ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

"DISEÑO E IMPLEMENTACIÓN DE UN RADIOENLACE PARA LA TRANSMISIÓN DE DATOS UTILIZANDO MODULACIÓN DIGITAL DE BANDA ANCHA CON EQUIPOS NANOSTATION5"

TESIS DE GRADO

Previa la obtención del título de

INGENIERO EN ELECTRÓNICA Y COMPUTACIÓN

Presentado por:

JUAN PABLO NARANJO ROJAS

RIOBAMBA – ECUADOR
2010

AGRADECIMIENTO

A los Ingenieros Edwin Altamirano y José Guerra, por ser excelentes docentes y gran amigos.

A mi hermano Jorge por apoyarme en la implementación de mi tesis y a su familia por motivarme a seguir mi camino.

A mi Viejito y a mi Madrecita querida, gracias a su apoyo económico y moral, logré cumplir mi Sueño esperando que se sientan orgullosos de mi Triunfo.

A mis hermanitos Piruky, Pimpo y Pinta, mi esposa y mi pequeñita, para ustedes mi esfuerzo.

DEDICATORIA

A mi Virgencita del Cisne, por darme valor, seguridad y la fuerza necesaria para cumplir mi Sueño, ya que nunca me dejó desmayar frente a las adversidades que se me presentaron.

A mis hermanos, a mi Viejito Lindo y a mi Madrecita Querida, porque estuvieron apoyándome incondicionalmente.

A mi esposa Gabriela y a mi pequeñita linda, gracias por formar parte de mi vida.

NOMBRE	FIRMA	FECHA
Dr. Iván Menes **DECANO FACULTAD DE** **INFORMÁTICA Y ELECTRÓNICA**	_____	_____
Ing. José Guerra **DIRECTOR DE ESCUELA** **INGENIERÍA ELECTRÓNICA**	_____	_____
Ing. Edwin Altamirano **DIRECTOR DE TESIS**	_____	_____
Ing. José Guerra **MIEMBRO DEL TRIBUNAL**	_____	_____
Lcdo. Carlos Rodríguez **DIR. DPTO.** **DOCUMENTACIÓN**	_____	_____

NOTA DE LA TESIS _____

"Yo, Juan Pablo Naranjo Rojas, soy responsable de las ideas, doctrinas y resultados expuestos en esta Tesis de Grado; y, el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO".

Juan Pablo Naranjo Rojas

ÍNDICE DE ABREVIATURAS

AAP Adaptive Antenna Polarity (Polaridad de antena adaptable)

ACL Access Control List (Lista de Control de Acceso)

ACK Acknowledgement (Acuse de recibo)

AES Advanced Encryption Standar (Encriptación Estándar Avanzada)

AP Access Point (Punto de acceso)

AS Servidor de Autenticación

CCMP Counter Mode with CBC-Mac Protocol (modo contador con protocol CBC-Mac)

CPE Customer Premise Equipment (Equipo local del cliente)

CNAC Closed Network Access Control (Red cerrada de control de acceso)

CONATEL Consejo Nacional de Telecomunicaciones

DHCP Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica)

DNS Domain Name System (Sistema de Nombres de Dominio)

DPSK Differential Phase Shift Keying (Manipulación por cambio de fase diferenciada)

EAP Extensible Authentication Protocol (Protocolo de Autentificación Extensible)

EAP-TLS Extensible Authentication Protocol with Transport Layer Security (Protocolo de Autenticación Extensible con Seguridad en el Transporte Capa)

EAP-TTLS EAP with Tunneled Transport Layer Security (EAP con Túnel Seguridad en el Transporte Capa)

EWMA Exponential Weighted Moving Average (Media móvil exponencial ponderado)

FTP File Transfer Protocol (Protocolo de transferencia de archivos)

GPS Global Positioning System (Sistema de Posicionamiento Global)

IDS Sistemas Detectores de Intrusos

IEEE Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y Electrónicos).

IP Internet Protocol (Protocolo de Internet)

IrDa Infrared Data Association (Asociación de datos por infrarrojos)

IV Vector de Inicialización

LEAP Lightweigh EAP

LED Light Emitting Diode (Diodo Emisor de Luz)

MAC Media Access Control

MIC Código de integración de mensajes

NIC Network Interface Card (Interfaz controladora de red)

NTP Network Time Protocol (Protocolo de red Tiempo)

OSA Open System Authentication (Sistema de Autenticación Abierto)

OUI Identificador Único Organizacional

P2MP Point to multipoint (Punto a multipunto)

PEAP Protected Extensible Authentication Protocol

POE Power Over Ethernet (Poder sobre la Red)

PPPoE Protocol Point to Point over Ethernet (Protocolo Punto a Punto sobre Ethernet)

PSK Phase Shift Keying (Manipulación por cambio de fase)

QoS Quality of Service (Calidad de Servicio)

QPSK Quadrature Phase Shift Keying (Manipulación por cambio de fase en cuadratura)

RF Radio Frecuencia

RP-SMA Reverse Polarity – SubMiniature Version A (Polaridad invertida - Versión Sub Miniatura)

RSSI Receive Signal Strength Indication (Indicador de fuerza de señal de recepción)

RTS/CTS Request To Send/Clear To Send (Solicitud de envío/Listo para enviar)

Rx Recepción

SAI Sistemas de Alimentación Ininterrumpida

SENATEL Secretaría Nacional de Telecomunicaciones

SNMP Simple Network Management Protocol (Protocolo Simple de Administración de Red)

SNR Relación señal ruido

SSID Server Set ID (Identificación de conjunto de servidor)

STP Spanning Tree Protocol

TKIP Temporal Key Integrity Protocol (Protocolo de Integridad de Clave Temporal)

TSC TKIP Sequence Counter (TKIP contador de secuencia)

Tx Transmisión

ULA Upper Layer Protocol (Protocolo de capa superior)

VoIP Voice over IP (Voz sobre IP)

WAP Wireless Access Point (Punto de Acceso Inalámbrico)

WDS Wireless Distribution System (Sistema de Distribución Inalámbrico)

WEP Wired Equivalent Privacy (Privacidad Equivalente al Cableado)

WIMAX Worldwide Interoperability for Microwave Access (Interoperabilidad Mundial para el acceso por microondas)

WISP Wireless Internet Service Providers (Proveedores de Servicio de Internet Inalámbrico)

WNIC Wireless Network Interface Card (Tarjeta de interfaz de red inalámbrica)

ÍNDICE GENERAL

CAPITULO III: SISTEMAS DE MODULACIÓN DIGITAL DE BANDA ANCHA

CAPÍTULO IV: SEGURIDAD EN REDES INALÁMBRICAS

CAPITULO V: EQUIPOS NANOSTATION

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Uno de los avances más representativos en los últimos años en el panorama de las TI (Tecnologías Informáticas) son las redes inalámbricas, pues no sólo liberó a millones de usuarios permitiéndoles un nuevo grado de productividad, sino que también inauguró oficialmente la tecnología.

La razón por la que nos vemos inmersos en el nuevo mundo de la tecnología es cada vez más indispensable, pensar en crear equipos que tengan el mismo funcionamiento o mejoras pero cada vez en tamaños más pequeños, es ahí donde aparece la nanotecnología.

Si nos remontamos a la primera era de la computadora cuando se usó los tubos de vacío y actualmente conocemos las computadoras portátiles, pda, palms, celulares, ya queda demostrado de qué forma hemos avanzando y que nos espera a futuro.

Asimismo en la forma que han evolucionado nuestros aparatos electrónicos, también hay un paso importante en las futuras tecnologías de redes, es por ello que el presente diseño e implementación es factible con el uso de las nuevas tecnologías como es la utilización de Equipos NanoStation5 en redes inalámbricas.

Debido a que nuestro mundo tecnológico crece diariamente, y por ende el mundo de las telecomunicaciones avanza, nos vemos en la necesidad de usar tecnologías cada vez más nuevas, es por ello que surge la necesidad de presentar un Diseño e Implementación de un radioenlace para la transmisión de datos utilizando modulación digital de banda ancha con Equipos NanoStation5.

Con la única finalidad de estudiar si a futuro es factible que esta tecnología sea el nuevo estándar de las telecomunicaciones, cómo influyen o cuan ventajoso resulta para empresas que transmiten información, empresas proveedoras de internet o cualquier empresa que pretenda usar este tipo de tecnología.

Este diseño e implementación ayudará a analizar de una manera técnica las especificaciones y ventajas de los Equipos NanoStation5, comprobar su confiabilidad y velocidad en la transmisión de datos de una forma segura, sus frecuencias de operación, interferencias que se presentan y su área de cobertura.

CAPITULO I

NANOTECNOLOGÍA

La palabra "**nanotecnología**" es usada extensivamente para definir las ciencias y técnicas que se aplican a un nivel de nanoescala, esto es unas medidas extremadamente pequeñas "nanos" que permiten trabajar y manipular las estructuras moleculares y sus átomos. En síntesis nos llevaría a la posibilidad de fabricar materiales y máquinas a partir del reordenamiento de átomos y moléculas. El desarrollo de esta disciplina se produce a partir de las propuestas de Richard Feynman.

La mejor definición de Nanotecnología es: el estudio, diseño, creación, síntesis, manipulación y aplicación de materiales, aparatos y sistemas funcionales a

través del control de la materia a nano escala, y la explotación de fenómenos y propiedades de la materia a nano escala.

Cuando se manipula la materia a la escala tan minúscula de átomos y moléculas, demuestra fenómenos y propiedades totalmente nuevas. Por lo tanto, científicos utilizan la nanotecnología para crear materiales, aparatos y sistemas novedosos y poco costosos con propiedades únicas.

1.1 TECNOLOGÍA NANOSTATION

Su nombre hace referencia a "Estación Pequeña", en sí es la tecnología encargada de crear dispositivos los cuales estén diseñados para la transmisión y recepción de información, y a su vez promover la industria mundial de la ISP inalámbrico al siguiente nivel.

Con un diseño compacto para interiores y exteriores y una interfaz tan intuitiva, incluso personas con pocos conocimientos podrán instantáneamente convertirse en expertos.

1.2 ARQUITECTURA DE DISEÑO

La arquitectura de diseño del NanoStation fue desarrollada en base a los requerimientos de la comunidad WISP (Wireless Internet Service

Providers). Cada aspecto del diseño del producto, desde los tornillos y tuercas, al sistema, hardware de radio y la antena fueron 100% desarrollados a partir de cero en base a las propuestas y sugerencias de los operadores WISP.

El NanoStation tiene un fenomenal desempeño con un diseño revolucionario combinado además con un sistema de 4 antenas de alta ganancia, avanzada arquitectura de radio, y tecnología de firmware altamente investigada y desarrollada; permitiendo así estabilidad en transferencia de datos, y capacidad de desempeño que rivaliza aún con redes WiMax de última generación.

1.3 TECNOLOGÍA DE POLARIDAD DE ANTENA ADAPTATIVA

El NanoStation utiliza tecnología de Polaridad de Antena Adaptable (AAP), lo cual habilita la opción de operar en polarización fija (Vertical u Horizontal) o "conmutada adaptativamente" que es el uso de la misma antena en múltiples polaridades. Adicionalmente cuenta con un conector RP-SMA para antena externa, para casos donde pueda ser necesario un patrón de cobertura mayor o menor al incluido.

Tradicionalmente al instalar antenas en exteriores, la polarización es fijada en operación vertical u horizontal, donde cada una de ellas tiene sus ventajas y desventajas.

1.4 SOFTWARE DE PLATAFORMA ABIERTA

La noción de sistema abierto suele vincularse con los sistemas informáticos. Son aquellos sistemas que son susceptibles de portabilidad e interoperabilidad (distintos software pueden operar de manera simultánea), y que utilizan estándares abiertos. Por otra parte, el concepto puede hacer referencia a los sistemas que permiten el acceso libre y sin restricciones por parte de personas u otros sistemas.

La idea de sistema abierto en la informática se desarrolló a finales de 1970 e inicios de la década del ’80, con el avance de Unix. Este tipo de sistemas presentaba interfaces de programación e interconexiones periféricas estandarizadas, lo que promovía el desarrollo de software y hardware por parte de terceros.

Es importante distinguir entre un sistema abierto y un software de código abierto, ya que el segundo se refiere a los programas informáticos que pueden ser manipulados y modificados por los usuarios. Esta característica no implica que sean interoperables con los demás sistemas.

El acceso y promoción del estándar permite la compatibilidad e interoperabilidad entre diferentes componentes de hardware y software,

ya que sólo se requieren conocimientos técnicos para construir nuevos productos. En la figura I.1 se puede apreciar los diferentes Sistemas Operativos Abiertos con los que operan los equipos NanoStation5.

Figura I.1 Sistemas Operativos Abiertos

1.5 MODOS DE OPERACIÓN

El modo de operación depende de los requisitos de la topología de red. Los equipos NanoStation cuentan con 4 modos de funcionamiento:

- **Estación**: Éste es un modo de cliente, el cual se puede conectar con un AP (Punto de Acceso).

  Es comúnmente usado para enlazarse con un AP. En modo estación el dispositivo actúa como la estación del suscriptor (CPE) mientras que se conecta con el punto de acceso primario definido por el SSID y re-direcciona todo el tráfico entrante y saliente de la red a los dispositivos conectados en la interfaz Ethernet.

- **Estación WDS**: WDS representa sistema de distribución inalámbrica. El modo Estación WDS debe ser utilizado mientras que se conecta con el punto de acceso que está funcionando en modo WDS.

  Este modo permite re-direccionar los paquetes en el nivel de la capa 2.

- **Access Point:** Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

- **Access Point WDS:** Éste es un punto de acceso 802.11 que permite a la capa 2 hacer un puente con equipos que trabajen en modo WDS usando el protocolo WDS.

  WDS le permite hacer un puente de tráfico inalámbrico entre dispositivos que operan en modo punto de acceso. El punto de acceso generalmente está conectado con una red alámbrica (LAN Ethernet) que permite la conexión inalámbrica con la red alámbrica.

Conectando los puntos de acceso uno con otro usando un determinado servicio extendido WDS, Ethernet(s) distantes se pueden unir en una sola LAN.

1.6 NANOSTATION Y NANOLOCO

La diferencia entre NanoStation y NanoLoco se inicia en el tamaño (Fig. I.2) Nanoloco es 30% más pequeño que Nanostation.

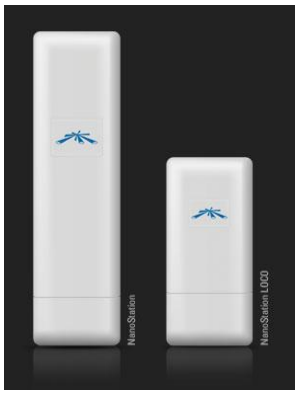

Figura I.2 NanoStation y NanoLoco

Antes de precisar las diferencias es bueno saber las semejanzas. NanoStation y NanoLoco tienen la misma velocidad en su chipset (180 MHz) y la misma cantidad de memoria (4Mb, 16 Mb). Ambos productos son CPE, es decir, antena, tarjeta y caja intemperie integrado en un sólo artículo. Tanto NanoStation como NanoLoco funcionan con PoE lo cual da comodidad al usuario pues solo se necesita cable de red UTP. Ambos artículos son operados con el mismo firmware.

Las diferencias específicas se encuentran en la potencia emitida en cada equipo. Nanostation emite 26 dBm, esto es, 400 mW. Por su parte, Nanoloco tan solo emite 100 mW. Otra diferencia es la ganancia de la antena integrada en los equipos: Nanostation posee una antena de 10 dBi. Nanoloco presenta una antena de tan solo 8 dBi. Conviene saber también que a diferencia de la NanoStation, la nanoloco no tiene conector para antena externa.

En síntesis, la menor potencia, la menor ganancia y la imposibilidad de agregar una antena externa convierte a Nanoloco en un artículo de menor posibilidad que Nanostation y en consecuencia de menor costo. Por lo tanto, adquirir la una o la otra no debe depender de cuál es más económica sino de cuál satisface la necesidad.

1.7 PODER SOBRE LA RED (POE)

Cada vez son más dispositivos electrónicos para el hogar y empresa digital (pasarela residencial, puntos de acceso WiFi, teléfono IP, switches, etc.) que implementan el estándar PoE (*Power over Ethernet*).

Figura I.3 PoE (Power Over Ethernet)

Esta tecnología permite que la alimentación eléctrica sea suministrada al dispositivo de red usando el mismo cable que se utiliza para la conexión de red. De este modo, se reduce la cantidad de cables facilitando la instalación y ahorrando espacio y se elimina la necesidad de que todos los dispositivos se encuentren cerca de un enchufe.

También facilita la conexión a los sistemas de alimentación ininterrumpida (SAI) para garantizar el funcionamiento permanente, incluso por cortes temporales de la corriente eléctrica.

El estándar 802.3at o PoEP (Power over Ethernet Plus), aún en desarrollo, ofrece a los dispositivos de red un volumen de energía alrededor del doble que su antecesor 802.3af. PoEP, al ser compatible con PoE, permite que los dispositivos puedan operar en baja potencia. El objetivo de 802.3at es que pueda llegar a suministrar hasta 50W por dispositivo, tasa suficiente para soportar cámaras IP monitorizadas o puntos de acceso duales WiFi 802.11n, que necesitan más energía que los que ofrecía PoE. De momento 802.3at duplica los 15,4W que proporciona 802.3af (sólo unos 12,95W están disponibles debido a las pérdidas del cable).

PoE no hace disminuir el rendimiento de la comunicación de datos en la red o reducir el alcance de la red.

La corriente suministrada a través del cable Ethernet se activa de forma automática cuando se identifica un terminal compatible y se bloquea ante dispositivos que no sean compatibles.

Las desventajas de PoE es que los dispositivos que lo soportan son un poco más caros que el resto, si bien los precios irán bajando a medida que se estandarice. También se han detectado ciertos problemas de interoperabilidad y de calentamiento, por lo que probablemente el nuevo estándar 802.at transporte la corriente por los cuatro cables de par trenzado de Ethernet en vez de por dos. El IEEE estudia también posibles interferencias entre la electricidad de alta potencia y las señales de datos.

1.7.1 Características Generales

PoE se rige bajo las normas del estándar IEEE 802.3af. Dicho estándar se encarga de definir todo lo necesario para poder usar esta tecnología, esto es, los voltajes y las corrientes necesarias para su uso, el tipo de conexión que se debe realizar, los cables que se deben usar.

La figura I.4, muestra las fases que debe realizar un PoE para poder alimentar usando un cable. Estas fases son 4, y cada una se corresponde con un bloque:

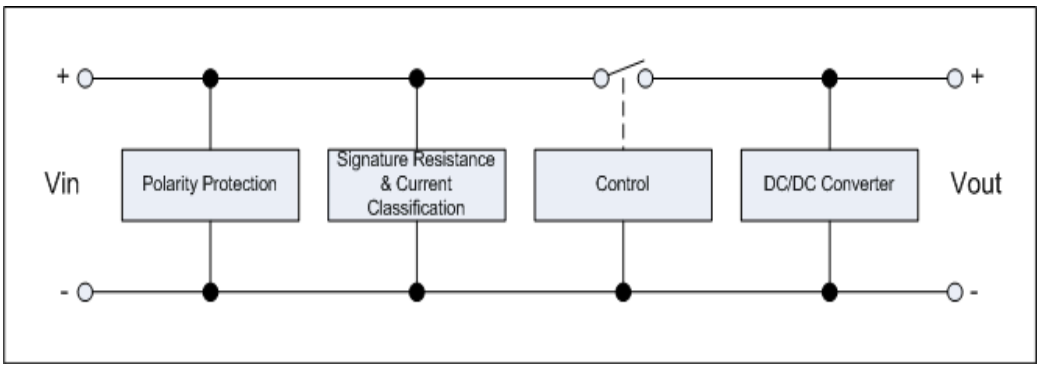

Figura I.4 Fases de un Poe

- **Primer Bloque: "Protección de Polaridad" o "Circuito de Auto-Polaridad"**. Como indica la norma, el voltaje introducido puede venir de dos formas posibles: una de las formas consiste en usar los cables de datos del cable de Ethernet como fuente de alimentación. Dicha forma permite transmitir datos y alimentar a la vez. La segunda forma usa otros cables alternativos para enviar la tensión. La ventaja de la primera forma es que usa 2 cables, en vez de 4, que son los necesarios para implementar la segunda forma.

- **Segundo Bloque: "Firma y Circuitos de Clase".** Para asegurarse que el dispositivo no aplica una tensión a un dispositivo que no implementa PoE, el dispositivo empezará a dar unos determinados niveles de tensión. Estos niveles de tensión se dividen en 4 etapas. Al principio el dispositivo aplicará una tensión baja (2.7V a 10.1V) buscando una resistencia de 25KΩ.

Si es demasiado alta o demasiado baja, no hará nada. Esta fase permite proteger un dispositivo que no es PoE de uno que sí lo es. En caso de que resulte ser PoE, buscará que clase de alimentación requiere. Para ello, elevará la alimentación entre 14,5-20,5V y medirá la corriente que circula a través de él. Dependiendo del resultado obtenido, el dispositivo sabrá cual es la máxima alimentación permitida para que trabaje el dispositivo PoE. A continuación, se adjuntan unas tablas que permiten ver esto de forma más clara.

Tabla I-1 Etapas de los niveles de tensión

Fase	Acción	Voltios especificados por 802.3af	Volts usados por el chipset (LM5071)
Detección	Comprueba si el dispositivo conectado tiene una resistencia comprendida entre 15 – 33 KΩ	2.7-10.0	1.8–10.0
Clasificación	Comprueba a que clase pertenece el dispositivo (ver tabla siguiente)	14.5-20.5	12.5–25.0
Inicio	Empieza a alimentar al dispositivo	>42	>38 (LM5072)
Operación Normal	Alimenta al dispositivo	36-57	25.0–60.0

Tabla I-2 Clasificación del dispositivo

Clase	Modo de uso	Niveles máximos para alimentar el dispositivo
0	Default	0.44 a 12.94
1	Optional	0.44 a 3.84
2	Optional	3.84 a 6.49
3	Optional	6.49 a 12.95
4	Reserved	(PSEs classify as Class 0)

- **Tercer bloque: "Etapa de Control".** Es importante que el convertidor Dc/Dc no funcione mientras el dispositivo está realizando la fase de clasificación del bloque dos. El controlador deberá estar encendido cuando V = 35V.

- **Cuarto bloque: "Convertidor DC/DC"**. Generalmente la tensión nominal usada es de 48V y no suele ser práctica en muchas aplicaciones, dónde se requiere un voltaje menor (3.3V, 5V o 12V). Una manera muy efectiva de lograr este objetivo es usar un convertidor Buck DC/DC. Este convertidor es capaz de trabajar en un amplio rango de tensiones (36V a 57V), en condiciones de mínima y máxima carga.

  Después de explicar esto, debemos conocer cuál es la máxima potencia que puede entregar. Aunque ya se mencionó algo en la fase 2, creemos que es muy recomendable explicar esto. La máxima potencia que puede dar la fuente de alimentación es de 15.4W (400mA a 48V o 350mA a 44V)[La norma no deja muy clara estas últimas medidas]. Si contamos las pérdidas, entonces la potencia máxima será de 12.95W (350mA a 37V). En muchos casos esta cifra también se queda algo corta, pues, supone que el convertidor DC/DC tiene eficiencia máxima.

Al final, la potencia será un valor comprendido entre 12.95 – 10.36 W (el último valor será el peor caso posible).

CAPITULO II

ANTENA GRILLA PARABÓLICA

Una antena es un dispositivo diseñado con el objetivo de emitir o recibir ondas electromagnéticas hacia el espacio libre. Una antena transmisora transforma voltajes en ondas electromagnéticas, y una receptora realiza la función inversa.

