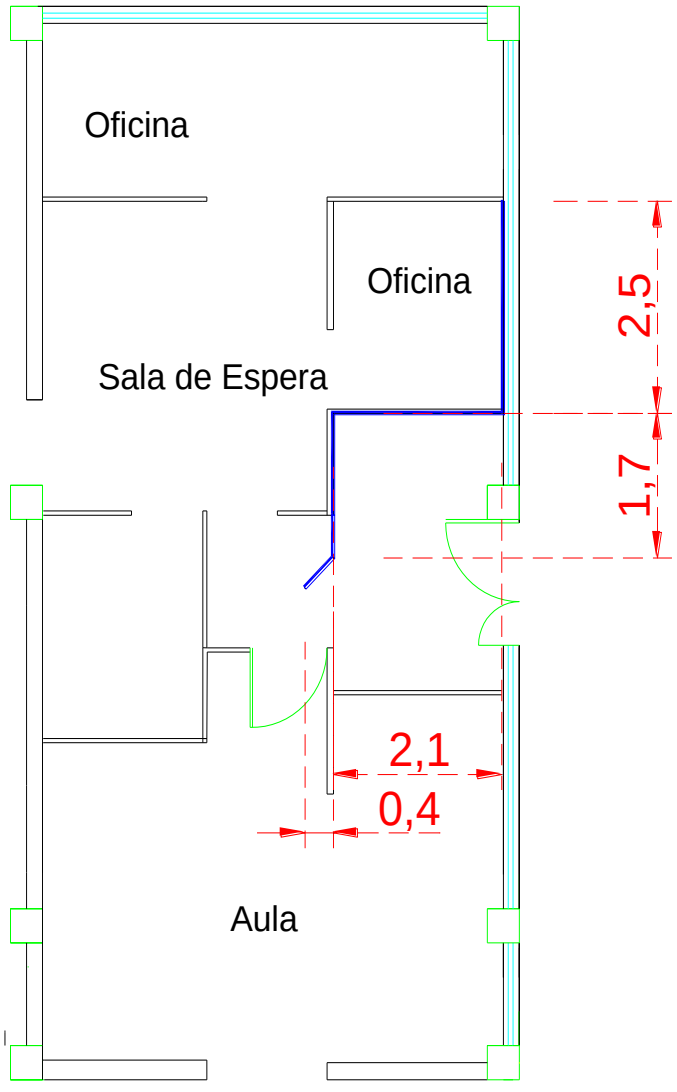


Figura. 5.7. Trayectoria y Distancia de CAFDER_AULAS

5.2.1.6 Certificación del cableado estructurado

Para la certificación de los puntos de red instalados, se utilizó el equipo DTX Cable Analizer; el mismo que necesita del software Fluke networks Linkware para descargar los resultados de la certificación.

LinkWare Cable Test Management Software.

"El software de comprobación de cableado LinkWare, permite administrar los datos de los resultados de varios certificadores desde una única aplicación de software."[1]

"LinkWare permite administrar los datos de los resultados procedentes de múltiples instrumentos de pruebas con una aplicación informática para PC; además permite que la configuración del proyecto sea mucho más sencilla ya que ayuda a organizar, editar, visualizar, imprimir, guardar o archivar resultados de las pruebas por centro de trabajo, cliente, campus o edificio.

Por otra parte; es posible combinar los resultados de las pruebas en una base de datos de LinkWare ya existente y, a continuación, ordenar, buscar y organizar los resultados por campos o parámetros de datos. Y todo ello contando con la integridad segura de todos los datos. Cualquier dato que se cargue a su ordenador con LinkWare garantiza que los resultados que almacena proceden de la memoria de los certificadores."[2]

Los resultados se muestran en la Figura 5.8. Certificación de CAFDER_PLANTABAJA, como se observa el archivo de certificación nos muestra datos de pérdida de inserción, mapa del cableado, entre otros los mismo que son necesarios para certificar que el punto de red realizado trabajará de una manera optima, los demás resultados se encuentran en el ANEXO 3.

[1] LinkWare Cable Test Management Software, www.flukenetworks.com/fnet/es-es/products/LinkWare/Overview, Abril2010
[2] LinkWare Cable Test Management Software, www.flukenetworks.com/fnet/es-es/products/LinkWare/Overview, Abril 2010

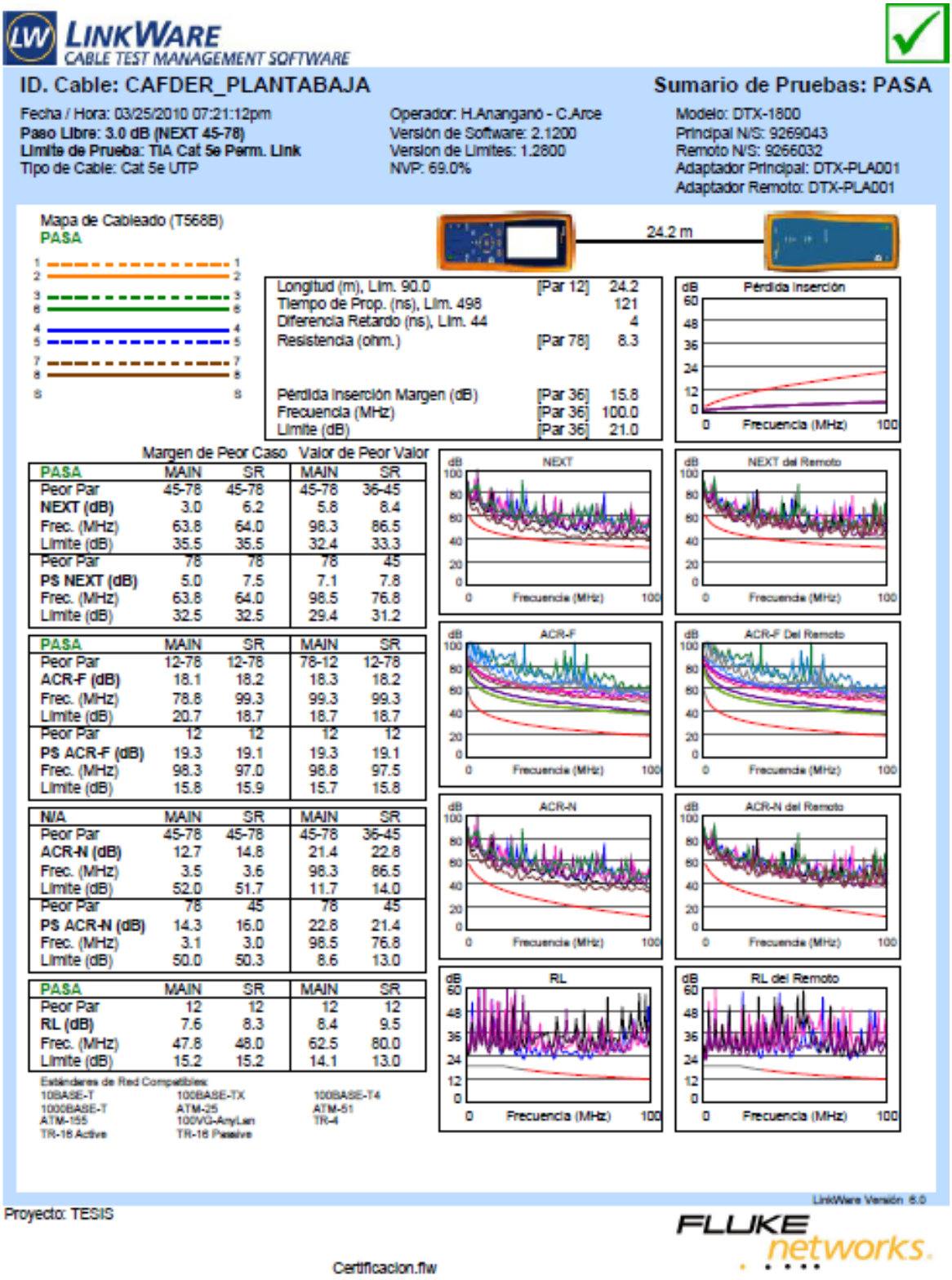


Figura. 5.8. Certificación, Punto de Red CAFDER_PLANTABAJA

5.2.1.7 Identificación de los puntos de red implementados

Después de certificar todos los puntos realizados se procede a realizar la identificación de los mismos, como se muestra en la Tabla 5.1:

Tabla. 5.1. Identificación de Puntos de Red Implementados

	RACK	
UBICACIÓN	**IDENTIFICACIÓN**	**N° DE PUERTO**
SEGUNDO PISO - Sala de espera	R21-P3-01	33
SEGUNDO PISO - Corredor	R21-P3-02	34
PRIMER PISO - Segundo Nivel	R21-P3-03	35
PRIMER PISO - Primer Nivel	R21-P3-04	36
PLANTA BAJA - Corredor	R21-P3-05	37
COLISEO - Aula	R21-P3-06	38
FISIOTERAPIA - Sala de espera	RXX-P3-07	Switch no def

El punto de red implementado en las antiguas oficinas de fisioterapia; no se define en el puerto del switch ni el número del rack ya que el mismo, al momento no se encuentra implementado.

5.2.2 Análisis de retardos

Para realizar el análisis de mediciones de tráfico de la nueva red inalámbrica se procedió a la toma de datos, para nuestro caso se decidió apuntar a la dirección IP de uno de nuestros APs, para así lograr medir todo el porcentaje de tráfico que esté pasando por medio del router inalámbrico. Para ello se procedió nuevamente a utilizar el equipo de medición de tráfico SUNSET MTT con su respectivo módulo para Ethernet, todos los datos obtenidos de la medición de tráfico se muestran en el ANEXO 4.

En la Tabla 5.2 se muestran los resultados de medición de latencia cuyos valores dados en milisegundos no sobrepasan el valor límite propuesto para redes inalámbricas, que es de valores menores a 200 ms.

Tabla 5.2. Resultados de medición de latencia para la red inalámbrica

LATENCY TABLE			
LENGTH (bits)	**RATE (%)**	**LATENCY (msec)**	**STATUS**
64	17.97	32,9253	PASS
128	43.75	50,1580	PASS
256	81.25	70,6608	PASS
512	96.09	102,1641	PASS
1024	100.00	110,8974	PASS

5.2.3 Throughput

La Tabla. 5.3., y la Figura 5.9., muestran los resultados para las mediciones de throughput, para este caso se eligieron tamaños de tramas de hasta 1024 bits, provocando resultados de throughput razonables y que garantizan el correcto funcionamiento de la nueva red inalámbrica.

Tabla 5.3. Resultados de throughput para tramas de 64, 128, 256, 512 y 1024 bits

THROUGHPUT TEST TABLE		
LENGTH (bits)	**THROUGHPUT (%)**	**STATUS**
64	17,97	PASS
128	43,75	PASS
256	81,25	PASS
512	96,09	PASS
1024	100	PASS

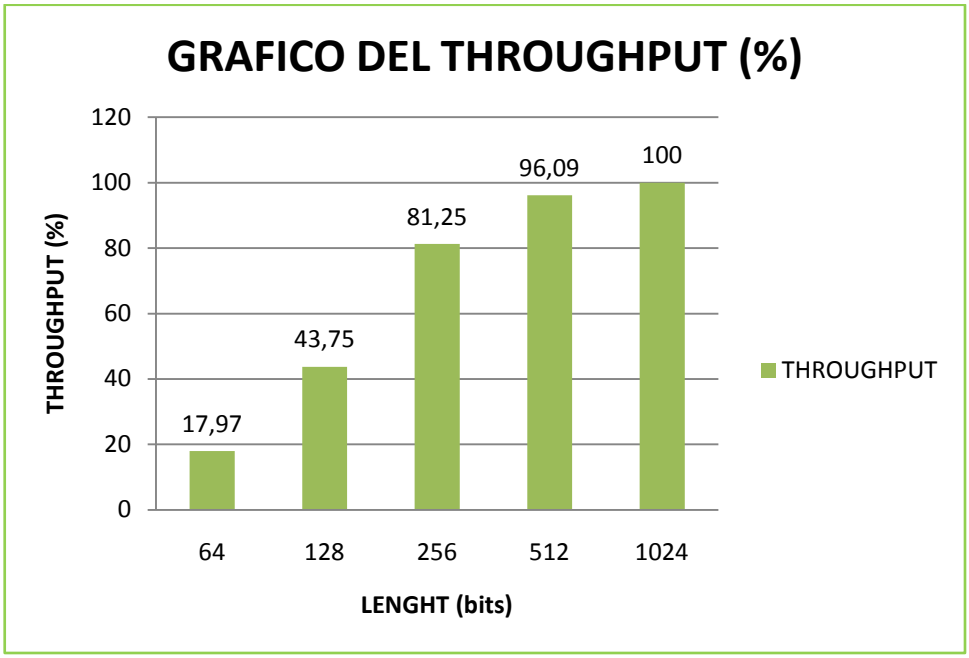


Figura 5.9. Gráfica de throughput para medición de tráfico en la red inalámbrica

5.2.4 Congestión de tráfico

Los resultados de medición de la cogestión de tráfico son analizados mediante las tablas de *FRAME LOSS RATE y BACK TO BACK FRAMES,* cuyos datos se muestran en la Tablas 5.12., 5.13., 5.14 y Figuras 5.10, 5.11, 5.12, 5.13 y 5.14; cuyos resultados indican una pérdida de datos aceptable en este tipo de redes, en las cuales influye mucho el medio de transmisión, en este caso aire, cabe resaltar que los datos obtenidos no superan los límites propuestos para este tipo de redes.

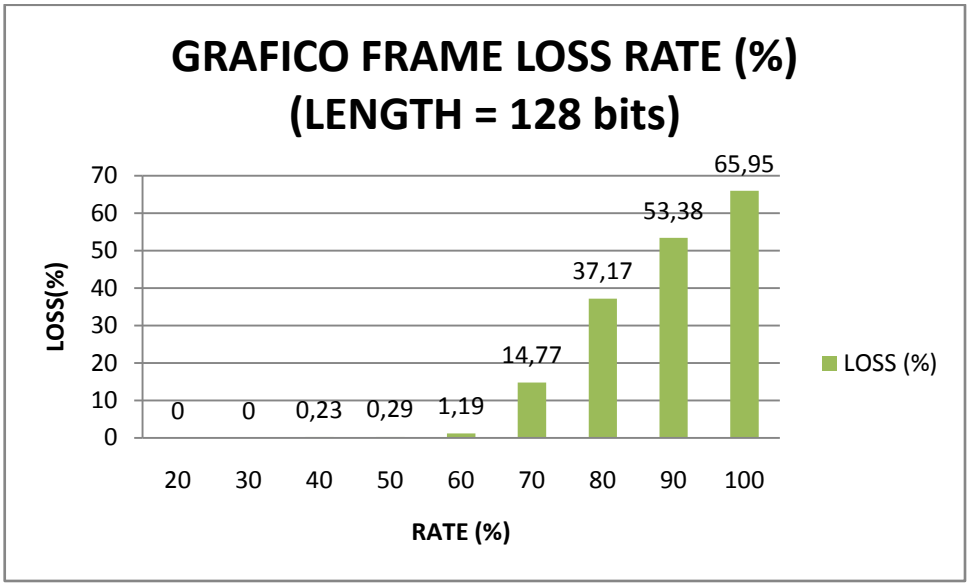


Figura 5.10. Gráfico de Frame Loss Rate (%) para una longitud de trama de 128 bits.

Tabla 5.4. Resultados específicos de medición de *BACK TO BACK FRAMES*

BACK TO BACK FRAMES (#FRAMES)			
LENGHT (bits)	**Min**	**Max**	**AVG**
64	3013	4068	3100
128	141120	844594	830210
256	452898	452898	452898
512	234962	234962	234962
1024	119731	119731	119731

5.2.5 Comparación del tráfico inicial, con el tráfico final de la red

Para realizar el análisis de tráfico inicial con el tráfico final, verificamos las mediciones de throughput antes y después de instalar la red inalámbrica; como resultado de realizar esta comparación de dato, se verifica que el throughput inicial no varía mucho, es decir se presentan resultados de throughput de 100% para longitudes desde 256 bits hasta 1024 bits. Para las mediciones iniciales y para mediciones finales se presentan resultados de throughput entre 80% y 100%, para longitudes de 256 bits hasta 1024; presentando una variación entre el 10% y 20% de las mediciones iniciales, esto se da debido al aumento de tráfico en la red, al implementarse la nueva VLAN para la red inalámbrica.

En cuanto al análisis de las latencias observadas en las mediciones antes de la implementación; se observan valores menores a 100 m, demostrándose que la red se encontraba en buen estado. En las mediciones finales se encontraron resultados que garantizaban que la nueva red implementada; a pesar del aumento de tráfico, se encuentra con tiempos de latencia de entre 100 y 200 ms que son valores razonables para redes inalámbricas.

Con respecto a los resultados obtenidos en cuanto a pérdida de tramas (FRAME LOSS RATE); se verifican resultados iniciales que indican que al enviar tramas de longitudes de 64 bits en adelante se obtienen pérdidas cercanas al 0% del total de las tramas enviadas, indicando que la red se encontraba descongestionada. En los resultados de las mediciones finales se verifica que en los datos finales tomados , existe también valores cercanos a 0% para longitudes de tramas desde 128 bits, aumentando un poco el porcentaje de pérdidas; esto debido al aumento de tráfico en la nueva red inalámbrica implementada, se registran aumentos entre 1 y 2% del tráfico inicial.

Tabla. 5.5 Frame loss rate inicial vs. final

FRAME LOSS RATE			
LENGTH	**RATE (%)**	**LOSS INICIAL(%)**	**LOSS FINAL(%)**
64	100	39,2	99,07
128	100	15,75	65,95
256	100	0	0,14
512	100	0,04	0
1024	100	0	0

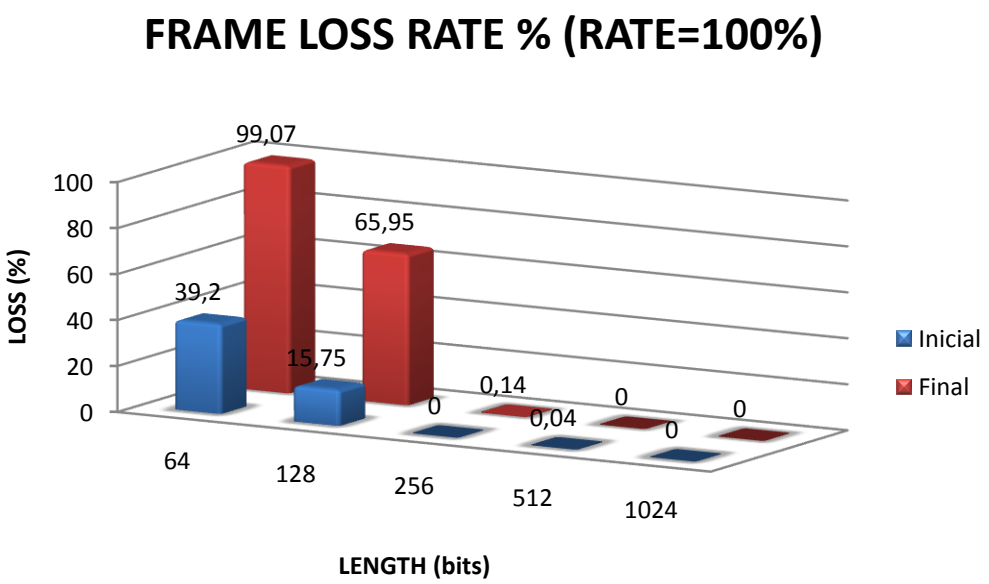


Figura. 5.11. Frame Loss Rate Inicial vs. Final

Tabla. 5.6. Throughput Inicial vs. Final

THROUGHPUT			
LENGTH(bits)	**THROUGHPUT (%) INICIAL**	**THROUGHPUT (%) FINAL**	**STATUS**
64	49,22	17,97	PASS
128	83,59	43,75	PASS
256	100	81,25	PASS
512	100	96,09	PASS
1024	100	100	PASS

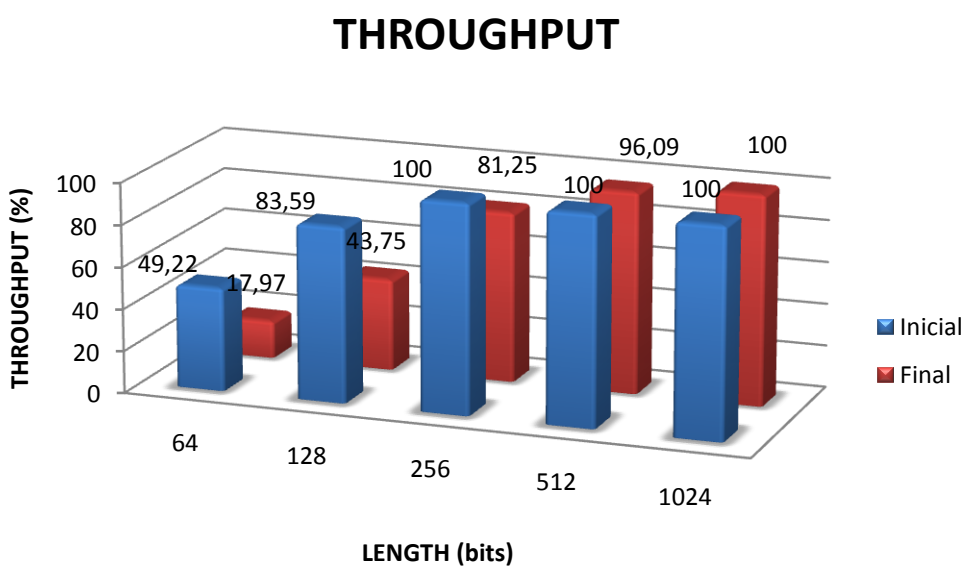


Figura. 5.12 Throughput Inicial vs. Final

Tabla. 5.7. Latencia Inicial vs. Final

LATENCIA				
LENGTH	**RATE (%)**	**LATENCY (msec) INICIAL**	**RATE (%)**	**LATENCY (msec) FINAL**
64	49.22	21,475	17.97	32,9253
128	83.59	21,475	43.75	50,158
256	100.00	21,475	81.25	70,6608
512	100.00	21,475	96.09	102,1641
1024	100.00	21,475	100.00	110,8974

5.3 ANALISIS DE COBERTURA

Para realizar el análisis de coberturas se necesito del software WirelessMon.

5.3.1 WirelessMon

“Con esta herramienta se podrá mantener un correcto rendimiento de la señal inalámbrica con tan solo controlar algunos aspectos tales como el nivel de señal, control de canales de radio y además, es capaz de capturar información de tráfico de una red si es que posee conexión Wireless.

WirelessMon es un programa que permite a los usuarios monitorear el status de sus adaptadores WiFi y obtener información acerca de puntos de acceso y hot spots cercanos en tiempo real. También puede almacenar la información recopilada en un archivo, el cual provee imágenes con el nivel de las señales y estadísticas 802.11 WiFi. Cualquier adaptador Wireless que cumpla con el estándar 802.11 podrá reportar información a WirelessMon“[3]

Para realizar los diagramas de cobertura de cada uno de los AP’s implementados, fue necesario verificar la señal obtenida en cada uno de los pisos y en cada aula, esto con el objetivo de determinar un porcentaje señal emitida.

A continuación, se muestra los resultados de señal obtenidos tanto en dBi como en % logrados con la implementación, la figura 4.7 aplica para las coberturas diseñadas.

5.3.2 Cobertura CAFDER_PLANTA BAJA

El porcentaje de cobertura del SSID: CAFDER_PALNTABAJA que existe en cada lugar se muestra en la siguiente Tabla 5.8.

Tabla. 5.8. Cobertura CAFDER_PLANTABAJA

CAFDER_PLANTABAJA		
LUGAR	**SEÑAL**	
	%	**dbi**
TERCER NIVEL	47	-52
BODEGA	40	-58
INGRESO	56	-45
PUERTA COLISEO	51	-49
GRADAS	61	-41
INGRESO GIMNASIO	11	-81

[3] Wirelessmon, www.passmark.com/products/wirelessmonitor.htm, 04-2010

En el ANEXO 3, se puede observar cada uno de los diagramas de cobertura.