Existe una gran diversidad de tipos de antenas, dependiendo del uso al que van a ser destinadas. En unos casos deben expandir en lo posible la potencia radiada, es decir, no deben ser directivas (ejemplo: una emisora de radio comercial o una estación base de teléfonos móviles), otras veces deben serlo

para canalizar la potencia en una dirección y no interferir a otros servicios (antenas entre estaciones de radioenlaces). También es una antena la que está integrada en la computadora portátil para conectarse a las redes Wi-Fi.

Las características de las antenas dependen de la relación entre sus dimensiones y la longitud de onda de la señal de radiofrecuencia transmitida o recibida.

Si las dimensiones de la antena son mucho más pequeñas que la longitud de onda las antenas se denominan elementales, si tienen dimensiones del orden de media longitud de onda se llaman resonantes, y si su tamaño es mucho mayor que la longitud de onda son directivas.

2.1 DISEÑO DE LA ANTENA

La antena grilla es una variación de la antena parabólica, su diferencia fundamental radica en que aunque su contorno es parabólico, el reflector no es un plato, sino un arreglo de varillas horizontales y perpendiculares como indica la figura II.5.

En el siguiente diseño, se consideran los mismos parámetros de geometría considerados en la parábola.

Figura II. 5 Antena Grilla Parabólica

Datos:

$$F = 5.8GHz$$

$$n = 10$$

Relación $\frac{D}{f} = 2.7$

$$\lambda = 0.0517m$$

$$D = 2.5f = 0.35m$$

$$2.7 * \lambda = 0.13959$$

$$\rho = 0.2$$

La profundidad del reflector desde el vértice de la parábola hasta el punto de intersección entre las rectas comprendidas por el eje focal y la línea que une los extremos de la parábola es:

$$z_0 = \frac{D^2}{16f} = \frac{0.348^2}{16 * 0.13959} = 0.058$$

La separación entre varillas es:

$$y * \lambda = 0.01$$

$$y * 0.0517 = 0.01$$

$$y = 0.19$$

En el diseño se consideran dos parábolas transversales como lo indica la figura II.6 y II.7, que se utilizan como guía, luego haciendo operaciones de simetría y matriz se obtienen las figuras II.8 y II.9.

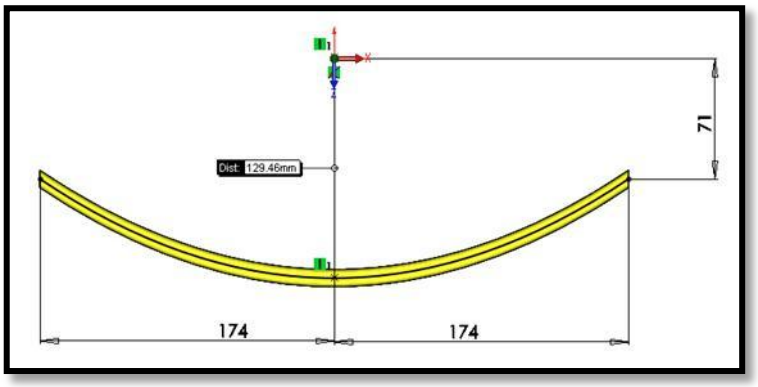

Figura II.6 Sección horizontal

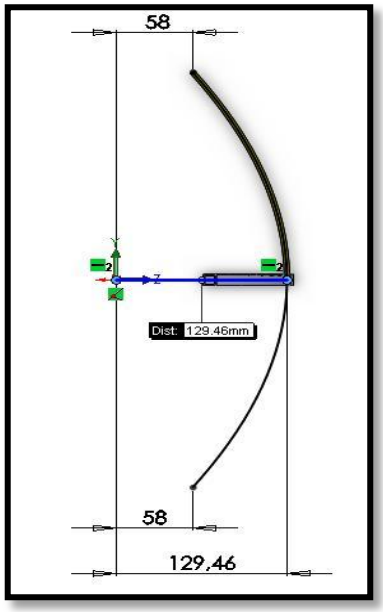

Figura II.7 Sección vertical.

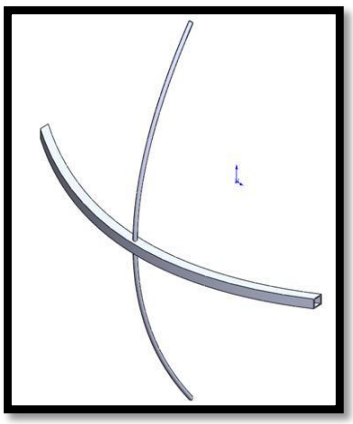

Figura II.8 Ejes guías transversales.

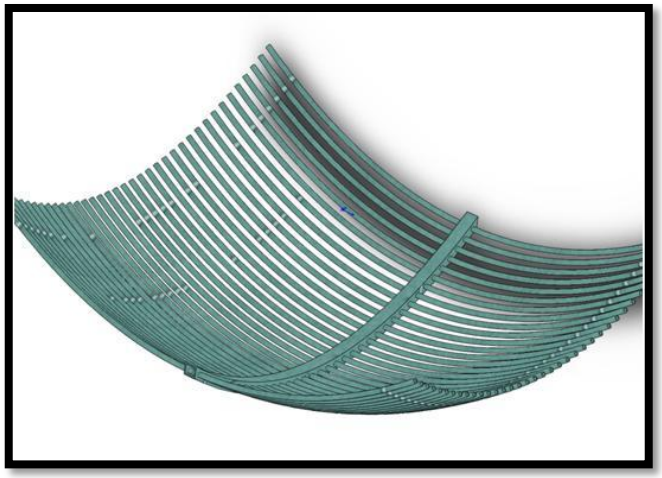

Figura II.9 Operaciones de matriz para antena grilla.

Resultados del Diseño:

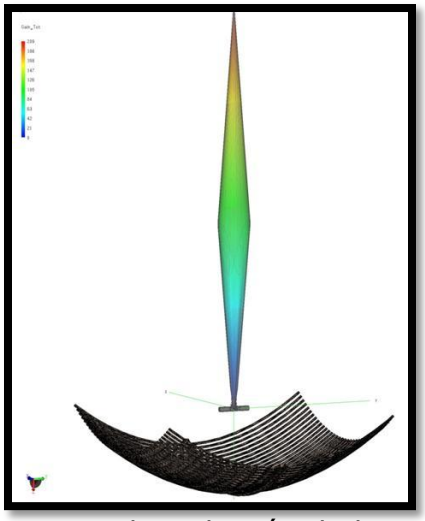

Figura II.10 Diagrama de radiación de la antena Grilla.

2.2 ESPECIFICACIONES TÉCNICAS

La antena WIFI grilla 24 dbi 2.4GHz direccional 8º puede ser instalada en polarización horizontal o vertical.

- Durable a prueba de mal tiempo
- La antena tiene un kit de montaje para girar e inclinar a 60 grados (Figura II.11). Esto permite instalaciones a varios grados de inclinación para un fácil alineamiento.

Figura II.11 Montaje de giro

2.2.1 Especificaciones Eléctricas

Frecuencia	2.4 - 2.5 GHZ
Ganancia	24 dBi
-3 dBi Ancho de onda	8 grados
Respuesta polarización cruzada	26 dBi

Relación Frente Retorno	24 dB
Sidelobe	-20dB Max
Impedancia	50 Ohm
Maxima Potencia de entrada	50 Watts
VSWR	< 1.5:1 avg.

2.2.2 Especificaciones Mecánicas

Peso	4.8 lbs. (2.18 kg)
Dimensiones, rejilla	39.5 in (100 cm) x 23.5 in (60 cm)
Montaje	2 in. (50.8 mm) max. diámetro mástil
Angulo de elevación	0 to +10 grados
Temperatura de operación	-40° C to 85° C (-40° F to 185° F)

2.2.3 Patrones de ganancia RF de la Antena

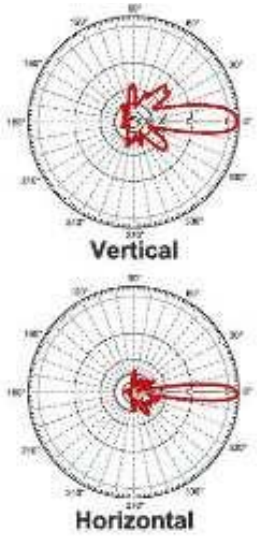

Figura II.12 Patrones de ganancia

2.3 APLICACIONES

- Enlazar oficinas y negocios inalámbricamente sin necesidad de cables ni contrato de enlaces.

- Compartir Internet, reducir costos (cabinas, oficinas, condominios, universidades).

- Interconectar sucursales y oficinas de empresas públicas y privadas.

- Conectarse a Hotspots Libres.

- Proveer servicios de Internet inalámbrico (ISP inalámbrico)

- Aumentar la Calidad de Recepción

- Implementar Telefonía por IP (VOIP).

- Vigilancia y monitoreo remoto con cámaras IP.

- Especialmente diseñada para captura y recepción de señales WiFi débiles y lejanas de hasta 15km.

- Antena para Conectar Directo a Routers, Access Points o Tarjetas Inalámbricas.

2.4 VENTAJAS Y DESVENTAJAS

Ventajas

- Performance superior 24 dBi.
- Conexiones Inalámbricas de hasta 15 kilómetros de distancia.
- Opera en todo tipo de clima.
- Amplitud de onda 8°
- Ideal para aplicaciones punto a punto, multipunto de largo alcance.
- Fácil de armar.
- Compatible con todas las marcas de Access Point 802.11b/g.

Desventajas

- Necesitan alimentación eléctrica.
- Ocupan mayor espacio físico.
- Incomodidad al momento de ser instaladas.
- En la actualidad están siendo reemplazas, por equipos más compactos y eficientes.

CAPITULO III

SISTEMAS DE MODULACIÓN DIGITAL DE BANDA ANCHA

Sistemas de radiocomunicaciones que utilizan técnicas de codificación o modulación digital en una anchura de banda asignada con una densidad espectral de potencia baja compatible con la utilización eficaz del espectro.

El Conatel aprobará la operación de sistemas de radiocomunicaciones que utilicen técnicas de Modulación Digital de Banda Ancha en las siguientes bandas de frecuencias:

BANDA (MHz)

902 - 928

2400 - 2483.5

5150 – 5250

5250 – 5350

5470 – 5725

5725 - 5850

3.1 REQUISITOS PARA USO DE FRECUENCIAS – PERSONAS NATURALES O JURÍDICAS

Los interesados en instalar y operar sistemas de espectro ensanchado de gran alcance, sean estos PRIVADOS o de EXPLOTACIÓN, en cualquier parte del territorio nacional, deberán presentar los siguientes requisitos:

a) Información Legal

1. Solicitud dirigida al Señor Secretario Nacional de Telecomunicaciones, indicando el tipo de Servicio al cual aplica; debe también constar el nombre y la dirección del solicitante (para personas jurídicas, de la compañía y el nombre de su representante legal).

2. Copia de la cédula de ciudadanía (para personas jurídicas, del representante legal).

3. Otros documentos que la SENATEL solicite.

b) Información Técnica

4. Estudio técnico del sistema elaborado en los formularios disponibles en la página Web del CONATEL, suscrito por un Ingeniero en Electrónica y Telecomunicaciones, con licencia profesional vigente en una de las filiales del Colegio de Ingenieros Eléctricos y Electrónicos del Ecuador (CIEEE) y registrado para tal efecto en la SENATEL.

5. Copia de la licencia profesional vigente del ingeniero que ha realizado el estudio de ingeniería correspondiente.

3.2 ENLACE PUNTO – MULTIPUNTO

Punto a multipunto de comunicación es un término que se utiliza en el ámbito de las telecomunicaciones (Figura III.13), que se refiere a la comunicación que se logra a través de un punto específico y distintos tipos de conexión multipunto, ofreciendo varias rutas desde una única ubicación a varios lugares. Una conferencia puede ser considerada una

comunicación punto a multipunto ya que existe solo un orador (transmisor) y múltiples asistentes (receptores). Punto a multipunto es a menudo abreviado como P2MP, PTMP, o PMP.

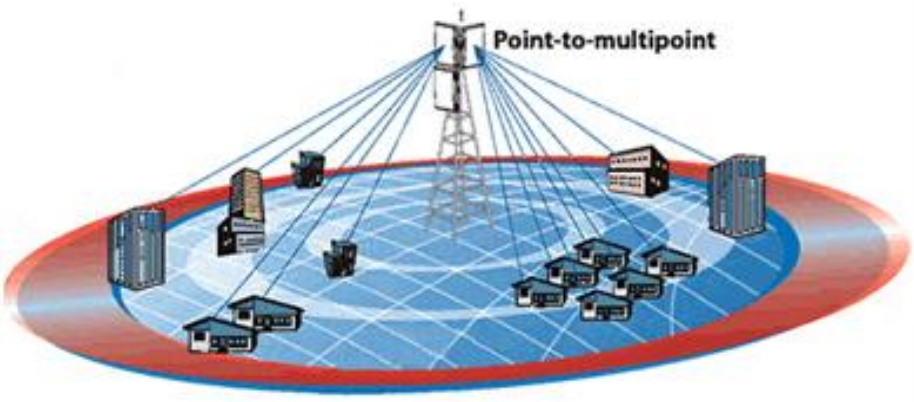

Figura III.13 Enlace Punto – Multipunto

Los enlaces punto multipunto permiten establecer áreas de cobertura de gran capacidad para enlazar diferentes puntos remotos hacia una central para implementar redes de datos voz y video.

El punto a multipunto de telecomunicaciones es el más típico utilizado en conexión inalámbrica a Internet y la telefonía IP a través de radiofrecuencias de gigahercios. Los sistemas P2MP han sido diseñados tanto como sistemas únicos como bi-direccionales. Una antena o antenas que reciben las emisiones de varias antenas y el sistema utiliza una forma de multiplexación por división en el tiempo para permitir el regreso de canales de tráfico.

Existen diferentes tipos de conexiones punto a multipunto:

- **Estrella:** Un host conectado a varias terminales remotas.

- **Bus:** Un medio de comunicación común conectado a muchas estaciones remotas.

- **Anillo:** Todas las terminales conectadas a un mismo cable. Si una falla hay problemas con todas.

- **Malla:** Es el tipo de conexión utilizado en las centrales telefónicas. Todas las terminales interconectadas entre sí.

3.3 ENLACE PUNTO – PUNTO

Punto a Punto son aquellas comunicaciones que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos nodos, en contraposición a las redes multipunto, en las cuales cada canal de datos se puede usar para comunicarse con diversos nodos.

En una red punto a punto, los dispositivos en red actúan como socios iguales, o pares entre sí. Como pares, cada dispositivo puede tomar el rol de esclavo o la función de maestro. En un momento, el dispositivo A,

por ejemplo, puede hacer una petición de un mensaje/dato del dispositivo B, y este es el que le responde enviando el mensaje/dato al dispositivo A. El dispositivo A funciona como esclavo, mientras que B funciona como maestro. Un momento después los dispositivos A y B pueden revertir los roles: B, como esclavo, hace una solicitud a A, y A, como maestro, responde a la solicitud de B. A y B permanecen en una relación reciproca o par entre ellos.

Las redes punto a punto (Figura III.14) son relativamente fáciles de instalar y operar. A medida que las redes crecen, las relaciones punto a punto se vuelven más difíciles de coordinar y operar. Su eficiencia decrece rápidamente a medida que la cantidad de dispositivos en la red aumenta.

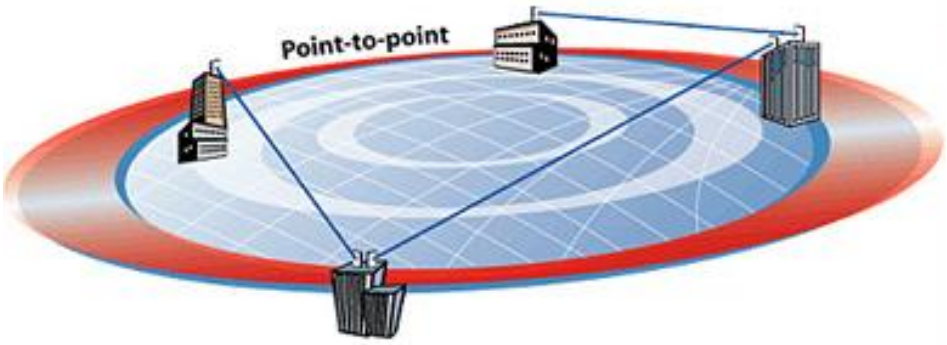

Figura III.14 Enlace Punto - Punto

Los enlaces punto a punto, son enlaces dedicados para empresas que están implementando conectar remotamente puntos en otras zonas.

Este tipo de soluciones proveen al cliente una alta capacidad de ancho de banda, eficiencia, y calidad de servicio asegurada.

Los enlaces que interconectan los nodos de una red punto a punto se pueden clasificar en tres tipos según el sentido de las comunicaciones que transportan:

Simplex.- La comunicación sólo se efectúa en un solo sentido.

Half-dúplex.- La comunicación se realiza en ambos sentidos, pero de forma alternativa, es decir solo uno puede transmitir en un momento dado, no pudiendo transmitir los dos al mismo tiempo.

Full-Dúplex.- La comunicación se puede llevar a cabo en ambos sentidos simultáneamente.

3.4 MODULACIÓN DIGITAL EN BANDA ANCHA

Una de las técnicas empleadas para ello, es la denominada Banda Ancha, que resulta ser la más utilizada actualmente en Transmisión de Datos. En Banda Ancha de lo que se trata esencialmente es de efectuar una transformación de la señal digital en una analógica, mediante técnicas de Modulación.

El concepto de modulación se basa en poder controlar la variación de alguno de los parámetros (amplitud, frecuencia, fase) de una señal, denominada portadora.

Ahora bien, el control de la variación antes mencionado, se puede hacer con arreglo a otra señal, que denominaremos moduladora, por dar forma a la variación del parámetro de la portadora, de esta forma, las variaciones de la señal moduladora, se recogen como variaciones de alguno de los parámetros de la señal modulada.

Se suele calificar una determinada modulación, en función de su señal moduladora, de modo que si ésta es analógica, la modulación también lo será y si la moduladora es digital, entonces, la modulación la adjetivaremos como modulación Digital.

3.4.1 Modulación de Amplitud (ASK)

Esta técnica consiste en hacer variar la amplitud de la portadora en función de la moduladora. Sabemos que la moduladora son impulsos que representan los datos y es en función de estos impulsos, cómo habrá de variar la amplitud de la portadora. En la figura III.15, se representa el esquema genérico de la modulación de amplitud.

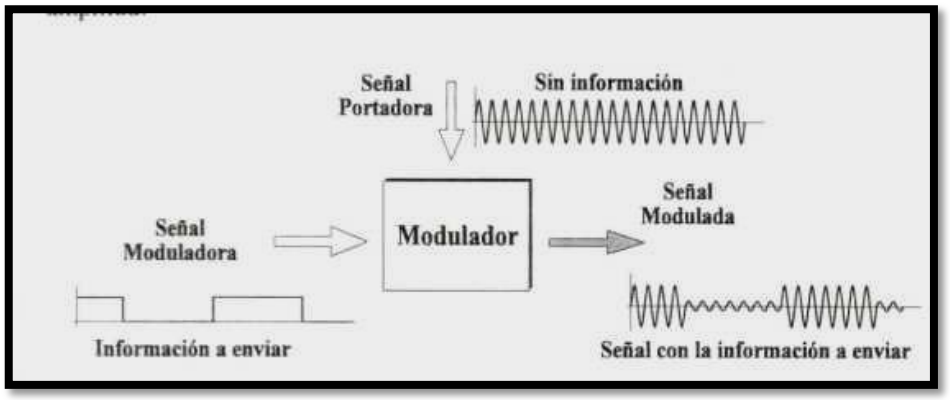

Figura III.15 Esquema de modulación en Amplitud.

La frecuencia de la portadora, que no lleva ningún tipo de información, permanecerá constante e influirá en otras características de la transmisión como es la velocidad, etc.

La primera y más simple modulación de este tipo sería asignar la presencia de señal portadora con un nivel fijo, al bit "1" y la ausencia de portadora al bit "0", esto último se denomina "portadora de nivel cero", figura III.16.

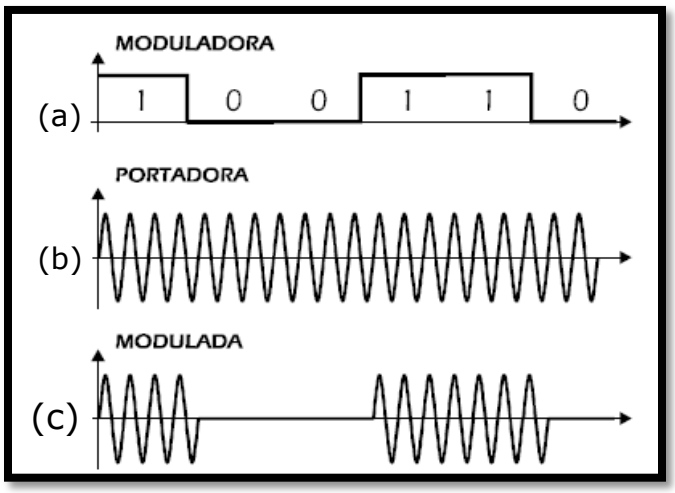

Figura III.16 Modulación de amplitud con ausencia de portadora:
(a)Señal de Datos o Moduladora, (b) Señal Portadora, (c) Señal Modulada.

Como es fácil de comprender, este método ofrece pocas posibilidades de resultar indemne a las perturbaciones más leves del sistema de transmisión, por lo que se tiende a otros tipos de modulación de amplitud.

El uso de cualquier tipo de modulación de amplitud exclusivamente, es decir sin combinar con otros métodos, no es aconsejable para la Transmisión de Datos y aún, cuando para altas velocidades este método suele ser utilizado, se tiende a las modulaciones de frecuencia o fase. No obstante, para documentar este tipo de modulación, podemos decir que otro sistema de llevarlo a cabo es asignar distintos niveles de una señal sinusoidal a los estados de los bits, tal como se muestra en la figura III.17.

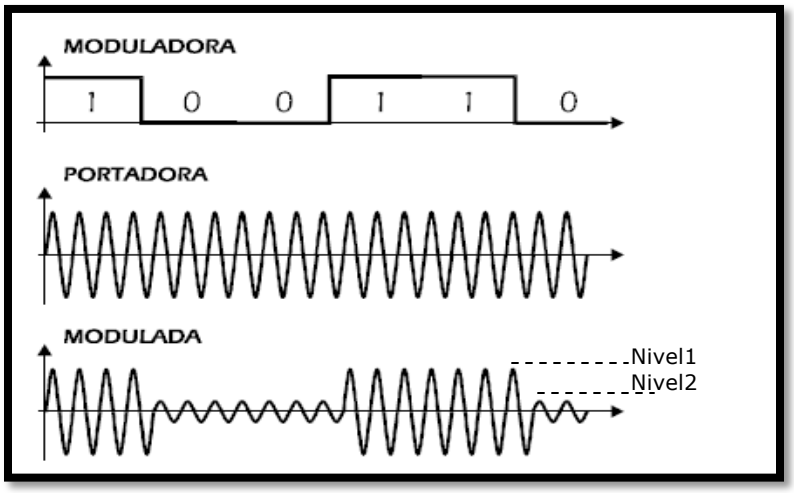

Figura III.17 Modulación de amplitud con diferentes niveles

(a) Señal de Datos ó Moduladora, (b) Señal Portadora, (c) Señal Modulada.

3.4.2 Modulación de Frecuencia (FSK)

El proceso de modulación de frecuencia, se basa en hacer variar la frecuencia de la señal portadora en función de la señal moduladora, permaneciendo constante la amplitud de la portadora y por tanto la potencia asociada a la señal modulada, también lo será, figura III.18.

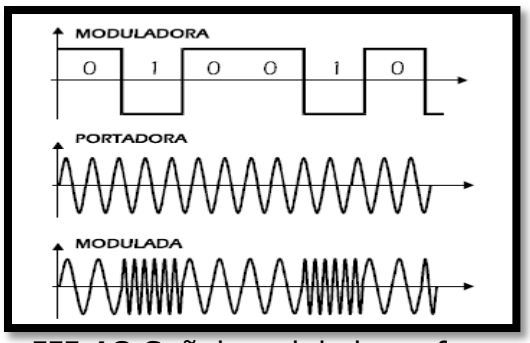

Figura III.18 Señal modulada en frecuencia.

El hecho de que a este tipo de modulación se le clasifique como un tipo de modulación angular, se debe a la representación vectorial que de la misma se puede utilizar, tal como se representa en la figura III.19.

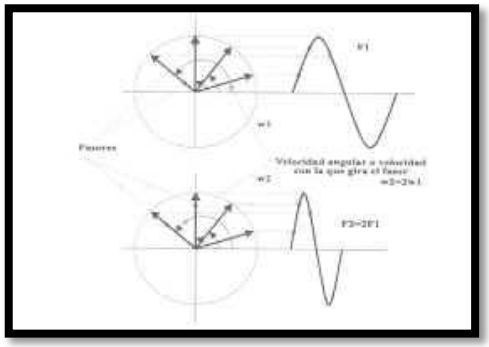

Figura III.19 Representación vectorial de una señal modulada en frecuencia.

Se basa en que la frecuencia portadora puede representarse como un vector giratorio o fasor con velocidad angular constante (w_1). Si su frecuencia aumenta ($w_1=2w_2$) o disminuye levemente, el fasor girará más rápida o más lentamente que con la velocidad angular constante que antes se mencionaba, lo que significará una variación angular y por tanto una nueva frecuencia.

Al ser la moduladora una señal digital, la modulación de frecuencia se basa en la conmutación brusca de frecuencias. De modo que se asigna una frecuencia diferente a cada símbolo, por ejemplo, 1.300 Hz para representar el "1" y 1.700 Hz para representar el "0", como consecuencia se produce un aprovechamiento deficiente del soporte de transmisión. No obstante, esta modulación se emplea mucho en transmisión de datos a bajas velocidades (<1.200 bps) por resultar sencilla la demodulación y ser la relación señal/ruido favorable frente a la de la modulación de amplitud.

En lo relativo a los receptores, éstos incorporan limitadores y discriminadores para eliminar las variaciones de amplitud y convertir las variaciones de frecuencia en variaciones de amplitud, reproduciendo así la señal original. Estos receptores requieren una ganancia de amplitud mayor que los utilizados en modulación

de amplitud, con el fin de que el discriminador trabaje correctamente.

En este tipo de modulación, el cambio de frecuencia se puede realizar sin afectar a la fase de la señal, el contemplar esto, nos lleva a los dos métodos de modulación de frecuencia, que son Modulación de Frecuencia Coherente y Modulación de Frecuencia No Coherente.

3.4.3 Modulación de Fase (PSK)

La técnica de modulación en fase utiliza las variaciones de fase de la onda portadora, según la señal digital. Por ejemplo, el bit 1 con fase M y el bit 0 con fase O. Gráficamente la modulación en fase se representa en la Figura III.20.

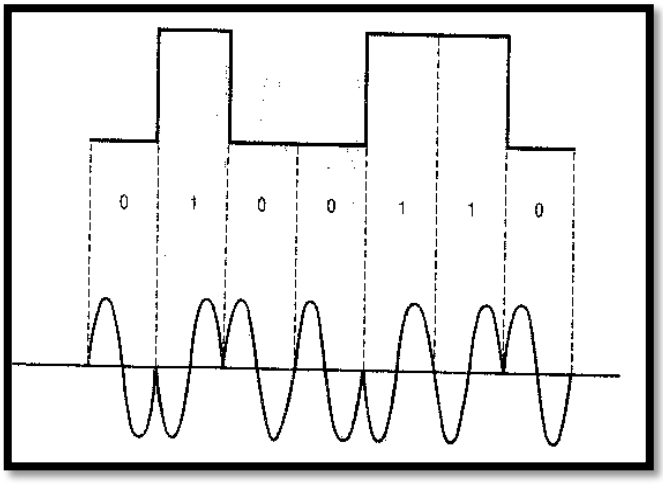

Figura III.20 Modulación en fase

La modulación en fase se puede realizar de diferentes maneras:

PSK (Phase Shift Keying) (Manipulación por Cambio de Fase): Cada vez que hay un cambio de estado (0 o 1) ocurre un cambio de 180°. Se realiza en dos fases (0° y 180°) podemos obtener hasta 2 señales.

La modulación PSK es el método más eficiente para transmitir datos binarios en presencia de ruido. La desventaja es que el diseño del emisor y receptor se complica extraordinariamente. Es ideal para comunicaciones síncronas.

DPSK (Differential Phase Shift Keying) (Manipulación por Cambio de Fase Diferenciada): Ocurre un cambio de fase cada vez que se transmite un 1, caso contrario la fase permanece constante. Se realiza en dos fases (0° y 180°) podemos obtener hasta dos señales.

QPSK (Quadrature Phase Shift Keying) (Manipulación por Cambio de Fase en Cuadratura): Implica la división de la señal en 4 fases de manera que una sola frecuencia puede tomar cualquiera de los cuatro valores de cambio de fase (0º, 90°, 180°, 270°). Se

obtiene hasta 4 señales y por cada una representaríamos 2 bits de información.

00 => 0°
01 => 90°
10 => 180°
11 => 270°

3.4.4 Modulaciones Complejas

Utilizan dos portadoras para modular la señal. Para poder transmitir dos portadoras moduladas sin interferencias entre ellas se desfasan 90º, dando lugar a la denominada modulación en cuadratura, figura III.21.

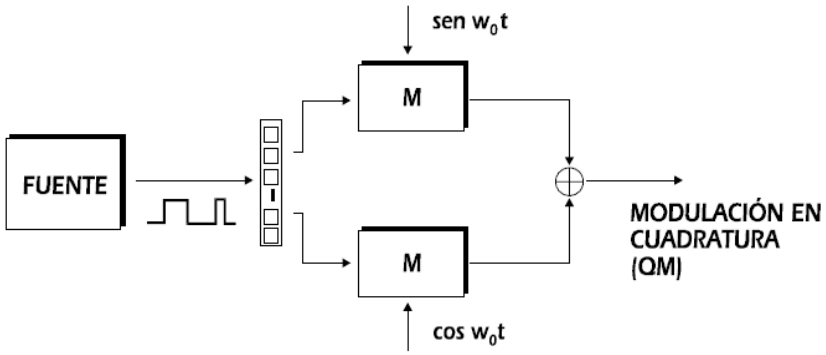

Figura III.21 Modulación en cuadratura

a) Modulación de Amplitud en Cuadratura (QAM)

Las dos portadoras se modulan en amplitud con cuatro niveles. Los bits se agrupan de cuatro en cuatro: los dos

primeros modulan en amplitud la portadora A y los dos últimos la B (16 estados). Ver figura III.22.

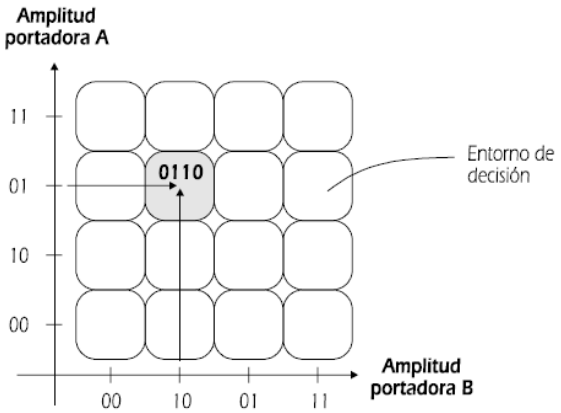

Figura III.22 Modulación QAM

b) Modulación de Fase en Cuadratura (QPM)

También se agrupan los bits de 4 en cuatro. Ahora los dos primeros y los dos últimos modulan las dos portadoras en fase QPSK.

c) Modulación de Fase y Amplitud en Cuadratura (QAPM)

Utiliza una única portadora que ahora se modula en fase y amplitud en función de los bits de la agrupación.

CAPITULO IV

SEGURIDAD EN REDES INALÁMBRICAS

Cuando se habla de Seguridad de la información en cualquier tipo de red de datos, el objetivo es poder garantizar estos tres conceptos:

Confidencialidad: La confidencialidad es la garantía de que un mensaje no ha sido leído por nadie que no sea el receptor para el que estaba destinado. Por ejemplo, un número de tarjeta de crédito se debe mantener de manera confidencial al enviarse a través de Internet. Un ejemplo de mecanismo destinado a preservar la confidencialidad es el cifrado de datos, mediante el cual la información sólo puede ser legible aplicándole una cierta clave que sólo emisor y receptor conocen.

Autenticación: La autenticación es la comprobación de una identidad reivindicada. Por ejemplo, al utilizar una cuenta bancaria, es imperativo que sólo el propietario real de la cuenta pueda hacer operaciones. Varios recursos pueden proporcionar la autenticación. Un ejemplo común de autenticación es un sistema simple de usuario y contraseña.

Integridad: La información debe mantenerse completa y libre de manipulaciones fortuitas o deliberadas. La integridad es la garantía de que los datos son completos y precisos, y que no se ven alterados en su recorrido de emisor a receptor. La integridad de los datos es la que se encarga, por ejemplo, de garantizar que una transferencia realizada mediante banca electrónica sea del importe deseado.

Un ejemplo de mecanismo para garantizar la integridad de los datos es la firma digital en un correo electrónico, un método criptográfico que garantiza la autoría del mensaje y la no manipulación del contenido.

4.1 RIESGOS DE LAS REDES INALÁMBRICAS

Dentro de los aspectos de seguridad de la red inalámbrica no se puede pasar por alto los elementos que la componen.

Existen 4 tipos de redes inalámbricas: la basada en tecnología BlueTooth, la IrDa (Infrared Data Association), la HomeRF y la Weca (Wi-Fi). La primera de ellas no permite la trasmisión de grandes cantidades de datos entre ordenadores de forma continua y la segunda tecnología, estándar utilizado por los dispositivos de ondas infrarrojas, debe permitir la visión directa entre los dos elementos comunicantes. Las tecnologías HomeRF y Wi-Fi están basadas en las especificaciones 802.11 (Ethernet Inalámbrica) y son las que utilizan actualmente las tarjetas de red inalámbrica.

La topología de estas redes consta de dos elementos clave, las estaciones cliente (STA) y los puntos de acceso (AP). La comunicación puede realizarse directamente entre estaciones cliente o a través del AP. El intercambio de datos sólo es posible cuando existe una autentificación entre el STA y el AP y se produce la asociación entre ellos (un STA pertenece a un AP). Por defecto, el AP transmite señales de gestión periódicas, el STA las recibe e inicia la autentificación mediante el envío de una trama de autentificación. Una vez realizada esta, la estación cliente envía una trama asociada y el AP responde con otra.

La utilización del aire como medio de trasmisión de datos mediante la propagación de ondas de radio ha proporcionado nuevos riesgos de seguridad. La salida de estas ondas de radio fuera del edificio donde

está ubicada la red permite la exposición de los datos a posibles intrusos que podrían obtener información sensible a la empresa y a la seguridad informática de la misma. Varios son los riesgos derivables de este factor. Por ejemplo, se podría perpetrar un ataque por inserción, bien de un usuario no autorizado o por la ubicación de un punto de acceso ilegal más potente que capte las estaciones cliente en vez del punto de acceso legítimo, interceptando la red inalámbrica.

También sería posible crear interferencias y una más que posible denegación de servicio con solo introducir un dispositivo que emita ondas de radio a una frecuencia de 2.4GHz (frecuencia utilizada por las redes inalámbricas).

La posibilidad de comunicarnos entre estaciones cliente directamente, sin pasar por el punto de acceso permitiría atacar directamente a una estación cliente, generando problemas si esta estación cliente ofrece servicios TCP/IP o comparte ficheros. Existe también la posibilidad de duplicar las direcciones IP o MAC de estaciones clientes legítimas.

Los puntos de acceso están expuestos a un ataque de Fuerza bruta para averiguar los passwords, por lo que una configuración incorrecta de los mismos facilitaría la irrupción en una red inalámbrica por parte de intrusos.

A pesar de los riesgos anteriormente expuestos, existen soluciones y mecanismos de seguridad para impedir que cualquiera con los materiales suficientes pueda introducirse en una red. Unos mecanismos son seguros, otros, como el protocolo WEP fácilmente "rompibles" por programas distribuidos gratuitamente por internet.

4.2 MECANISMOS DE SEGURIDAD

4.2.1 Privacidad equivalente al Cableado (WEP)

El protocolo WEP es un sistema de encriptación estándar propuesto por el comité 802.11, implementada en la capa MAC y soportada por la mayoría de vendedores de soluciones inalámbricas. En ningún caso es comparable con IPSec. WEP comprime y cifra los datos que se envían a través de las ondas de radio.

Con WEP, la tarjeta de red encripta el cuerpo y el CRC de cada trama 802.11 antes de la trasmisión utilizando el algoritmo de encriptación RC4 proporcionado por RSA Security. La estación receptora, sea un punto de acceso o una estación cliente es la encargada de desencriptar la trama.

Como parte del proceso de encriptación, WEP prepara una estructura denomina 'seed' obtenida tras la concatenación de la llave secreta proporcionada por el usuario de la estación emisora con un vector de inicialización (IV) de 24 bits generada aleatoriamente. La estación cambia el IV para cada trama transmitida.

A continuación, WEP utiliza el 'seed' en un generador de números pseudoaleatorio que produce una llave de longitud igual a el payload (cuerpo mas CRC) de la trama más un valor para chequear la integridad (ICV) de 32 bits de longitud.

El ICV es un checksum que utiliza la estación receptora para recalcularla y compararla con la enviada por la estación emisora para determinar si los datos han sido manipulados durante su envío. Si la estación receptora recalcula un ICV que no concuerda con el recibido en la trama, esta queda descartada e incluso puede rechazar al emisor de la misma.

WEP especifica una llave secreta compartida de 40 o 64 bits para encriptar y desencriptar, utilizando la encriptación simétrica. Antes de que tome lugar la transmisión, WEP combina la llave con el payload/ICV a través de un proceso XOR a nivel de bit que

producirá el texto cifrado. Incluyendo el IV sin encriptar sin los primeros bytes del cuerpo de la trama.

La estación receptora utiliza el IV proporcionado junto con la llave del usuario de la estación emisora para desencriptar la parte del payload del cuerpo de la trama.

Cuando se trasmiten mensajes con el mismo encabezado, por ejemplo FROM de un correo, el principio de cada payload encriptado será el mismo si se utiliza la misma llave. Tras encriptar los datos, el principio de estas tramas será el mismo, proporcionando un patrón que puede ayudar a los intrusos a romper el algoritmo de encriptación. Esto se soluciona utilizando un IV diferente para cada trama.

La vulnerabilidad de WEP reside en la insuficiente longitud del Vector de Inicialización (IV) y lo estáticas que permanecen las llaves de cifrado, pudiendo no cambiar en mucho tiempo. Si utilizamos solamente 24 bits, WEP utilizará el mismo IV para paquetes diferentes, pudiéndose repetir a partir de un cierto tiempo de trasmisión continua. Es a partir de entonces cuando un intruso puede, una vez recogido suficientes tramas, determinar incluso la llave compartida.

En cambio, 802.11 no proporciona ninguna función que soporte el intercambio de llaves entre estaciones. Como resultado, los administradores de sistemas y los usuarios utilizan las mismas llaves durante días o incluso meses. Algunos vendedores han desarrollados soluciones de llaves dinámicas distribuidas. A pesar de todo, WEP proporciona un mínimo de seguridad para pequeños negocios o instituciones educativas, si no está deshabilitada, como se encuentra por defecto en los distintos componentes inalámbricos.

4.2.2 Autenticación de Sistema Abierto (OSA)

Es otro mecanismo de autenticación definido por el estándar 802.11 para autentificar todas las peticiones que recibe. El principal problema que tiene es que no realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar, aun activando WEP, por lo tanto es un mecanismo poco fiable.

4.2.3 Lista de Control de Acceso (ACL)

Este mecanismo de seguridad es soportado por la mayoría de los productos comerciales. Utiliza como mecanismo de autenticación,

la dirección MAC de cada estación cliente, permitiendo el acceso a aquellas MAC que consten en la Lista de control de acceso.

4.2.4 Red Cerrada de Control de Acceso (CNAC)

Este mecanismo pretende controlar el acceso a la red inalámbrica y permitirlo solamente a aquellas estaciones cliente que conozcan el nombre de la red (SSID) actuando este como contraseña.

4.3 MÉTODOS DE DETECCIÓN DE REDES INALÁMBRICAS

El método de detección de una red inalámbrica se denomina Wardriving y es bastante sencillo. Bastaría con la simple utilización de una tarjeta de red inalámbrica WNIC (Wireless Network Interface Card), un dispositivo portátil (ordenador portátil o incluso un PDA) con un software para verificar puntos de acceso y pasearse por un centro de negocios o algún sitio donde nos conste la utilización de una red inalámbrica.

El ordenador portátil puede estar equipado con un sistema GPS para marcar la posición exacta donde la señal es más fuerte, o incluso una antena direccional para recibir el tráfico de la red desde una distancia considerable.

Una vez detectada la existencia de una red abierta, se suele dibujar en el suelo una marca con la anotación de sus características. Es lo que se denomina Warchalking, y cuya simbología se muestra en la Tabla IV-3.

Tabla IV-3 Simbología Warchalking

SIMBOLO	SIGNIFICADO
SSID)(Ancho de Banda	Nodo Abierto
SSID ()	Nodo Cerrado
SSID Contacto (W) Ancho de Banda	Nodo WEP

Por ejemplo el dibujo:

Xarxa
)(
1.5

Indicaría un nodo abierto, que utiliza el SSID Xarxa y que dispone de un ancho de banda de 1.5Mbps.

Esta simbología permite disponer de un mapa donde constan los puntos de acceso con sus datos (SSID, WEP, direcciones MAC,….). Si la red tiene DHCP, el ordenador portátil se configura para preguntar continuamente por una IP de un cierto rango, si la red no tiene DHCP activado podemos analizar la IP que figure en algún paquete analizado.

Existen varias herramientas útiles para detectar redes inalámbricas, las más conocidas son el AirSnort o Kismet para Linux y el NetStumbler para sistemas Windows.

Este mecanismo de detección de redes inalámbricas nos muestra lo fácil que es detectarlas y obtener información (incluso introducirnos en la red). A continuación en la Tabla IV-4 se muestra un estudio realizado a fecha del 10 de julio del 2008 en la ciudad de Manhattan:

Tabla IV-4 Estadísticas Wardriving en la ciudad de Manhattan

APs	Número	Porcentaje
WEP INHABILITADO	198	75%
WEP HABILITADO	65	25%
TOTAL	**263**	**100%**

Los estudios realizados indican un número elevado de redes inalámbricas sin el protocolo WEP activado o con el protocolo WEP activado pero con el SSID utilizado por defecto.

4.4 DISEÑO RECOMENDADO

Se podrían hacer varias recomendaciones para diseñar una red inalámbrica e impedir lo máximo posible el ataque de cualquier intruso.

Como primera medida, se debe separar la red de la organización en un dominio público y otro privado. Los usuarios que proceden del dominio público (los usuarios de la red inalámbrica) pueden ser tratados como cualquier usuario de Internet (externo a la organización). Así mismo, instalar cortafuegos y mecanismos de autentificación entre la red inalámbrica y la red clásica, situando los puntos de acceso delante del cortafuegos y utilizando VPN a nivel de cortafuegos para la encriptación del tráfico en la red inalámbrica.

Los clientes de la red inalámbrica deben acceder a la red utilizando SSH, VPN o IPSec y mecanismos de autorización, autenticación y encriptación del tráfico (SSL). Lo ideal sería aplicar un nivel de seguridad distinto según que usuario accede a una determinada aplicación.

La utilización de VPNs nos impediría la movilidad de las estaciones cliente entre puntos de acceso, ya que estos últimos necesitarían intercambiar información sobre los usuarios conectados a ellos sin reiniciar la conexión o la aplicación en curso, cosa no soportada cuando utilizamos VPN.

Como contradicción, es recomendable no utilizar excesivas normas de seguridad por que podría reducir la rapidez y la utilidad de la red inalámbrica. La conectividad entre estaciones cliente y AP es FCFS, es

decir, la primera estación cliente que accede es la primera en ser servida, además el ancho de banda es compartido, motivo por el cual se debe asegurar un número adecuado de puntos de acceso para atender a los usuarios.

También se podrían adoptar medidas extraordinarias para impedir la intrusión, como utilizar receivers (Signal Leakage Detection System) situados a lo largo del perímetro del edificio para detectar señales anómalas hacia el edificio además de utilizar estaciones de monitorización pasivas para detectar direcciones MAC no registradas o clonadas y el aumento de tramas de re-autentificación.

Por último también podrían ser adoptadas medidas físicas en la construcción del edificio o en la utilización de ciertos materiales atenuantes en el perímetro exterior del edificio, debilitando lo máximo posible las señales emitidas hacia el exterior. Algunas de estas recomendaciones podrían ser, aún a riesgo de resultar extremadas:

- Utilizar cobertura metálica en las paredes exteriores.
- Vidrio aislante térmico (atenúa las señales de radiofrecuencia).
- Persianas venecianas de metal, en vez de plásticas.
- Poner dispositivos WLAN lejos de las paredes exteriores.
- Utilizar pinturas metálicas.

- Limitar el poder de una señal cambiando la atenuación del trasmisor.
- Revestir los closets (rosetas) de la red con un revestimiento de aluminio.

4.5 POLÍTICAS DE SEGURIDAD

Aparte de las medidas que se hayan tomado en el diseño de la red inalámbrica, se debe aplicar ciertas normas y políticas de seguridad que ayudarían a mantener una red más segura:

- Utilizar WEP, aunque sea rompible con herramientas como AirSnort o WEPCrack, como un mínimo de seguridad.

- Utilizar mecanismos de intercambio de clave dinámica aportado por los diferentes productos comerciales hasta que el comité 802.11i, encargado de mejorar la seguridad en las redes inalámbricas, publique una revisión del estándar 802.11 con características avanzadas de seguridad, incluyendo AES (Advanced Encryption Standar) e intercambio dinámico de claves.

- Inhabilitar DHCP para la red inalámbrica. Las IPs deben ser fijas.

- Actualizar el firmware de los puntos de acceso para cubrir los posibles agujeros en las diferentes soluciones wireless.

- Proporcionar un entorno físicamente seguro a los puntos de acceso y desactivarlos cuando se pretenda un periodo de inactividad largo (ej. ausencia por vacaciones).

- Cambiar el SSID (Server Set ID) por defecto de los puntos de acceso, conocidos por todos. El SSID es una identificación configurable que permite la comunicación de los clientes con un determinado punto de acceso. Actúa como un password compartido entre la estación cliente y el punto de acceso. Ejemplos de SSID por defecto son "tsunami" para Cisco, "101" para 3Com, "Intel" para intel….

- Inhabilitar la emisión broadcast del SSID.

- Reducir la propagación de las ondas de radio fuera del edificio.

- Utilizar IPSec, VPN, firewalls y monitorizar los accesos a los puntos de acceso.