El mapa de cobertura para el SSID indicado, se muestra en la figura 5.13

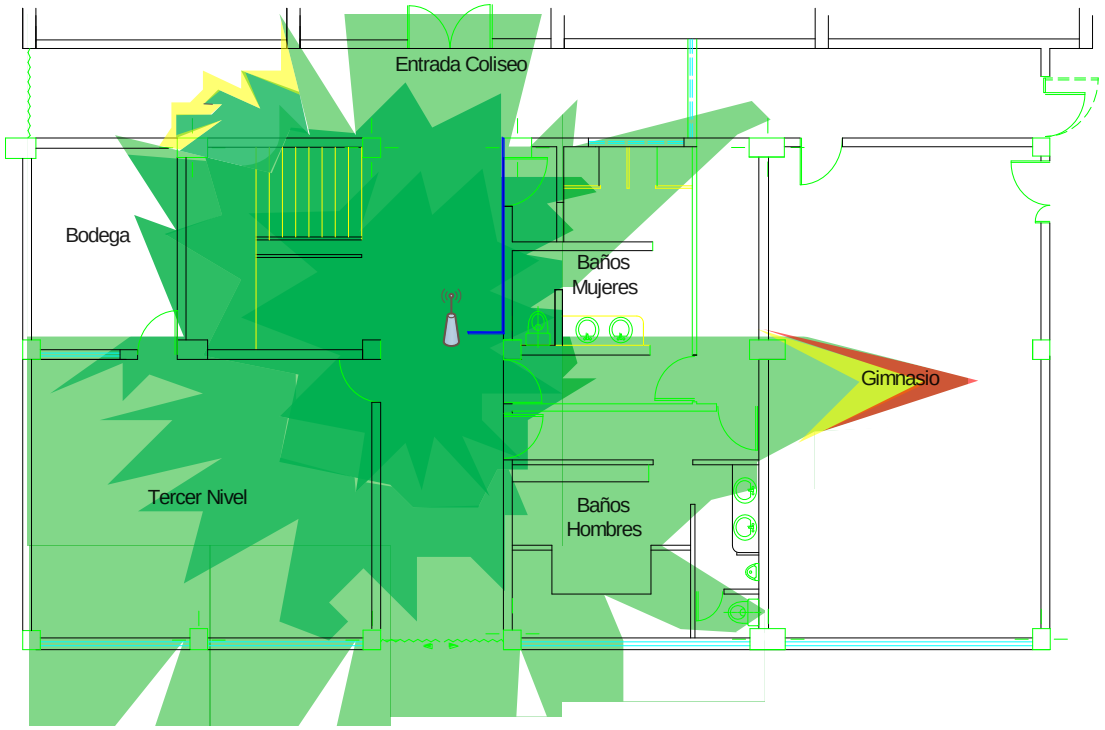


Figura. 5.13. Cobertura CAFDER_PLANTABAJA

Como se observa en la Figura; la cobertura que se tiene tanto en el tercer nivel como en la mayoría de planta baja es óptima, por tanto se puede decir que se tiene cobertura en todo el piso.

5.3.3 Cobertura CAFDER_PISO1a

El porcentaje de cobertura para esta área se muestra en la Tabla 5.9, la misma que muestra el porcentaje, tanto en dBi como en %, obtenido con la implementación del punto de red R21-P3-04.

Tabla. 5.9. Cobertura CAFDER_PISO1a

CAFDER_PISO1a		
LUGAR	**SEÑAL**	
	%	**dbi**
BIBLIOTECA	53	-47
QUINTO NIVEL	36	-61
SEGUNDO NIVEL	46	-53
PRIMER NIVEL	31	-65
SEXTO NIVEL	10	-82
SALA DE DIBUJO Y AUDIVISUALES	0	0
PASILLO	86	-21
GRADAS	45	-54

El mapa de cobertura se muestra en la Figura 5.14.; como se observa en la figura mencionada, la prioridad de cobertura son las aulas de estudio que es el quinto nivel, segundo nivel, biblioteca.

Sin embargo, como se puede notar se tiene una cobertura buena en el resto de las aulas del primer piso; como se detalla, la cobertura es mínima en la sala de dibujo, audiovisuales y en el sexto nivel por lo cual para garantizar cobertura en todo el piso se procedió a la colocación de otro AP.

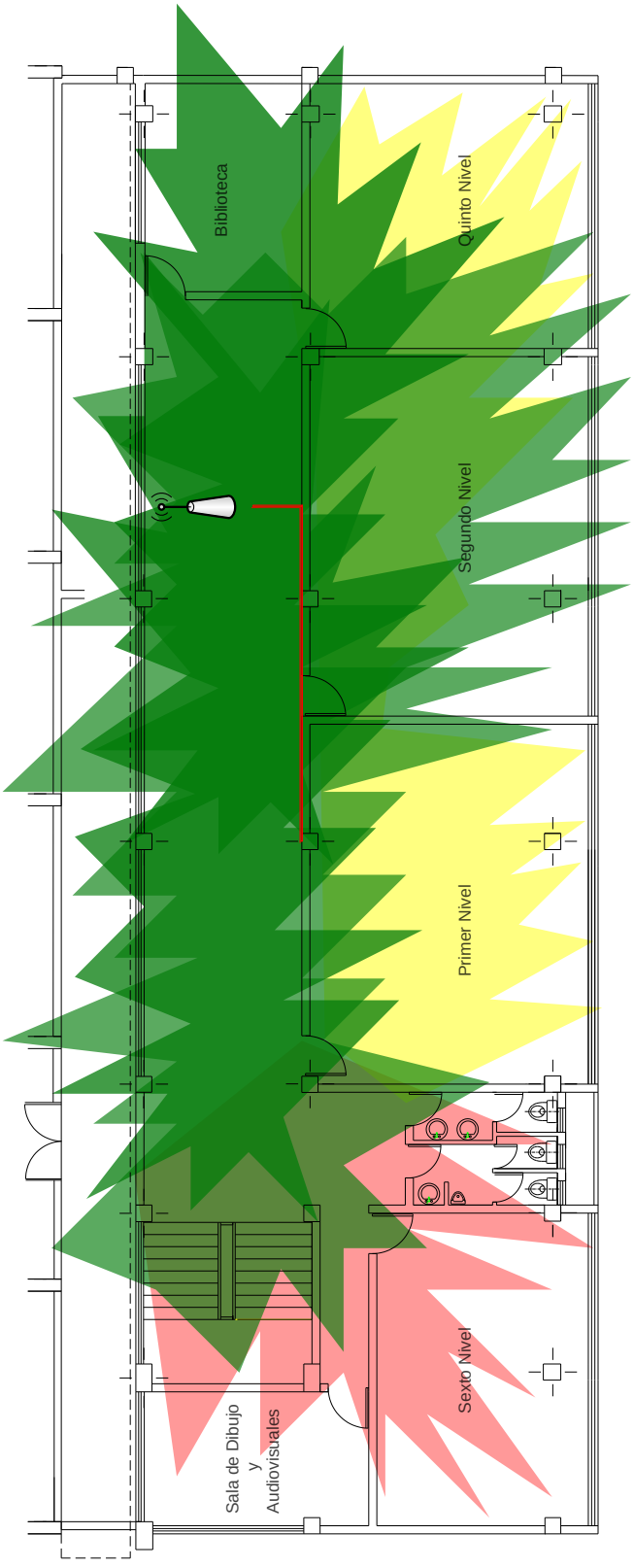


Figura. 5.14. Cobertura CAFDER_PISO1a

5.3.4 Cobertura CAFDER_PISO1b

Los porcentajes obtenidos con el software wirelessmon se muestran en la Tabla 5.10., para el punto de red R21-P3-04.

Tabla. 5.10. Cobertura CAFDER_PISO1b

CAFDER_PISO1b		
LUGAR	**SEÑAL**	
	%	**dbi**
BIBLIOTECA	47	-52
QUINTO NIVEL	19	-75
SEGUNDO NIVEL	24	-71
PRIMER NIVEL	42	-57
SEXTO NIVEL	43	-56
SALA DE DIBUJO Y AUDIVISUALES	45	-54
PASILLO	86	-21
GRADAS	75	-30

El diagrama de cobertura de CAFDER_PISO1b se muestra en la Figura 5.15.; en la misma se muestra la cobertura de las aulas primer nivel, sexto nivel, sala de dibujo y audiovisuales.

Con la implementación de CAFDER_PISO1b, se logró tener cobertura en todo el primer piso incluyendo las áreas críticas en CAFDER_PISO1a.

Figura. 5.15. Cobertura CAFDER_PISO1b

5.3.5 Cobertura CAFDER_PISO2

Para el segundo piso se realizó la implementación con dos AP´s; al igual que lo implementado en CAFDER_PISO2 y CAFDER_ADMIN, la implementación de CAFDER_PISO2 fue realizada para dar servicio a las aulas de cuarto nivel, octavo nivel y séptimo nivel, como se muestra en la Tabla 5.11., ya que éste será de uso para los estudiantes.

Tabla. 5.11. Cobertura CAFDER_PISO2

CAFDER_PISO2		
LUGAR	**SEÑAL**	
	%	**dbi**
DEPARTAMENTO DE CLUBES	20	-74
OFIC. DIRECTOR	0	0
OFIC. SUBDIRECTOR	0	0
COORDINADOR ESTUDIANTIL	22	-72
SECRETARIA	49	-50
DT. BASKETBALL	0	0
OFIC. A.OBANDO	0	0
OFIC. M.VACA	0	0
CUBICULO	22	-72
SALA DE REUNIONES	41	-57
CAFETERÍA	40	-58
CUBICULO	38	-44
CUARTO NIVEL	50	-50
OCTAVO NIVEL	42	-56
SEPTIMO NIVEL	36	-60
PASILLO	42	-56
GRADAS	66	-37

A continuación, la Figura 5.16., muestra el diagrama de cobertura de CAFDER_PISO2.

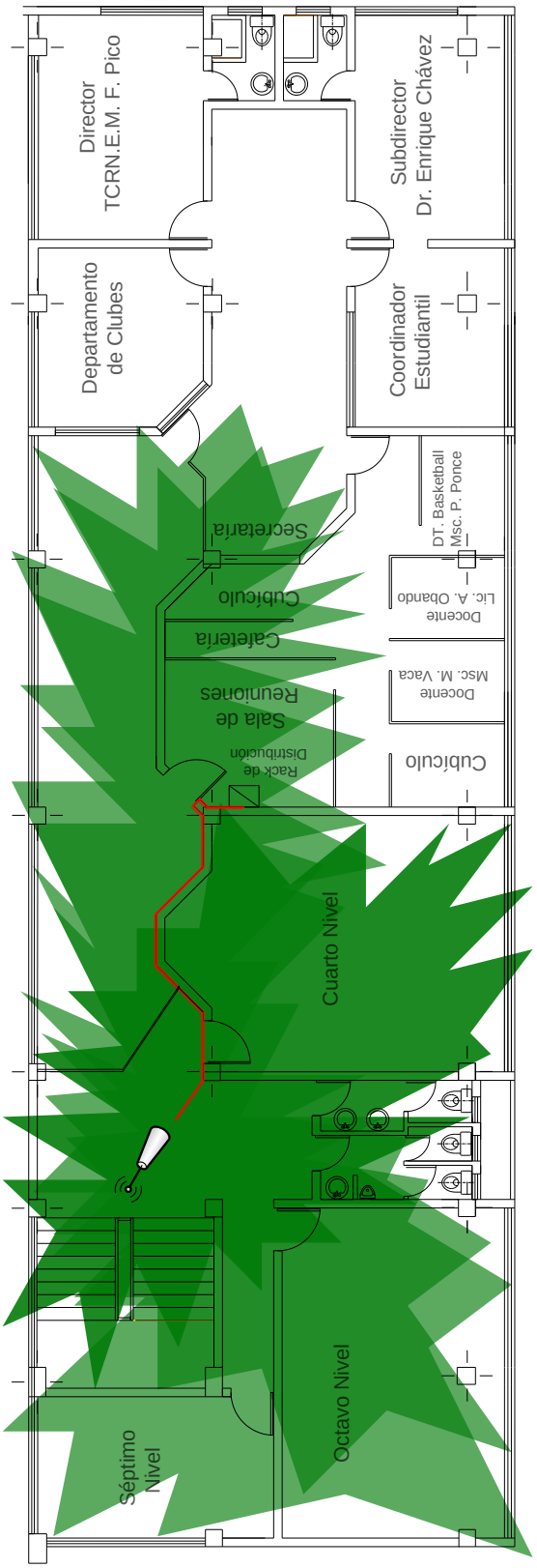


Figura. 5.16. Cobertura CAFDER_PISO2

5.3.6 Cobertura CAFDER_ADMIN

CAFDER_ADMIN; será de uso exclusivo para el personal de docentes ya que el mismo, fue diseñado e implementado para dar cobertura a toda el área administrativa. La información al respecto se observa en la Tabla 1.12.

Tabla. 5.12. Cobertura CAFDER_ADMIN

CAFDER_ADMIN		
LUGAR	**SEÑAL**	
	%	**dbi**
DEPARTAMENTO DE CLUBES	45	-54
OFIC. DIRECTOR	51	-49
OFIC. SUBDIRECTOR	62	-40
COORDINADOR ESTUDIANTIL	63	-39
SECRETARIA	65	-38
DT. BASKETBALL	53	-47
OFIC. A.OBANDO	52	-46
OFIC. M.VACA	48	-51
CUBICULO	47	-52
SALA DE REUNIONES	40	-58
CAFETERÍA	50	-50
CUBICULO	57	-44
CUARTO NIVEL	20	-74
OCTAVO NIVEL	0	0
SEPTIMO NIVEL	0	0
PASILLO	20	-74
GRADAS	3	-87

La Figura 5.17., muestra el diagrama de cobertura de CAFDER_ADMIN.

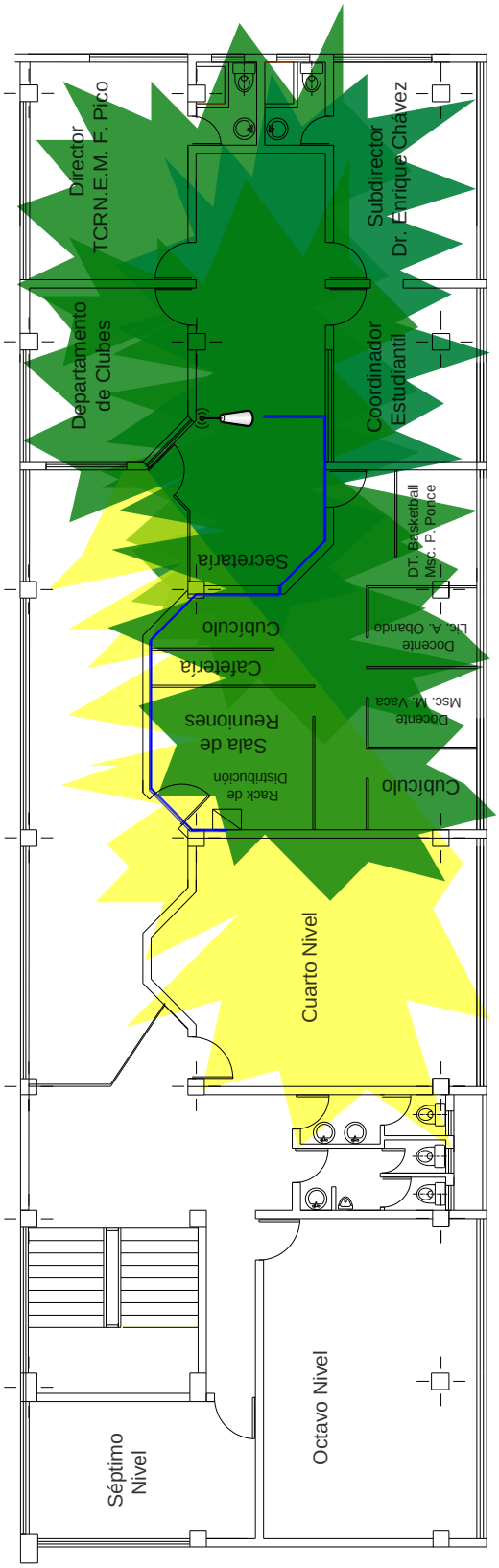


Figura. 5.17. Cobertura CAFDER_ADMIN

5.3.7 Cobertura CAFDER_COLISEO

La implementación de CAFDER_COLISEO se realizó con dos antenas omnidireccionales de 5dBi cada una, esto debido a que se debió tomar en consideración la distancia de cobertura y también la cobertura en línea de vista.

Tabla. 5.13. Cobertura CAFDER_COLISEO

CAFDER_COLISEO		
LUGAR	**SEÑAL**	
	%	**dbi**
AULA	51	49
GRADAS DERECHA	48	-52
GRADAS IZQUIERDA	49	-51
BODEGA	46	-53
TARIMA	48	-51
CAMERINO	45	-54
BAÑOS DERECHA	35	-62
BAÑOS IZQUIERDA	35	-62
INGRESO	10	-82

Con los cambios realizados tanto en antenas como en la ubicación del AP, se logró la cobertura mostrada en la Figura 5.18.; se debe tomar en cuenta que el Coliseo es un punto crítico ya que en el mismo se gestiona las matriculas estudiantiles para el ingreso a clases, razón por la cual se realizo las modificaciones ya antes mencionadas.

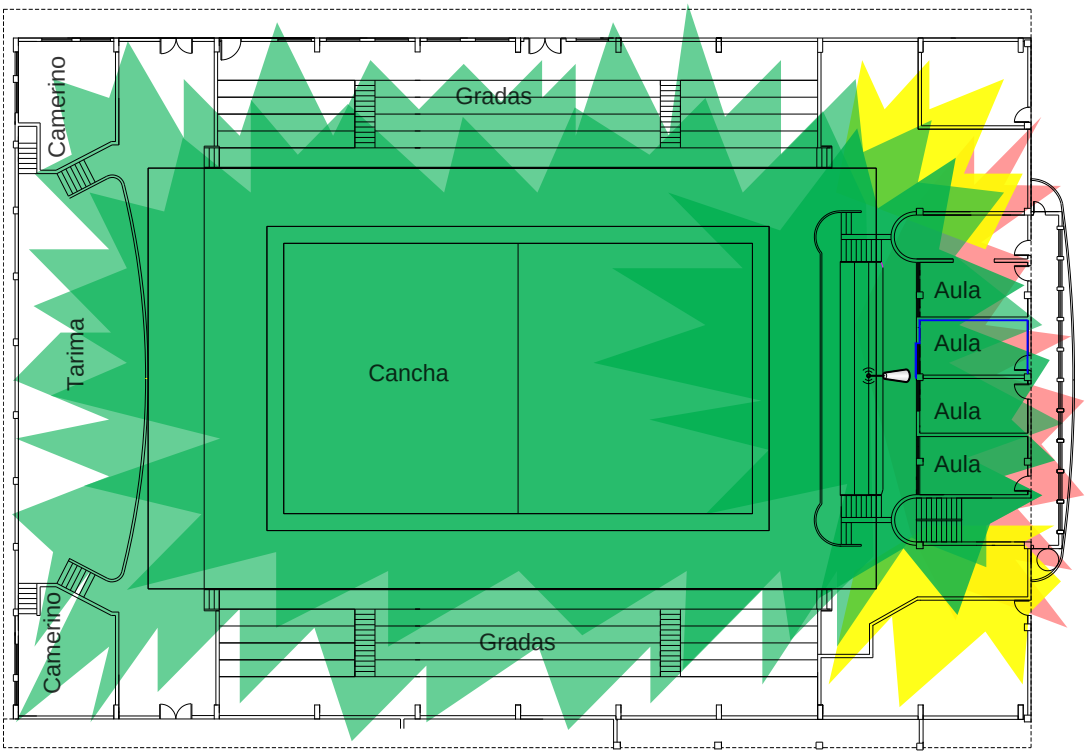


Figura. 5.18. Cobertura CAFDER_COLISEO

5.3.8 Cobertura CAFDER_AULAS

Para la implementación de CAFDER_AULAS fue necesario implementar un nuevo rack, ya que la distancia entre este lugar y el rack de distribución de CAFDER es mayor a 100 metros; el sitio exacto de ubicación del nuevo rack es desconocido por el momento sin embargo el origen del punto CAFDER_AULAS tiene la suficiente distancia para realizar cambios.

Por otra parte; se debe tener en cuenta que para la implementación de CAFDER_AULAS, se debe cubrir las aulas nuevas y las oficinas que tendrán las mismas. Ver la Figura 5.19.

Tabla. 5.14. Cobertura CAFDER_AULAS

CAFDER_AULAS		
LUGAR	**SEÑAL**	
	%	**dbi**
AULA 1	55	-46
AULA 2	47	-57
OFICINA	72	-32
SALA DE ESPERA	68	-35
INGRESO	86	-21

En la Figura 5.19 se muestra la cobertura obtenida en las antiguas oficinas de fisioterapia

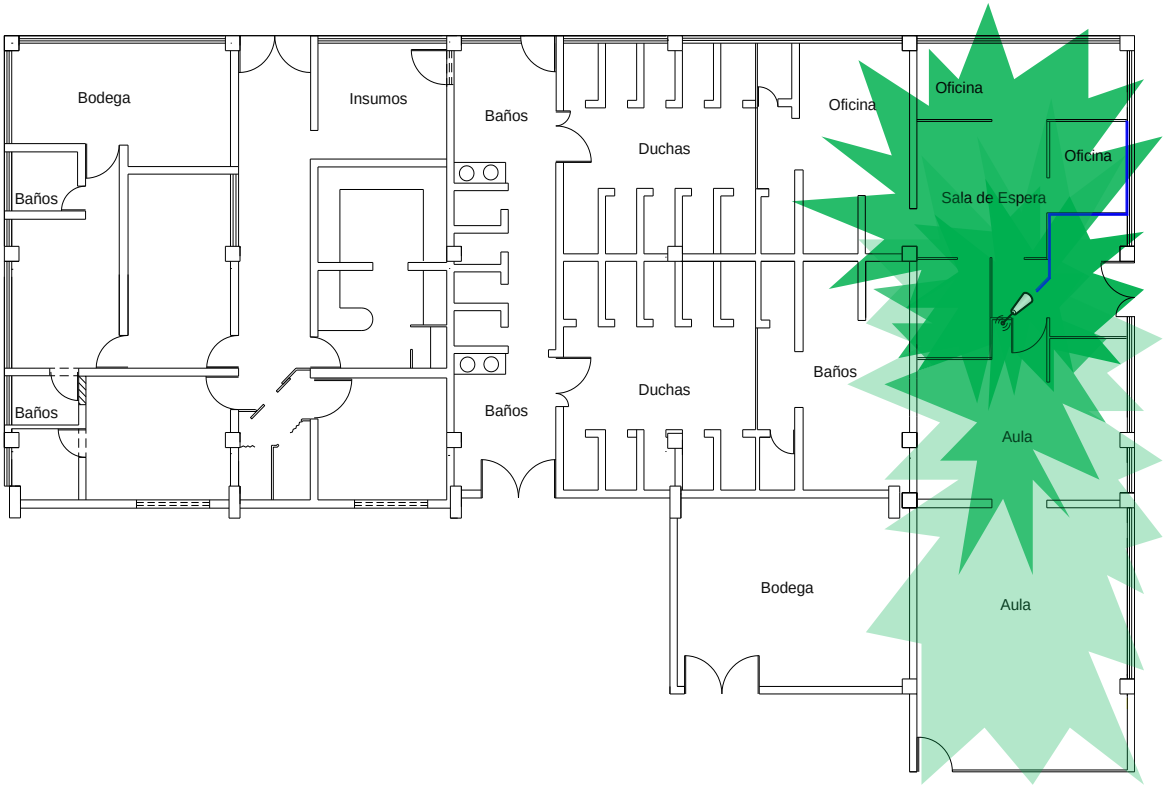


Figura. 5.19. Cobertura CAFDER_AULAS

En el ANEXO. 5. Se muestra los puntos de red implementados.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Las soluciones basadas en redes inalámbricas están disponibles hoy en día, y es sólo el principio de una tendencia creciente. El estándar 802.11n promete un gran ancho de banda para permitir un buen número de nuevas aplicaciones; aunque aún existen varios obstáculos que se tiene que vencer como son: la seguridad e interferencia. Las redes inalámbricas ofrecen por lo pronto una comunicación eficiente tanto en interiores como exteriores.

- Los equipos de la marca Linksys utilizados en la implementación trabajan con los estándares 802.11a, 802.11b, y 802.11g, para futuras implementaciones el estándar 802.11n sería una gran alternativa tecnológica para migrar, debido al aumento en la velocidad de transmisión.

- En cuanto a las mediciones iniciales y finales se presentan resultados de throughput entre 80% y 100%, para longitudes de 256 hasta 1024 bits; presentando una variación entre el 10% y 20% de las mediciones iniciales, se concluye que estas variaciones se dan debido al aumento de tráfico en la red, al implementarse la nueva VLAN para la red inalámbrica.

- En cuanto al análisis de las latencias observadas en las mediciones antes de la implementación; se observan valores menores a 100 m, demostrándose que la red se encontraba en buen estado. En las mediciones finales se encontraron resultados que

garantizaban que la nueva red implementada; a pesar del aumento de tráfico, se encuentra con tiempos de latencia de entre 100 y 200 ms que son valores razonables para redes inalámbricas.

- Con respecto a los resultados obtenidos en cuanto a pérdida de tramas (FRAME LOSS RATE); se verifican resultados iniciales que indican que al enviar tramas de longitudes de 64 bits en adelante se obtienen pérdidas cercanas al 0% del total de las tramas enviadas, indicando que la red se encontraba descongestionada. En los resultados de las mediciones finales se verifica que en los datos finales tomados , existe también valores cercanos a 0% para longitudes de tramas desde 128 bits, aumentando un poco el porcentaje de pérdidas; esto debido al aumento de tráfico en la nueva red inalámbrica implementada, se registran aumentos entre 1 y 2% del tráfico inicial.

- El ancho de banda que posea un usuario para hacer uso de la red inalámbrica, está directamente relacionada con el número de usuarios concurrentes que accedan a la red.

- El software utilizado para el diseño de la red inalámbrica es de la marca 3COM, se lo utilizó en vista de que en la ESPE se manejan equipos inalámbricos de esta marca y con los cuales se realizó el análisis, diseño y pruebas de cobertura de la nueva red.

- El servidor de autenticación RADIUS se lo implementó en una computadora de prueba en vista de que no se realizó la adquisición del equipo solicitado, pero como parte integrada de la documentación se entregarán las configuraciones y respaldos de los servidores.

- Las pruebas de la red inalámbrica implementada fueron realizadas con los equipos de la marca Linksys, no se concluyó con la implementación total debido a inconvenientes con respecto a la parte logística de adquisición de los equipos, sin embargo la infraestructura de los APs que se utiliza en la ESPE es de la marca 3COM.

- Después de analizar todas las posibles soluciones para proveer de servicio a todos los usuarios del bloque CAFDER, se decide por la solución inalámbrica ya que la misma

proveerá de cobertura a la mayor parte de alumnos del departamento, además de dar movilidad a cada uno de los mismos.

- En la elección de los equipos se puso mucho énfasis en la potencia de transmisión (18dbm), la autenticación y autorización (mecanismo de acceso 802.1x), y que tengan la tecnología incorporada de PoE.

- Después de analizar los datos obtenidos en las mediciones de tráfico se concluye que es posible adicionar la solución inalámbrica ya que la misma proveería de conectividad a todos los usuarios de la CAFDER, garantizando la conectividad y calidad de servicio.

- Al utilizar plataformas de open source, tanto Linux Fedora 12, FreeRADIUS y dalo RADIUS, se realizo los cambios deseados dentro del código fuente pero respetando los derechos de autor.

- FreeRADIUS es una plataforma modular, de gran potencialidad, con diversas y completas características que lo convierte en uno de los más utilizados y potentes servidores RADIUS de clase AAA (autenticación, autorización y registro).

- FreeRADIUS mantiene abierta la posibilidad de migrar la base de datos en nuestro caso de MySQL hacia otras plataformas de base de datos, mas robustas y con mejor desempeño.

- Los certificados generados tienen un tiempo de caducidad de 6 meses, con lo que se garantiza que al inicio del nuevo semestre nuevos alumnos no puedan conectarse a la red inalámbrica o a su vez la sigan utilizando alumnos que no se encuentren matriculados en el departamento.

- La creación de los certificados es la parte que proveerá de conectividad al usuario que intente conectarse a cualquier AP mismo que se encuentre conectado al servidor RADIUS; es decir el certificado es el que valida el usuario en cualquier computador.

- Al momento de realizar el cableado estructurado se lo realizó con cable utp cat 5e y su trayectoria se encuentra dentro de una canaleta lisa de 20*12 la misma que evita las pérdidas por disipación (PoE) ó atenuación de la señal por interferencia por inducción de magnetismo en la misma.

6.2 RECOMENDACIONES

- Al diseñar una red inalámbrica, se debe tener especial cuidado con la elección de canales de radio para la formación de celdas de cobertura, pues de ello depende la posible interferencia en la red inalámbrica, sin embargo posee la característica de AUTO configuración la cual realiza un escaneo general de los canales de radio y la ubica en un canal libre.

- Para redes de mayor complejidad y que necesiten métodos de seguridad más robustos; se puede plantear la elección de puntos de acceso que cumplan con el estándar 802.11i y el trabajo con los protocolos WPA-2 con cifrado AES.

- Se podrá mejorar la cobertura instalando más Puntos de Acceso, o realizando cambio de antenas con mayor ganancia, siempre y cuando los AP's soporten el aumento de la potencia.

- Para redes inalámbricas de mayor capacidad, por ejemplo de más de 500 usuarios, se recomienda el uso de un directorio de tipo LDAP para la organización de los distintos sectores de la entidad o empresa.

- Para realizar la configuración del servidor RADIUS es necesario descargar la versión más estable y reciente del sistema; ya que el mismo puede presentar errores al momento de su compilación y posterior ejecución en servidores virtuales *"virtual server"*.

- Una posible mejora para este sistema de autenticación en caso de que no existiese daloRADIUS, puede darse en la implementación de una interfaz gráfica para el sistema operativo Windows; el cual pueda acceder a la base de datos MySQL del servidor de Linux, para realizar la creación y eliminación de cuentas. De esta manera, no es

necesario manejar el sistema operativo Linux para poder realizar un monitoreo sobre la red inalámbrica.

- La característica de PoE (Power Over Ethernet), es muy importante y necesaria en la elección del AP ya que si el equipo no dispusiese de la misma, se debería implementar puntos de UPS en la implementación del cableado.

- Al momento de utilizar el software de diseño 3com Wireless Switch Manager, para introducir el mapa del edificio se debe tomar en cuenta que para el reconocimiento de cada línea del grafico como objeto RF debe ser dibujado con anterioridad con la herramienta capas de AUTOCAD.

- Se recomienda realizar la respectiva actualización del sistema operativo en el cual se vaya a montar ó implementar el servidor RADIUS, en nuestro caso LINUX (Fedora 12) con el comando #yum update.

- Se recomienda antes de realizar algún cambio en el servidor; es decir antes de realizar cambios en los respectivos ficheros de configuración de Free-RADIUS, realizar un backup de todos los ficheros.

- En la trayectoria de cada punto de red (cableado estructurado), tomar en cuenta las rutas a tomar es decir desechar en lo posible rutas por las cuales exista transformadores de energía o alto voltaje y equipos que manejen corrientes altos.

- Tener especial cuidado en la trayectoria de cada punto de red en la distancia de los mismos ya que en algunos casos la mejor solución sería la implementación de un nuevo rack de distribución ó a su vez cambio de medio de transmisión de cobre por fibra.

- Se debe controlar la distribución de los certificados generados ya que los mismos con la identidad de usuario y contraseña, pueden ingresar personas con diferentes propósitos a nuestra red.

- Para mejorar la cobertura de un punto de acceso es estos equipos se posee la facilidad de cambio de antenas es decir se puede cambiar las dos antenas de 2dbi omnidireccionales por antenas de mayor ganancia como de 7dbi.

- Se debe tener especial cuidado al momento de realizar la conexión de MySQL con freeRADIUS y a la postre con daloRADIUS ya que el mismo será luego la base de datos de todos los usuarios, grupos, y características de cada uno de los mismos.

- Para realizar la configuración del servidor RADIUS es necesario descargar la versión más estable y reciente del sistema; ya que el mismo puede presentar errores al momento de su compilación y posterior ejecución en servidores virtuales *"virtual server"*.

- Para la verificación de cualquier daño del servidor o cualquier función anormal del mismo siempre se debe revisar los logs tanto del servidor como del sistema operativo.

- Para revisar paso por paso el proceso de conexión de un usuario al servidor se lo revisa en modo debug del servidor radius

ANEXOS

7.1 ANEXO 1

7.1.1 Planos CAFDER

A continuación de observa los planos correspondientes a la distribución de aulas en el CAFDER

Figura. 7.1. Planos CAFDER

7.2 ANEXO 2

7.2.1 Mediciones realizadas

- **PRIMERA MEDICIÓN**

  - **Configuración del equipo de Medición**

Tabla. 7.1. Configuración de hora y fecha de medición

NOMBRE DEL ARCHIVO	RFC_001	
DATOS GUARDADOS	08H39 AM	11/01/10

Tabla. 7.2. Configuración de IP destino

RFC2544 FRAME FORMAT	
TEST	IP ROUTED
IP DST	10.1.45.18

Referido al destino o a la dirección a donde se quiere medir el tráfico, se realiza la medición, en nuestro caso se elige la primera medición en la dirección IP de la oficina de Secretaría

Tabla. 7.3. Configuración de longitudes de medición

RFC2544 FRAME LENGTH (bits)	
64	YES
128	YES
256	NO
512	NO
1024	NO
1280	NO
1518	NO
4096	NO

Tabla. 7.4. Configuración de la secuencia de medición

RFC2544 TEST SEQUENCE	
LOOPBACK	YES
THROUGHPUT MEASUREMENT	YES
LATENCY MEASUREMENT	YES
FRAME LOSS RATE	YES
BACK TO BACK	YES
USER THRESHOLD	NO

En esta parte de la configuración, se escoge la secuencia de medición que se desea el equipo realice.

Tabla. 7.5. Configuración del test de *throughput*

THROUGHPUT TEST CONFIGURATION	
MAX BANDWIDTH	100.0%
RESOLUTION	1.0%
DURATION	10sec

En este paso, se realiza la configuración de medición de *Throughput*, el cual está configurado para mediciones en porcentaje y una duración de 10 segundos.

Tabla. 7.6. Configuración de medición de latencia

LATENCY TEST CONFIGURATION	
BANDWIDTH	THROUGHPUT
DURATION	60sec

Tabla. 7.7. Configuración de *FRAME LOSS RATE*

FRAME LOSS RATE CONFIGURATION	
START BANDWIDTH	100%
STEP SIZE	10%
DURATION	10sec

Para la configuración de los paquetes perdidos se realiza lo siguiente, se realizará una medición empezando en el 100% del envío total de los paquetes y se verifica el porcentaje de pérdida de paquetes.

Tabla. 7.8. Configuración de *BACK TO BACK FRAMES*

BACK TO BACK CONFIGURATION	
MAX BANDWIDTH	100%
DURATION	2sec
MAX DURATION	10sec
REPETITIONS	50
RESOLUTION	1frame(s)

Para esta medición, se verificará el número de tramas con el mayor tamaño de ráfaga para el cual la red puede manejarlas sin pérdida; se configurará el equipo de tal forma que exista una duración máxima de 10 segundos y con una resolución de paquete en paquete.

Tabla. 7.9. Resultados generales de medición de throughput para longitudes de 64 y 128 bits para el primer día de medición

LENGTH	RATE (%)	STATUS
64	100	FAIL
64	50	FAIL
64	25	FAIL
64	12,5	FAIL
64	6,25	FAIL
64	3,13	FAIL
64	1,56	FAIL
64	0,78	PASS
128	100	FAIL
128	50	FAIL
128	25	FAIL
128	12,5	FAIL
128	6,25	FAIL
128	3,13	FAIL
128	1,56	PASS
128	2,34	PASS

Tabla. 7.10. Resultados específicos de medición para longitudes de 64 y 128 bits para el primer día de medición

LENGTH(bits)	THROUGHPUT (%)
64	0,78
128	2,34

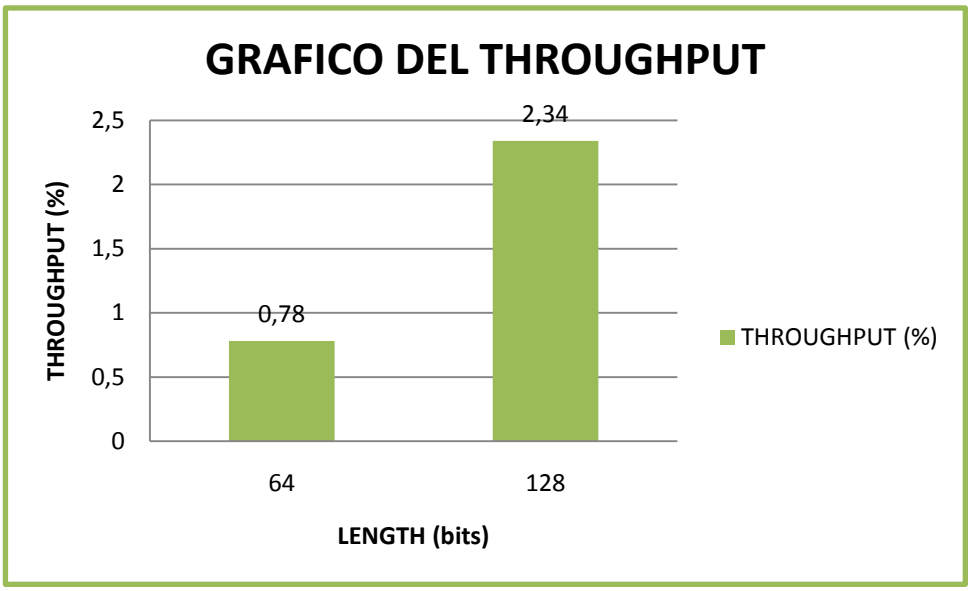


Figura. 7.2. Gráfica de medición de Throughput Vrs la longitud de la trama para el primer día de medición

Como se puede observar en las Tablas 7.9., 7.10., y la Figura. 7.2 se observa que debido al aumento de tráfico (primer día de matriculas) el throughput se ve afectado en gran medida observándose resultados en el porcentajes del total de las tramas enviadas (muy pequeños), como es el caso que para una longitud de trama de 128 bits sólo hubo un porcentaje de *throughput* del 2,34%, este porcentaje es extremadamente pequeño, para este tipo de redes los porcentajes deben estar entre 30% y 40% de la longitud total de la trama.

Tabla. 7.11. Resultados de medición de latencia para longitudes de 64 y 128 bits para el primer día de medición

LENGTH	RATE (%)	LATENCY (msec)	STATUS
64	0,78	55,69333	PASS
128	128	34,24838	PASS

Como se observa en la Tabla 7.11 los resultados de medición de latencia se encuentran dentro del rango de tiempo permitido para este tipo de redes, que son tiempos menores a 100 ms.

Tabla. 7.12. Resultados de medición de paquetes perdidos para longitudes de 64 y 128 bits para el primer día de medición

LENGTH	RATE (%)	LOSS (%)
64	10	14,23
64	20	24,02
64	30	44,61
64	40	63,85
64	50	97,99
64	60	99,99
64	70	99,99
64	80	99,93
64	90	99,91
64	100	99,91
128	10	9,2
128	20	22,32
128	30	38
128	40	48,04
128	50	55,6
128	60	73,63
128	70	96,92
128	80	99,99
128	90	99,85
128	100	99,86

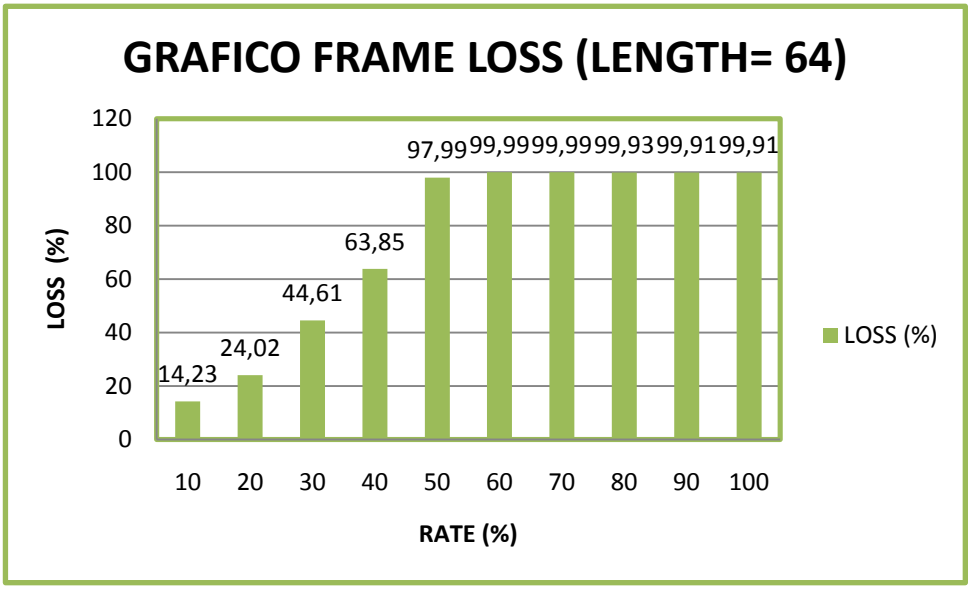


Figura. 7.3. Gráfica de pérdidas de paquetes para longitud de 64 bits para el primer día de medición

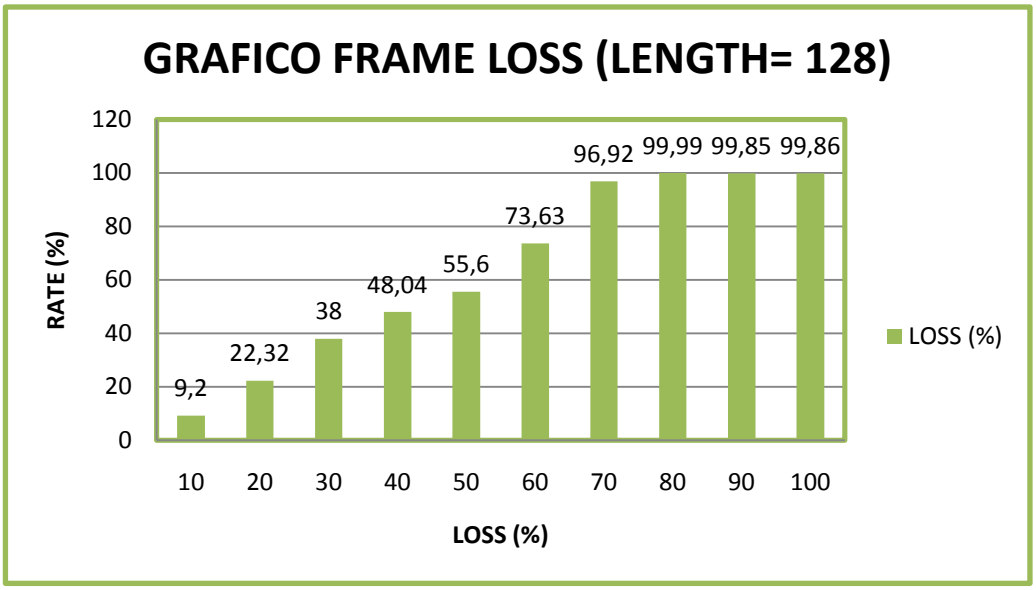


Figura. 7.4. Gráfica de pérdidas de paquetes para longitud de 64 bits para el primer día de medición

En cuanto a los resultados de paquetes perdidos, la Tabla 7.12 y las Figuras 7.3 y 7.4 se puede verificar que existe un gran porcentaje de paquetes perdidos; esto es debido a la gran cantidad de tráfico que se presentó en el primer día de medición y primer día de matrículas.

Tabla. 7.13. Resultados Generales de medición del *Test Back- To- Back frames* para longitudes de 64 y 128 bits para el primer día de medición

LENGTH	# FRAMES	STATUS
64	872	FAIL
64	591	FAIL
64	436	FAIL
64	582	FAIL
64	242	FAIL
64	584	FAIL
64	944	FAIL
64	872	FAIL
64	1163	FAIL
64	727	FAIL
64	454	PASS
64	193	PASS
64	144	PASS
64	665	FAIL
64	663	FAIL
64	937	FAIL
64	288	FAIL
64	265	FAIL
64	663	PASS
64	634	FAIL
64	242	FAIL
64	295	PASS
64	531	PASS
64	582	PASS
64	238	PASS
64	591	PASS
64	233	FAIL
64	311	PASS
64	229	FAIL
64	209	PASS
64	874	FAIL
64	180	PASS
64	284	PASS
64	736	FAIL
64	636	FAIL
64	256	PASS
64	618	FAIL
64	908	FAIL
64	327	FAIL

64	540	FAIL
64	363	FAIL
64	347	FAIL
64	256	PASS
64	727	FAIL
64	1181	FAIL
64	206	FAIL
64	595	FAIL
64	1167	FAIL
64	727	FAIL
64	476	FAIL
128	146	FAIL
128	96	PASS
128	180	FAIL
128	330	FAIL
128	495	FAIL
128	187	FAIL
128	116	FAIL
128	170	FAIL
128	170	PASS
128	134	PASS
128	108	PASS
128	391	FAIL
128	139	PASS
128	197	FAIL
128	160	FAIL
128	249	FAIL
128	165	PASS
128	108	PASS
128	340	FAIL
128	216	FAIL
128	350	FAIL
128	216	FAIL
128	124	PASS
128	247	FAIL
128	168	PASS
128	195	PASS
128	149	FAIL
128	330	FAIL
128	108	FAIL
128	209	PASS
128	157	FAIL
128	195	FAIL
128	149	FAIL
128	168	FAIL

128	340	FAIL
128	146	FAIL
128	185	PASS
128	216	FAIL
128	108	FAIL
128	103	PASS
128	167	FAIL
128	190	FAIL
128	218	FAIL
128	124	FAIL
128	330	FAIL
128	414	FAIL
128	175	PASS
128	118	FAIL
128	95	FAIL
128	206	FAIL

Tabla. 7.14. Resultados específicos de medición del *Test Back- To- Back frames* para longitudes de 64 y 128 bits para el primer día de medición

LENGTH(bits)	64	128
MIN	144	94
MAX	1180	494
AVG	534	199

Como se muestra en las Tablas 7.13 y 7.14 consecutivamente, se analiza las diferentes mediciones observándose que los valores de *back to back frames* con los mayores tamaños de ráfagas para una longitud de 64 y 128 bits son valores aceptables puesto que se encuentran dentro del rango de valores ideales para esta medición.

- **SEGUNDA MEDICIÓN**

Configuración del equipo de Medición

Fecha y hora de Medición

- **12/01/10**
- **11:10:53**

Tabla 7.15. Resultados generales de medición de throughput para longitudes de 64 y 128 bits para el segundo día de medición

LENGTH	RATE (%)	STATUS
64	100	FAIL
64	50	FAIL
64	25	FAIL
64	12,5	PASS
64	18,75	PASS
64	21,88	PASS
64	23,44	PASS
64	24,22	FAIL
128	100	FAIL
128	50	PASS
128	75	FAIL
128	62,5	FAIL
128	56,25	FAIL
128	53,13	FAIL
128	51,56	PASS
128	52,34	PASS

Tabla 7.16. Resultados específicos de medición de throughput para longitudes de 64 y 128 bits para el segundo día de medición

LENGTH	THROUGHPUT(%)	STATUS
64	23,44	N/A
128	52,34	N/A

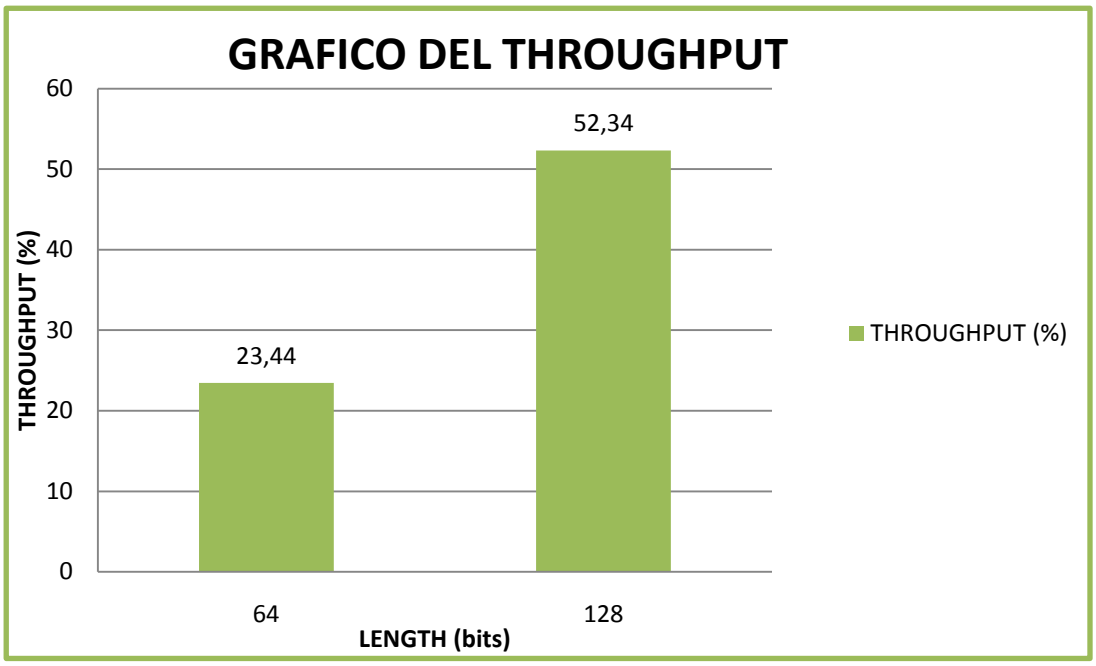


Figura 7.5. Gráfica de throughput vs. longitud de los paquetes para el segundo día de medición

Para el segundo día de medición se muestran resultados de throughput en las tablas 7.15, 7.16 y figura 7.5 con porcentajes a considerables puesto que este día ya hubo un poco menos de tráfico en la red.