4.6 SISTEMAS DETECTORES DE INTRUSOS

Los sistemas detectores de intrusos, IDS, totalmente integrados en las redes clásicas cableadas, están tomando forma también en las redes inalámbricas. Sin embargo, aún son pocas las herramientas disponibles y sobretodo realmente efectivas, aunque empresas privadas están

desarrollando y adaptando sus sistemas detectores de intrusos para redes inalámbricas (como ISS en su software Real Secure).

Las redes inalámbricas nos proporcionan cambios nuevos respecto a los sistemas de detección de intrusos situados en las redes clásicas cableadas.

En primer lugar, la localización de la estación capturadora de tráfico debe estar instalada en la misma área de servicios WLAN que se quiera monitorizar. Este punto es crítico y se obtendrá muchos falsos positivos si la localización es inapropiada o la sensibilidad del agente tan elevada que puede incluso capturar tráfico procedente de otras WLANs.

Otro punto crítico en los sistemas detectores de intrusos para redes es la identificación de tráfico anómalo, ya que existen aplicaciones como el NetStumbler y Dstumbler que utilizan técnicas de descubrimiento de redes inalámbricas especificadas en 802.11 junto con otras propias, por lo que el agente IDS debe detectar y distinguir un tráfico de otro.

4.7 PROTOCOLO DE CAPA SUPERIOR (ULA)

Los protocolos ULA proporcionan intercambio de autenticación entre el cliente y un servidor de autenticación. La mayoría de los protocolos de autenticación incluyen:

- EAP-TLS (Extensible Authentication Protocol with Transport Layer Security), protocolo de autenticación basado en certificados y soportado por Windows XP. Necesita la configuración de la máquina para establecer el certificado e indicar el servidor de autentificación.

- PEAP (Protected Extensible Authentication Protocol), proporciona una autentificación basada en el password. En este caso, solamente el servidor de autentificación necesitaría un certificado.

- EAP-TTLS (EAP with Tunneled Transport Layer Security), parecido al PEAP, está implementado en algunos servidores Radius y en software diseñado para utilizarse en redes 802.11 (inalámbricas).

- LEAP (Lightweigh EAP), propiedad de Cisco y diseñado para ser portable a través de varias plataformas wireless. Basa su popularidad por ser el primero y durante mucho tiempo el único mecanismo de autenticación basado en password y proporcionar diferentes clientes según el sistema operativo.

4.8 ESTÁNDAR 802.1X

Es un estándar de control de acceso a la red basado en puertos. Como tal, restringe el acceso a la red hasta que el usuario se ha validado.

El sistema se compone de los siguientes elementos:

- Una estación cliente.
- Un punto de acceso.
- Un servidor de Autenticación (AS).

Es este nuevo elemento, el Servidor de Autenticación, el que realiza la autenticación real de las credenciales proporcionadas por el cliente. El AS es una entidad separada situada en la zona cableada (red clásica), pero también se puede implementar en un punto de acceso. El tipo de servidor utilizado podría ser el RADIUS, u otro tipo de servidor que se crea conveniente.

El estándar 802.1x introduce un nuevo concepto de puerto habilitado/inhabilitado en el cual hasta que un cliente no se valide en el servidor no tiene acceso a los servicios ofrecidos por la red. El esquema se muestra en la Figura IV.23

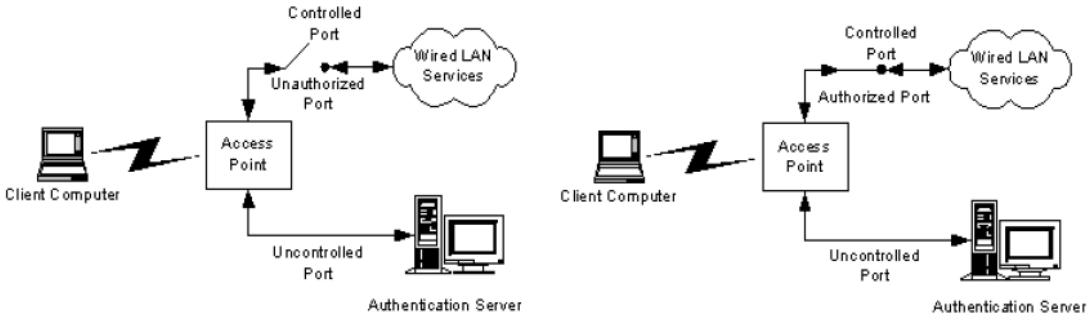

Figura IV.23 Esquema puerto habilitado/inhabilitado 802.1x

En sistemas con 802.1x activado, se generan 2 llaves, la llave de sesión (pairwise key) y la llave de grupo (groupwise key). Las llaves de grupo se comparten por todas las estaciones cliente conectadas a un mismo punto de acceso y se utilizan para el tráfico multicast, las llaves de sesión son únicas para cada asociación entre el cliente y el punto de acceso y se creará un puerto privado virtual entre los dos.

El estándar 802.1x mejora la seguridad proporcionando las siguientes mejoras sobre WEP:

- Modelo de seguridad con administración centralizada.

- La llave de encriptación principal es única para cada estación, por lo tanto, el tráfico de esta llave es reducido.

- Existe una generación dinámica de llaves por parte del AS, sin necesidad de administrarlo manualmente.

- Se aplica una autenticación fuerte en la capa superior.

4.9 PROTOCOLO DE INTEGRIDAD DE CLAVE TEMPORAL (TKIP)

Este protocolo pretende resolver las deficiencias del algoritmo WEP y mantener la compatibilidad con el hardware utilizado actualmente mediante una actualización del firmware.

El protocolo TKIP está compuesto por los siguientes elementos:

- Un código de integración de mensajes (MIC), encripta el checksum incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11. Esta medida protege contra los ataques por falsificación.

- Contramedidas para reducir la probabilidad de que un atacante pueda aprender o utilizar una determinada llave.

- Utilización de un IV de 48 bits llamado TSC (TKIP Sequence Counter) para protegerse contra ataques por repetición, descartando los paquetes recibidos fuera de orden.

La estructura de encriptación TKIP propuesta por 802.11i se muestra en la figura IV.24

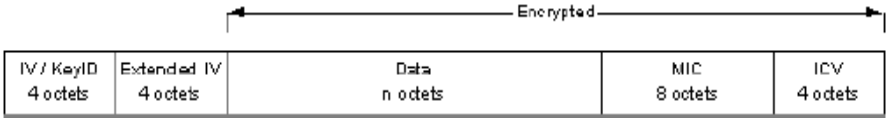

Figura IV.24 Estructura de encriptación TKIP

La utilización del TSC extiende la vida útil de la llave temporal y elimina la necesidad de redecodificar la llave temporal durante una sola asociación.

Pueden intercambiarse 2^{48} paquetes utilizando una sola llave temporal antes de ser rehusada. En el proceso de encapsulación TKIP mostrado en la figura IV.25.

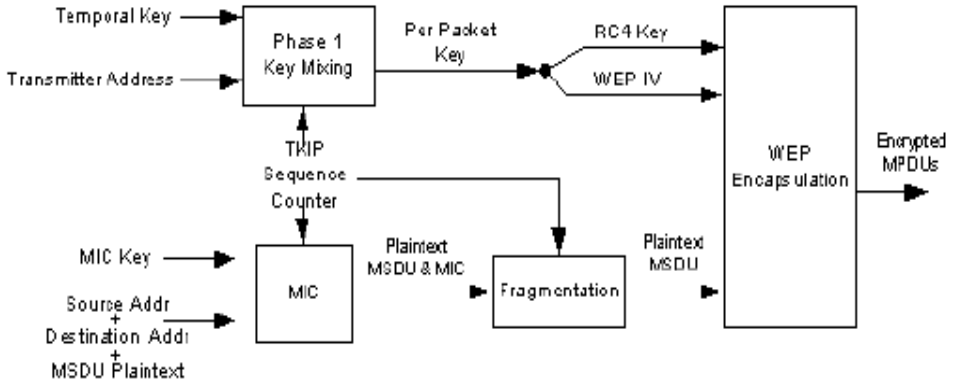

Figura IV.25 Proceso de encapsulación TKIP

Se combinan en dos fases la llave temporal, la dirección del emisor y el TSC para la obtención de una llave de 128 bits por paquete, dividido en una llave RC4 de 104 bits y en un IV de 24 bits para su posterior encapsulación WEP.

El MIC final se calcula sobre la dirección física origen y destino y el MSDU (MAC Service Data Unit o texto plano de los datos en la trama 802.11) después de ser segmentado por la llave MIC y el TSC.

La función MIC utiliza una función hash unidireccional, si es necesario, el MSDU se fragmenta incrementando el TSC para cada fragmento antes de la encriptación WEP.

En la desencriptación se examina el TSC para asegurar que el paquete recibido tiene el valor TSC mayor que el anterior. Sino, el paquete se descartará para prevenir posibles ataques por repetición. Después de que el valor del MIC sea calculado basado en el MSDU recibido y desencriptado, el valor calculado del MIC se compara con el valor recibido.

4.10 MOCO CONTADOR CON PROTOCOLO CBC-MAC

Este protocolo es complementario al TKIP y representa un nuevo método de encriptación basado en AES (Encriptación Estándar Avanzada), cifrado simétrico que utiliza bloques de 128 bits, con el algoritmo CBC-MAC. Así como el uso del TKIP es opcional, la utilización del protocolo CCMP es obligatorio si se está utilizando 802.11i.

En la figura IV.26 se observa el formato tras la encriptación CCMP.

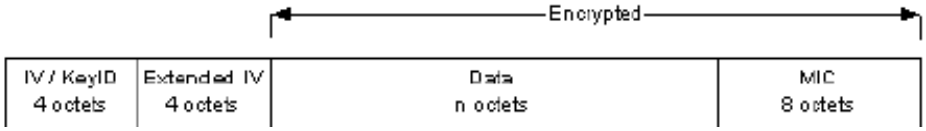

Figura IV.26 Estructura encriptación CCMP

CCMP utiliza un IV de 48 bits denominado Número de paquete (PN) utilizado a lo largo del proceso de cifrado, junto con la información

para inicializar el cifrado AES para calcular el MIC y la encriptación de la trama.

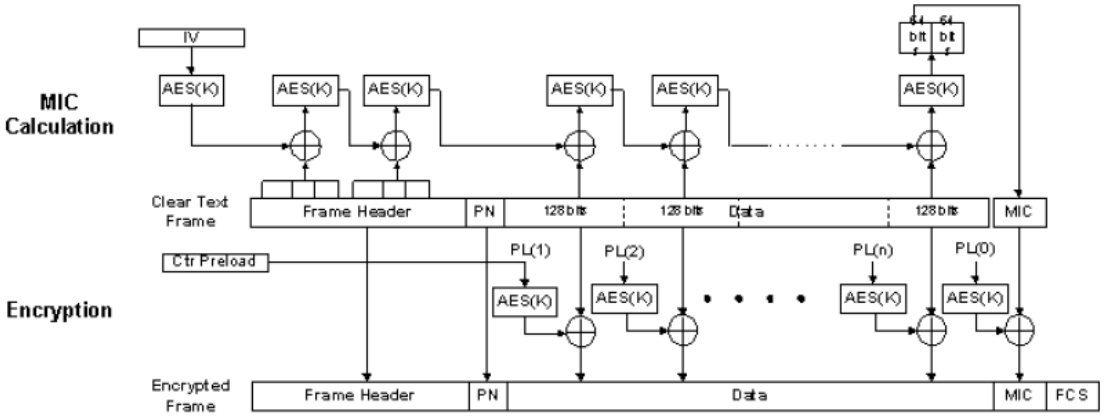

Figura IV.27 Proceso de encriptación CCMP

En el proceso de encriptación CCMP, la encriptación de los bloques utiliza la misma llave temporal tanto para el cálculo del MIC como para la encriptación del paquete. Como en TKIP, la llave temporal se deriva de la llave principal obtenida como parte del intercambio en 802.1x. En la figura IV.27 se observa, el cálculo del MIC y la encriptación se realiza de forma paralela. El MIC se calcula a partir de un IV formado por el PN y datos extraídos de la cabecera de la trama. El IV se convierte en un bloque AES y su salida a través de la operación XOR conformará el siguiente bloque AES.

CAPITULO V

EQUIPOS NANOSTATION

Ingresando la IP por defecto 192.168.1.20 se muestra la ventana de acceso, digitamos "ubnt" para el login y password, accediendo al menú de configuración dividido en categorías. Estos son: Main, Link Setup, Network, Advanced, Services y System, ver figura V.28

Figura V.28 Menú de configuración de administración

5.1 NAVEGACIÓN

Cada una de las páginas del Sistema de configuración Web (enumeradas a continuación) contienen parámetros relacionados con un aspecto específico del dispositivo:

La Página Principal (Main Page) muestra el estado actual del dispositivo e información estadística. También hay herramientas muy útiles relacionadas con la administración de red y monitoreo en la página principal (por ejemplo: herramienta de alineación de antena, pruebas de velocidad y análisis del sitio mientras se opere en modo de Punto de Acceso).

La página de Configuración del enlace (Link Setup) contiene los parámetros para la configuración del enlace inalámbrico. Se relaciona con las configuraciones inalámbricas básicas, como definir el modo de operación, detalles de asociación y opciones de seguridad de datos.

La página de Red (Network) cubre la configuración del modo de operación de la red, configuración IP, filtrado de paquetes y servicios de red (por ejemplo: Servidor DHCP).

La página Configuración Avanzada está dedicada a un control más preciso de la interfaz inalámbrica. Ésta también incluye configuración de polaridad de la antena, priorización de tráfico y Calidad de Servicio (QoS).

La página de Servicios trata acerca del sistema de administración de servicios (por ejemplo: SNMP, NTP, Historial de sistema, Ping Watchdog).

La página de Sistema contiene los controles para el sistema de mantención, administración de la cuenta Administrador, personalización del dispositivo y respaldo de configuración.

5.2 PÁGINA PRINCIPAL

La página principal muestra un resumen del estado del enlace, valores actuales de la configuración básica (dependiendo del modo operativo), parámetros de red y estadísticas de tráfico de todas las interfaces.

La administración de red y las utilidades de monitoreo como la herramienta de alineación de antena, ping y traceroute, prueba de velocidad son también accesibles desde la página principal. Ver figura V.29.

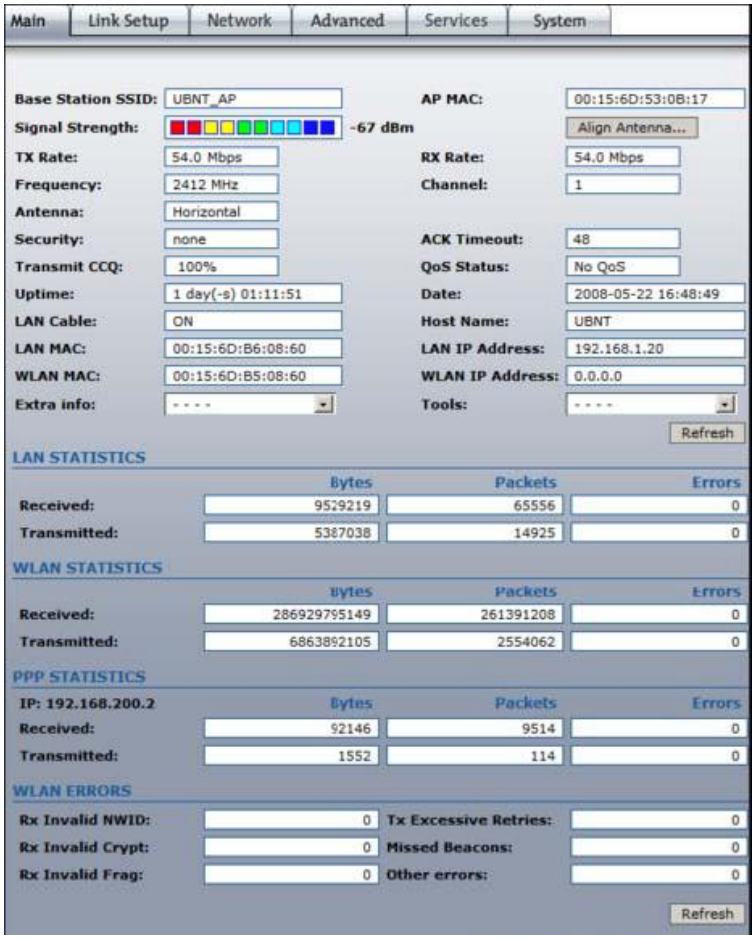

Figura V.29 Estado actual del dispositivo basado en AirOs

5.2.1 Reporte de Estado

SSID de Estación Base: El nombre de la red inalámbrica 802.11 (determinado por el Punto de Acceso anfitrión) al cual el dispositivo está conectado:

Mientras opera en modo Estación, muestra el BSSID del Punto de Acceso al cual el dispositivo está conectado.

Mientras opera en modo Punto de Acceso, muestra el BSSID del propio dispositivo.

MAC del AP (AP MAC): muestra la dirección MAC del Punto de Acceso donde el dispositivo está asociado mientras que opera en modo Estación. MAC (Media Access Control) es un identificador único de cada radio 802.11. El cual consta de dos partes:

Un identificador único organizacional (OUI)
Una secuencia de interfaz controladora de red (NIC)

Intensidad de señal (Signal Strength): Muestra los niveles de señal inalámbrica recibidos (lado Cliente) mientras opera en modo Estación. Los valores representados coinciden con la barra gráfica. Usando la herramienta de alineación de antena se obtiene un mejor enlace entre los dispositivos. La antena del cliente inalámbrico debe estar ajustada a máxima potencia. La intensidad de señal es medida en dBm. La conversión entre dBm y mW es dBm=10log10(P/1mW). Entonces, 0dBm sería 1mW y -72dBm sería 0.0000006mW. Un nivel de señal de -85dBm o mejor es recomendado para un enlace estable.

Tasa de Recepción y Envío (Tx Rate and Rx Rate): Muestra la actual tasa de transmisión (Tx Rate) y tasa de recepción (Rx

Rate) mientras opera en modo Estación. Las tasas de transmisión disponibles son 1,2,5.5,11Mbps (802.11b) y 6,9,12,18,24,36,48,54Mbps (802.11g, 802.11a). Generalmente a mayor señal, mayor será la tasa de transmisión y mayor el ancho de banda real. Para conseguir el mayor ancho de banda (54Mbps) se requiere una tasa igual o superior a -70dBm.

Frecuencia (Frequency): Hace referencia a la frecuencia en la que opera el Punto de Acceso al que está conectado el dispositivo (cliente). El dispositivo utiliza esta frecuencia para enviar y recibir datos. Para el estándar 802.11a están disponibles las frecuencias desde 5.1 a 5.9GHz y para el estándar 802.11b/g están disponibles las frecuencias 2412MHz a 2472MHz. Sin embargo, el rango de frecuencia depende de las regulaciones locales (secretaria de telecomunicaciones de su país).

Canal (Channel): Este es el número del canal 802.11 correspondiente a la frecuencia operativa. Los dispositivos utilizan el canal seleccionado para transmitir y recibir datos.

Antena (Antenna): Muestra cual antena está siendo utilizada por el dispositivo basado en AirOS actualmente. La mayoría de los dispositivos Ubiquiti tienen tres opciones de antena: Vertical,

Horizontal o Polaridad de Antena Adaptativa (AAP). En algunos modelos también está disponible la opción de antena externa.

Ruido base (Noise Floor): Muestra el nivel actual de ruido en dBm. El ruido base se calcula evaluando la calidad de la señal (Relación entre Señal-Ruido SNR) hasta que el valor promedio de la intensidad de señal esté por sobre el ruido base.

Seguridad (Security): Indicia la actual configuración de seguridad. "Ninguna" (None) es el valor que se muestra cuando la seguridad inalámbrica está deshabilitada. WEP, WPA o WPA2 son los valores que aparecen dependiendo del método de seguridad utilizado.

Pausa ACK (ACK Timeout): Muestra el actual valor de timeout (pausa) para los cuadros ACK. El timeout ACK puede ser especificado manualmente o ajustable automáticamente. La pausa ACK (Acknowledgement frame Timeout) especifica cuanto debe esperar el dispositivo AirOS por un acuse de recibo por parte del otro dispositivo confirmando la correcta recepción del paquete de datos antes de que el paquete sea considerado erróneo y deba ser reenviado. La Pausa ACK es muy importante

para los parámetros de rendimiento en enlaces inalámbricos en el exterior.

Transmitir CCQ (Transmit CCQ): Este es un índice de cómo se evalúa la calidad de la conexión del cliente inalámbrico. Tiene en consideración el conteo de errores de transmisión, latencia, y rendimiento, mientras evalúa la tasa de paquetes correctamente transmitidos en relación con los que deben ser retransmitidos, y tiene en cuenta la actual tasa en relación con la mayor tasa especificada. El nivel está basado en un porcentaje donde 100% corresponde a un enlace perfecto.

Estado de Calidad de Servicio (QoS Status): muestra la actual configuración de Calidad de Servicio (QoS), puede priorizar un determinado cliente o una determinada aplicación como Voz IP y video, que requiere gran consistencia, estabilidad y baja latencia en el rendimiento.

Tiempo de funcionamiento (Uptime): Muestra el tiempo total que lleva el dispositivo funcionando desde la última vez que se realizó un reinició mayor (hard-reboot) o actualización de software. El tiempo está expresado en días, horas, minutos y segundos.

Fecha (Date): Indica la fecha y hora actual del sistema. Expresado en formato "año- mes-día horas:minutos:segundos". La fecha y hora exacta es sincronizada utilizando NTP (Network Time Protocol). En caso que se haga un reinicio (reboot) de sistema, y no esté activa la función NTP la hora quedará desactualizada, ya que el sistema no cuenta con un reloj interno con alimentación autónoma que le permita mantenerla en caso de reinicio.

Cable LAN (LAN cable): Muestra el estado actual de la conexión al puerto Ethernet. Esto puede alertar al operador o técnico del sistema que el cable de red no está conectado al dispositivo, y que no hay una conexión de red activa.

Nombre del anfitrión (Host Name): muestra el nombre personalizable (ID) del dispositivo basado en AirOS. El nombre de anfitrión estará disponible en la mayoría de los Sistemas Operativos de enrutadores y herramientas de descubrimiento de red.

MAC de la LAN (LAN MAC): muestra la dirección MAC de la interfaz LAN (Ethernet) del dispositivo.

Dirección IP de la LAN (LAN IP Address): muestra la actual dirección IP de la interfaz LAN (Ethernet) del dispositivo.

MAC de la WLAN (WLAN MAC): muestra la dirección MAC de la interfaz WLAN (Inalámbrica) del dispositivo.

Dirección IP de la WLAN (WLAN IP Address): muestra la actual dirección IP de la interfaz WLAN (Inalámbrica) del dispositivo.

La dirección IP LAN y la dirección IP WLAN mostrarán el mismo valor mientras el dispositivo opera en modo Puente (Bridge mode).

5.2.2 Información de Estadísticas

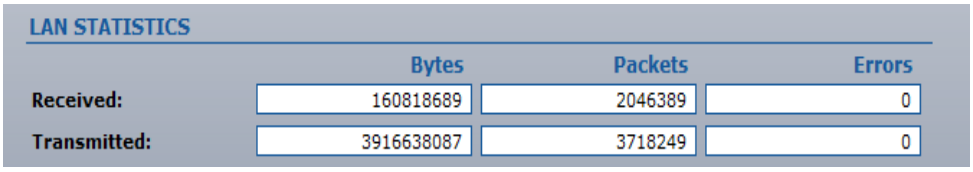

Figura V.30 Estadísticas de la interfaz LAN

Estadísticas de LAN: Muestra las estadísticas detalladas de bytes, Paquetes y Errores de envío y recepción de la interfaz LAN. Estas estadísticas representan la cantidad total de datos y

de paquetes transferidos entre los dispositivos a través del interfaz Ethernet en cualquier dirección.