Tabla 7.17. Resultados de medición de latencia para longitudes de 64 y 128 bits para el segundo día de medición

LENGTH	RATE (%)	LATENCY (msec)	STATUS
64	23,44	50,088	N/A
128	52,34	44,657	N/A

Los resultados obtenidos en cuanto a medición de latencia son considerables puesto que se encuentran dentro de los valores aceptables de latencia para este tipo de tramas.

Tabla 7.18. Resultados generales de medición de pérdidas de tramas para longitudes de 64 y 128 bits para el segundo día de medición

LENGTH	RATE (%)	LOSS (%)
64	20	0
64	30	0
64	40	0,05
64	50	0
64	60	0,27
64	70	0,45
64	80	6,16
64	90	16,82
64	100	24,92
128	70	0
128	80	0
128	90	6,42
128	100	15,77

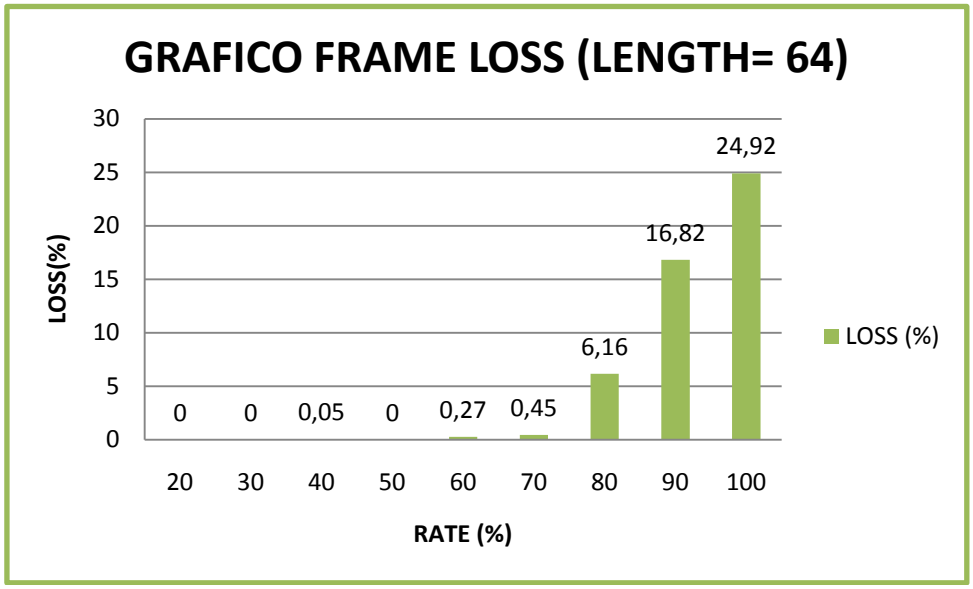


Figura 7.6. Gráfica de pérdida de paquetes para longitud de trama de 64 bits para el segundo día de medición

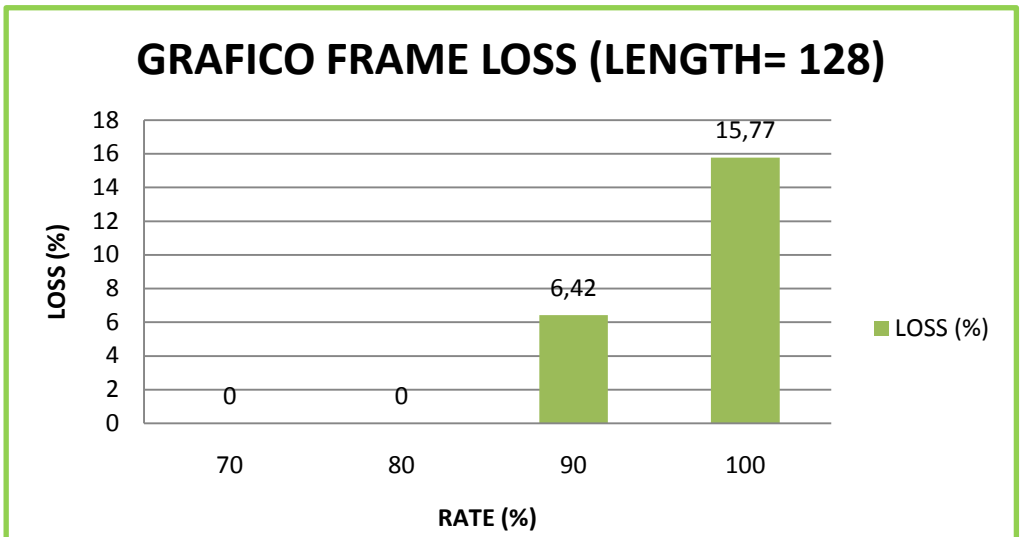


Figura 7.7. Gráfica de pérdida de paquetes para longitud de trama de 128 bits para el segundo día de medición

En cuanto a los resultados obtenidos en la tabla 7.18 y las figura 7.6 y 7.7 consecutivamente se observa que ahora el porcentaje de paquetes perdidos disminuyó en un gran porcentaje esto es debido a que el tráfico en la red disminuye a la vez.

Tabla 7.19. Resultados Generales de medición del Test Back- To- Back frames para longitudes de 64 y 128 bits para el segundo día de medición

LENGTH	#FRAMES	STATUS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS

64	1488095	PASS
64	1488095	PASS
64	1488095	PASS

128	844594	PASS
128	844594	PASS
128	844594	PASS

Tabla 7.20. Resultados Específicos de medición del Test Back- To- Back frames para longitudes de 64 y 128 bits para el segundo día de medición

LENGTH	64	128
MIN	1488095	844594
MAX	1488095	844594
AVG	1488095	844594

Así mismo se observan resultados del número de back to back frames que pasaron el test con valores que son aceptables.

- **TERCERA MEDICIÓN**

Configuración del equipo de medición

Fecha y hora de Medición

- **16/01/10**
- **09:36:22**

Para este día de medición se decidió apuntar al tráfico del *swicht* localizado en el coliseo puesto que para los días de matrículas se lo coloca para tratar de reducir un poco el tráfico de la red y realizar una buena distribución de los distintos puntos de red implementados para este día.

En cuanto a la configuración de la longitud de las tramas a medir se aumento el número de tramas hasta un valor de 1024 bits esto es debido a que se realizará la medición del tráfico que se transfiere a través del *switch*.

Tabla 7.21. Resultados generales de medición de throughput para longitudes de 64, 128, 256, 512 y 1024 bits para el tercer día de medición

LENGTH	RATE (%)	STATUS
64	100	FAIL
64	50	FAIL
64	25	FAIL
64	12,5	FAIL
64	6,25	FAIL
64	3,13	FAIL
64	1,56	FAIL
64	0,78	FAIL
128	100	FAIL
128	50	FAIL
128	25	FAIL
128	12,5	FAIL
128	6,25	FAIL
128	3,13	FAIL
128	1,56	FAIL
128	0,78	FAIL
256	100	FAIL
256	50	FAIL
256	25	FAIL
256	12,5	FAIL
256	6,25	FAIL
256	3,13	FAIL
256	1,56	FAIL
256	0,78	FAIL
512	100	FAIL
512	50	FAIL
512	25	FAIL
512	12,5	FAIL
512	6,25	FAIL
512	3,13	FAIL
512	1,56	FAIL
512	0,78	FAIL
1024	100	FAIL
1024	50	FAIL
1024	25	FAIL
1024	12,5	FAIL
1024	6,25	FAIL
1024	3,13	FAIL
1024	1,56	FAIL
1024	0,78	PASS

Tabla 7.22. Resultados específicos de medición de throughput para longitudes de 64, 128, 256, 512 y 1024 bits para el tercer día de medición

LENGTH	THROUGHPUT (%)
64	0
128	0
256	0
512	0
1024	0,78

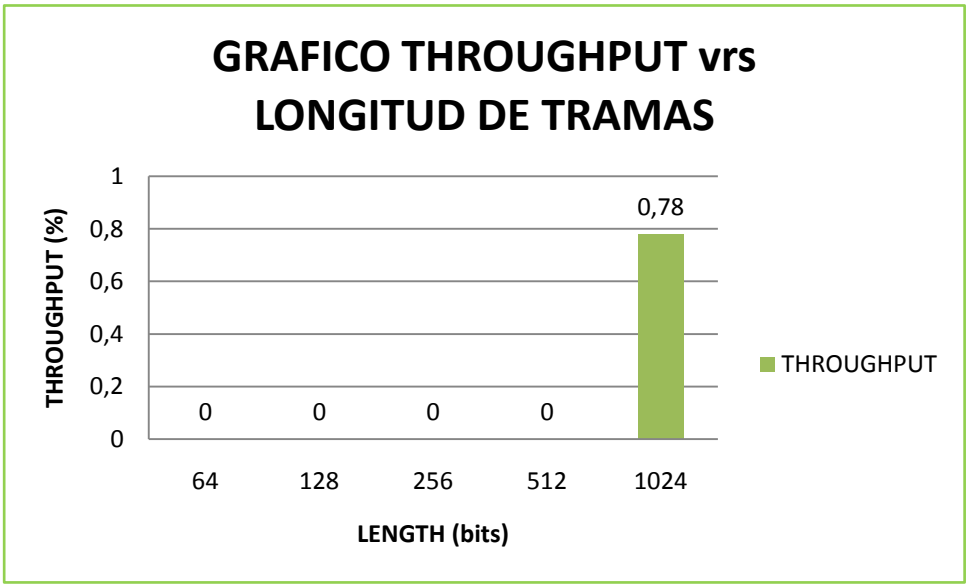


Figura 7.8. Gráfica de Throughput Vrs la longitud de las tramas para el tercer día de medición

Como se puede verificar en los resultados obtenidos de la medición de Throughput para nuestro tercer día de medición se puede observar que existe un porcentaje extremadamente pequeño, esto es debido a que el tráfico aumento totalmente debido a que este era uno de los últimos días de matrículas, indicándonos que estos valores ya no son aceptables para este tipo de redes.

Tabla 7.23. Resultados de medición de latencia para longitudes de 64, 128, 256, 512 y 1024 bits para el tercer día de medición

LENGTH	RATE (%)	LATENCY (msec)	STATUS
64	100.00	21.475	PASS
128	100.00	21.475	PASS
256	100.00	21.475	PASS
512	100.00	21.475	PASS
1024	0.78	21.475	PASS

Estos resultados obtenidos en cuanto a la medición de latencia son considerables y se encuentran dentro del rango permitidos para este tipo de redes y longitudes de tramas.

Tabla 7.24. Resultados de medición de pérdidas de paquetes para longitudes de 64, 128, 256, 512 y 1024 bits para el tercer día de medición

LENGTH	RATE (%)	LOSS (%)
64	10	96,17
64	20	99,98
64	30	99,99
64	40	99,99
64	50	100
64	60	100
64	70	100
64	80	100
64	90	99,96
64	100	99,96
128	10	94,48
128	20	97,77
128	30	98,87
128	40	99,05
128	50	99,78
128	60	99,84
128	70	99,91
128	80	99,91
128	90	99,93
128	100	99,95
256	10	86,38
256	20	91,79
256	30	99,25
256	40	98,22

256	50	97,98
256	60	99,98
256	70	99,97
256	80	99,98
256	90	99,99
256	100	99,98
512	10	69,83
512	20	86,23
512	30	92,44
512	40	99,13
512	50	94,95
512	60	97,57
512	70	99,97
512	80	99,99
512	90	99,96
512	100	99,98
1024	10	30,44
1024	20	75,86
1024	30	94,18
1024	40	99,24
1024	50	90,83
1024	60	93,53
1024	70	99,65
1024	80	99,67
1024	90	99,71
1024	100	99,87

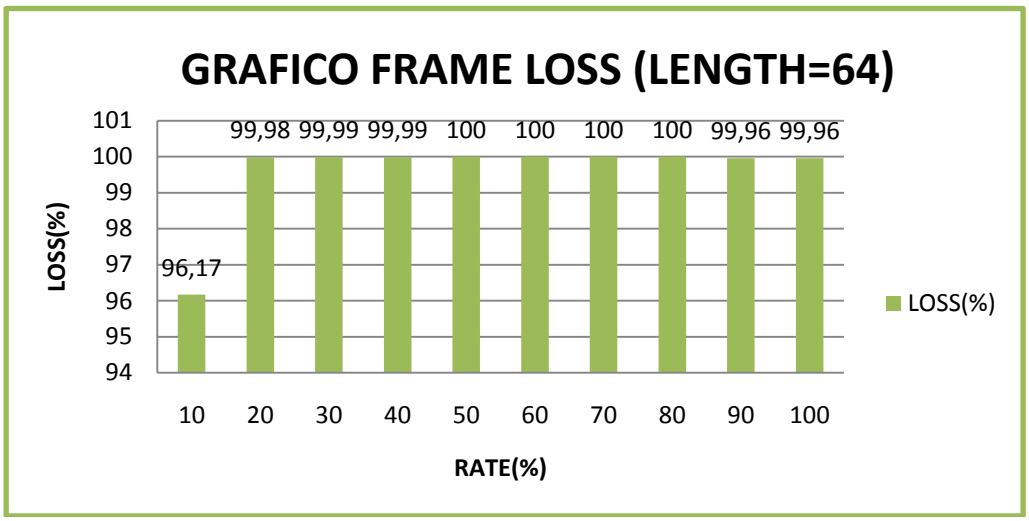


Figura. 7.9. Gráfica de medición de pérdida de paquetes para una longitud de 64 bits para el tercer día de medición

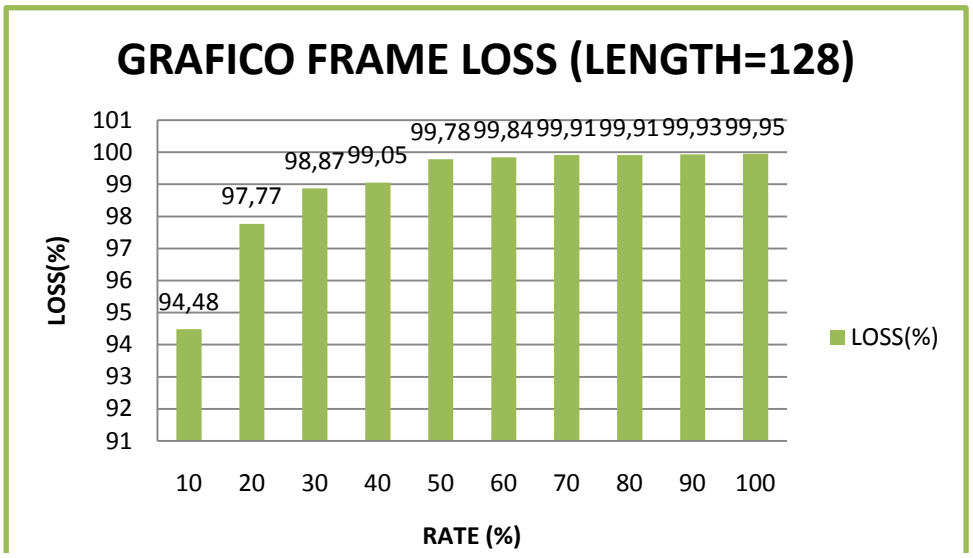


Figura.7.10. Gráfica de medición de pérdida de paquetes para una longitud de 128bits para el tercer día de medición

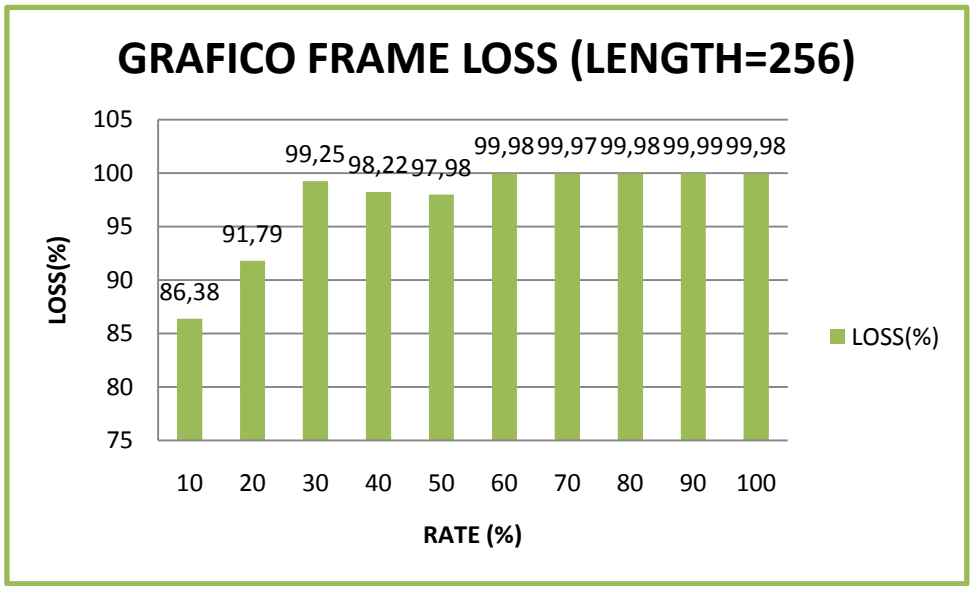


Figura. 7.11. Gráfica de medición de pérdida de paquetes para una longitud de 256 bits para el tercer día de medición

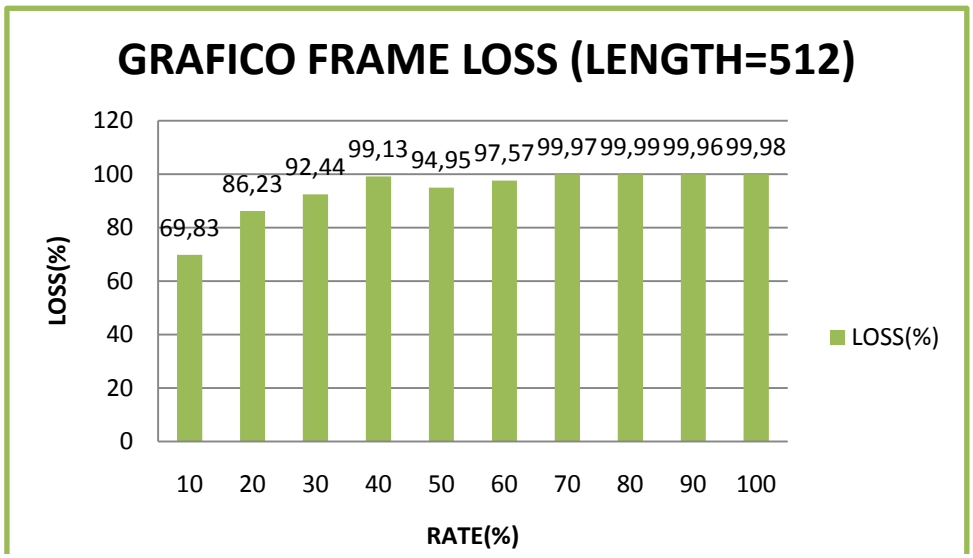


Figura. 7.12. Gráfica de medición de pérdida de paquetes para una longitud de 512 bits para el tercer día de medición

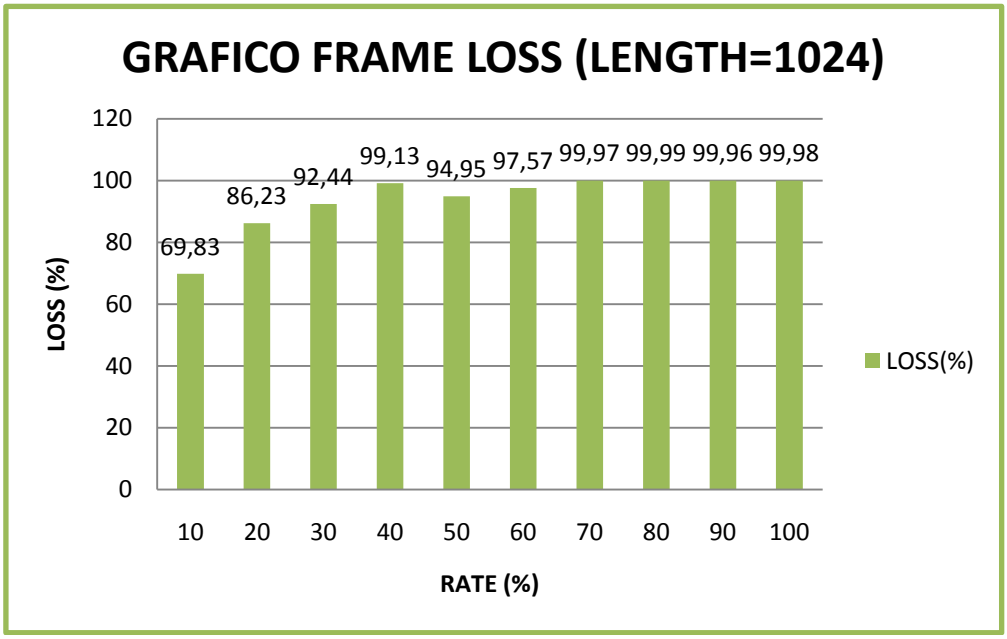


Figura. 7.13. Gráfica de medición de pérdida de paquetes para una longitud de 1024 bits para el tercer día de medición

Al verificar los datos obtenidos en este día en cuanto a medición de paquetes perdidos se observa un gran porcentaje de paquetes perdidos esto nos indica un mal funcionamiento de la red cuanto se incrementa el número de puntos de red y aumenta el tráfico dentro de la red.

Tabla. 7.25. Resultados Generales de medición de back to back frames para longitudes de 64, 128, 256, 512 y 1024 bits para el tercer día de medición

LENGTH	#FRAMES	STATUS
64	17	PASS
64	48	FAIL
64	35	FAIL
64	61	FAIL
64	48	FAIL
64	73	FAIL
64	21	PASS
64	86	FAIL
64	64	PASS
64	43	FAIL
64	46	FAIL
64	291	FAIL
64	23	PASS
64	50	FAIL
64	46	PASS
64	291	FAIL
64	363	FAIL
64	41	PASS
64	35	FAIL
64	28	FAIL
64	48	FAIL
64	34	FAIL
64	62	FAIL
64	95	FAIL
64	70	FAIL
64	28	PASS
64	26	PASS
64	75	FAIL
64	146	FAIL
64	34	FAIL
64	291	FAIL
64	39	FAIL
64	73	FAIL

64	26	PASS
64	39	FAIL
64	48	FAIL
64	34	FAIL
64	30	PASS
64	39	PASS
64	73	FAIL
64	35	FAIL
64	41	FAIL
64	50	FAIL
64	41	FAIL
64	30	PASS
64	37	FAIL
64	55	FAIL
64	30	FAIL
64	39	PASS
64	46	PASS
128	31	FAIL
128	39	FAIL
128	23	FAIL
128	23	FAIL
128	52	FAIL
128	24	PASS
128	23	FAIL
128	21	FAIL
128	19	FAIL
128	19	FAIL
128	26	FAIL
128	42	FAIL
128	21	FAIL
128	24	PASS
128	33	FAIL
128	21	PASS
128	24	PASS
128	19	PASS
128	24	PASS
128	26	PASS
128	36	FAIL
128	23	FAIL
128	21	PASS
128	21	PASS
128	31	FAIL
128	28	FAIL
128	31	FAIL
128	26	FAIL

128	23	FAIL
128	18	FAIL
128	21	FAIL
128	19	PASS
128	31	FAIL
128	24	FAIL
128	24	PASS
128	23	FAIL
128	19	PASS
128	21	PASS
128	21	PASS
128	19	FAIL
128	18	FAIL
128	21	FAIL
128	31	FAIL
128	21	PASS
128	21	FAIL
128	21	PASS
128	23	FAIL
128	26	FAIL
128	19	FAIL
128	28	FAIL
256	20	FAIL
256	15	PASS
256	18	PASS
256	15	FAIL
256	20	FAIL
256	15	PASS
256	17	FAIL
256	20	FAIL
256	15	PASS
256	14	FAIL
256	18	FAIL
256	15	PASS
256	18	PASS
256	15	PASS
256	15	PASS
256	14	FAIL
256	15	PASS
256	15	PASS
256	15	PASS
256	26	FAIL
256	15	PASS
256	21	PASS
256	20	FAIL

256	17	FAIL
256	17	FAIL
256	20	FAIL
256	12	PASS
256	12	PASS
256	12	PASS
256	12	PASS
256	12	PASS
256	17	FAIL
256	15	PASS
256	17	FAIL
256	18	FAIL
256	15	PASS
256	21	FAIL
256	20	FAIL
256	17	FAIL
256	17	FAIL
256	15	PASS
256	12	PASS
256	17	FAIL
256	20	FAIL
256	15	PASS
256	18	FAIL
256	12	PASS
256	20	FAIL
256	20	FAIL
256	20	FAIL
512	20	FAIL
512	23	FAIL
512	17	FAIL
512	23	FAIL
512	15	PASS
512	12	PASS
512	20	FAIL
512	21	PASS
512	20	FAIL
512	23	FAIL
512	20	FAIL
512	12	FAIL
512	23	PASS
512	20	FAIL
512	12	PASS
512	23	FAIL
512	20	FAIL
512	12	PASS

512	21	PASS
512	21	PASS
512	25	FAIL
512	20	FAIL
512	15	PASS
512	17	FAIL
512	17	FAIL
512	17	FAIL
512	92	FAIL
512	20	FAIL
512	17	FAIL
512	14	FAIL
512	21	FAIL
512	18	FAIL
512	21	PASS
512	23	FAIL
512	21	FAIL
512	20	FAIL
512	18	FAIL
512	25	FAIL
512	20	FAIL
512	18	PASS
512	18	PASS
512	21	FAIL
512	17	FAIL
512	20	FAIL
512	17	FAIL
512	17	FAIL
512	18	FAIL
512	18	PASS
512	17	FAIL
512	15	PASS
1024	22	FAIL
1024	16	PASS
1024	24	FAIL
1024	19	PASS
1024	21	FAIL
1024	16	PASS
1024	21	FAIL
1024	16	PASS
1024	16	FAIL
1024	19	PASS
1024	24	FAIL
1024	16	PASS
1024	19	FAIL

1024	18	FAIL
1024	18	FAIL
1024	13	FAIL
1024	15	FAIL
1024	18	FAIL
1024	16	PASS
1024	16	PASS
1024	19	FAIL
1024	24	FAIL
1024	21	FAIL
1024	21	FAIL
1024	16	PASS
1024	24	PASS
1024	19	FAIL
1024	16	FAIL
1024	24	FAIL
1024	13	FAIL
1024	16	PASS
1024	18	FAIL
1024	13	FAIL
1024	16	PASS
1024	24	FAIL
1024	13	FAIL
1024	18	FAIL
1024	47	FAIL
1024	24	FAIL
1024	21	FAIL
1024	16	PASS
1024	29	FAIL
1024	16	FAIL
1024	16	FAIL
1024	19	PASS
1024	24	FAIL
1024	15	FAIL
1024	19	FAIL
1024	24	FAIL
1024	94	FAIL

Tabla. 7.26. Resultados específicos de medición de back to back frames para longitudes de 64, 128, 256, 512 y 1024 bits para el tercer día de medición

LENGTH	64	128	256	512	1024
MIN	17	17	12	11	12
MAX	362	51	25	91	93
AVG	67	24	16	19	20

Así mismo estos resultados de back to back frames demuestran la ineficacia de la red en estos días picos de matrículas, demostrándose que la red se encontraba totalmente saturada.

➢ CUARTA MEDICIÓN

Configuración del equipo de medición

Fecha y hora de medición

- 18/01/10
- 08:24:04

Tabla 7.27. Resultados Generales de medición de Throughput para longitudes de 64, 128, 256, 512 y 1024 bits para el cuarto día de medición

LENGTH	RATE (%)	STATUS
64	100	FAIL
64	50	PASS
64	75	FAIL
64	62,5	PASS
64	68,75	PASS
64	71,88	FAIL
64	70,31	FAIL
64	69,53	FAIL
128	100	FAIL
128	50	PASS
128	75	FAIL
128	62,5	PASS
128	68,75	FAIL
128	65,63	PASS
128	67,19	PASS
128	67,97	FAIL
256	100	FAIL

256	50	PASS
256	75	PASS
256	87,5	FAIL
256	81,25	FAIL
256	78,13	PASS
256	79,69	PASS
256	80,47	PASS
512	100	FAIL
512	50	PASS
512	75	PASS
512	87,5	PASS
512	93,75	PASS
512	96,88	FAIL
512	95,31	FAIL
512	94,53	FAIL
1024	100	FAIL
1024	50	PASS
1024	75	PASS
1024	87,5	PASS
1024	93,75	PASS
1024	96,88	FAIL
1024	95,31	FAIL
1024	94,53	FAIL

Tabla. 7.28. Resultados específicos de medición de Throughput para longitudes de 64, 128, 256, 512 y 1024 bits para el cuarto día de medición

LENGTH (bits)	THROUGHPUT (%)
64	68,75
128	67,19
256	80,47
512	93,75
1024	93,75

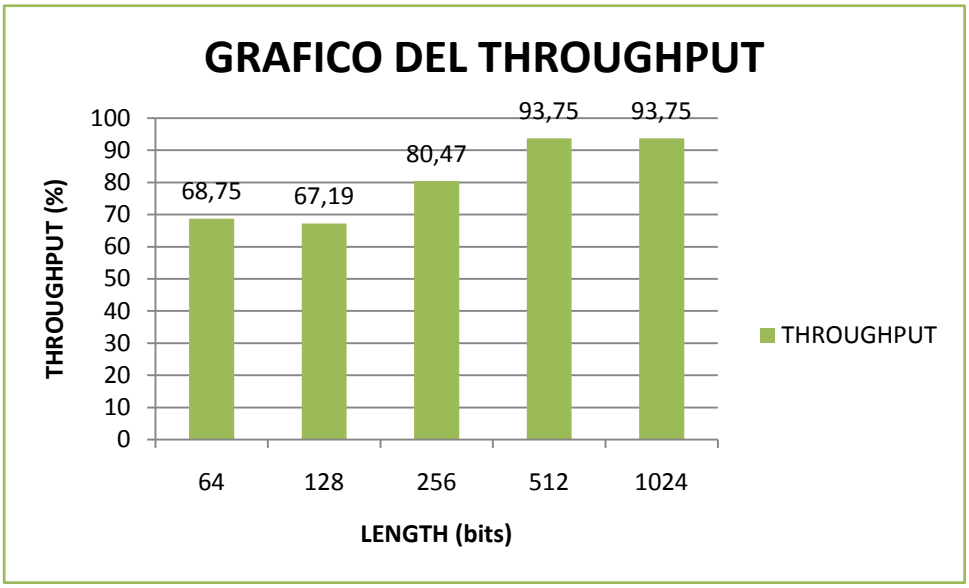


Figura 7.14. Gráfica de medición de Throughput VRS la longitud de para el cuarto día de medición

Como se puede verificar en los resultados obtenidos en las tablas 7.27, 7.28 y en la figura 7.14 existe un porcentaje de Throughput completamente mejorado, esto es debido a que la medición se la realizó ya no en días de matriculas sino en un día de trabajo normal de la red, y como se observa los valores de throughput son completamente aceptables para este tipo de redes.

Tabla. 7.29. Resultados de medición de Latencia para longitudes de 64, 128, 256, 512 y 1024 bits para el cuarto día de medición

LENGTH	RATE (%)	LATENCY (msec)	STATUS
64	68,75	21,474	PASS
128	67,19	21,474	PASS
256	80,47	32,834	PASS
512	93,75	42,756	PASS
1024	93,75	21,474	PASS

De la misma forma se observa en la Tabla. 7.29., que los resultados de tiempos de latencia son considerablemente aceptables y están dentro del rango de tiempos permitidos para este tipo de mediciones.

Tabla. 7.30. Resultados de medición de Pérdidas de paquetes para longitudes de 64, 128, 256, 512 y 1024 bits para el cuarto día de medición

LENGTH	RATE (%)	LOSS (%)
64	50	0
64	60	0
64	70	0
64	80	7,81
64	90	22,37
64	100	37,99
128	60	0
128	70	0
128	80	0,07
128	90	6,49
128	100	15,8
256	60	0
256	70	0
256	80	0,01
256	90	0,35
256	100	1,33
512	80	0
512	90	0
512	100	0,33
1024	80	0
1024	90	0
1024	100	0,39

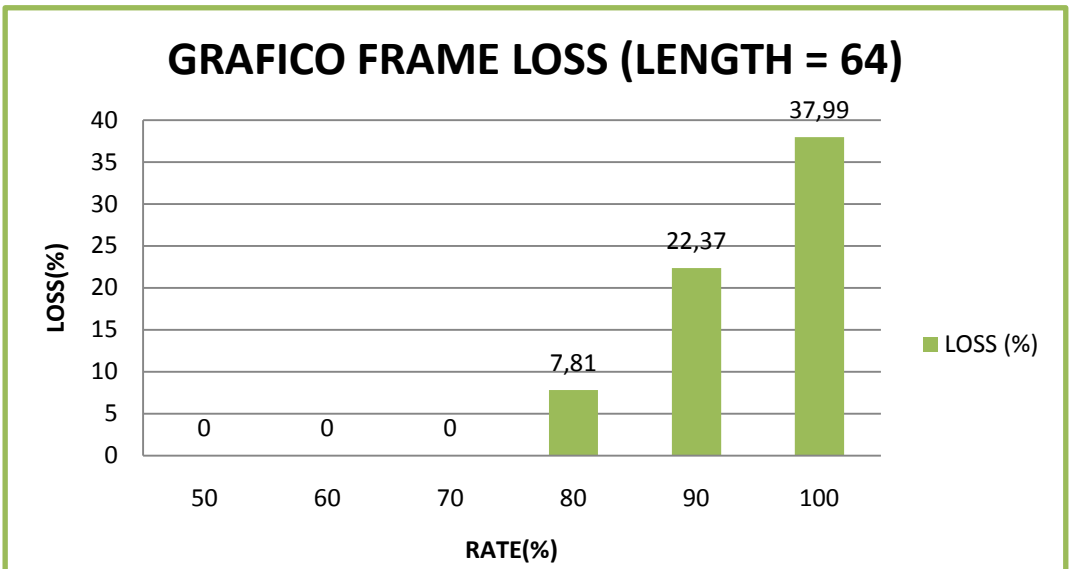


Figura. 7.15. Gráfica de medición de pérdidas de paquetes para una longitud de 64 bits para el cuarto día de medición

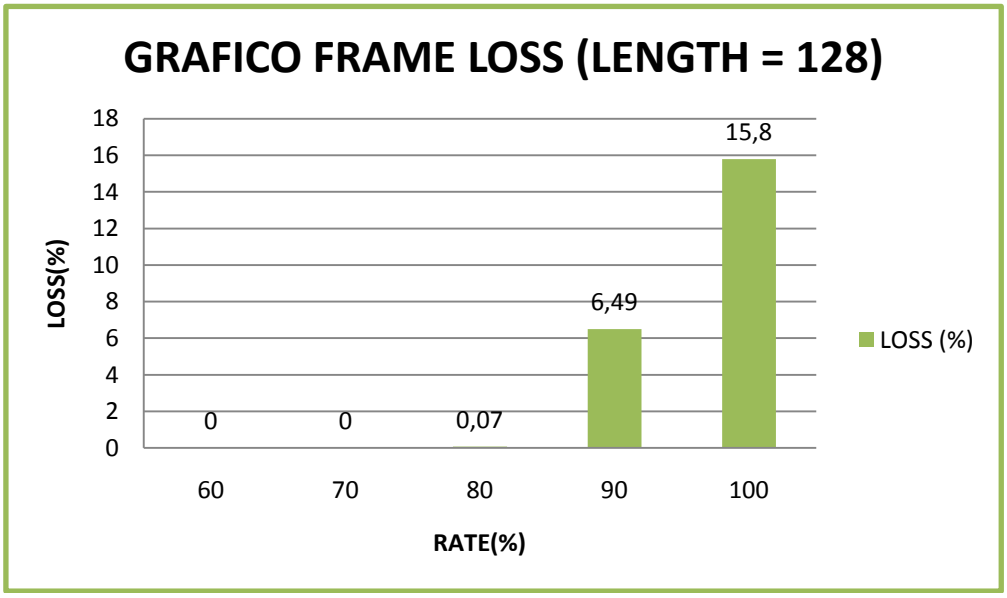


Figura. 7.16. Gráfica de medición de pérdidas de paquetes para una longitud de 128 bits para el cuarto día de medición

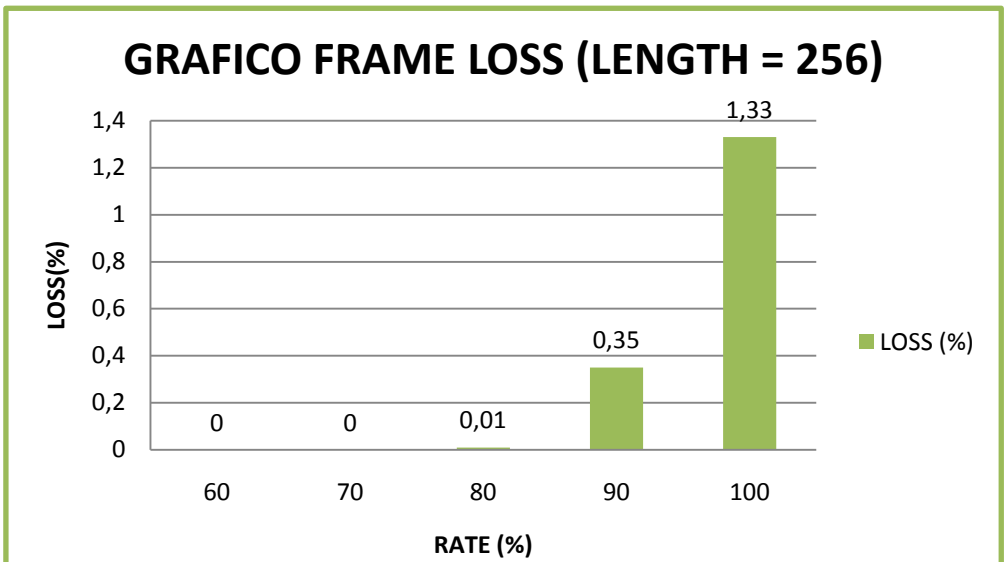


Figura. 7.17. Gráfica de medición de pérdidas de paquetes para una longitud de 256 bits para el cuarto día de medición

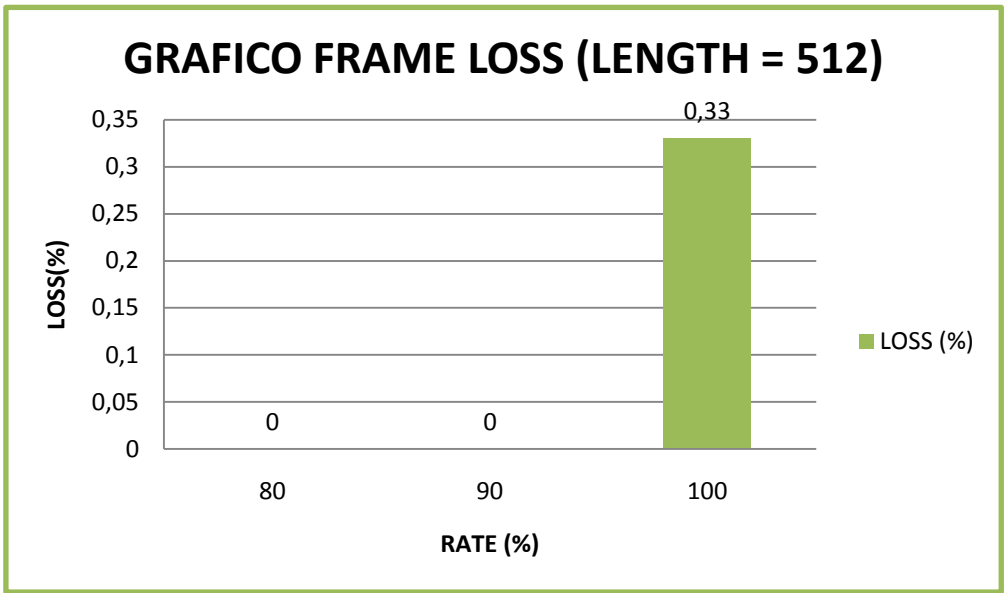


Figura. 7.18. Gráfica de medición de pérdidas de paquetes para una longitud de 512 bits para el cuarto día de medición

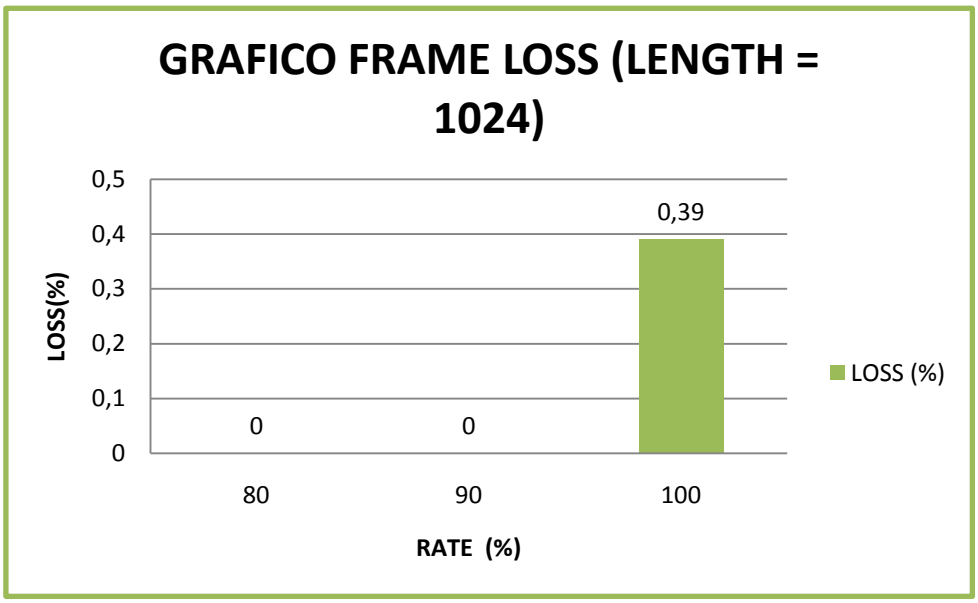


Figura. 7.19. Gráfica de medición de pérdidas de paquetes para una longitud de 1024 bits para el cuarto día de medición

Los resultados obtenidos en la tabla 7.30 y en las figura 7.15, 7.16, 7.17, 7.18 y 7.19 muestran que la pérdida de paquetes es mínima para las longitudes de tramas seleccionadas es decir que la red actualmente está funcionando de manera eficaz, sin provocar demasiadas pérdidas de datos, es así que para longitudes de 1024 bits existe una pérdida del 0,39% del 100% del total de la rata de transmisión indicándonos una pérdida mínima.

Tabla. 7.31. Resultados Generales de medición de back to back frames para longitudes de 64, 128, 256, 512 y 1024 bits para el cuarto día de medición

LENGTH	#FRAMES	STATUS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS

64	1488095	PASS
64	1488095	PASS
64	1488095	PASS

128	844594	PASS
128	844594	PASS
128	844594	PASS

128	844594	PASS
128	844594	PASS
128	844594	PASS
128	844594	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS

256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
512	234962	PASS
512	234962	PASS
512	234962

512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS

1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS

Tabla. 7.32. Resultados específicos de medición de back to back frames para longitudes de 64, 128, 256, 512 y 1024 bits para el cuarto día de medición

LENGTH	64	128	256	512	1024
MIN	1488095	84459	452898	234962	119731
MAX	1488095	84459	452898	234962	119731
AVG	1488095	84459	452898	234962	119731

Como se observa en las tablas 7.31 y 7.32 los valores obtenidos para números de back to back frames son adecuados para este tipo de redes, es decir la red se encuentra trabajando de manera correcta y eficaz.

- **QUINTA MEDICIÓN**

  - **Configuración del equipo de medición**

Tabla. 7.33. Configuración de hora y fecha de medición

NOMBRE DEL ARCHIVO	RFC_005	
DATOS GUARDADOS	10:20	20/01/10

Tabla. 7.34. Configuración de IP destino

RFC2544 FRAME FORMAT	
TEST	IP ROUTED
IP DST	10.1.45.5

Tabla. 7.35. Configuración de longitudes de medición

RFC2544 FRAME LENGTH (bits)	
64	YES
128	YES
256	YES
512	YES
1024	YES
1280	NO
1518	NO
4096	NO

Tabla. 7.36. Configuración de la secuencia de medición

RFC2544 TEST SEQUENCE	
LOOPBACK	YES
THROUGHPUT MEASUREMENT	YES
LATENCY MEASUREMENT	YES
FRAME LOSS RATE	YES
BACK TO BACK	YES
USER THRESHOLD	NO

Tabla. 7.37. Configuración del test de *throughput*

THROUGHPUT TEST CONFIGURATION	
MAX BANDWIDTH	100.0%
RESOLUTION	1.0%
DURATION	10sec

Tabla. 7.38. Configuración de medición de latencia

LATENCY TEST CONFIGURATION	
BANDWIDTH	**THROUGHPUT**
DURATION	**60sec**

Tabla. 7.39. Configuración de *FRAME LOSS RATE*

FRAME LOSS RATE CONFIGURATION	
START BANDWIDTH	100%
STEP SIZE	10%
DURATION	10sec

Tabla. 7.40. Configuración de *BACK TO BACK FRAMES*

BACK TO BACK CONFIGURATION	
MAX BANDWIDTH	100%
DURATION	2sec
MAX DURATION	10sec
REPETITIONS	50
RESOLUTION	1frame(s)

Tabla. 7.41. Resultados Generales de medición de *Throughput* longitudes de 64, 128, 256, 512 y 1024 bits para el quinto día de medición

LENGTH(bits)	RATE (%)	STATUS
64	100	FAIL
64	50	FAIL
64	25	PASS
64	37,5	PASS
64	43,75	PASS
64	46,88	PASS

64	48,44	PASS
64	49,22	PASS
128	100	FAIL
128	50	PASS
128	75	PASS
128	87,5	FAIL
128	81,25	PASS
128	84,38	FAIL
128	82,81	PASS
128	83,59	PASS
256	100	PASS
512	100	PASS
1024	100	PASS

Tabla. 7.42. Resultados Específicos de medición de *Throughput* longitudes de 64, 128, 256, 512 y 1024 bits para el quinto día de medición

LENGTH(bits)	THROUGHPUT (%)
64	49,22
128	83,59
256	100
512	100
1024	100

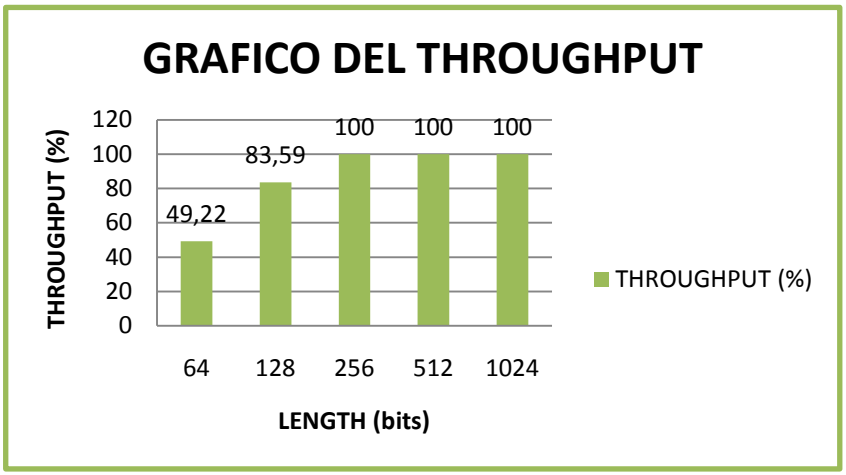


Figura. 7.20. Gráfica de medición de *Throughput* Vrs la Longitud de paquetes para el quinto día de medición

De igual manera, se realizaron las últimas mediciones de *Throughput* en un día fuera de matrículas encontrando buenos resultados como lo muestran las Tablas 7.41, 7.42 y la Figura 7.20, se observa datos obtenidos para tramas de 1024 bits en donde el *Throughput* es el máximo alcanzado del 100%, el cual representa el buen desempeño de la red.