El tráfico IP unicast (conversaciones entre dos anfitriones usando el protocolo HTTP, SMTP, SSH y otros protocolos) y el tráfico de difusión (mientras se direccionan todos los anfitriones en un determinado rango con una dirección IP de destino específica).

Mientras haya un cierto tráfico de red que es generado o que pase a través de la interfaz LAN, los bytes y paquetes recibidos y transmitidos seguirán aumentando. Los valores de error representan el número total de paquetes transmitidos y recibidos para los cuales ocurrió un error en la capa de enlace. Un elevado número de errores puede indicar fallas o problemas de configuración del dispositivo.

Estadísticas de la WLAN: Muestra estadísticas detalladas de bytes, paquetes y errores en la interfaz inalámbrica.

Esta estadística representa la cantidad total de datos IP unicast y de difusión transferidos entre los dispositivos a través de la interfaz inalámbrica en cualquier dirección.

Mientras haya un cierto tráfico de red que es generado o que pase a través de la interfaz inalámbrica, los valores de bytes, paquetes y de los errores (si es que hay) tanto recibidos como transmitidos seguirán aumentando.

Estadísticas del PPP: Ésta sección muestra la dirección IP de la interfaz PPP y las estadísticas detalladas de los bytes, paquetes y errores que se reciben y transmiten mediante la interfaz PPP mientras que el dispositivo basado AirOS funciona en modo enrutador con la opción de PPPoE activada.

La dirección IP de la interfaz PPP se mostrará si pudo ser obtenida a través de la conexión PPPoE establecida, en caso contrario un mensaje de "No conectado" será visible.

Presionando el botón del **volver a conectar** (Reconnect) se inicializará la rutina de reconexión PPPoE, la cual podrá requerir un reinicio del sistema. Este control debe utilizarse solamente para los propósitos de localización de problemas cuando se establece el túnel PPPoE pero la conexión IP esté inactiva (Idle).
Esta estadísticas representan la cantidad total de datos IP unicast y de difusión transferidos entre el dispositivo con AirOS y el servidor de PPPoE con el cual hace un túnel PPP.

Errores de WLAN: muestra el conteo de errores específicos 802.11 que fueron registrados en la interfaz inalámbrica:

El **valor inválido Rx NWID** representa el número de paquetes recibidos con diferentes NWID o ESSID – de los paquetes que tenían como destino otro punto de acceso. Esto puede ayudar a detectar problemas en la configuración o a identificar la existencia de otra red inalámbrica adyacente en la misma frecuencia.

El **valor inválido de Crypt Rx** representa el número de paquetes transmitidos y recibidos que fueron encriptados con la llave de encriptación incorrecta y en los cuales hubo fallos de desencriptación. Esto puede ser utilizado para detectar ajustes inválidos en las políticas de seguridad inalámbrica e intentos de ruptura de la encriptación.

El **valor inválido de Rx Frag** representa el número de paquetes perdidos durante la transmisión y la recepción. Estos paquetes se perdieron debido a una falla en el re-ensamblamiento.

El **Tx Excessive Retries** representa el número de paquetes que no pudieron ser entregados a su destino. Los paquetes sin

entregar se retransmiten un número de veces antes de que ocurra un error.

El valor de **pérdidas en las alertas de señal** (Missed beacons) representa el número de alertas de señal (paquetes de administración enviados en intervalos regulares por el Punto de Acceso) los cuales fueron perdidos por el cliente. Esto puede indicar que el cliente inalámbrico está fuera de cobertura.

Otros valores de error representan el número total de paquetes transmitidos y recibidos que fueron perdidos o desechados por otras razones.

El contenido de la página principal puede ser actualizado usando el botón de **refrescar**

5.3 CONFIGURACIÓN DEL ENLACE

La página de configuración del enlace contiene todo lo necesario para que el operador configure la parte inalámbrica de la conexión. Esto incluye requisitos regulatorios (ej: potencia máxima de transmisión), los ajustes del canal y de la frecuencia, modo de funcionamiento del dispositivo, las tasas de datos, y seguridad inalámbrica. Ver Fig. V.31.

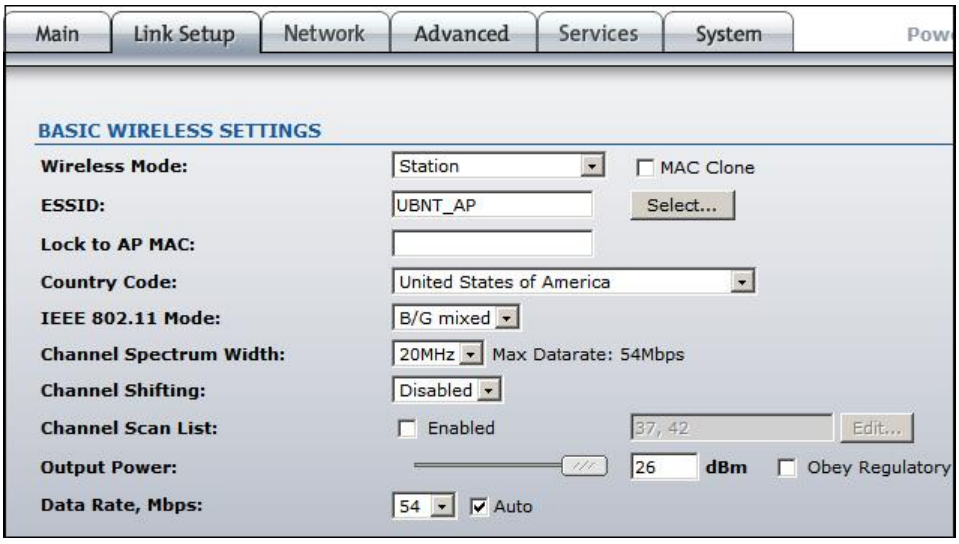

Figura V.31 Ajustes inalámbricos básicos de la estación

Los ajustes inalámbricos generales, tales como BSSID del dispositivo inalámbrico, código de país, potencia de salida y tasas de datos se pueden configurar en esta sección. **Modo inalámbrico** (Wireless Mode): especifica el modo de funcionamiento del dispositivo. El modo depende de los requisitos de la topología de red. Hay 4 modos de funcionamiento soportados en el software de AirOS v3.0:

Estación: Éste es un modo de cliente, el cual se puede conectar con un AP. Es comúnmente usado para enlazarse con un AP. En modo estación el dispositivo actúa como la estación del suscriptor (CPE) mientras que se conecta con el punto de acceso primario definido por el SSID y re-direcciona todo el tráfico entrante y saliente de la red a los dispositivos conectados en la interfaz Ethernet.

Las especificaciones de este modo es que la estación del suscriptor utiliza la técnica arpnat, la cual puede provocar fallas de transparencia mientras pasa a través los paquetes de difusión en modo de puente.

Estación WDS: WDS representa un sistema de distribución inalámbrica. El modo Estación WDS debe ser utilizado mientras que se conecta con el punto de acceso que está funcionando en modo WDS.

El modo estación WDS permite re-direccionar los paquetes en el nivel de la capa 2. La ventaja de la *estación* WDS es que mejora el rendimiento. "Estación WDS - modo puente" es completamente transparente para todos los protocolos de capa 2.

Punto de acceso: Esto es un modo de punto de acceso 802.11.

Punto de acceso WDS: Éste es un punto de acceso 802.11 que permite a la capa 2 hacer un puente con dispositivos estación WDS usando el protocolo WDS. Vea la Figura V.32.

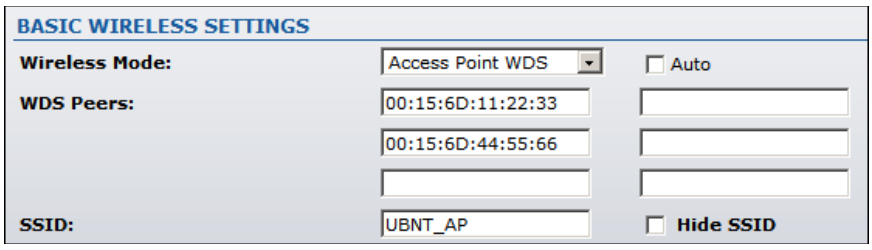

Figura V.32 Ajustes inalámbricos básicos del AP WDS

WDS le permite hacer un puente de tráfico inalámbrico entre dispositivos que operan en modo punto de acceso. El punto de acceso generalmente está conectado con una red alámbrica (LAN Ethernet) que permite la conexión inalámbrica con la red alámbrica. Conectando los puntos de acceso uno con otro usando un determinado servicio extendido WDS, Ethernet(s) distantes se pueden unir en una sola LAN.

Es muy importante que los aros de la red tampoco se formen con otros puentes WDS o mediante cable (Ethernet) y de puentes WDS simultáneamente. La topología de red en forma de árbol o de estrella debe utilizarse en todos los casos de uso WDS. Las topologías de red malladas y de anillo no son soportadas por WDS y deben evitarse en todos los casos de uso.

Usar WDS en modo estación y en modo AP WDS utiliza el protocolo WDS, el cual no ha sido definido como estándar, así que podría tener problemas de compatibilidad entre equipamiento de diferentes fabricantes.

Pares WDS (WDS Peers): Las estaciones WDS y/o los puntos de acceso WDS conectados con el punto de acceso basado en AirOS deben especificarse en esta lista para crear una infraestructura de red inalámbrica.

Escriba la dirección MAC de los dispositivos pares WDS en el campo de entrada: par WDS (WDS Peer). Sólo una dirección MAC debe ser especificada en caso de conexión de punto a punto, hasta seis pares WDS pueden ser especificados para el caso de uso en conexión Punto a Multipunto.

La **opción automática** se debe habilitar para establecer la conexión WDS entre los puntos de acceso en caso de no estar especificados. Si se habilita la opción automática (auto) el punto de acceso basado en AirOS elegirá los pares WDS (puntos de acceso) según el ajuste de SSID. Los puntos de acceso que funcionen en modo WDS deben tener el mismo SSID que el par WDS para establecer la conexión automáticamente mientras que esté habilitada la opción automática. Esta configuración también se conoce con el nombre de modo repetidor. El punto de acceso que funcione en modo WDS y todos los pares WDS deben funcionar en el mismo canal de frecuencia y utilizar la misma anchura de espectro del canal.

SSID: El identificador de servicio determinado (Service Set Identifier) es usado para identificar su red inalámbrica 802.11, debe ser especificado mientras que opera en modo de punto de acceso. Todos los dispositivos clientes dentro del alcance recibirán mensajes de difusión desde el punto de acceso que publicita este SSID.

ESSID: Especifica el ESSID del punto de acceso al cual AirOS debe asociarse mientras que funciona en modo de estación o estación WDS. Puede haber varios puntos de acceso con el mismo ESSID. Si el ESSID se fija como "cualquiera" la estación conectará con cualquier AP disponible.

SSID oculto inhabilitará la difusión de mensajes del SSID que emite el punto de acceso a las estaciones inalámbricas. La opción deseleccionado hará el SSID visible durante exploraciones de la red en las estaciones inalámbricas. El control está solamente disponible mientras que funciona en modo de punto de acceso.

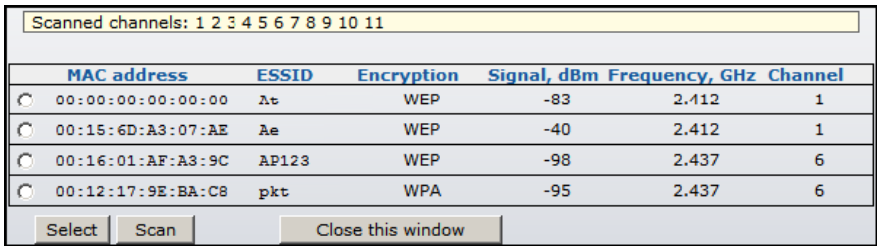

Figura V.33: Herramienta de encuesta sobre el sitio para seleccionar el AP

La lista de los puntos de acceso disponibles puede ser obtenida usando el botón seleccionar (Select), figura V.33. Este control activa la herramienta de encuesta sobre el sitio que se utiliza para la selección del AP. La encuesta sobre el sitio buscará todas las redes inalámbricas disponibles dentro del rango del dispositivo, en los canales soportados por el mismo y le permitirá seleccionar uno para la asociación. En caso

que la red seleccionada utilice encriptación, se necesitará fijar los parámetros de seguridad en la sección de seguridad inalámbrica. Seleccione el punto de acceso de la lista y presione el botón seleccionar (Select) para establecer la asociación.

El botón de exploración (Scan) refresca la lista de redes inalámbricas disponibles. Al cerrar esta ventana se cerrará la ventana de utilidad de encuesta sobre el sitio. La lista de canales a explorar usados por la encuesta sobre el sitio puede ser modificada en control de la lista canales a explorar. Vea la Figura V.34.

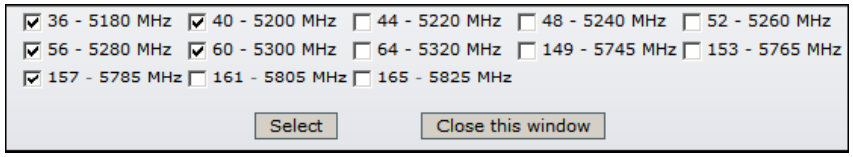

Figura V.34 Selección canales de exploración en NanoStation5

Lista de canales a explorar: Esto limitará la exploración solamente a los canales seleccionados. Las ventajas de esto son una exploración más rápida así como un mejor filtrado de los AP no deseados en los resultados. La herramienta de encuesta sobre el sitio buscará los puntos de acceso solamente en los canales seleccionados.

Administración de la lista de canales para seleccionar el modo IEEE 802.11 y el ancho específico del espectro de canal puede ser habilitado

seleccionando la opción habilitado (Enabled). Hay dos maneras de fijar la lista de exploración del canal: enumerando los canales requeridos (separados por coma) en el campo de entrada o usando el botón de editar (Edit). La herramienta de encuesta sobre el sitio buscará los puntos de acceso solamente en los canales seleccionados si la exploración o la función de encuesta sobre el sitio se realiza en modo estación.

Mantenerse en una MAC del AP: Esto permite que la estación se mantenga siempre conectada a un AP particular con una MAC específica. Esto es útil cuando hay algunos SSID con el mismo nombre (AP) con diversas direcciones MAC. Con la opción mantener en una MAC del AP activada, la estación se trabará a la dirección MAC y no pasará entre varios puntos de acceso con el mismo ESSID.

Código de País: Diferentes países tendrán diferentes niveles de energía y selección de frecuencia disponible. Para asegurar que la operación del dispositivo esté acorde a las regulaciones asegúrese de seleccionar correctamente el país en donde el dispositivo será utilizado. La lista de canales, los límites de potencia de salida, el IEEE 802.11 y los modos de anchura del espectro del canal serán fijados según las regulaciones del país seleccionado.

Modo IEEE 802.11: Éste es el estándar de radio usado para la operación de su dispositivo basado en AirOS. 802.11b es el modo 2.4GHz más antiguo mientras que el 802.11g (2.4GHz) y 802.11a (5GHz) son estándares más nuevos basados en una modulación ortogonal más rápida de la multiplexación de división de frecuencia (OFDM).

Anchura del espectro de canal: Este es el ancho espectral del canal de radio. Anchuras soportadas de canal inalámbrico:

5MHz - Es el espectro de canal con ancho de 5 MHz (conocido como modo de Cuarto-Tasa).

10MHz - Es el espectro de canal con ancho de 10 MHz (conocido como modo de Media-Tasa).

20MHz - Es la anchura estándar del espectro del canal (seleccionada por defecto).

40MHz - Es el espectro de canal más ancho requerido para conectarse con una red 802.11a (o en banda 3GHz) que soporta la función Turbo Estática.

La reducción de anchura espectral proporciona como ventajas:

Aumentar la cantidad de canales sin traslapo. Esto puede permitir que las redes escalen mejor.

Aumentará la densidad espectral de la energía del canal y permitirá una mayor distancia de enlace. Y como desventaja:

Reducirá el rendimiento proporcionalmente a la reducción de tamaño del canal. Entonces mientras que el modo turbo (40MHz) aumenta la velocidad posible dos veces, el medio canal de espectro (10MHz), disminuirá la velocidad posible a la mitad.

Desplazamiento del canal: Esta opción activa los canales especiales que están fuera de la frecuencia de los canales estándares 802.11b/g y 802.11a. Esta es una característica propietaria desarrollada por Ubiquiti. Mientras que las redes 802.11 tienen canales estándares, como canal 1 (2412MHz), el canal 2 (2417MHz), etc. espaciado por 5MHz, el desplazamiento de canal permitirá la operación de nuevos canales no-802.11 fuera de los canales estándar. Todos los canales se pueden modificar en intervalos de 5MHz (en el modo 802.11a y 3GHz) o 2MHz (en el modo 802.11b/g/b+g) desde la frecuencia central de canal por defecto.

Las ventajas de esto son el establecimiento de una red privada y seguridad inherente. Usando la opción de desplazamiento de canal, las redes se vuelven inmediatamente invisibles a millones de dispositivos de WiFi en el mundo.

Canal (Channel): Permite seleccionar el canal inalámbrico mientras que el dispositivo opera en modo de punto de acceso. Los canales múltiples de frecuencia están disponibles para evitar interferencia entre los puntos de acceso colindantes. La lista de canales varía dependiendo del código de país, del modo de IEEE 802.11, de la anchura del espectro del canal y de si la opción de desplazamiento del canal fue seleccionada. Vea la Figura V.35.

Figura V.35 Selección de canal inalámbrico en NanoStation5

Potencia de salida: Esto configurará la máxima potencia de salida de transmisión, promedio (en dBm) del dispositivo inalámbrico. El nivel de potencia de salida inalámbrica a la que el módulo inalámbrico transmite los datos puede ser especificado usando la barra deslizante. Al ingresar

el valor de potencia de salida manualmente, la posición de la barra deslizante cambiará según el valor ingresado. El máximo nivel de energía de transmisión está limitado según las regulaciones del país. Si el dispositivo basado AirOS tiene una antena interna (es decir NanoStation), la Potencia de salida es la potencia entregada a la antena interna.

La opción obedecer potencia regulatoria debe estar activa para forzar la potencia de salida en la transmisión de acuerdo con las regulaciones del país seleccionado. En este caso no será posible definir la energía isotrópica irradiada por sobre el máximo nivel permitido por la autoridad reguladora (diferentes niveles máximos y ganancia de la antena son permitidos por la autoridad reguladora de cada país para IEEE 802.11a/b/g).

Tasas de datos: Define las tasas de datos (en Mbps) a la cual el dispositivo debe transmitir los paquetes inalámbricos, ver figura V.36. Si se activa la opción auto, el algoritmo de tasas seleccionará la mejor tasa de datos dependiendo de las condiciones de la calidad del enlace. Si una tasa de datos por debajo de 54Mbps es seleccionada mientras que se activa la opción auto, entonces esta tasa definida será la máxima que podrá ser utilizada. Se utiliza la opción automático (auto) si se tiene problemas para conectarse o si la pérdida de datos es muy alta. En este

caso las tasas de datos más bajas serán usadas automáticamente por el dispositivo. En caso de utilizar un canal con espectro de 40MHz la tasa de datos máxima será 108Mbps.

Figura V.36: Tasa de datos

Seguridad inalámbrica: Esta sección permite determinar los parámetros que controlan cómo la estación del suscriptor se asocia a un dispositivo inalámbrico y el cifrado/descifrado de datos. Ver figura V.37.

Figura V.37 Ajustes de la seguridad inalámbrica

El método de seguridad debe seleccionarse según la política de seguridad del punto de acceso. La estación de suscriptor deberá estar autorizada por el punto de acceso para acceder a la red y todos los

datos de los usuarios transmitidos entre la estación de suscriptor y el punto de acceso serán encriptados, en el caso de utilizarse los métodos de seguridad inalámbrica.

Seguridad: AirOS soporta las siguientes opciones de seguridad WEP, WPA, y WPA2.

WEP se basa en el estándar IEEE 802.11 y utiliza el algoritmo de encriptación RC4. Activar WEP permite incrementar la seguridad cifrando los datos que son transferidos mediante la red inalámbrica. WEP es el algoritmo de seguridad más antiguo (fácilmente vulnerable).

WPA (Wi-Fi de acceso protegido), WPA(IEEE 802.11i/D3.0) y WPA2(IEEE 802.11i) administración de protocolo con llave pre-compartida ofrece métodos mejorados pues éstos son los nuevos protocolos creados bajo el estándar 802.11i para corregir vulnerabilidades de WEP.

WPA y WPA2 soporta los siguientes cifrados para la encriptación de datos:

TKIP Protocolo de integridad de la clave temporal utiliza algoritmo de encriptación RC4.

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) utiliza el algoritmo estándar de encriptación avanzado.

El dispositivo utilizará el cifrado más sólido (CCMP) en modo inalámbrico de estación y punto de acceso por defecto. Si CCMP no es soportado en el otro lado del vínculo, la encriptación TKIP será utilizada como en la situación cuando el dispositivo actúa como punto de acceso con la seguridad de WPA activada y por lo menos una estación inalámbrica (sin soporte CCMP) está conectado con este.

Tipo de autentificación: Este campo sólo se relaciona con la opción de seguridad WEP. Uno de los siguientes modos de autentificación debe ser seleccionado si se utiliza el método de seguridad WEP:

Autentificación abierta la estación es autentificada automáticamente por el AP (seleccionado por defecto).

Autentificación compartida la estación se autentifica después de superar el desafío, generado por el AP.

Longitud de llave WEP: La longitud de llave WEP de 64-bit (seleccionada por defecto) o 128-bit debe ser seleccionada si se utiliza el

método de seguridad WEP. La opción de 128-bit proporcionará un mayor nivel de seguridad inalámbrica.

Tipo de llave: La opción HEX (seleccionada por defecto) o ASCII define el formato de los caracteres para la llave WEP si se utiliza el método de seguridad WEP.

Llave WEP: La llave de encriptación WEP para la encriptación y la desencriptación del tráfico inalámbrico debe ser especificada si se utiliza el método de seguridad WEP:

Para **64-bit** especificar la llave WEP como 10 caracteres hexadecimales (0-9, A-F o a-f) (ej: 00112233AA) o 5 caracteres ASCII.

Para **128-bit** especificar la llave de WEP como 26 caracteres hexadecimales (0-9, A-F o a-f) (ej: 00112233445566778899AABBCC) o 13 caracteres ASCII.

Índice de llave: Permite especificar el índice de la llave WEP utilizado. 4 diferentes llaves de WEP se pueden configurar al mismo tiempo, pero se utiliza solamente una. La llave efectiva se fija con una opción de 1, 2, 3 o 4.

Autentificación WPA: se debe definir uno de los siguientes métodos de llave WPA si se utiliza el método de seguridad WPA o WPA2. Vea la Figura V.38.

Figura V.38 Seguridad WPA/WPA2 PSK

PSK WPA o WPA2 con el método de llave pre-compartido (seleccionado por defecto).

EAP WPA o WPA2 con método de autentificación EAP (protocolo de autentificación extensible) IEEE 802.1x. Este método es comúnmente usado en redes empresariales. Se debe considerar que: El GUI de administración Web de AirOS soporta solamente el método de autentificación EAP-TTLS.

Llave pre-compartida WPA (WPA Pre-shared Key): La frase de paso (pass phrase) para el método de seguridad WPA o WPA2 debe ser especificada si se selecciona el método de llave pre-compartida. La llave pre-compartida es una contraseña alfanumérica con un largo de entre 8 y 63 caracteres. Vea la Figura V.39.

Figura V.39 Seguridad WPA/WPA2 EAP

Identidad WPA: credenciales de identificación que son usadas por el solicitante para la autentificación EAP (EAP-TTLS), para lo cual se requiere nombre de usuario y contraseña.