Tabla. 7.43. Resultados de medición de Latencia para longitudes de 64, 128, 256, 512 y 1024 bits para el quinto día de medición

LENGTH	RATE (%)	LATENCY (msec)
64	49.22	21,475
128	83.59	21,475
256	100.00	21,475
512	100.00	21,475
1024	100.00	21,475

La Tabla 7.43., muestra los resultados de latencia los cuales indican que las tramas están siendo enviadas en los tiempos adecuados.

Tabla. 7.44. Resultados de medición de Pérdidas de paquetes para longitudes de 64, 128, 256, 512 y 1024 bits para el quinto día de medición

LENGTH	RATE (%)	LOSS (%)
64	60	0
64	70	0
64	80	6,4
64	90	21,93
64	100	39,2
128	70	0
128	80	0
128	90	6,38
128	100	15,75
256	90	0
256	100	0
512	80	0
512	90	0
512	100	0,04
1024	90	0
1024	100	0

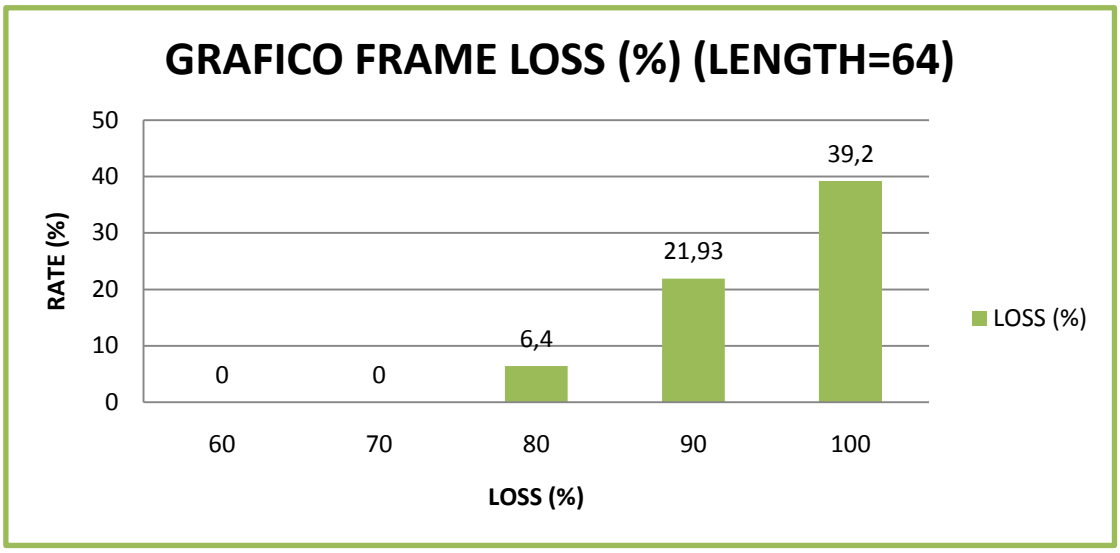


Figura. 7.21. Gráfica de medición de Pérdidas de tramas para longitudes de paquetes de 64 bits para el quinto día de medición

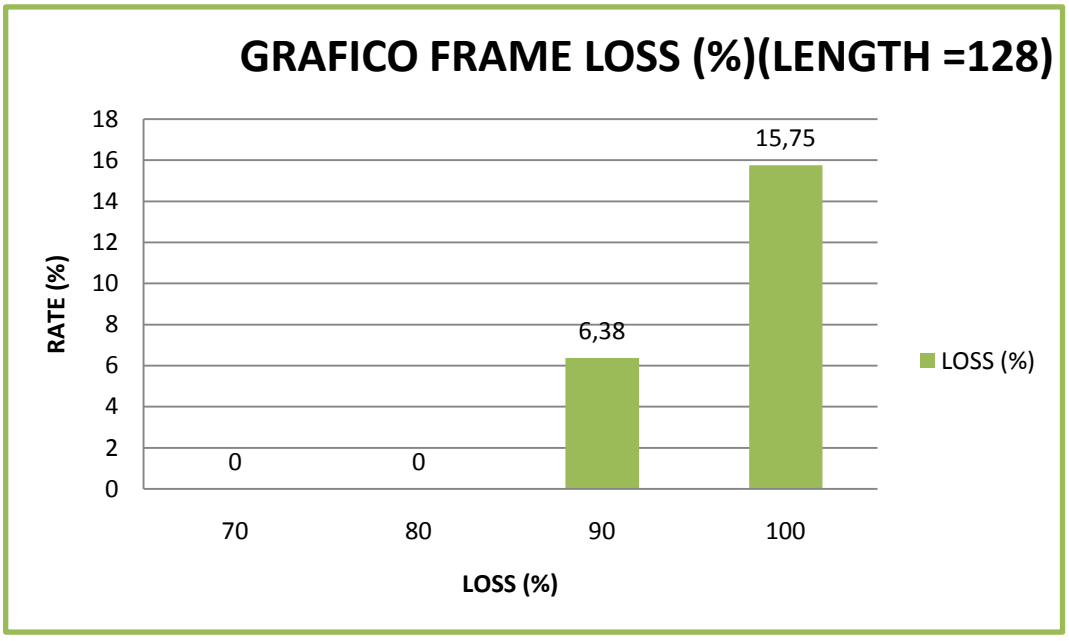


Figura. 7.22. Gráfica de medición de Pérdidas de tramas para longitudes de paquetes de 128 bits para el quinto día de medición

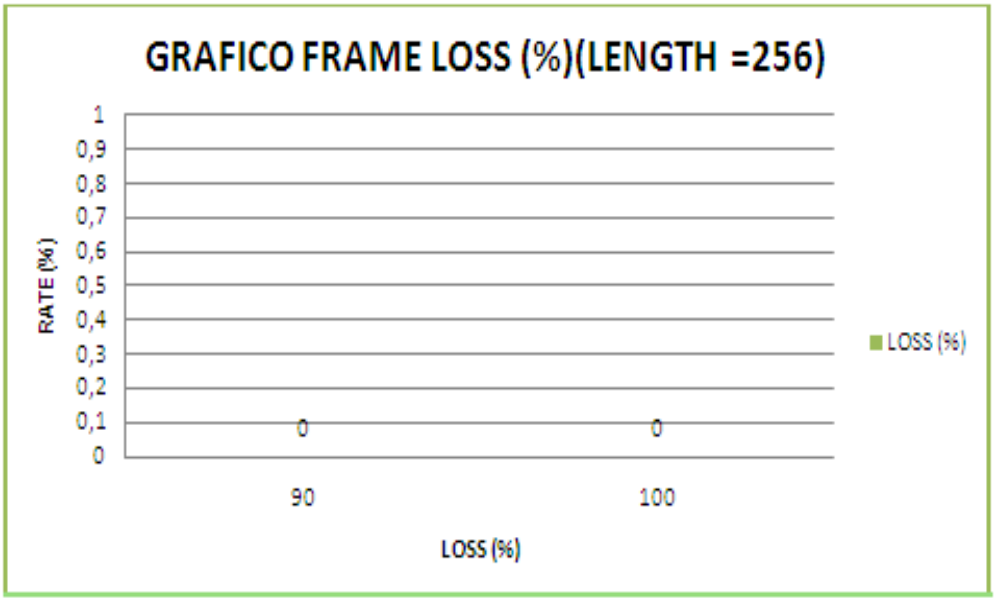


Figura. 7.23. Gráfica de medición de Pérdidas de tramas para longitudes de paquetes de 256 bits para el quinto día de medición

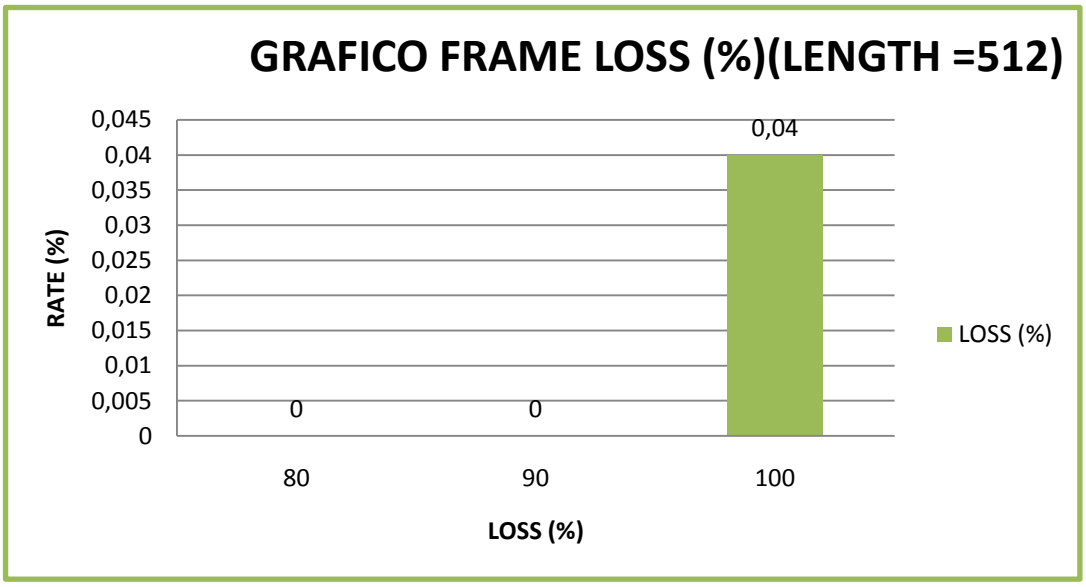


Figura. 7.24. Gráfica de medición de Pérdidas de tramas para longitudes de paquetes de 512 bits para el quinto día de medición

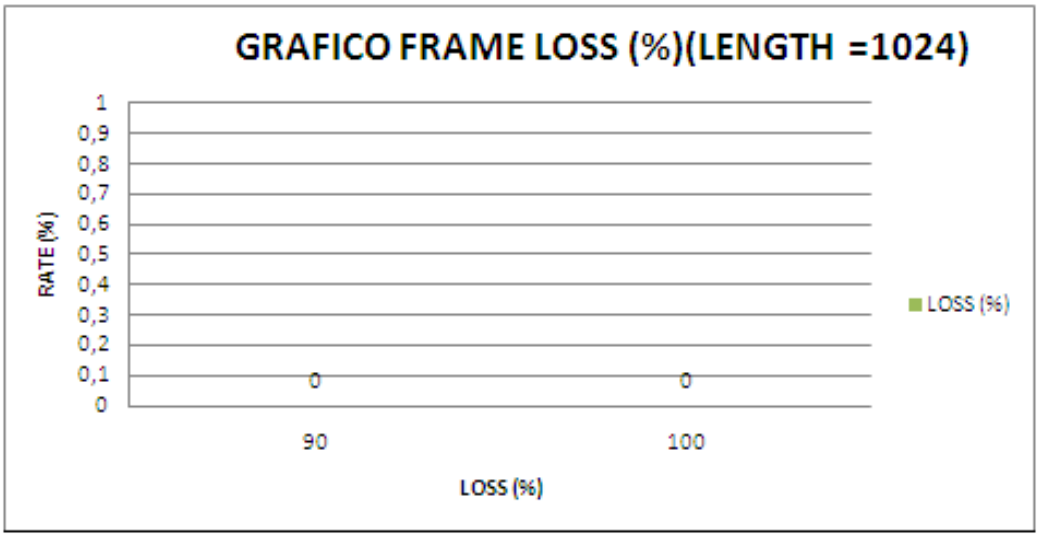


Figura. 7.25. Gráfica de medición de Pérdidas de tramas para longitudes de paquetes de 1024 bits para el quinto día de medición

Los datos que se obtuvieron indican que existen mínimas pérdidas de paquetes para las diferentes longitudes de tramas, como es el caso de la medición realizada para una longitud de trama de 1024 bits en donde existen 0% de pérdidas, lo cual ratifica que la red está totalmente descongestionada y con un correcto funcionamiento.

Tabla. 7.45. Resultados de medición de *back-to-back frames* para longitudes de 64, 128, 256, 512 y 1024 bits para el quinto día de medición

LENGTH	#FRAMES	STATUS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS
64	1488095	PASS

64	1488095	PASS
64	1488095	PASS
64	1488095	PASS

128	844594	PASS
128	844594	PASS
128	844594	PASS

256	452898	PASS
256	452898	PASS
256	452898	PASS

256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
512	234962	PASS
512	234962	PASS
512	234962

512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731

1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS

Tabla 7.46. Resultados de medición de *back to back frames* para longitudes de 64, 128, 256, 512 y 1024 bits para el quinto día de medición

LENGTH	64	128	256	512	1024
MIN	1488095	84459	452898	234962	119731
MAX	1488095	84459	452898	234962	119731
AVG	1488095	84459	452898	234962	119731

Como se puede observar en los resultados obtenidos en las Tablas 7.45 y 7.46 se puede concluir que los valores de número de ráfagas que se obtuvieron se encuentran dentro del rango permitido para el tipo de tráfico que se está analizando en la red, puesto que todo el porcentaje de tráfico se está recibiendo al 100% de las ráfagas transmitidas para las diferentes longitudes de tramas.

7.3 ANEXO 3

7.3.1 Certificaciones

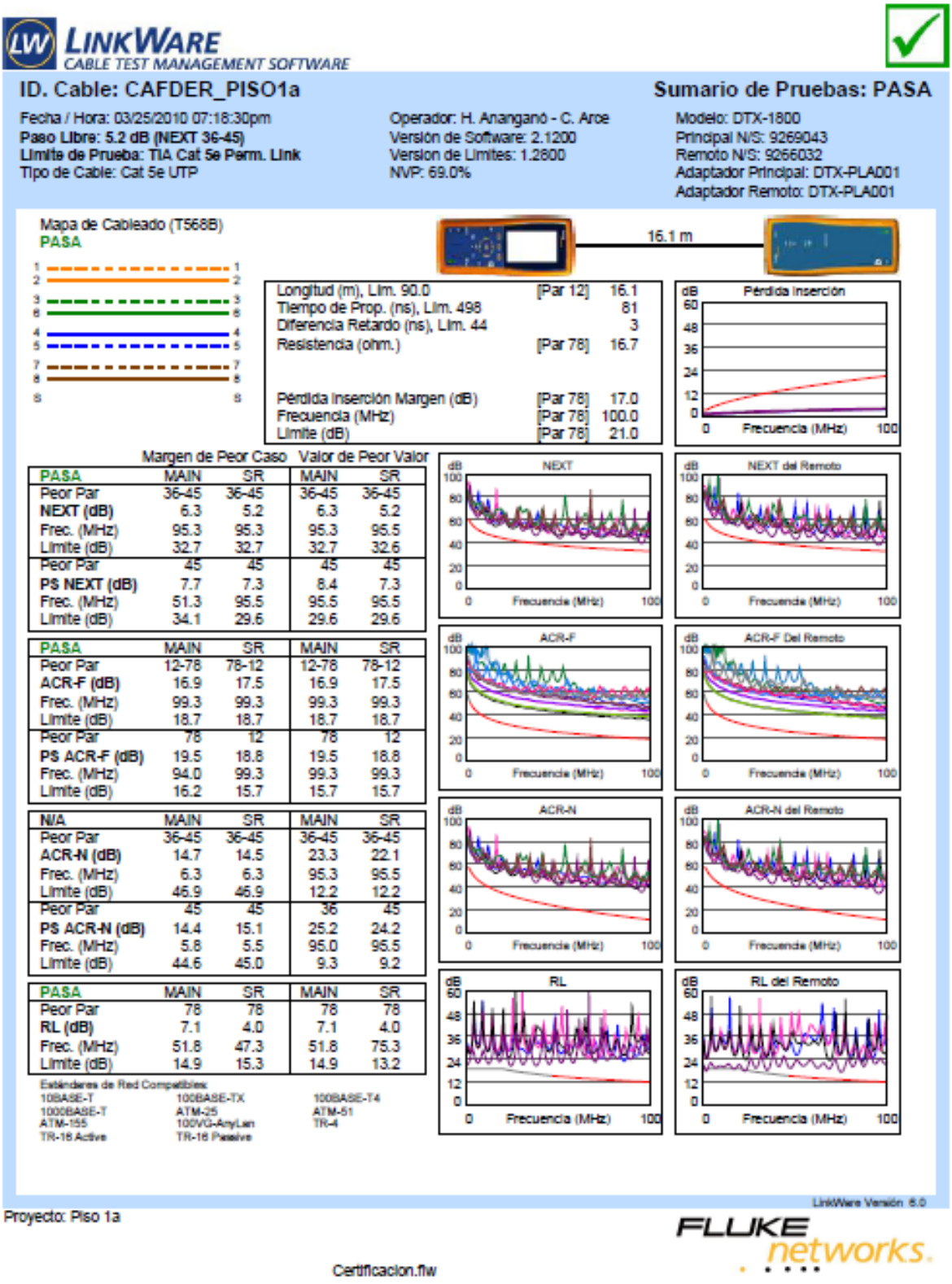


Figura. 7.26. Certificación CAFDER_PISO1a

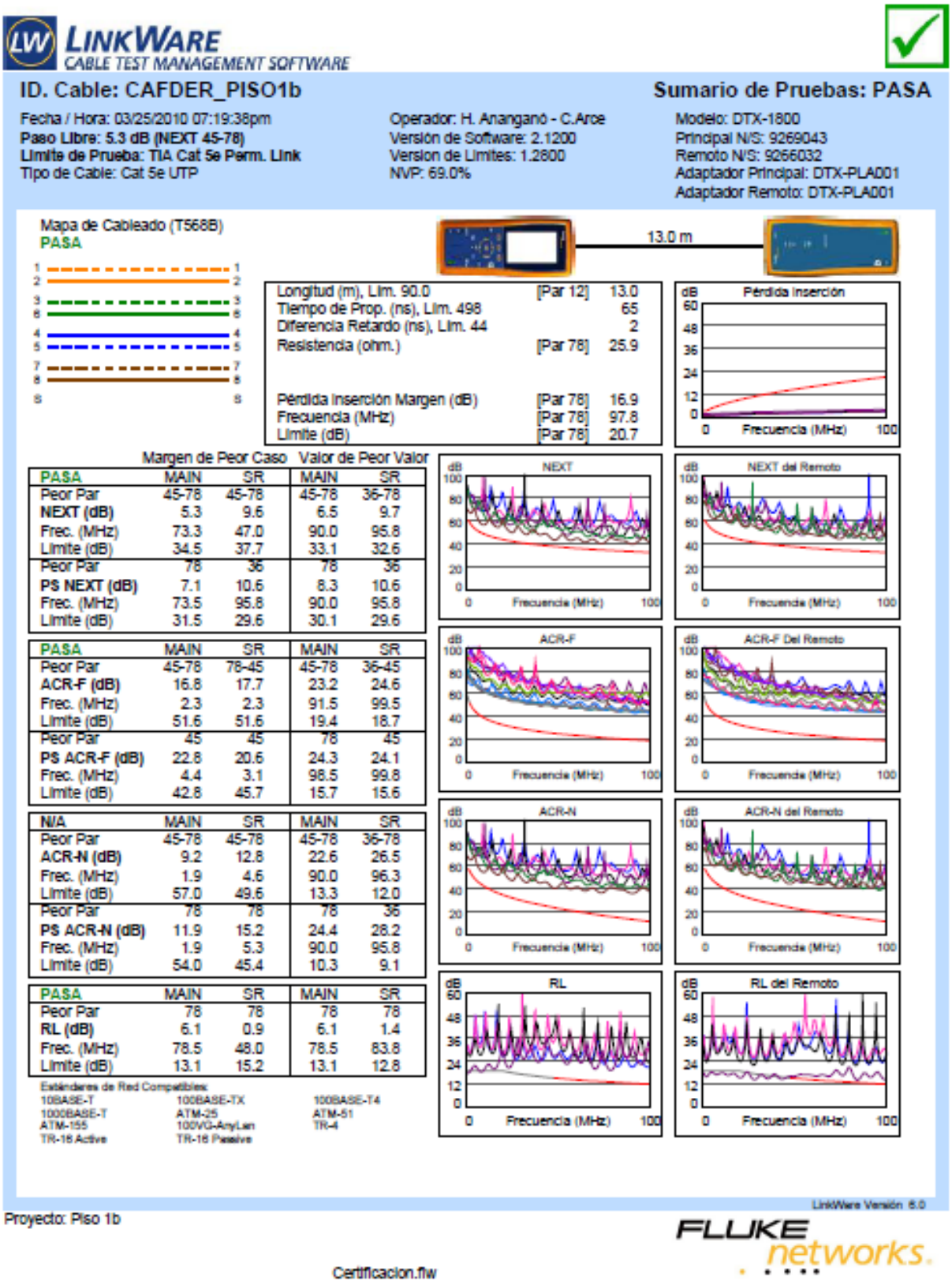


Figura. 7.27. Certificación CAFDER_PISO1b

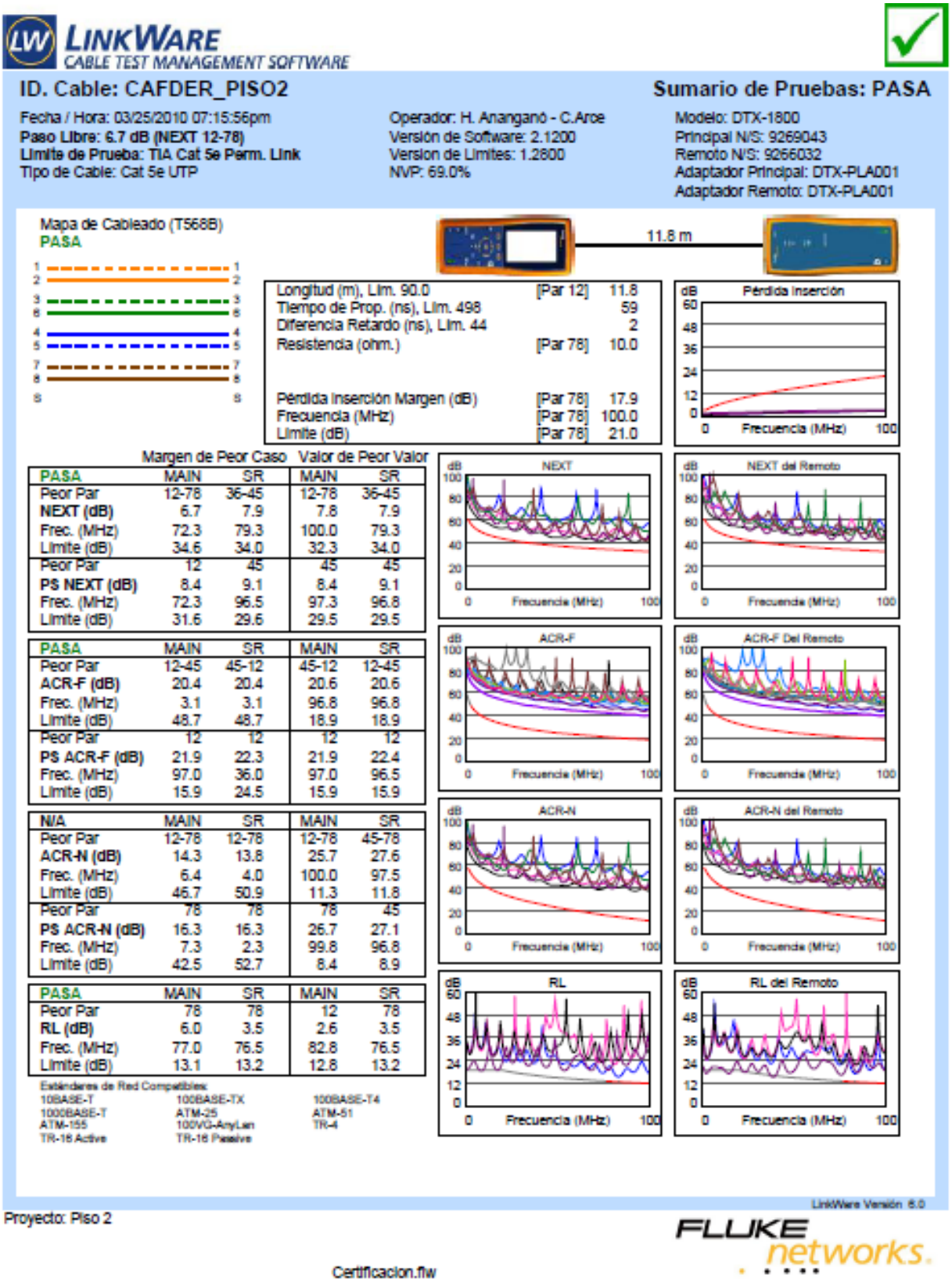


Figura. 7.28. Certificación CAFDER_PISO2

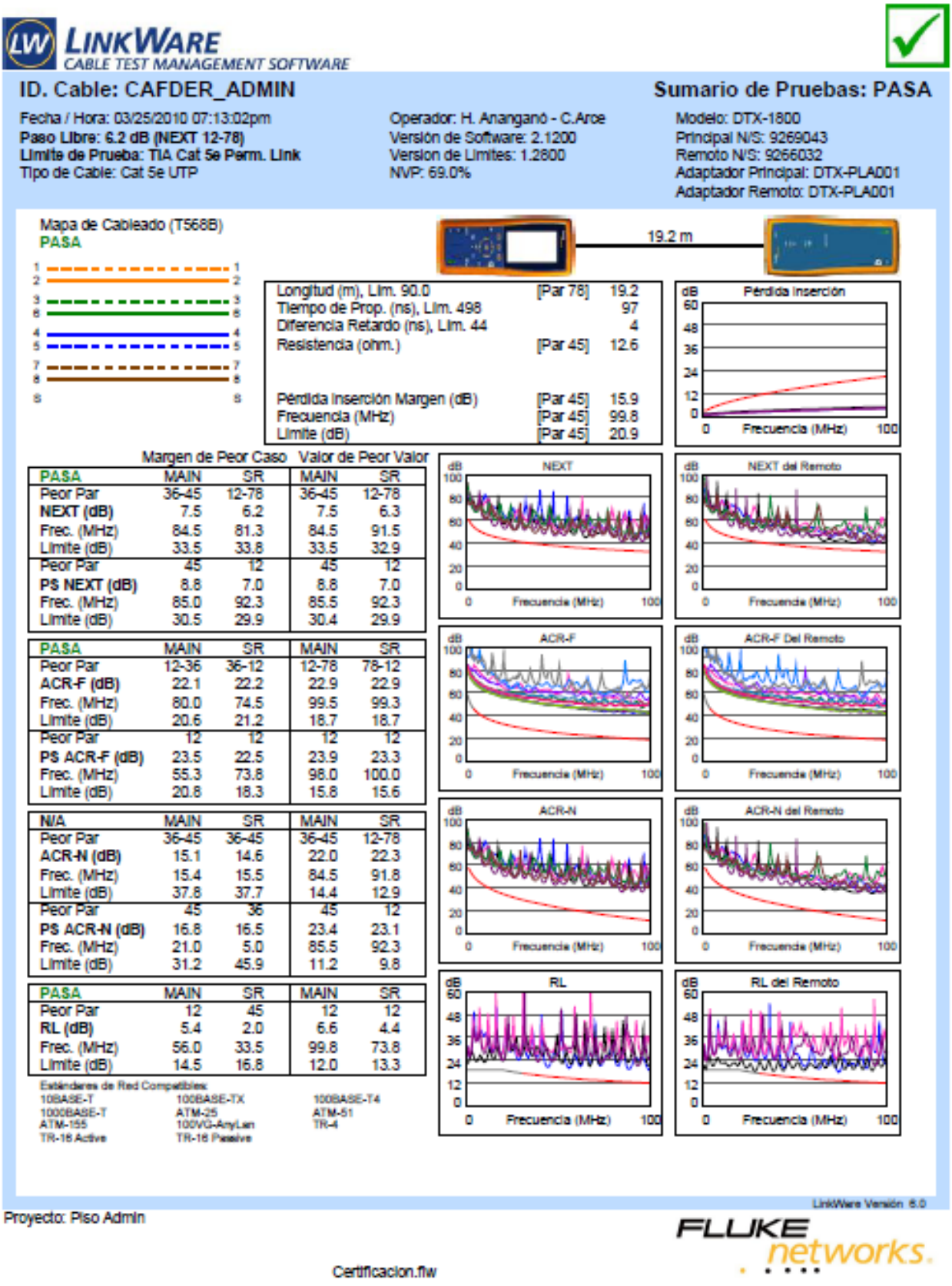


Figura. 7.29. Certificación CAFDER_ADMIN

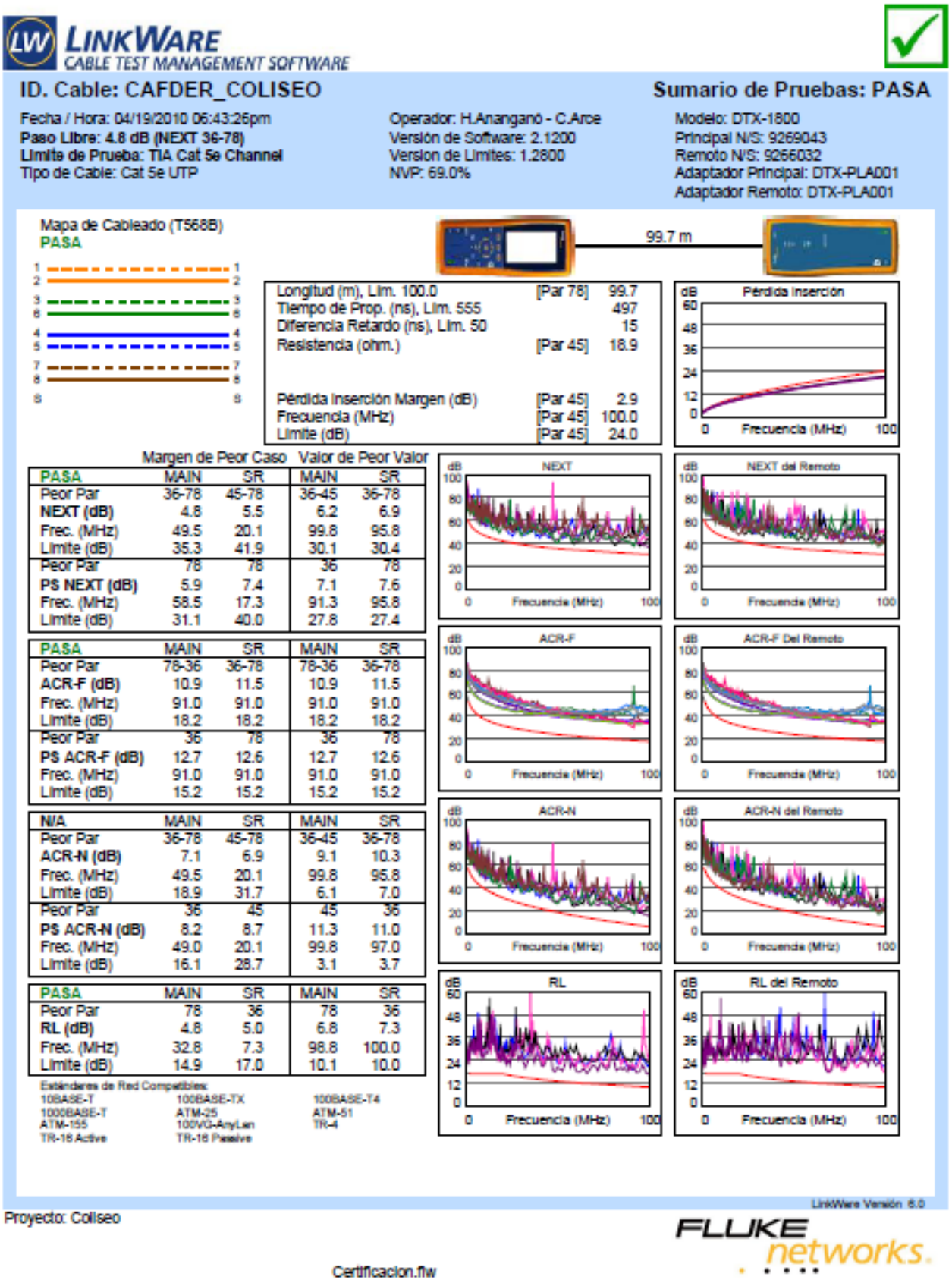


Figura. 7.30. Certificación CAFDER_COLISEO

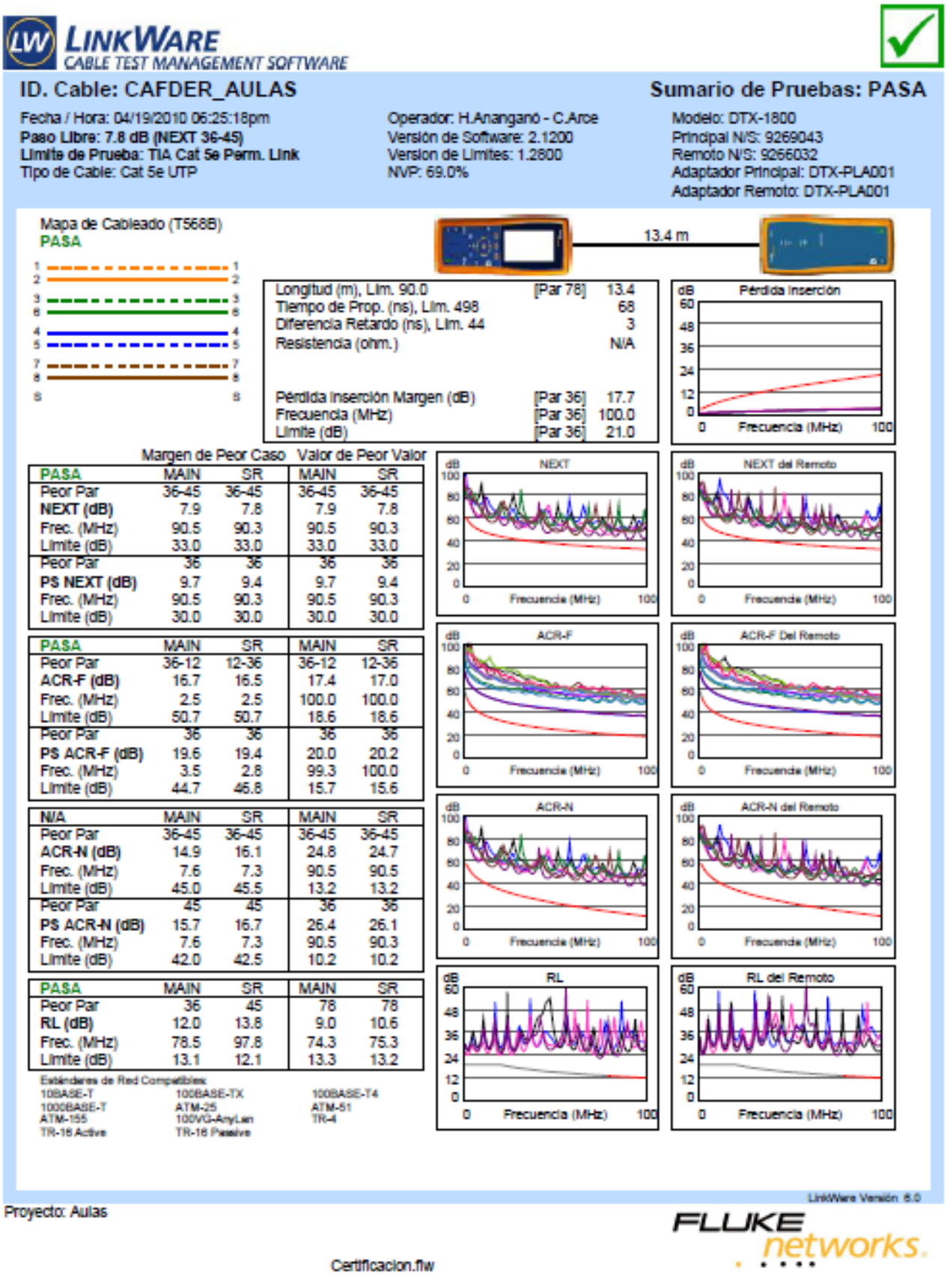


Figura. 7.31. Certificación CAFDER_AULAS

7.4 ANEXO 4

7.4.1 Análisis de tráfico

Para realizar el análisis de mediciones de tráfico de la nueva red inalámbrica se procedió a la toma de datos, para nuestro caso se decidió apuntar a la dirección IP de uno de nuestros APs, para así lograr medir todo el porcentaje de tráfico que esté pasando por medio del router inalámbrico. Para ello se procedió nuevamente a utilizar el equipo de medición de tráfico SUNSET MTT con su respectivo módulo para Ethernet.

- **Configuración del equipo de medición**

Las configuraciones del equipo se muestran en las Tablas que se indican a continuación.

Tabla. 7.47. Configuraciónón de hora y fecha de medición

Nombre del archivo	RFC_0012	
Datos guardados	14:39	05 06/05/10

Tabla 7.48. Configuración de IP destino

RFC2544 FRAME FORMAT	
TEST	IP ROUTED
IP DST	192.168.1.1

Tabla 7.49. Configuración de longitudes de medición

RFC2544 FRAME LENGTH (bits)	
64	YES
128	YES
256	YES
512	YES
1024	YES
1280	NO
1518	NO
4096	NO

Tabla 7.50. Configuración de la secuencia de medición

RFC2544 TEST SEQUENCE	
LOOPBACK	YES
THROUGHPUT MEASUREMENT	YES
LATENCY MEASUREMENT	YES
FRAME LOSS RATE	YES
BACK TO BACK	YES
USER THRESHOLD	NO

Tabla 7.51. Configuración del test de *throughput*

THROUGHPUT TEST CONFIGURATION	
MAX BANDWIDTH	100.0%
RESOLUTION	1.0%
DURATION	10sec

Tabla 7.52. Configuración de medición de latencia

LATENCY TEST CONFIGURATION	
BANDWIDTH	THROUGHPUT
DURATION	60sec

Tabla 7.53. Configuración de *FRAME LOSS RATE*

FRAME LOSS RATE CONFIGURATION	
START BANDWIDTH	100%
STEP SIZE	10%
DURATION	10sec

Tabla 7.54. Configuración de *BACK TO BACK FRAMES*

BACK TO BACK CONFIGURATION	
MAX BANDWIDTH	100%
DURATION	2sec
MAX DURATION	10sec
REPETITIONS	50
RESOLUTION	1frame(s)

Con las configuraciones mostradas anteriormente, se obtuvieron los siguientes resultados de medición de retardos (*Latency(ms)).*

En la Tabla 7.55 se muestran los resultados de medición de latencia cuyos valores dados en milisegundos no sobrepasan el valor límite propuesto para redes inalámbricas, que es de valores menores a 200 ms.

Tabla 7.55. Resultados de medición de latencia para la red inalámbrica

LATENCY TABLE			
LENGTH (bits)	**RATE (%)**	**LATENCY (msec)**	**STATUS**
64	17.97	32,9253	PASS
128	43.75	50,1580	PASS
256	81.25	70,6608	PASS
512	96.09	102,1641	PASS
1024	100.00	110,8974	PASS

La Tabla 7.56., y la Figura 7.32., muestran los resultados para las mediciones de throughput, para este caso se eligieron tamaños de tramas de hasta 1024 bits, provocando resultados de throughput razonables y que garantizan el correcto funcionamiento de la nueva red inalámbrica.

Tabla. 7.56. Resultados de throughput para tramas de 64, 128, 256, 512 y 1024 bits

THROUGHPUT TEST TABLE		
LENGTH (bits)	**THROUGHPUT (%)**	**STATUS**
64	17,97	PASS
128	43,75	PASS
256	81,25	PASS
512	96,09	PASS
1024	100	PASS

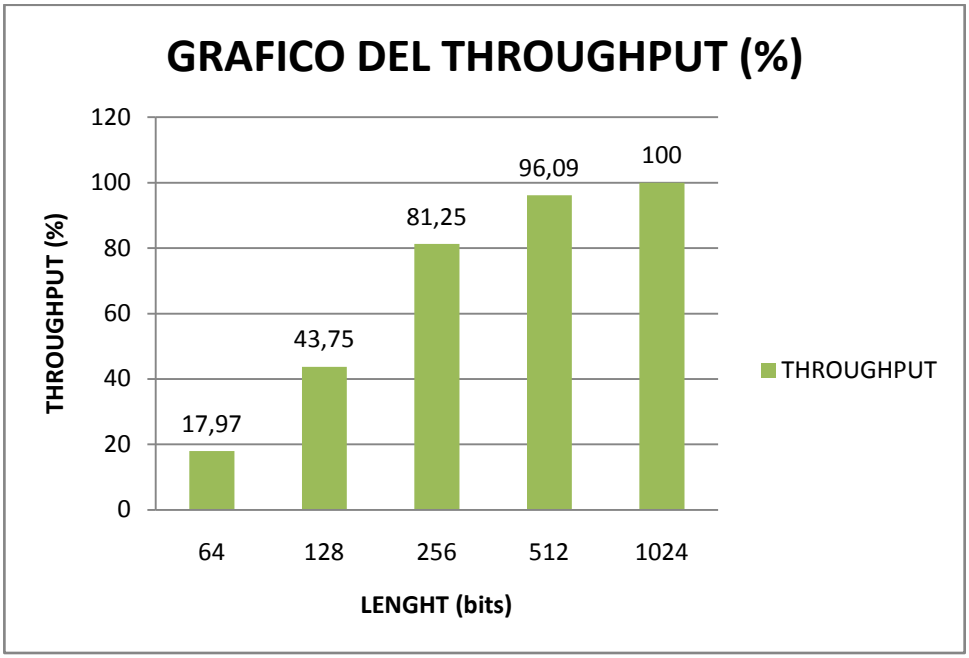


Figura. 7.32. Gráfica de throughput para medición de tráfico en la red inalámbrica

Los resultados de medición de la cogestión de tráfico son analizados mediante las tablas de *FRAME LOSS RATE y BACK TO BACK FRAMES*, cuyos datos se muestran en la Tablas 7.57., 7.58., 7.59 y Figuras 7.33, 7.34, 7.35, 7.36 y 7.37; cuyos resultados indican una pérdida de datos aceptable en este tipo de redes, en las cuales influye mucho el medio de transmisión, en este caso aire, cabe resaltar que los datos obtenidos no superan los límites propuestos para este tipo de redes.

Tabla. 7.57. Resultados de medición de *FRAME LOSS RATE* para la red inalámbrica

FRAME LOSS TABLE		
LENGTH (bits)	**RATE (%)**	**LOSS (%)**
64	100.00	99.07
64	90.00	99.47
64	80.00	95.12
64	70.00	85.64
64	60.00	70.21
64	50.00	48.40
64	40.00	12.83
64	30.00	0.15
64	20.00	0.05
64	10.00	0.00
128	100.00	65.95

128	90.00	53.38
128	80.00	37.17
128	70.00	14.77
128	60.00	1.19
128	50.00	0.29
128	40.00	0.23
128	30.00	0.00
128	20.00	0.00
256	100.00	0.14
256	90.00	0.11
256	80.00	0.22
256	70.00	0.00
256	60.00	0.00
512	100.00	0.00
512	90.00	0.00
1024	100.00	0.00
1024	90.00	0.00

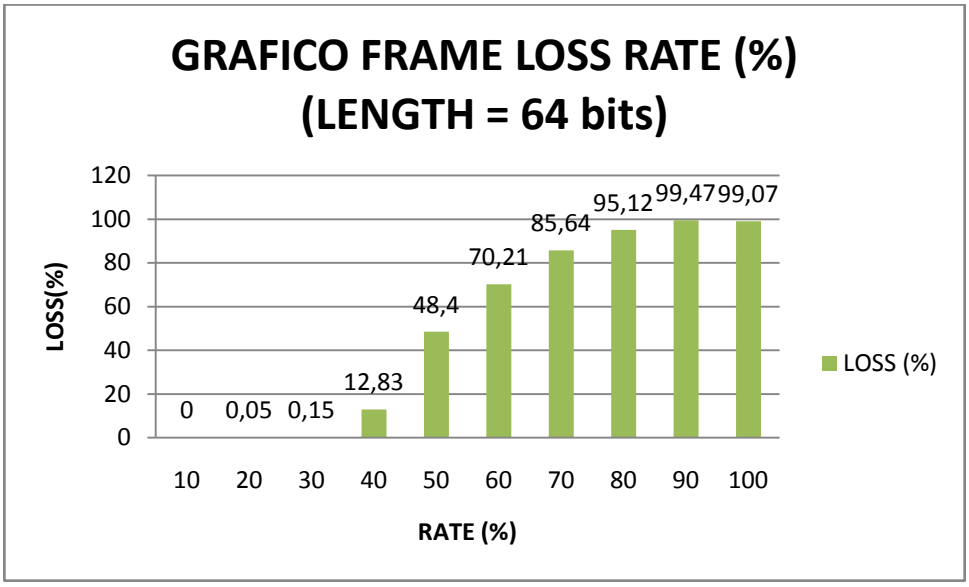


Figura. 7.33. Gráfico de Frame Loss Rate (%) para una longitud de trama de 64 bits.

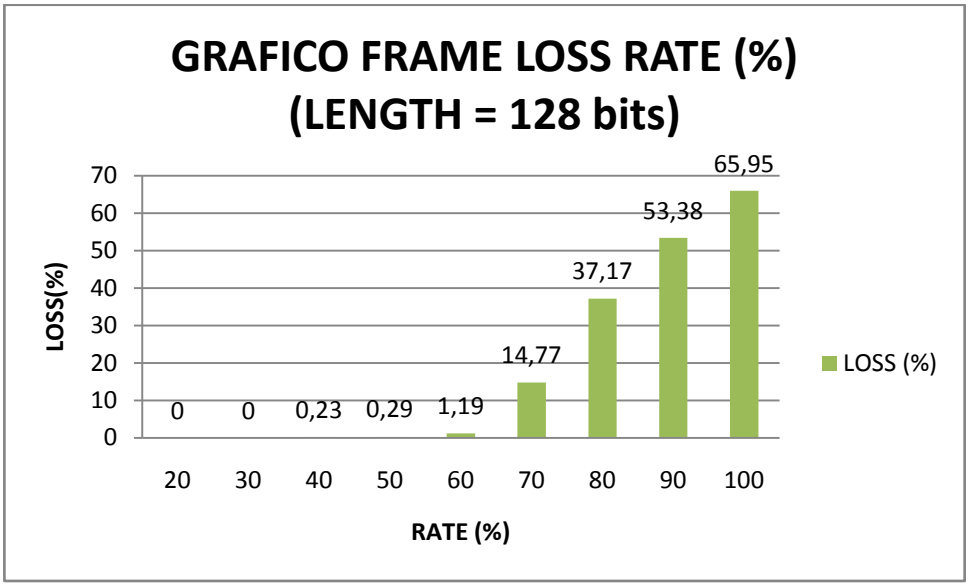


Figura. 7.34. Gráfico de Frame Loss Rate (%) para una longitud de trama de 128 bits.

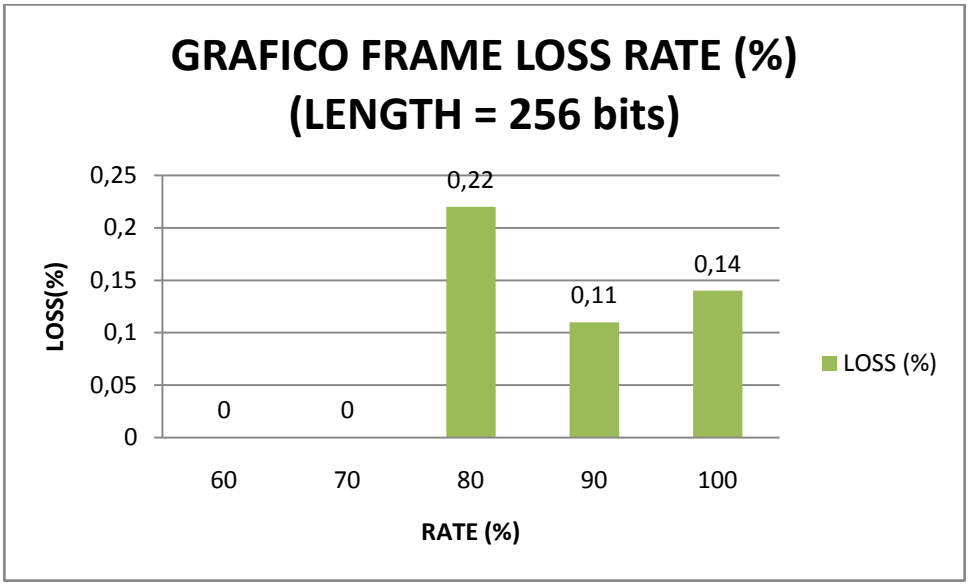


Figura. 7.35. Gráfico de Frame Loss Rate (%) para una longitud de trama de 256 bits.