MAC ACL: La lista de control de acceso de MAC, proporciona la capacidad de negar o permitir a ciertos clientes conectarse con el AP. El MAC ACL puede ser activado seleccionando la opción "Enabled". Existen dos maneras de determinar la lista de control de acceso MAC. Vea la Figura V.40:

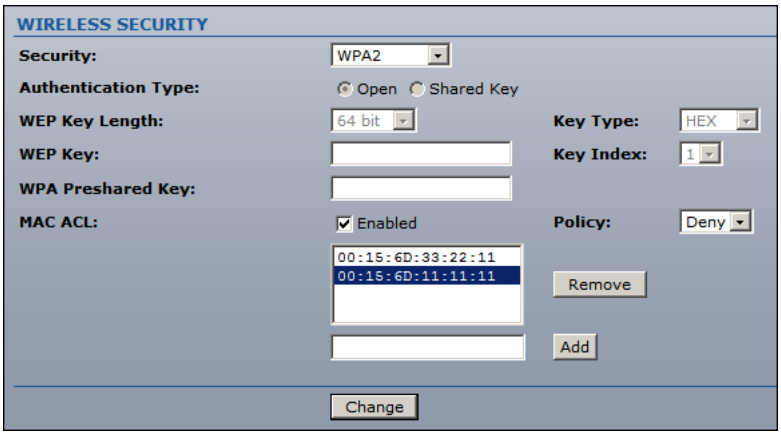

Figura V.40 Ajustes de seguridad inalámbrica del AP

Si la política del MAC ACL se fija a permitir (Allow). Permite que ciertos clientes inalámbricos en la lista puedan conectarse al punto de acceso mientras que será denegado para el resto de los clientes.

Si la política de MAC ACL se fija en rechazar (Deny). Entonces sólo negará el acceso a los clientes inalámbricos de la lista, y el resto de clientes mantendrá su acceso.

Las direcciones MAC de los clientes inalámbricos pueden ser agregadas y eliminadas usando los respectivos botones "add y remove". Presionando el botón Cambiar (Change) se guardan los cambios.

5.4 RED

La página de red permite al administrador fijar la funcionalidad de puente de enrutamiento. Los dispositivos basados en AirOS pueden operar en modo puente (Bridge) o enrutador (Router). La configuración IP debe ser especificada para propósitos de administración del dispositivo. Las direcciones IP se pueden obtener desde un servidor DHCP o configurar manualmente.

Modo de red: Especifica el modo de red en el cual opera el dispositivo. El modo depende de los requisitos de la topología de red. Vea la Figura V.41.

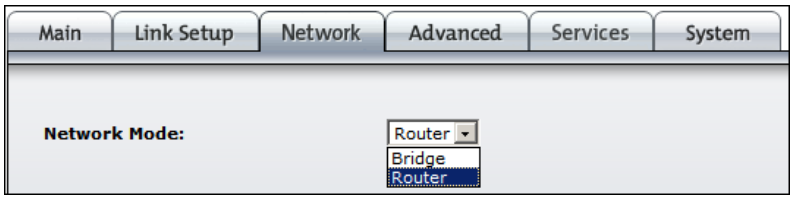

Figura V.41 Selección de modo de red AirOS

El modo de funcionamiento puente es seleccionado por defecto pues es ampliamente utilizado en las estaciones del suscriptor, mientras se conecta con un punto de acceso o usando WDS. En este modo el dispositivo actuará como puente transparente y funcionará en la capa 2. No habrá segmentación de la red mientras que el dominio de difusión sea igual. El modo puente no bloqueará ningún tráfico de difusión o multicast. Los ajustes adicionales del cortafuegos pueden configurarse para filtrado de paquete en la capa 2 y el control de acceso en modo de puente.

Al operar en modo enrutador puede ser configurado para funcionar en la capa 3 para realizar enrutamiento y para activar la segmentación de la red, los clientes inalámbricos estarán en diferentes subredes IP. El modo de enrutador bloqueará las difusiones mientras que no sea transparente. AirOS soporta el traspaso de paquetes multicast en modo enrutador.

El enrutador basado en AirOS puede actuar como un servidor DHCP y utilizar la característica de conversión de la dirección de red (NAT)

(Masquerading), la cual es ampliamente utilizada por los puntos de acceso. El NAT actuará como un cortafuego entre las redes LAN y WLAN. Los ajustes adicionales del cortafuegos pueden configurarse para la filtración de paquetes en la capa 3 y el de control de acceso en modo enrutador.

Deshabilitar red: Las opciones pueden utilizarse para deshabilitar la interfaz WLAN o LAN. Este ajuste deberá ser usado con el cuidado debido, ya que ninguna conexión Capa 2 o Capa 3 podrá ser establecida a través de la interfaz deshabilitada. Será imposible tener acceso al dispositivo basado AirOS a través de la interfaz inalámbrica o alámbrica que se encuentre deshabilitada. Vea la Figura V.42.

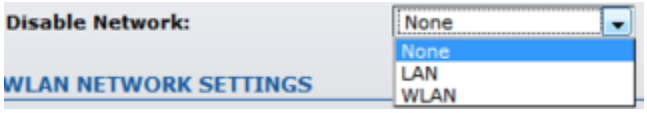

Figura V.42 Deshabilitar Red

5.4.1 Modo Puente

En modo puente el dispositivo basado en AirOS remite todos los paquetes de administración y de datos de la red desde una interfaz de red a la otra sin ningún enrutamiento inteligente. Para usos simples esto proporciona una solución de red eficiente y completamente transparente. Las interfaces WLAN (inalámbrica)

y LAN (Ethernet) pertenecen al mismo segmento de la red que tiene la misma dirección IP. Las interfaces WLAN y LAN forman la interfaz virtual que actúa como un puente entre los puertos. El puente ha asignado los ajustes de IP para los propósitos de administración, ver figura V.43.

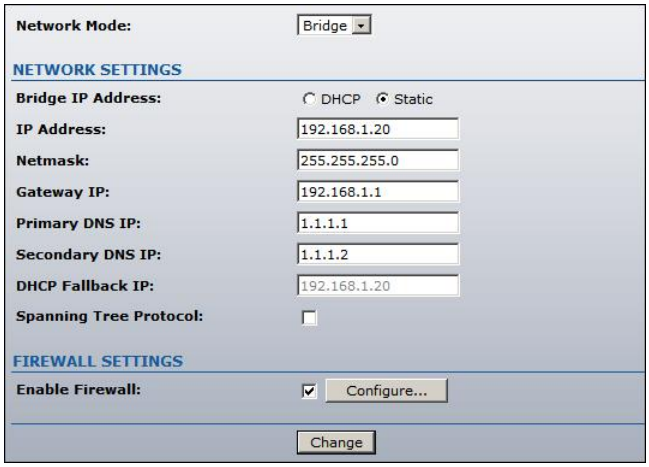

Figura V.43 Ajustes de red en modo puente

Dirección IP del Puente: El dispositivo se puede fijar para utilizar una dirección IP estática o para obtener una dirección IP del servidor DHCP al que está conectado.

Uno de los siguientes modos de asignación IP debe ser seleccionado:

DHCP esta opción permite asignar la dirección IP, la puerta de enlace y la dirección del DNS dinámicamente por el servidor local DHCP.

Estática (Static) esta opción sirve para asignar una dirección IP estática a la interfaz del puente.

Dirección IP: Escriba la dirección IP del dispositivo mientras que se selecciona el modo estático de dirección IP del puente. Esta IP será utilizada para los propósitos de administración del dispositivo AirOS. Los ajustes de dirección IP (IP Address) y de máscara de red (Netmask) deben coincidir con el rango de dirección del segmento de red donde se encuentra el dispositivo AirOS. Si los ajustes IP del dispositivo y la IP de la PC del administrador (la que está conectada con el dispositivo mediante una red alámbrica o inalámbrica) utilizan diferentes rangos de dirección, el dispositivo de AirOS no podrá ser accedido. Vea la Figura V.44.

Figura V.44 Modo puente con IP estática

Máscara de red (Netmask): Éste es un valor que cuando se amplía en binario proporciona un mapeo para definir cuál porción del grupo de direcciones IP pueden ser clasificadas como

dispositivos anfitrión (host) y dispositivos de red. La máscara de red define el rango de direcciones IP del segmento de red donde se encuentra el dispositivo AirOS. La máscara de red 255.255.255.0 (o /24) es comúnmente usada por muchas redes IP de clase C.

IP de la puerta de enlace: Típicamente, ésta es la dirección IP del enrutador anfitrión que proporciona el punto de conexión a la Internet. Esta puede ser un módem DSL, módem de cable, o un enrutador de la puerta de enlace de un WISP (Proveedor de Servicios de Internet Inalámbrico). El dispositivo AirOS dirigirá los paquetes de datos a la puerta de enlace si el anfitrión de destino no está dentro de la red local. La dirección IP de la puerta de enlace deberá encontrarse en el mismo segmento de red que el dispositivo AirOS.

IP primaria/secundaria de DNS: El Sistema de nombres de dominio (Domain Name System) es un directorio telefónico de la Internet que traduce los nombres de dominio a las direcciones IP. Estos campos identifican las direcciones IP del servidor de donde el dispositivo de AirOS busca información para la traducción. La dirección IP primaria del servidor de DNS debe ser especificada para los propósitos de la administración del dispositivo.

La dirección IP secundaria del servidor de DNS es opcional. Se utiliza como respaldo en caso de que el servidor DNS primario llegue a fallar.

DHCP IP de respaldo: En caso de que el puente se coloque en el modo de dirección IP dinámica (DHCP) y no pueda obtener una dirección IP de un servidor DHCP válido, recurrirá a la dirección IP estática. En caso de que las configuraciones IP del dispositivo basado en AirOS sean desconocidas pueden ser recuperadas con la ayuda de la utilidad del descubrimiento "UBNT_Discovery_Utility Ubiquiti". La utilidad multi-plataforma deberá ejecutarse en la PC del administrador que se encuentre en el mismo segmento de la red que el dispositivo AirOS. El sistema AirOS volverá a la configuración IP por defecto (192.168.1.20/255.255.255.0) si se inicia la rutina de volver a valores por defecto (Reset to defaults).

Protocolo Spanning Tree: Múltiples puentes interconectados forman redes más grandes usando el protocolo de expansión de árbol IEEE 802.1d (STP), el cual es utilizado para encontrar el camino más corto dentro de la red y eliminar loops (“vueltas”) de la topología.

Si la opción STP se activa, el puente de AirOS se comunicará con otros dispositivos de la red enviando y recibiendo unidades de datos del protocolo de puente. STP deberá ser desactivado cuando el dispositivo de AirOS es el único puente en la LAN o cuando no hay loops (lazos, entiéndase como vueltas) en la topología ya que en este caso no se justifica el uso de STP.

La funcionalidad de cortafuegos en la interfaz de puente puede ser activada usando la opción de "activar cortafuegos" (Enable Firewall). Las reglas del puente cortafuegos pueden ser configuradas, ser activadas o ser inhabilitadas usando la ventana de configuración del cortafuego, la cual se abre presionando el botón "configurar" (Configure). Vea la Figura V.45.

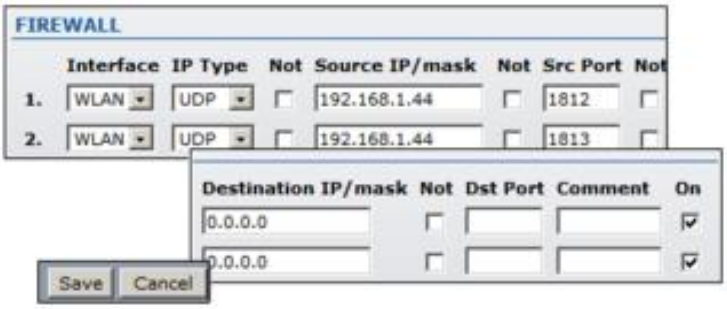

Figura V.45 Configuración del cortafuegos en modo puente

Las entradas del cortafuego pueden especificarse usando los siguientes criterios:

La interfaz (WLAN o LAN) donde se filtran los paquetes entrantes/(que pasan a través de) se procesan;

Tipo de IP determina un tipo de protocolo de Capa 3 en particular (IP, ICMP, TCP, UDP) que debe ser filtrado;

IP/máscara de origen es la IP de origen del paquete, generalmente es la dirección IP del sistema anfitrión (host system) que envía los paquetes;

El puerto de origen es el puerto de origen del paquete TCP/UDP, generalmente es el puerto del sistema anfitrión que envía los paquetes;

IP/máscara de destino es la dirección IP de destino del paquete, generalmente es la dirección IP del sistema a la cual se envían los paquetes;

El puerto de destino es el puerto de destino del paquete TCP/UDP, generalmente es el puerto del sistema al cual se envían los paquetes. Considerar que tanto: la IP/máscara de origen, el puerto de origen, IP/máscara de destino, el puerto de destino, deben ser especificados en la cabecera del paquete.

Los **"comentarios"** (Comments) es el campo informal para comentar una entrada en particular del cortafuego. Generalmente se guardan aquí unas pocas palabras acerca del propósito de la entrada en particular del cortafuego.

La bandera activa o inactiva determina el uso de una entrada en particular del cortafuego. Todas las entradas agregadas al cortafuego son guardadas en el archivo de configuración del sistema, no obstante solamente las entradas activadas del cortafuego serán funcionales durante la operación de sistema AirOS.

No hay operadores que puedan ser utilizados para invertir la IP/máscara de origen, el puerto de origen, IP/máscara de destino y criterios de filtración del puerto de destino (es decir, si no se activa el puerto de destino 443, los criterios de filtración serán aplicados a todos los paquetes enviados a cualquier puerto de destino excepto el 443 que es generalmente usado por HTTPS).

Las entradas de firewall recién agregadas al cortafuegos pueden ser guardadas presionando el botón de Guardar (Save) o pueden ser descartadas presionando el botón cancelar (Cancel) en la ventana de la configuración del cortafuegos. Todas las entradas

activas del cortafuegos se almacenan en el encadenado del cortafuegos de la tabla de filtro ebtables, mientras que el dispositivo está funcionando en modo puente.

5.4.2 Modo Enrutador

La función de la interfaz LAN y WLAN cambiará de acuerdo al modo inalámbrico que el dispositivo basado en AirOS adopte en modo de enrutador. Ver Figura V.46

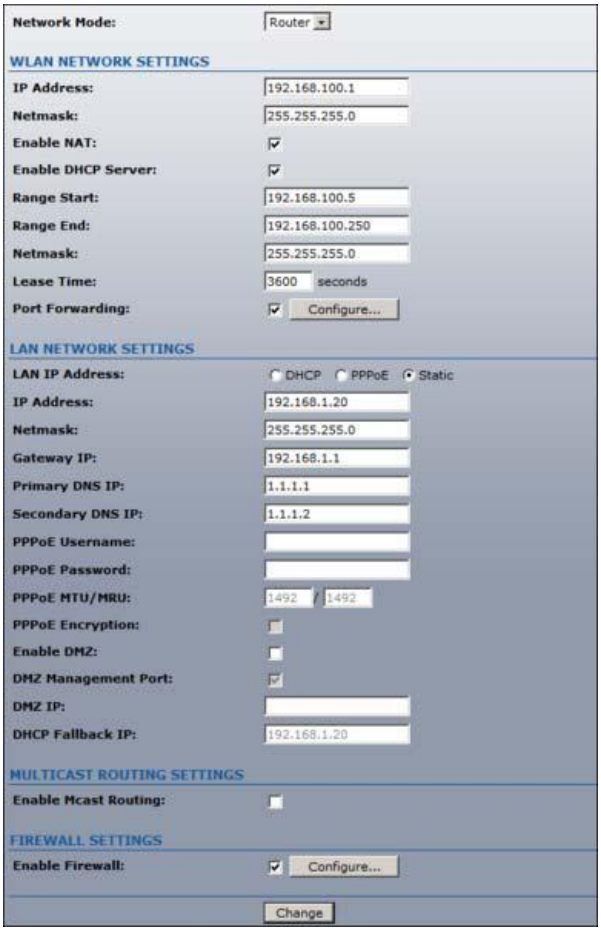

Figura V.46 Ajustes de red en el modo AP-Enrutador

- La interfaz inalámbrica y todos los clientes inalámbricos conectados son considerados parte de la LAN interna y la interfaz Ethernet se encuentra dedicada para la conexión con la red externa mientras que el dispositivo basado en AirOS funcione en modo inalámbrico de AP/APWDS.

- La interfaz inalámbrica y todos los clientes inalámbricos conectados son considerados como parte de la red externa; y todos los dispositivos de la red LAN, como la interfaz Ethernet en sí misma son considerados como la red interna, todo esto mientras que el dispositivo basado en AirOS opere en modo estación/estación WDS.

Los clientes inalámbricos/alámbricos son enrutados desde la red interna a la red externa por defecto. La funcionalidad de traducción de la dirección de red (NAT) funciona de la misma manera.

Dirección IP: Ésta es la dirección IP que tendrán las interfaces LAN o WLAN que está conectada con la red interna de acuerdo al modo de operación inalámbrico descrito anteriormente. Ésta será la IP utilizada para el enrutamiento de la red interna (será la IP de la puerta de enlace para todos los dispositivos conectados en la

red interna). Además ésta es la dirección IP que podrá ser usada para la administración del dispositivo basado en AirOs.

Dirección IP LAN/WLAN: Ésta es la dirección IP que tendrán las interfaces LAN o WLAN que está conectada con la red externa de acuerdo al modo de operación inalámbrico. Además es la dirección IP utilizada para el enrutamiento y la administración del dispositivo. La interfaz red externa puede ser definida para utilizar una dirección IP estática o para obtener una dirección IP desde el servidor DHCP, el cual debe encontrarse en la red externa. Uno de los modos de asignación IP deberá seleccionarse para la interfaz de red externa:

DHCP - PPPoE: para obtener la dirección IP, la puerta de enlace y la dirección DNS dinámicamente, desde un servidor externo sea este DHCP o PPPoE respectivamente.

Estática: para asignar los ajustes IP estáticamente para la interfaz externa.

Aliasing automático de IP una vez activada esta opción, configurará automáticamente la dirección IP generada para la interfaz WLAN/LAN según corresponda. La dirección IP generada

es una única dirección IP de clase B del rango 169.254.X.Y (máscara de red 255.255.0.0) la que es reservada solamente para el uso de un mismo segmento de red. La IP automática siempre comienza con 169.254.X.Y mientras que X y Y son los 2 últimos dígitos de la dirección MAC del dispositivo (es decir si la MAC es 00:15:6D:A3:04:E1:FB, entonces la IP única generada será 169.254.4.251).

Activar el NAT: La conversión de dirección de red habilita los paquetes que serán enviados desde la red alámbrica (LAN) a la dirección IP de la interfaz inalámbrica y luego sub-enrutará hacia los otros dispositivos clientes que se encuentren en la red local, y de forma inversa. El NAT es implementado usando las reglas del tipo "masquerade" en el cortafuego. Las entradas NAT en el cortafuego son almacenadas en la tabla nat del iptables, en caso que el dispositivo esté funcionando en modo enrutador. Las rutas estáticas deben ser especificadas en el orden que los paquetes pasan a través del (pass-through) dispositivo si es que el NAT se deshabilita mientras que opera en modo de enrutador.

Habilitar el servidor DHCP: El servidor DHCP asigna las direcciones IP a los clientes que se conectan a la interfaz inalámbrica del dispositivo.

Comienzo/Fin del rango: Se determina el rango de direcciones IP que el servidor DHCP ofrecerá a los dispositivos clientes en una red interna que utilizan la configuración IP dinámica.

Tiempo de concesión: Las direcciones IP otorgadas por el servidor DHCP sólo serán válidas por un período específico. Aumentando el tiempo de concesión se asegura la operación del cliente sin interrupciones, pero podría provocar conflictos potenciales. Disminuyendo el tiempo de concesión se evitarán conflictos de la dirección IP, pero podrá causar leves interrupciones al cliente mientras que renueve su dirección IP en el servidor DHCP. Vea la Figura V.47.

Figura V.47 Rango del servidor DHCP y Tiempo de concesión

Direccionamiento de puertos (Port Forwarding): Esta función permite que los puertos específicos de los anfitriones que se encuentran en la red interna puedan ser direccionados a la red exterior. Esto es útil para aplicaciones como servidores de ftp, juegos, etc., donde varios sistemas huéspedes (host system) necesitan utilizar una única dirección IP/puerto común.

PPPoE: El Protocolo Punto a Punto sobre Ethernet es una conexión virtual privada y segura entre dos sistemas, en la cual se activa el transporte de datos encapsulados vía túnel. Es comúnmente usado como el medio para que los suscriptores se conecten con los proveedores de servicios de internet (ISP).

Activar (DMZ): La zona desmilitarizada (DMZ) puede ser activada y utilizada como un lugar en donde se puede poner ciertos servicios como por ejemplo: servidor web, servidor proxy, y servidores de email, permitiendo así que estos servicios puedan servir a la red local y al mismo tiempo estén aislados de ella para una seguridad adicional. DMZ es comúnmente usada con la funcionalidad NAT como una alternativa para el direccionamiento de puertos, el cual hace que todos los puertos del dispositivo DMZ de la red sean visibles desde el lado externo de la red.

5.5 AVANZADO

En esta sección se maneja los ajustes de enrutamiento avanzado y ajustes inalámbricos. Vea Figura V.48

Las tasas de datos 802.11 incluyen 1, 2, 5.5, 11Mbps para el modo IEEE 802.11b y 6, 9, 12, 18, 24, 36, 48, 54Mbps para el modo IEEE

802.11a/g. El algoritmo de la tasa tiene un impacto crítico en el rendimiento de enlaces al aire libre pues generalmente tasas de datos más bajas son más inmunes al ruido, mientras que tasas más altas son más susceptibles, pero son capaces de lograr un rendimiento más alto.

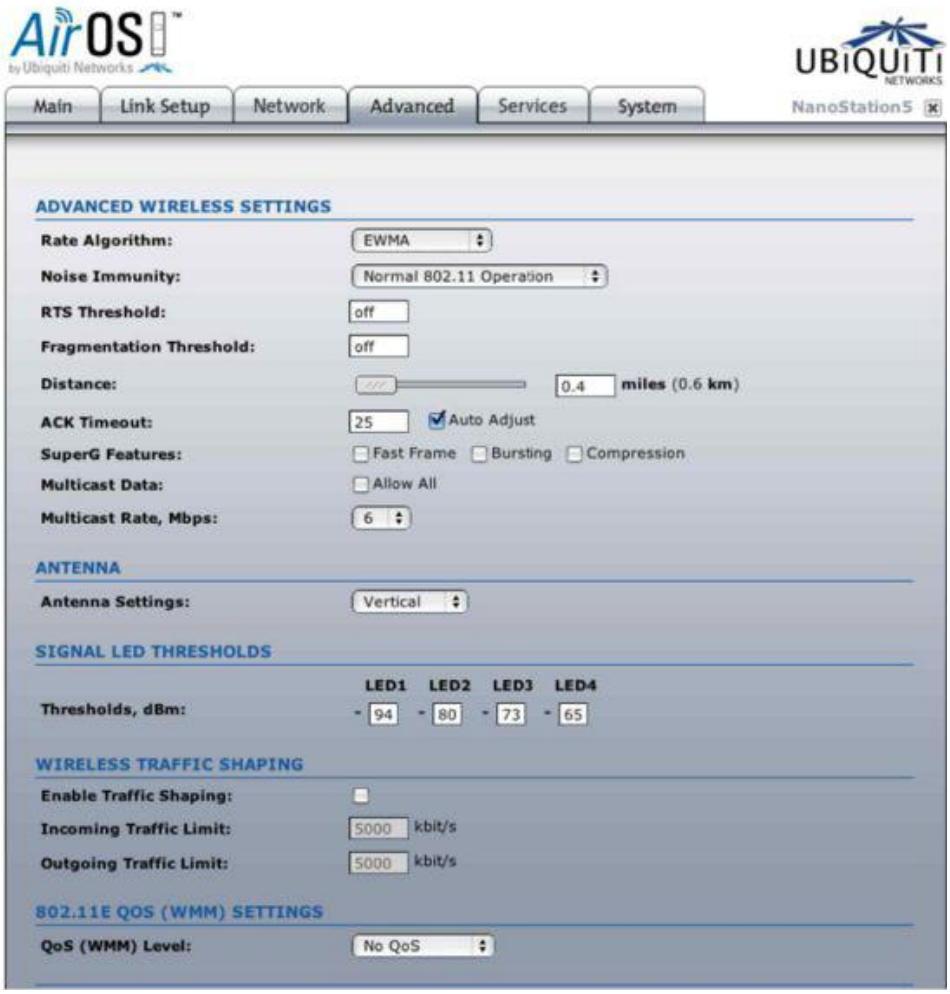

Figura V.48 Configuraciones inalámbricas avanzadas

Algoritmo de la Tasa: define la convergencia del algoritmo de la tasa de datos:

El Algoritmo Optimista es lo bastante agresivo para moverse hacia una tasa más alta pero también trata de manera precautoria de analizar las fluctuaciones del RSSI. Comienza con la tasa de datos más alta posible y después disminuye hasta que la tasa puede ser soportada, además periódicamente transmite los paquetes a tasas más altas y analiza el tiempo de transmisión. El algoritmo optimista siempre trata de alcanzar el rendimiento más alto mientras que sacrifica la inmunidad al ruido y robustez.