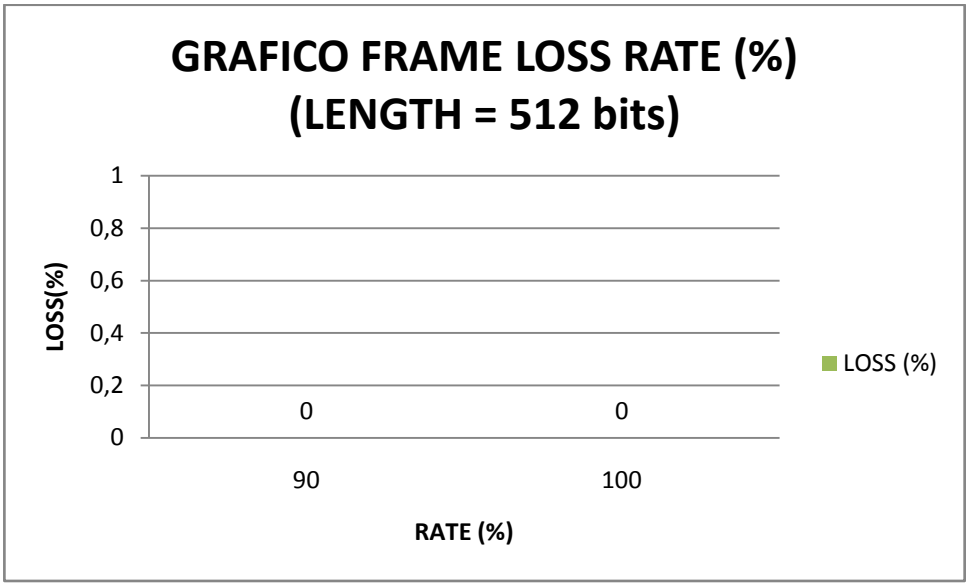


Figura. 7.36. Gráfico de Frame Loss Rate (%) para una longitud de trama de 512 bits.

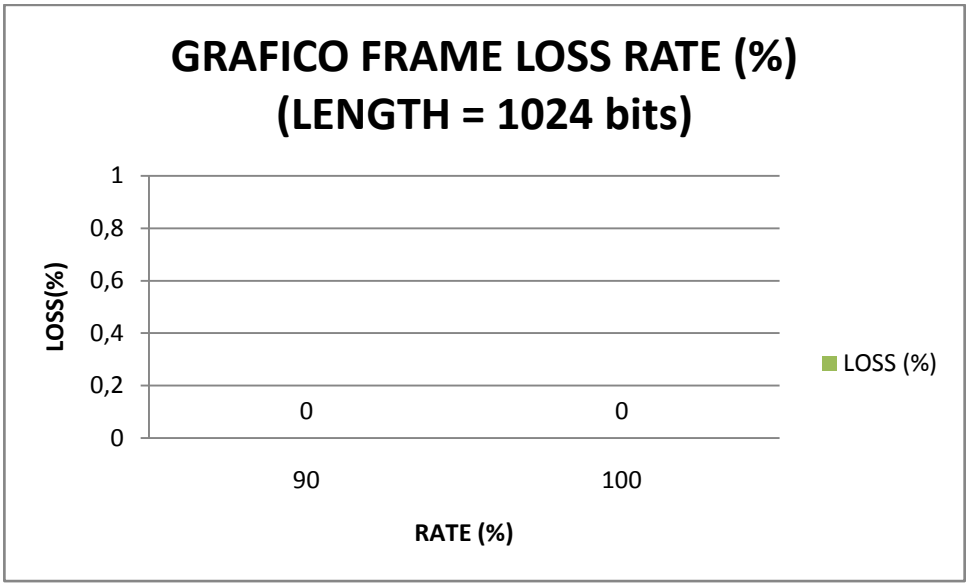


Figura. 7.37. Gráfico de Frame Loss Rate (%) para una longitud de trama de 512 bits.

Tabla. 7.58. Resultados de medición de *BACK TO BACK FRAMES*

BACK TO BACK TEST LOG		
LENGTH (bits)	**#FRAMES**	**STATUS**
64	3047	FAIL
64	3052	FAIL

64	3056	FAIL
64	3506	FAIL
64	3031	FAIL
64	3052	FAIL
64	3026	FAIL
64	3026	FAIL
64	3013	PASS
64	3022	PASS
64	3330	PASS
64	3542	FAIL
64	3022	PASS
64	3063	FAIL
64	3028	FAIL
64	3050	PASS
64	4069	FAIL
64	3040	PASS
64	3049	FAIL
64	3022	PASS
64	3031	PASS
64	3035	PASS
64	3037	PASS
64	3054	FAIL
64	3052	FAIL
64	3040	FAIL
64	3052	FAIL
64	3028	FAIL
64	3030	FAIL
64	3028	FAIL
64	3030	FAIL
64	3026	FAIL
64	3047	FAIL
64	3088	FAIL
64	3031	FAIL
64	3047	PASS
64	3033	PASS
64	3049	FAIL
64	3039	FAIL
64	3033	FAIL
64	3076	FAIL
64	3056	FAIL
64	3197	FAIL
64	3026	FAIL
64	3028	FAIL
64	3052	FAIL
64	3042	FAIL

64	3026	PASS
64	3195	PASS
64	3486	PASS
128	844594	PASS
128	844594	PASS
128	844594	PASS
128	844594	PASS
128	844594	PASS
128	844594	PASS
128	844251	FAIL
128	844593	PASS
128	844594	PASS
128	841623	PASS
128	844594	PASS
128	844594	PASS
128	844594	PASS
128	844594	PASS
128	844594	PASS
128	844594

128	844593	PASS
128	844594	PASS
128	844594	PASS
128	844594	PASS
128	832544	FAIL
128	844594	PASS
128	844256	FAIL
128	141120	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS

256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
256	452898	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS

512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
512	234962	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS

1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS
1024	119731	PASS

Tabla. 7.59 Resultados específicos de medición de *BACK TO BACK FRAMES*

BACK TO BACK FRAMES (#FRAMES)			
LENGHT (bits)	**Min**	**Max**	**AVG**
64	3013	4068	3100
128	141120	844594	830210
256	452898	452898	452898
512	234962	234962	234962
1024	119731	119731	119731

7.5 ANEXO 5

7.5.1 Puntos de red implementados

Figura. 7.38. Punto de red CAFDER_ADMIN

Figura. 7.39. Punto de red CAFDER_PISO2

Figura. 7.40. Punto de red CAFDER_PISO1a

Figura. 7.41. Punto de red CAFDER_PISO1b

Figura. 7.42. Punto de red CAFDER_PLANTABAJA

Figura. 7.43. Punto de red CAFDER_COLISEO

El punto de red CAFDER_AULAS se encuentra en Fisioterapia, mismo departamento se encuentra al momento cerrado por trabajos de obra civil realizados en el lugar.

7.6 ANEXO 6

7.6.1 Diagramas de cobertura implementados.

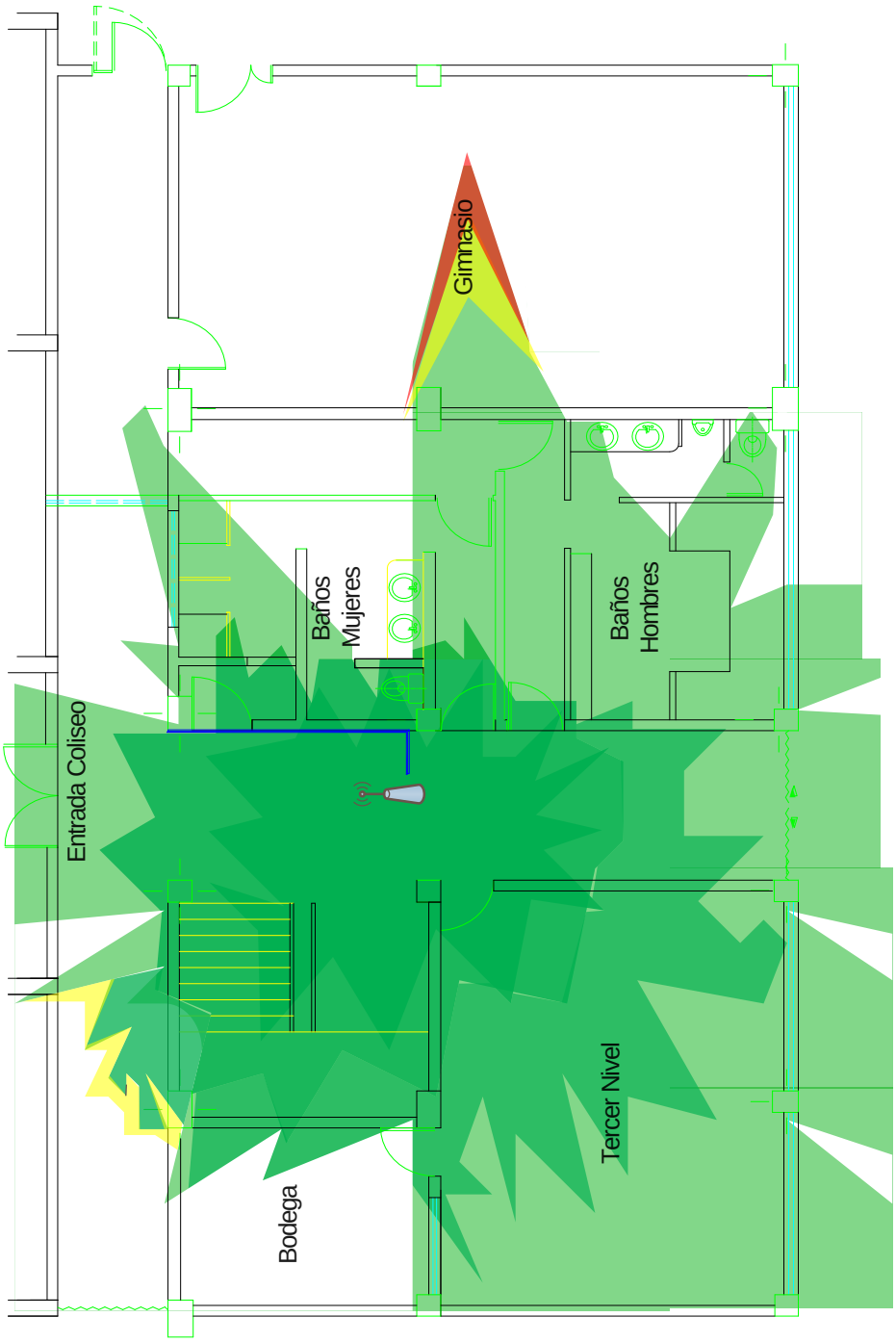


Figura. 7.44. Cobertura CAFDER_PLANTABAJA

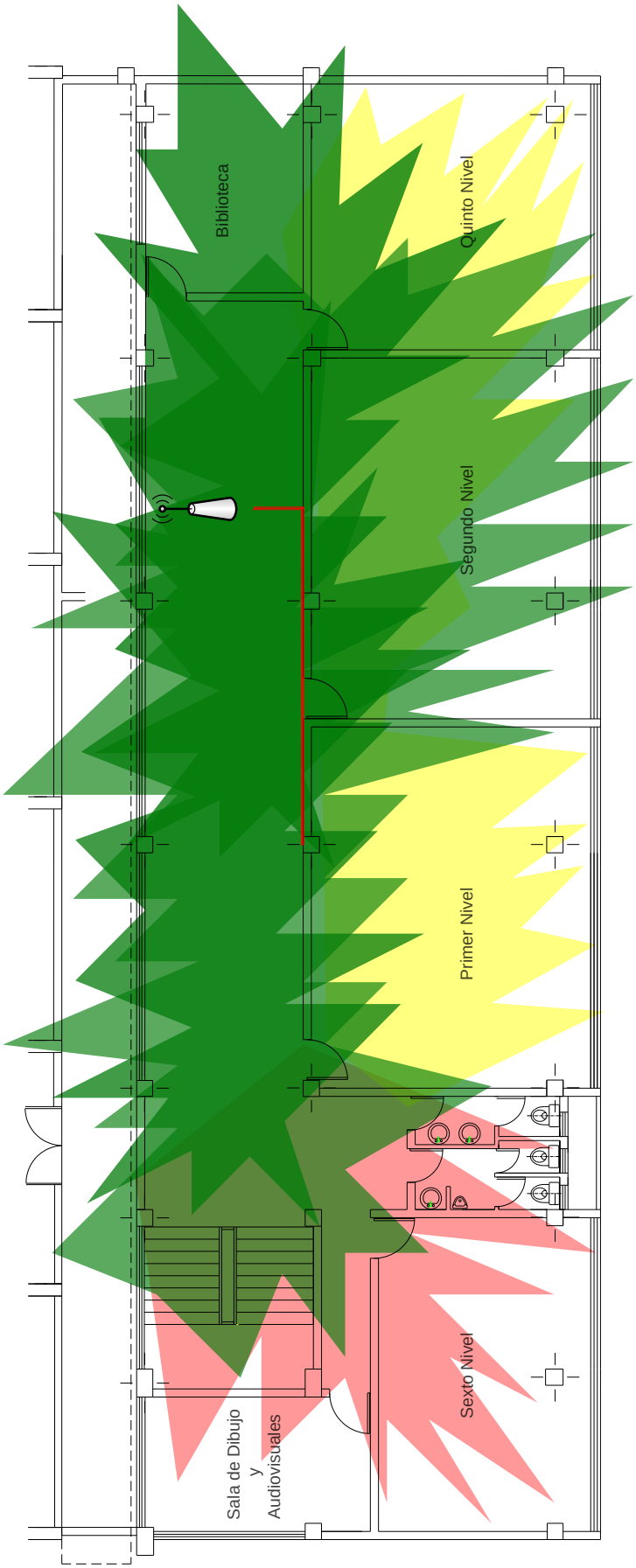


Figura. 7.45. Cobertura CAFDER_PISO1a

Figura. 7.46. Cobertura CAFDER_PISO1b

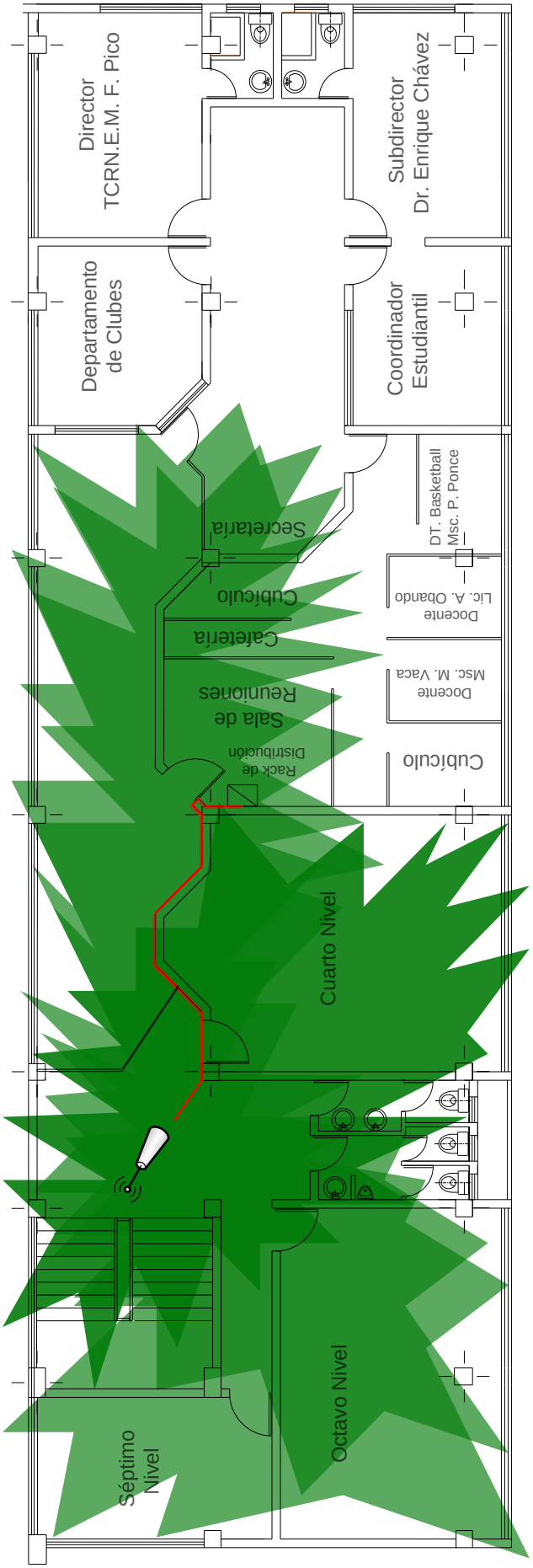


Figura. 7.47. Cobertura CAFDER_PISO2

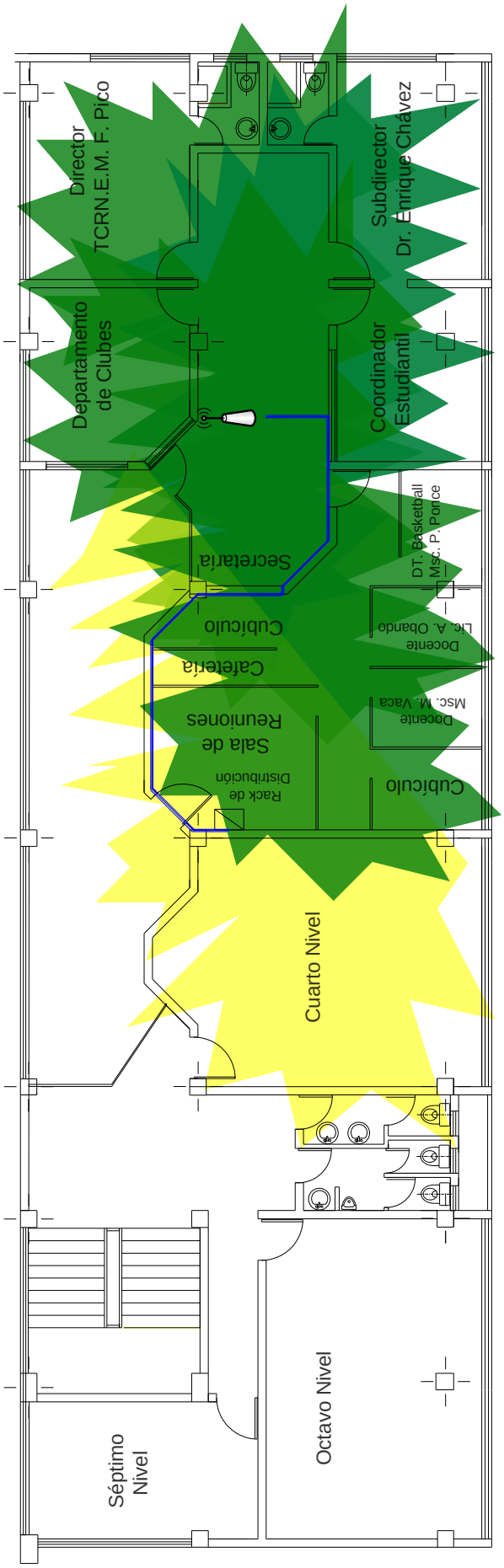


Figura. 7.48. Cobertura CAFDER_ADMIN

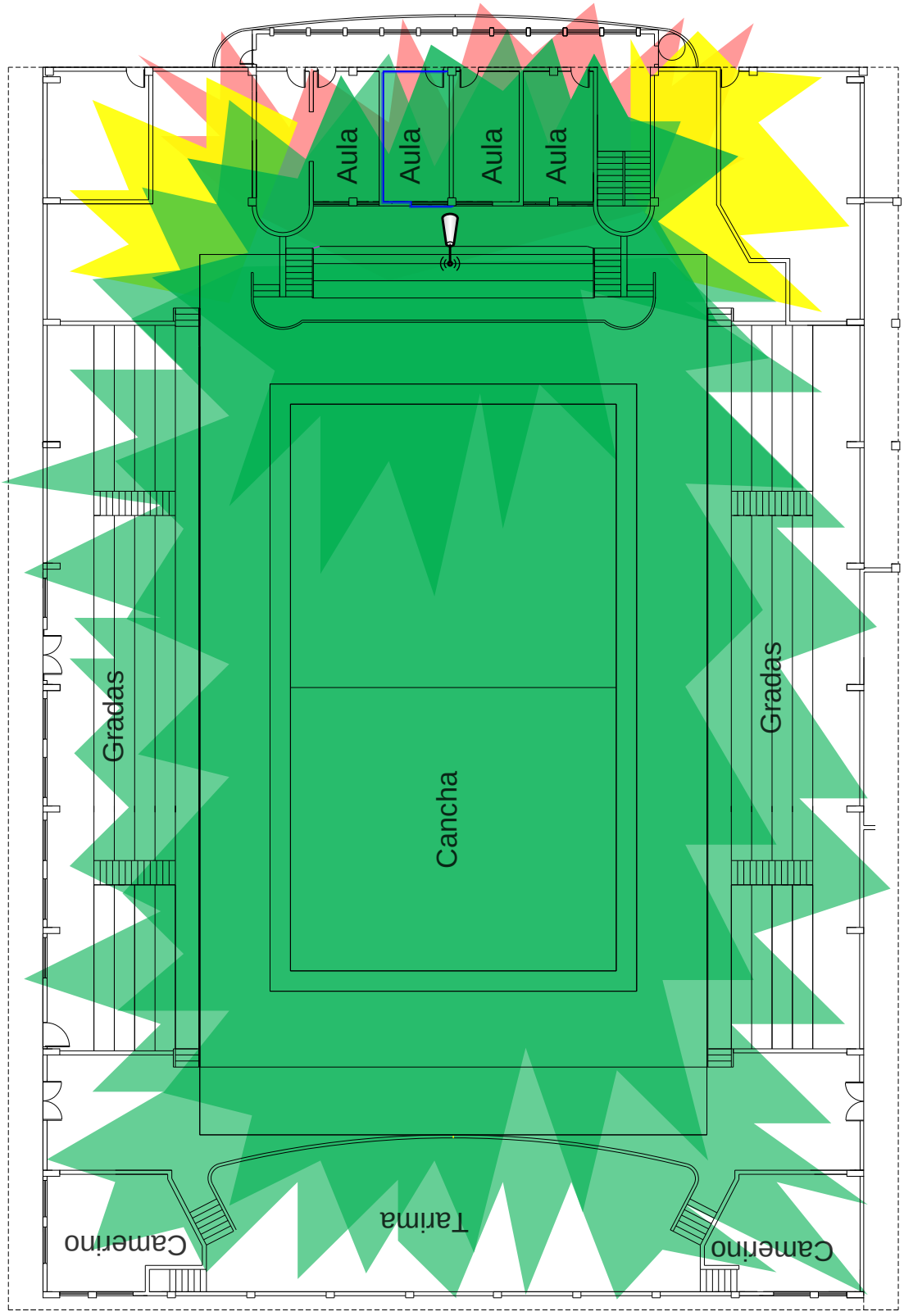


Figura. 7.49. Cobertura CAFDER_COLISEO

Figura. 7.50. Cobertura CAFDER_AULAS

BIBLIOGRAFIA

- http://www.canal-ayuda.org/a-informatica/inalambrica.htm,
- http://www.arubanetworks.com/pdf/technology/TB_11NPERF.pdf,
- http://kernel666.wordpress.com/2007/04/26/posibles-efectos-negativos-de-las-redes-
- http://es.wikipedia.org/wiki/IEEE_802.11,
- www.pcone.com.mx/images/TARJETA_DE_RED,
- http://bcognizance.iiita.ac.in/jan-mar07/t5_files/image003.jpg
- http:// www.canal-ayuda.org/a-informatica/inalambrica.htm
- www.canal-ayuda.org/a-informatica/inalambrica.htm
- www.canal-ayuda.org/a-informatica/inalambrica.htm
- http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/532/8/T10464CAP2.
- http://www.sunrisetelecom.com/products/mtt.php
- http://www.sunrisetelecom.com/products/mtt.php
- http://standards.ieee.org/getieee802/download/802.11-1999pdf 59- 68 pp
- http://www.faqs.org/rfcs/rfc2058.html
- http:// www.iec.org/online/tutorials/ acrobat/eap_methods.pdf
- http://www.faqs.org/rfcs/rfc2058.html
- www.cisco.com
- www.rsa.com
- http:// www.stargeek.com/item/20270.html
- http://www.weca.net

- ✓ www.linksysbycisco.com/EU/es/products/WRT54G
- ✓ www.3com.com/prod/es_LA_AMER/detail.jsp?tab=features&sku=3CWXM10
- ✓ *http://localhost/daloradius*
- ✓ www.flukenetworks.com/fnet/es-es/products/LinkWare/Overview
- ✓ www.passmark.com/products/wirelessmonitor.htm

Sangolquí ___ de Julio del 2010

_____

Ing. Gonzalo Olmedo, PH.D

Director de la Carrera

Ingeniería Electrónica en Telecomunicaciones

_____ _____

Sr. Héctor Ananganó

Autor

Sr. Cristian Arce

Autor