El algoritmo conservador es menos sensible a la falla de paquetes individuales pues se basa en una función del número de paquetes correctamente y erróneamente transmitidos/retransmitidos durante un período de muestra. Reduce a una tasa más baja después de una continua falla de paquetes e incrementa la tasa luego de un número de paquetes acertados. El algoritmo conservador de tasa proporciona la mejor estabilidad/robustez, pero puede comprometer un poco el rendimiento. Se recomienda seleccionar el algoritmo conservador de tasa cuando la fuerza de la señal es baja debido al ambiente ruidoso o la distancia del enlace.

El algoritmo EWMA trata de moverse a una tasa más alta pero continuamente monitorea los contadores de falla de paquetes. El Exponential Weighted Moving Average Algorithm es un híbrido entre el

algoritmo conservador y el optimista. Es el aconsejado para ser usado en la mayoría de los casos en redes inalámbricas.

La opción de inmunidad al ruido aumenta la robustez con la que el dispositivo funciona en ambientes con gran ruido, el cual generalmente es generado por fuentes externas de tráfico, señales de canal sobrepuesto y otras interferencias.

Umbral RTS: Determina el tamaño de paquete en una transmisión y, con el uso de un punto de acceso, ayuda al control del flujo de tráfico. El rango es entre 0 y 2347bytes, o la palabra "OFF". El valor por defecto es 2347 que significa que RTS está desactivado.

RTS/CTS (Request to Send / Clear to Send) es el mecanismo usado por el protocolo de red de una red inalámbrica para reducir las colisiones de cuadros introducidas por problemas de un terminal oculto. El umbral del tamaño de paquetes RTS/CTS está entre 0 y 2347bytes. Si el tamaño de paquete que el nodo quiere transmitir es más grande que el umbral, detendrá los paquetes. Si el tamaño del paquete es igual a o inferior que el umbral, los datos serán enviados inmediatamente. El sistema usa la petición de Enviar/Limpiar (Send/Clear) para enviar cuadros de datos para el establecimiento el cual provee una reducción en la colisión para el punto de acceso con estaciones ocultas. Las estaciones primero

envían un cuadro RTS mientras que los datos son enviados sólo después que el establecimiento con el punto de acceso se complete. Las estaciones responden con el cuadro CTS al RTS que proporciona los medios limpios para que la estación solicitante envíe los datos.

Administración de colisiones CTS tiene un intervalo de tiempo durante el cual hace que todo el resto de las estaciones suspendan momentáneamente sus transmisiones y esperen hasta que la estación solicitante termine la transmisión.

Umbral de fragmentación: Especifica el tamaño máximo de un paquete antes que los datos se fragmenten en múltiples paquetes. El rango es entre 256 y 2346 bytes, o la palabra "Apagado" (Off). Ajustes del umbral de fragmentación demasiado bajos puede provocar un mal rendimiento de la red. El uso de la fragmentación puede aumentar la confiabilidad de las transmisiones de cuadros. Ya que al enviar cuadros más pequeños, es mucho menos probable que ocurran colisiones. Se recomienda no modificar o modificar muy levemente estos valores, ya que el valor por defecto 2346 es el óptimo en la mayoría de las redes inalámbricas.

Distancia: Define el valor de la distancia en millas (o kilómetros) mediante la barra o ingresando el valor manualmente. La fuerza de la

señal y el rendimiento decaen con la distancia. Cambiar el valor de distancia modificará el intervalo ACK al valor adecuado para la distancia especificada.

Intervalo ACK: Especifique el intervalo ACK. Cada vez que la estación recibe un cuadro de datos envía un cuadro ACK al AP (si es que no hubo errores de transmisión). Si la estación no recibe ningún cuadro ACK desde el AP dentro del intervalo especificado, éste volverá a reenviar el cuadro. Las fugas de rendimiento son causadas porque muchos cuadros deben ser reenviados, así si el intervalo se fija demasiado corto o demasiado largo, resultará en un funcionamiento una conexión mala y bajo procesamiento de datos.

Ajustes de la Antena: Los dispositivos basados en AirOS tienen la opción de cambiar la polaridad de la antena con un simple control en la administración Web. Esto se logra utilizando la tecnología de Polaridad de Antena Adaptativa cuya patente pertenece a Ubiquiti. Vea la Figura V.49:

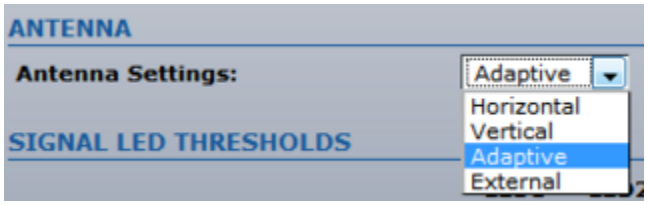

Figura V.49: Configuración de polaridad de la antena

La polaridad **vertical** y **horizontal** de la antena es la configuración que generalmente se utiliza;

El **modo adaptativo** de antena selecciona la mejor polaridad dinámicamente. Este modo permite cambiar las polaridades dinámicamente, en el acto, para mejorar el rendimiento en entornos altamente ruidosos;

La **opción de antena externa** permite la conexión de una antena de mayor ganancia conectada al puerto correspondiente del dispositivo.

Umbrales de los LED: Los LED en la parte posterior del dispositivo pueden ser usados para ver los valores de señal recibida de acuerdo con los valores definidos en los siguientes campos. Esto permite que un técnico instale fácilmente un CPE sin ingresar a la configuración web de la unidad (para alinear la antena).

Los umbrales de la señal LED especifican el valor marginal de la intensidad de señal (en dBm), los LED se encenderán si alcanzan el valor fijado en este campo. Vea la Figura V.50:

Figura V.50: Configuración de umbrales de los LED

Ejemplo de configuración: Si la Intensidad de señal (mostrada en la página principal) fluctúa alrededor de -63 dBm, los umbrales del LED pueden fijarse en los valores -70, -65, -62, -60. El signo "-" no debe utilizarse para especificar el valor de la Intensidad de señal, es decir, si se quiere fijar -70 dBm, entonces escriba 70.

Modificación de tráfico inalámbrico: Esta característica es usada para controlar el ancho de banda de subida y de bajada, basado en una tasa limitada por el usuario. Esto es QoS de capa 3.

Wi-Fi Multimedia (WMM) es un componente del estándar inalámbrico IEEE 802.11e para la calidad de servicio. El QoS asigna prioridad al tráfico de red seleccionado, previene las colisiones de paquetes y retrasos para así mejorar la calidad en las llamadas VOIP y ver vídeos sobre WLANs. 802.11e/WMM permite mejorar la latencia para usos de voz y vídeo.

5.6 SERVICIOS

Esta página permite la configuración de servicios de administración de sistema SNMP y Ping Watchdog.

El ping watchdog se fija para que el dispositivo realice continuamente un ping a una dirección IP definida por el usuario (por ejemplo puede ser la

puerta de enlace de Internet). Si el ping no obtiene respuesta dentro de los parámetros definidos, el dispositivo se reiniciará automáticamente. Esta opción crea una especie de mecanismo de anti-fallas.

El protocolo monitoreo de red simple es usado en sistemas de administración de red para supervisar los dispositivos adjuntos a la red para condiciones que necesiten atención administrativa garantizada. AirOS contiene un agente SNMP que permite comunicarse con una aplicación de administración SNMP que controle la red.

El agente SNMP proporciona una interfaz para el dispositivo de monitoreo usando el Simple Network Management Protocol (un protocolo de capa de aplicación que facilita el intercambio de información de administración entre los dispositivos de la red). El agente SNMP permite que los administradores de la red supervisen el funcionamiento de la red, encuentren y solucionen problemas en la misma. Para facilitar la identificación del equipo, es recomendable siempre configurar el agente SNMP con un contacto e información de localización. Vea Figura V.51

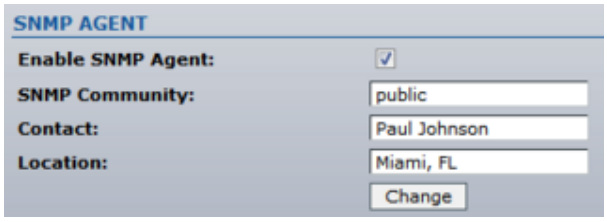

Figura V.51 Configuración Agente SNMP

5.7 SISTEMA

Esta página permite al administrador modificar, reiniciar el equipo, volver a los valores por defecto, subir un nuevo firmware, respaldar o actualizar la configuración y los ajustes de las credenciales de administrador.

Firmware: esta sección permite conocer la versión actual del programa y la opción de actualizar el dispositivo con un nuevo firmware. La actualización de firmware del dispositivo es compatible con todos los ajustes de configuración.

El botón de **Upgrade** deberá presionarse para iniciar la rutina de actualización de firmware la cual puede tomar entre 3 y 7 minutos. El dispositivo será inaccesible hasta que finalice el proceso de upgrade del firmware. Se debe tomar en cuenta las siguientes consideraciones:

- No se debe apagar, reiniciar o desconectar de la electricidad el dispositivo durante el proceso de upgrade del firmware, ya que esto ocasionará un daño al dispositivo.

- Es altamente recomendable realizar un respaldo del sistema antes de subir la nueva configuración.

Cuenta de administrador: Permite modificar la contraseña del administrador para proteger el dispositivo contra configuraciones no autorizadas. La contraseña por defecto del administrador deberá ser cambiada en la primera configuración del sistema.

Contraseña actual: Se requiere del administrador para ingresar la contraseña actual. Se requiere para la rutina de cambio de la contraseña o del nombre de usuario del administrador. Credenciales de acceso por defecto de administrador:

* Nombre de usuario (User Name): ubnt
* Contraseña (Password): ubnt

Idioma de la interfaz: AirOs soporta múltiples idiomas en la interfaz Web de administración. Las opciones de idioma cambian la vista y la sensación de la interfaz web de administración, mientras que renombran las etiquetas de todos los ajustes de configuración y los controles de acuerdo al idioma de traducción en particular.

Mantenimiento del dispositivo: Los controles en esta sección son utilizados para las rutinas de mantenimiento del dispositivo: **Reinicio** (rebooting), volver a los valores por defecto, generación de informes de información de soporte.

CAPITULO VI

IMPLEMENTACIÓN DEL RADIO ENLACE

En este capítulo se va a describir el proceso de diseño de la red. Empezando con unas consideraciones previas acerca de la geografía, y siguiendo luego con aspectos tecnológicos: como el diseño y ubicación del radioenlace y el direccionamiento de la red.

6.1 RADIOFRECUENCIA

Así como la infraestructura existente en la zona (Riobamba), existe otro factor que debe ser considerado, las propiedades que presenta la región

desde un punto de vista de propagación de ondas y de radiocomunicaciones.

Como lo expuesto anteriormente, cuanta más alta es la frecuencia de una onda, mayor será la velocidad con la que se transmitirá la información. Sin embargo se ve reducido su alcance y su capacidad de atravesar objetos sólidos. A continuación se analizan los aspectos más relevantes:

6.1.1 Línea de Vista y Claridad

El primer inconveniente que se plantea en el tipo de entorno en el cual se trabaja es la necesidad de línea de vista. Se entiende por línea de vista, no solamente la posibilidad de "observar" el otro emplazamiento sino además el tener la primera zona de Fresnel despejada en, al menos, un sesenta por ciento.

Puede ocurrir que dentro de la zona geográfica exista la presencia de copas de árboles, edificios en construcción, los cuales estén demasiado cerca de la ubicación de los equipos y por tanto lleguen a interponerse en el camino de estos.

Además se debe considerar que se necesita una claridad de veinte metros como mínimo desde cualquiera de los lados del enlace.

Se define claridad como la distancia mínima entre la línea que une las dos antenas/equipos con el objeto (árbol, loma, edificio…) más cercano a ésta. En otras palabras, siempre debe existir un mínimo de veinte metros "despejados" desde la línea de vista y el objeto más alto.

6.1.2 Reflexión, difracción y atenuación

De estos tres fenómenos el que tendrá más incidencia va a ser la atenuación, debido a la vegetación y al clima de la zona. Pudiendo encontrar reflexión y difracción aunque no como principales problemas.

Atenuación: Lluvias, viento, árboles, edificios.

Cuando las ondas electromagnéticas atraviesan algún material generalmente se debilitan o atenúan. La cantidad de potencia absorbida dependerá de la frecuencia de la onda y por supuesto del material que atraviese.

La presencia de lluvias fuertes, nubes bajas, niebla y vapor de agua son factores que añaden una atenuación nada despreciable al enlace.

Reflexión: Los tejados

Dada la poca densidad de población en la zona, no existe demasiada presencia de edificaciones que puedan provocar una reflexión, ni cercana ni lejana, con lo que el efecto de propagación multicamino disminuye y no causa los problemas que sí pueden provocarse en entornos urbanos.

Difracción: Dado que se trata siempre de conseguir un apuntamiento directo entre equipos/antenas, no hay necesidad (ni tampoco posibilidad) de que las ondas se difracten en picos de montañas o árboles, o en alguna esquina de un edificio. Por esta razón la repercusión de este efecto se estima poco importante.

6.2 ZONA DE FRESNEL

La zona de fresnel es la altura ideal (radio) en la cual se deben posicionar el nodo y CPE para poder realizar un enlace confiable dependiendo de la frecuencia y la distancia.

La zona de fresnel se considera también como una zona de despeje adicional que hay que tener en consideración en un enlace punto a punto (Figura VI.52), además de la visibilidad

directa entre las dos antenas. Este factor deriva de la teoría de ondas electromagnéticas, respecto de la expansión de las mismas al viajar en el espacio libre. Esta expansión resulta en reflexiones y cambios de fase al pasar por un obstáculo. El resultado es un aumento o disminución en el nivel de intensidad de la señal recibida.

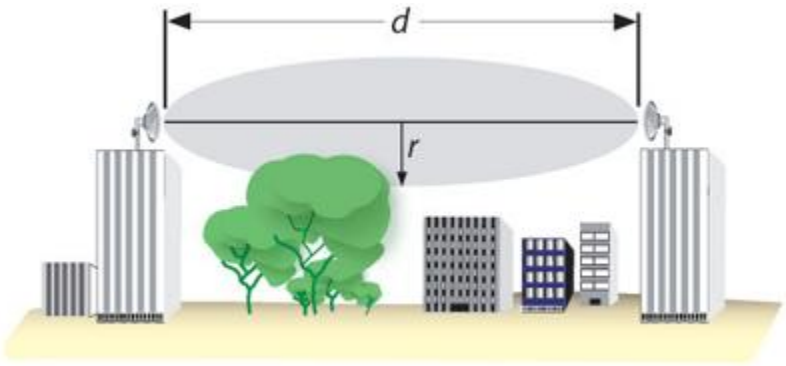

Figura VI.52 Zona de Fresnel

La obstrucción máxima permisible para considerar que no existe obstrucción es el 40% de la zona de Fresnel. La obstrucción máxima recomendada es el 20%. Para establecer las zonas de Fresnel primero debemos determinar la línea de vista, que en términos simples es una línea recta entre la antena transmisora y la receptora. Vea Figura VI.52.

Se puede aplicar la siguiente fórmula, en caso de no tener ningún obstáculo que interfiera entre emisor y receptor:

$$r = 17.32 \sqrt{\frac{D}{4f}}$$

Para el cálculo del radio de la enésima zona de Fresnel, con intervención de algún objeto entre emisor y transmisor, se aplica la siguiente fórmula:

$$r_n = 548 \sqrt{\frac{n \cdot d_1 \cdot d_2}{f \cdot D}}$$

Donde:

r = radio [m]

r_n = radio de la enésima zona de Fresnel [m]

d1 = es la distancia desde el transmisor al objeto en [Km]

d2 = es la distancia desde el objeto al receptor en [Km]

D = es la distancia total del enlace en [Km]

f = es la frecuencia en [MHz]

6.3 INSTALACIÓN DE LOS EQUIPOS NANOSTATION5

El enlace punto a punto, se encuentra instalado en las Ciudadelas Sultana de los Andes y Álamos, del cual se obtuvo la siguiente información, ver Figura VI.53.

Figura VI.53 Distancia del enlace entre AP y Cliente

Mediante el uso del GPS (Sistema de Posicionamiento Global), se obtuvo la siguiente información detallada en la Tabla VI.5

Tabla VI. 5 Ubicación GPS de los equipos

Puntos	Ubicación	Latitud	Longitud	Altura
AP	Sultana de los Andes	1º39'30.88"	78º40'28.31"	2875m
Cliente	Álamos	1º38'58.27"	78º40'05.31"	2849m

Verificar Línea de Vista

Uno de los factores principales para establecer el enlace es el verificar la existencia de línea de vista directa entre los dos puntos, para proceder a la instalación física de los equipos, vea Figura VI.54.

Figura VI.54 Línea de Vista

Cálculo de la zona de fresnel

Al no tener ningún obstáculo que interfiera entre emisor y receptor se realiza el cálculo aplicando su fórmula:

Datos:

$$r = 17.32 \sqrt{\frac{D}{4f}}$$

La distancia calculada entre los dos puntos es igual a 1050 m, y la frecuencia utilizada para su operación es 5180MHz, teniendo estos datos se procede a realizar el cálculo de la primera Zona de Fresnel.

$$r = 17.32 \sqrt{\frac{1050}{4\,(5180)}}$$

$$r = 3.9m$$

Una vez comprobados los factores principales que inciden en la implementación del Radio Enlace, se procede a instalar los equipos NanoStation5, en el punto mejor ubicado y que se encuentre libre de interferencias, que puedan afectar el rendimiento óptimo del enlace. Vea Figura VI.55.

AP Cliente

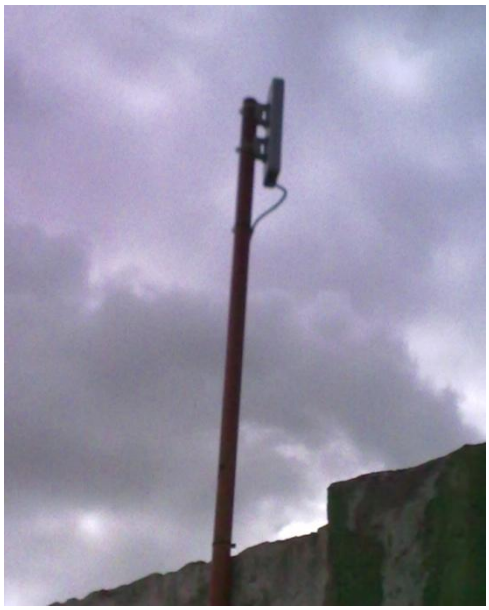

Figura VI.55 Instalación Equipos

6.4 CONFIGURACIÓN DE EQUIPOS

Considerar que este escenario es válido siempre que exista visión directa entre los dos puntos. El cual se va a implementar partiendo de dos puntos distantes en la ubicación indicada anteriormente, en el que uno de ellos asocia un PC que dispone de la Base de Datos y se requiere unirlo con otro punto remoto para poder compartir los recursos del primero y poder establecer una comunicación que permita la transmisión de la información.

Se requiere de dos equipos Ubiquiti modelo NanoStation5, para establecer conexión entre los puntos, dependiendo de la frecuencia en la que se va a operar. Los equipos tanto el Punto de Acceso como la estación son configurados en modo WDS. A continuación se observa un esquema detallado de instalación, donde aparecen todos los elementos comentados. Ver Figura VI.56

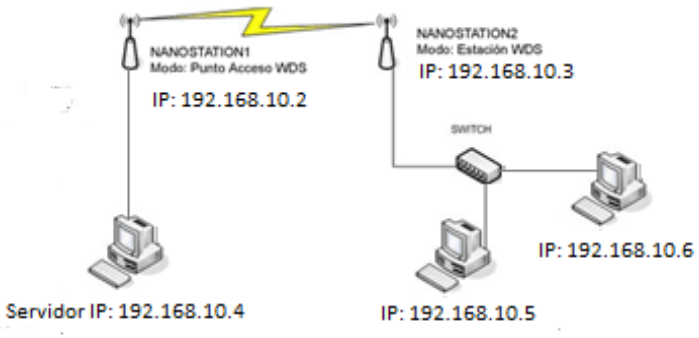

Figura VI.56 Esquema de Instalación

En el esquema se aprecia las configuraciones, pero de todas formas se detalla para que no exista lugar a errores.

Primero se configura el equipo NanoStation1 como Punto de acceso WDS, se asigna la dirección IP y se fija el SSID.

Configuración del NanoStation1:

Ingreso al Sistema de Gestión Web

Acceda al navegador del computador y escriba en la barra de direcciones la dirección IP del dispositivo, de la siguiente forma http://192.168.1.20, esta es la dirección IP por defecto de los dispositivos Ubiquiti.

Luego aparecerá una ventana que solicita ingresar las credenciales para iniciar sesión (Vea Figura VI.57):

Nombre de Usuario (User Name): ubnt
Contraseña (Password): ubnt

Una vez que se autentifique como administrador, se accede a la Página Principal (Main Page) en la interfaz de gestión Web.

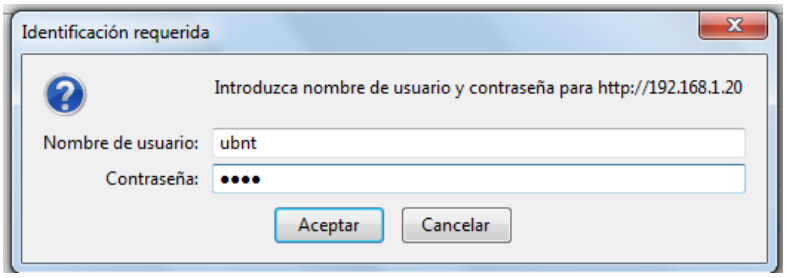

Figura VI. 57 Identificación requerida

Considerar que la computadora debe estar pre-configurada con una dirección estática de la subred 192.168.1.0 (con máscara de red 255.255.255.0) para poder establecer la conexión con el dispositivo en el mismo segmento físico de red. Como recomendación se puede utilizar la dirección IP 192.168.1.10.

Configuración del Enlace (Link Setup): Dentro del menú se especifica los siguientes parámetros:

Tabla VI.6 Parámetros de Configuración AP

Modo Inalámbrico	Punto de Acceso WDS
SSID	SOLUCIONES
Código de País	Ecuador
Modo IEEE 802.11	A
Anchura del Espectro	20 MHz
Canal	36
Seguridad	WPA

Configuración de red

La configuración IP es necesaria para los propósitos de administración del dispositivo. Estas direcciones pueden obtenerse desde un servidor DHCP o ser configuradas manualmente. Para la configuración de los parámetros IP se debe acceder al menú de red y especificar las siguientes opciones:

Modo de red (Network Mode): Seleccione el modo de operación Bridge (Puente). Este modo está seleccionado por defecto en el dispositivo.

Escoja el tipo de dirección IP del Bridge, sea este en modo DHCP o Estática (Static). Dependiendo del modo elegido se asignan las direcciones IP correspondientes al dispositivo. Para la implementación se opta por direcciones estáticas (Vea Fig.VI.58).

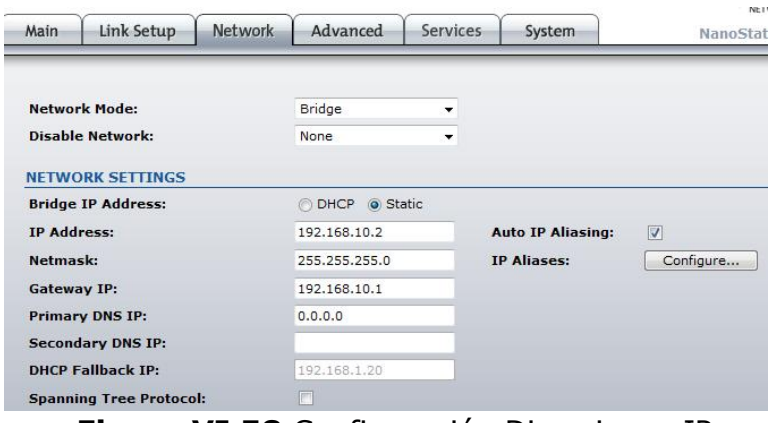

Figura VI.58 Configuración Direcciones IP

Definir el modo de seguridad inalámbrica

El método de seguridad debe seleccionarse de acuerdo a la política de seguridad del Punto de Acceso. La Estación cliente deberá ser autorizada por el Punto de Acceso (AP) para poder obtener acceso a la red, además toda la información trasferida entre el usuario y el AP será encriptada con el método de seguridad inalámbrica WPA.

Cambiar las credenciales de administrador

Por razones de seguridad las credenciales (nombre de usuario y contraseña) de administrador deberán ser cambiadas de manera inmediata una vez que sea configurado el equipo.

Dentro del menú sistema se especifican estos parámetros, ver figura VI.59.

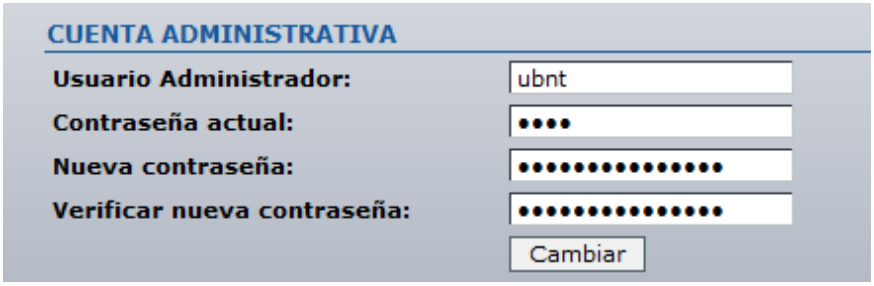

Figura VI.59 Cuenta Administrativa

Aplicar los cambios

Después de cada cambio de configuración aparecerá un mensaje avisando de la necesidad de aplicar los cambios y reiniciar el dispositivo. Presione el botón de **Aplicar** (Apply) para efectuar los cambios y reiniciar el dispositivo (Este paso se aplica tanto al AP como a la Estación).

Una ventana desplegable mostrará una barra con el progreso de la tarea, vea Figura VI.60.

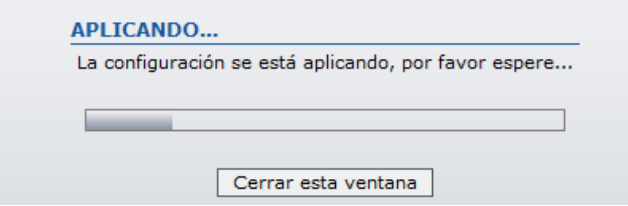

Figura VI.60 Aplicando cambios

Después de la configuración de los parámetros generales el dispositivo estará listo para su operación básica. La interfaz Web podrá ser utilizada en futuras ocasiones para nuevas modificaciones.

Una vez configurado el primer dispositivo como **"Punto de Acceso WDS"** se procede a configurar el segundo como **"Estación WDS"** de la manera que se muestra en el siguiente punto.

Configuración del NanoStation2:

De igual forma que el AP, se accede al dispositivo con su dirección por defecto http://192.168.1.20, y se toma en cuenta los siguientes parámetros de configuración:

Tabla VI.7 Parámetros de Configuración Cliente

Modo Inalámbrico	Estación WDS
SSID	SOLUCIONES
Código de País	Ecuador
Modo IEEE 802.11	A
Anchura del Espectro	20 MHz
Canal	36
Seguridad	WPA
Dirección IP	192.168.10.3

Una vez configurados los dos equipos uno como "Punto de Acceso" y el otro como "Estación WDS", lo único que se debe hacer es comprobar que se hayan enlazado y alinearlos para su correcto funcionamiento. Para comprobar que se hayan enlazado y conectado tenemos que acceder a la pestaña **"MAIN"** del NanoStation que está configurado como **"Estación WDS"** por ejemplo, y observar los valores de fuerza de señal. Vea Figura VI.61.

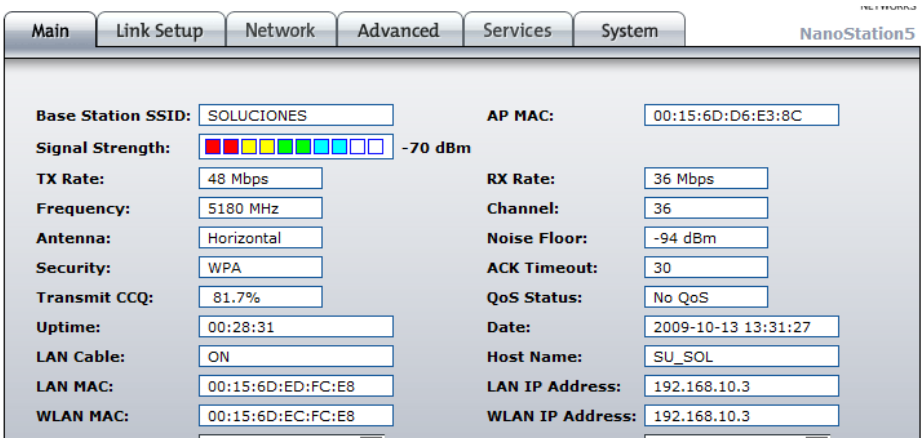

Figura VI.61 Fuerza de Señal

Los valores para establecer un enlace operativo que permita establecer la Transmisión de la Información, se encuentran comprendidos entre **"-85dbm y -65dbm",** inferiores a -85dbm causarán un posible corte en el enlace. Valores por encima de -65dbm indican un exceso de señal y causarán un comportamiento anómalo en el dispositivo. Se requiere ajustar la potencia de salida hasta conseguir estos valores de enlace.

Una vez comprobado que los equipos se hayan enlazado y estén conectados, se procede a alinear los equipos lo mejor posible y comprobar que los dispositivos instalados y configurados funcionan correctamente.

El siguiente paso y último, es ajustar los parámetros para obtener los mejores rendimientos. Se ha de ajustar la polaridad y distancia entre los puntos para un óptimo funcionamiento.

Moviendo la barra de Distancia según convenga **ajustándola a la Distancia Real** (en el menú Advanced). Realizado estos pasos queda comprobar el funcionamiento del enlace.

Para ello se abre una consola de MS-DOS (usando el comando cmd), y desde uno de los dispositivos se hará un **"ping"** a la dirección IP (192.168.10.2) del propio dispositivo y a la del otro dispositivo (192.168.10.3) y si todo funciona correctamente se obtendrá respuesta por parte de los dos, vea Figura VI.62.

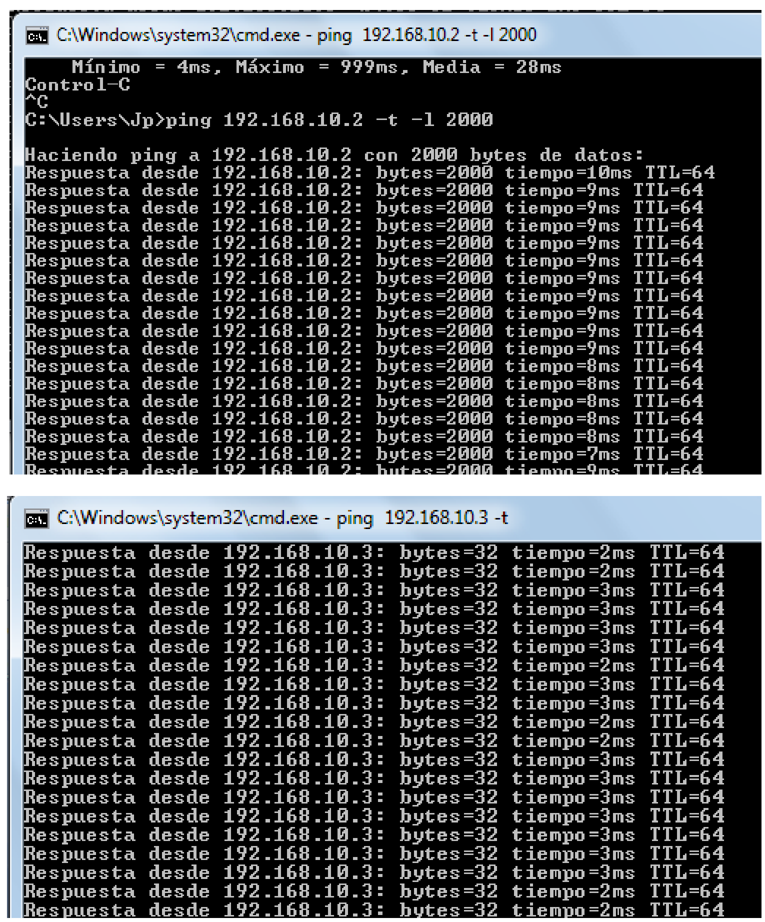

Figura VI.62 Enlace funcionando satisfactoriamente

6.5 INGRESO AL SISTEMA

Está aplicación fue creada con la finalidad de demostrar la Transmisión y Recepción de Información en tiempo real de los puntos establecidos, entre AP y Cliente. En la Figura VI.63 se demuestra el ingreso de un producto desde la estación cliente hacia la Base de Datos.

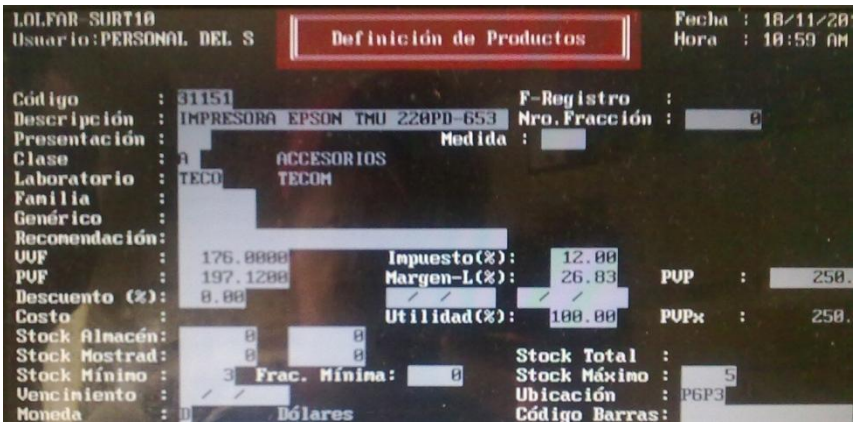

Figura VI.63 Ingreso de Producto

Registro de ventas se detallan los productos y la base de datos se actualiza automáticamente una vez realizada la venta. Fig. VI.64.

Figura VI.64 Proceso de Venta

6.6 COMPARACIÓN ENTRE EQUIPOS NANOSTATION5 Y ANTENAS TIPO GRILLA PARABÓLICA

6.6.1 Equipos NanoStation5

Se caracterizan por ser una caja compacta de diseño para interior/exterior y una Interfaz Web tan intuitiva que incluso el usuario menos experimentado puede obtener el máximo rendimiento en minutos.

Los NanoStation unen a su exponencial rendimiento un revolucionario diseño que combina un sistema de alta ganancia de 4 antenas, radio de arquitectura avanzada, y un alto nivel de investigación y desarrollo que se plasman en la tecnología de su firmware, que permite una velocidad, estabilidad y capacidad que rivalizan incluso con las redes WiMax de última generación.

El NanoStation utiliza tecnología de Polaridad de Antena Adaptable (AAP), lo cual habilita la opción de operar en polarización fija (Vertical u Horizontal) o "conmutada adaptativamente" que es el uso de la misma antena en múltiples polaridades. Adicionalmente cuenta con un

conector RP-SMA para antena externa, para casos donde pueda ser necesario un patrón de cobertura mayor o menor al incluido.

El Dispositivo NANO está diseñado para los más avanzados sistemas de redes WIFI como también para el usuario hogareño que poco tiene que saber de redes. Sus características principales es su excelente diseño y práctica instalación casi plug & play. Generando con su alta potencia coberturas de áreas extendidas outdoor como de 2kms, 7kms, 14kms con línea de vista sin agregarle ningún tipo de antena exterior.

Utiliza un Software de Plataforma Abierta AirOS.

Son dispositivos inteligentes que incluyen CPE, conocidos como todo en uno.

6.6.2 Antenas Tipo Grilla

Requieren de otros equipos o radios para poder trabajar sean estos: Rocket5M (Ubiquiti), WET11(Linksys), AP500(Orinoco), AP2000().

Requieren de una caja de exterior, para ubicar los equipos mencionados anteriormente, para evitar lluvias y otros factores que interfieran en su funcionamiento.

Se debe variar el sentido de la antena en forma Horizontal o Vertical dependiendo de la polaridad que se necesite, este trabajo se lo realiza físicamente.

Debido a su diseño y volumen no es factible el uso de estos equipos en espacios interiores.

Se limitan a trabajar de acuerdo a las especificaciones técnicas de los equipos con los que se asocian, frecuencia de trabajo, tipo de seguridad, potencia y alcance.

Su interfaz en la configuración varía, ya que adopta la del equipo con el cual se conecta, esto puede acarrear confusión, debido a la diversidad de marcas y modelos de equipos.

Necesitan corriente eléctrica los equipos que trabajan con antenas de Tipo Grilla.

6.6.3 Similitud entre equipos

Son equipos usados para la Transmisión y Recepción de información.

Utilizados por varios proveedores de servicios de Internet (ISP).

Estos equipos pueden ser usados tanto para enlaces punto a punto, y punto a multipunto.

Los NanoStation5 trabajan a frecuencias de 2.4 y 5.8GHZ, igual las antenas Tipo Grilla trabajan conjuntamente con equipos que usan estas frecuencias.

CONCLUSIONES

Se logró establecer la mejor frecuencia de transmisión y recepción en la que trabajan los equipos NANOSTATION5, para obtener un rendimiento óptimo del enlace.

Se demostró la conectividad de los equipos y capacidad de transferencia de información entre el AP y el Cliente, además la compatibilidad que existe tanto los equipos nanostation5, con equipos, D-Link, Cisco y Trendnet.

La integridad de la información está controlada a través del algoritmo conservativo que permite la retransmisión de los paquetes enviados, en caso de ser interferidos por fuentes externas.

Del análisis realizado en lo referente a seguridades que soportan los equipos NanoStation5 se optó por WPA, por ser la que presenta mayores prestaciones y compatibilidad con equipos de red que soporten este tipo de seguridad.

La facilidad de intercomunicación que tiene el equipo objeto de estudio con otros nodos dentro de un área geográfica, es óptima; ya que lo podemos utilizar no solo para enlaces punto a punto, punto a multipunto, o como un router inalámbrico con amplia cobertura.

La facilidad de instalación que tienen estos equipos permiten que personas con conocimientos básicos de red puedan instalarlos sin ningún problema.

El tamaño de los equipos NanoStation5 permite que estos puedan instalarse en sitios externos e internos dependiendo de la aplicación y necesidades del usuario.

El mantenimiento o configuración de estos equipos se lo realiza vía software desde una estación remota, lo que no sucede con las antenas de grilla que para su revisión se requiere estar en el punto físicamente.

RECOMENDACIONES

Se recomienda proteger los equipos NanoStation5 con un UPS, o con un Protector APC, con el fin de evitar que sufran desperfectos por variaciones de Voltaje.

No se recomienda utilizar la seguridad WEP, debido a que es muy vulnerable a ataques de red, y no presta la confiabilidad requerida que los usuarios necesitan.

Al instalar los Equipos NanoStation una vez comprobada la zona de fresnel, se debe revisar que no existan componentes externos (Antenas, repetidoras, microondas) que influyan en el rendimiento de la red.

En cuanto a compatibilidad, los equipos Cisco sería la mejor recomendación pero su costo es elevado.

Se recomienda que estos enlaces empiecen a popularizarse a nivel nacional en las diferentes empresas que utilizan enlaces descontinuados y requieran mejoras en sus procesos de comunicación.

RESUMEN

Se implementó un Radioenlace utilizando modulación digital de Banda Ancha para llevar el registro de gestión de la empresa Soluciones Tecnológicas NR.

Se instaló dos puntos de Transmisión situados en las ciudadelas Sultana de los Andes, y Álamos. Aplicando tecnología NanoStation5 y el Programa SOLNR, para la solución de gestión en la empresa.

Los dispositivos utilizados en la implementación del Radio Enlace fueron dos equipos NanoStation5, tres computadoras básicas con Sistema Operativo Windows XP con un mínimo de memoria de 256Mb para el buen desempeño del sistema, un switch D-LINK de 8 puertos, cable FTP encargado de comunicar los puntos internamente y a su vez alimentar de energía mediante el POE (Poder sobre la Red) a los equipos NanoStation5.

Como resultado del Radio Enlace se determinó la factibilidad de transmitir y recibir información desde la Base de Datos hacia sus terminales como si se lo hiciera con equipos normales de comunicación, garantizando la integridad, autenticación y confidencialidad de la información transmitida al 100% en la prueba realizada. Los procesos de transmisión y recepción a través de la nanotecnología tienen considerable ventaja frente al tamaño y la potencia en la transmisión, lo que se concluye que estos enlaces en la actualidad son los más idóneos para la Gestión y Transmisión de Datos.

Se recomienda que estos enlaces empiecen a popularizarse a nivel nacional en las diferentes empresas que utilizan enlaces descontinuados y requieran mejoras en sus procesos de comunicación.

BIBLIOGRAFIA

1. ACCESS POINT UBIQUITI NANOSTATION5

http://www.sistemsoft.com.ar/products/640-access-point-ubiquiti-nanostation5.aspx

12-10-2010

2. AirOS GUÍA INSTALACIÓN RÁPIDA

http://www.ubnt.com/wiki/AirOS_guia_instalacion_rapida

04-11-2010

3. ANTENAS CON REFLECTORES PARABÓLICOS

http://www.sisttel.com.ar/download/Antenas%20con%20reflectores%20parabolicos.pdf

01-06-2010

4. ANTENAS DE MICROONDAS

http://subversion.assembla.com/svn/MonoER/principal.pdf

04-06-2010

5. ANTENAS GRILLA

http://antenared.com/category/parabolicas/

http://www.netkrom.com/es/prod_ant_out_5.3ghz_ParabolicGrid.html

31-05-2010

6. CALCULO DEL RADIO DE LA ZONA DE FRESNEL

http://medusa.unimet.edu.ve/sistemas/bpis03/radiocomunicaciones/guiaspdf/guia05telecomunicaciones.pdf

15-10-2010

7. CÁLCULO DE ZONA DE FRESNEL

http://tamax.com.ar/blog/?p=517

20-10-2010

8. COMO MEJORAR CONEXIÓN WIFI?

http://www.tecnologiabit.com/como-mejorar-conexion-wifi-parte-1/

18-06-2010

9. CONFIGURACIÓN DE PUNTOS DE ACCESO

http://www.eslared.org.ve/tricalcar/05_es_configuracion-AP_laboratorio-redes-WDS_v02%5B1%5D.pdf

8-10-2010

10. ENLACES PUNTO MULTIPUNTO – ENLACE PUNTO A PUNTO

http://www.netlandchile.com/tecnologia.htm

15-08-2010

11. ESPECIFICACIONES TÉCNICAS EQUIPOS NANOSTATION5
http://www.syscom.mx/principal/detalles/id:7905
25-05-2010

12. ESTÁNDAR IEEE PARA REDES INALÁMBRICAS
http://webdiis.unizar.es/~chus/san/trabajos/7-802.11.PDF
13-07-2010

13. ESTUDIO, DISEÑO E IMPLEMENTACIÓN DE UNA RED MIXTA (ALÁMBRICA E INALÁMBRICA).
https://www.dspace.espol.edu.ec/bitstream/123456789/668/1/1175.pdf
28-10-2010

14. LAS ZONAS FRESNEL Y EL ALCANCE DE LOS EQUIPOS DE RADIO FRECUENCIA
http://asterion.almadark.com/2008/11/30/las-zonas-fresnel-y-el-alcance-de-los-equipos-de-radio-frecuencia/
26-10-2010

15. MANUAL DE CONFIGURACIÓN DEL UBIQUITI NANOSTATION5
http://www.wifisafe.com/downloads/soporte/Manual_Punto_a_Punto-Ubiquiti.pdf
30-10-2010

16. NANOTECNOLOGIA, NANOCIENCIA

http://www.portalciencia.net/nanotecno/

20-05-2010

17. POTENCIA, FRECUENCIA, ANTENAS

http://www.analfatecnicos.net/pregunta.php?id=21

04-06-2010

18. POWER OVER ETHERNET

http://es.wikipedia.org/wiki/PoE

28-05-2010

19. REDES INALÁMBRICAS MODO CLIENTE Y WDS

http://www.eslared.org.ve/tricalcar/05_es_configuracion-AP_laboratorio-redes-WDS_v02_lab1%5B2%5D.pdf

18-06-2010

20. SEGURIDAD EN REDES INALAMBRICAS

http://www.uv.es/montanan/ampliacion/trabajos/SegWLAN-presentacion.pdf

12-09-2010

21. SEGURIDAD WiFi

http://trajano.us.es/~fornes/RSR/2005/SeguridadWIFI/Trabajo%20WIFI.pdf

24-08-2010

22. SISTEMAS DE MODULACIÓN DIGITAL DE BANDA ANCHA

http://www.conatel.gov.ec/site_conatel/index.php?option=com_content&view=article&id=165%3Asistemas-de-modulacion-digital-de-banda-ancha&Itemid=165

28-06-2010

23. SOLUCIONES WIRELESS

http://www.solutionbox.com.ar/mailing/ineva/ubiquiti_08_05/info.htm

24-09-2010

24. ZONA DE FRESNEL

http://www.worldlingo.com/ma/enwiki/es/Fresnel_zone

16-10-2010