

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“Diseño e implementación de la expansión de la intranet de la Armada del Ecuador hacia las unidades navales acoderadas en los muelles de la Base Naval Sur”

PROYECTO INTEGRADOR

Previo la obtención del Título de:

Ingeniero en Telecomunicaciones

Presentado por:

Isaias Adrian Bajaña Conforme

Galo Rafael Vera Loor

GUAYAQUIL - ECUADOR

Año: 2023

DEDICATORIA

Este trabajo va dedicado a Dios por sus bendiciones, a mis padres Gloria y Gerardo por su inspiración para continuar, a mi hermano Fabio por ser demostrarme que todo es posible con esfuerzo y determinación, a Mildred por su compañía y ayuda en todo momento.

Isaias Adrian Bajaña Conforme

Este proyecto está dedicado a Sandra, Ernesto y Karen, por brindarme consejos precisos, darme aliento constante, y sobre todo su compañía incondicional.

Galo Rafael Vera Loor

AGRADECIMIENTOS

Agradezco a Dios por las grandes bendiciones recibidas, a mis padres Gloria y Gerardo por su invaluable apoyo y cariño ofrecidos siempre, a mi hermano Fabio por siempre inspirarme con su ejemplo. A Mildred por su apoyo y compañía incluso en los momentos más turbulentos.

Isaias Adrian Bajaña Conforme

Gracias a Dios, a los ángeles que Él puso en mi camino, a mis padres Sandra y Ernesto, a mis hermanas Karen y Freya, a mis tíos Héctor y Peggy, Guido y Maritza; a mis primos; a mi abuelita Consuelo, por su dedicación y ahínco para crear generaciones prósperas. A mis amigos de la ESPOL y a mis ex compañeros de los colegios.

Gracias a mí por no rendirme.

Galo Rafael Vera Loor

DECLARACIÓN EXPRESA

“Los derechos de titularidad y explotación, nos corresponde conforme al reglamento de propiedad intelectual de la institución; *Isaias Adrian Bajaña Conforme* y *Galo Rafael Vera Loor* damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual”



Isaias Bajaña Conforme



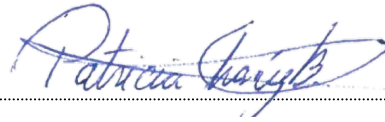
Galo Vera Loor

EVALUADORES



PhD. MEDINA MOREIRA WASHINGTON ADOLFO

PROFESOR DE LA MATERIA



PhD. PATRICIA XIMENA CHAVEZ BURBANO

PROFESOR TUTOR

RESUMEN

Este proyecto de titulación corresponde al diseño e implementación de la expansión de la intranet de la Armada del Ecuador hacia las unidades navales acoderadas en los muelles de la Base Naval Sur, el mismo presenta una solución eficiente que permite sobrellevar los problemas en las unidades, entre estos están la carencia de conectividad en los muelles, el aumento de la seguridad de la red para precautelar la sensibilidad de la información que se maneja dentro de la Base y la protección de los equipos de comunicación en el ambiente salino que se trabaja.

La primera etapa se enfoca en el diseño del segmento de red destinado para las embarcaciones acoderadas en los nueve muelles de la base sur. Se diseña una topología tipo estrella que utiliza un enlace Radio-Wifi del tipo Punto Multipunto y gracias a la cual se pueden agregar o desconectar nuevos dispositivos. Su gestión y monitoreo se realiza desde el edificio principal de DIRTIC, quienes son los encargados de controlar el tráfico de la red naval de Datos.

La segunda etapa se enfoca en la implementación del diseño de la red en 2 unidades navales, los submarinos Shyri y Huancavilca. Los equipos transmisores se ubican en la torre de comunicaciones de la base. Los equipos receptores se ubican en mástiles sujetos a los postes de alumbrado eléctrico cercano a los muelles. Cerca de las unidades navales se colocan cajas de conexiones que contienen puntos de red para que la embarcación se conecte y se desconecte según sus necesidades.

Al finalizar las etapas del proyecto se observaron resultados positivos que reflejaban un enlace estable, un bajo nivel de latencia y un SNR adecuado. Además, se comprobó la gestión de la red y la seguridad de la información cifrada por los protocolos de seguridad de los equipos.

Palabras Clave: Radio-Wifi, Acoderadas, Latencia, SNR

ABSTRACT

This degree project corresponds to the design and implementation to expand the Ecuadorian Navy's intranet to the naval units stationed at the docks of the South Naval Base. It presents an efficient new solution to overcome problems in the units, such as the lack of connectivity at the docks, the increase in network security to protect the sensitivity of the information handled within the Base as well as the protection of the communication equipment in the salty environment in which they work.

The first stage focuses on designing the network segment destined for the vessels docked at the nine docks at the southern base. A star-type topology is designed using a Radio-Wifi link of the Multipoint type and thanks to which new devices can be added or disconnected. Its management and monitoring are done from DIRTIC's main building, which controls the traffic of the naval data network.

The second stage focuses on the implementation of the network design in 2 naval units, the submarines Shyri and Huancavilca. The transmitting equipment is located in the base's communications tower. The receiving equipment is placed on masts attached to the electric lighting poles near the docks. Junction boxes containing network points are placed near the naval units for the vessel to connect and disconnect as needed.

At the end phase project stages, positive results were observed reflecting a stable link, low latency level, and adequate SNR. In addition, the network management and the security of the information encrypted by the equipment security protocols were tested.

Keywords: radio-wifi, layered, latency, SNR

INDICE DE CONTENIDO

EVALUADORES.....	V
RESUMEN	VI
ABSTRACT	VII
INDICE DE CONTENIDO	VIII
INDICE DE ILUSTRACIONES.....	X
INDICE DE TABLAS	XI
CAPITULO 1	1
1. INTRODUCCIÒN	1
1.1 DEFINICIÒN DEL PROBLEMA	2
1.2 JUSTIFICACION	3
1.3 OBJETIVOS	4
1.3.1 OBJETIVO GENERAL.....	4
1.3.2 OBJETIVOS ESPECIFICOS.....	4
1.4 ESTADO DEL ARTE	4
1.5 ALCANCE.....	7
1.6 METODOLOGÌA.....	8
CAPITULO 2	9
2. MARCO TEORICO.....	9
2.1 PRINCIPIO DE HUYGENS	9
2.2 INTERFERENCIA	9
2.3 LINEA VISUAL.....	10
2.4 ZONA DE FRESNEL	11
2.5 ESTANDAR IEEE 802.11	12
2.6 ELEMENTOS DE IMPLEMENTACIÒN	13
2.6.1 CABLE UTP CAT 6A	13
2.6.2 CONECTORES Y ADAPTADORES	14
2.6.3 TUBERIA FLEXIBLE BX	15
2.7 NANOBEAM GEN2 (RECEPTOR)	15
2.8 SECTOR AIRMAX PRISM AC (EMISOR).....	17
2.9 SEGURIDAD PARA REDES DE TELECOMUNICACIONES.....	18
2.9.1 TIPOS DE PROTOCOLOS.....	19
2.9.2 TIPOS DE AMENAZAS EN LA RED.....	20
2.9.3 SOLUCIONES EN SEGURIDAD	20

2.9.4 SEGURIDAD EN EQUIPOS DEL NÚCLEO DE LA RED	21
2.9.5 SEGURIDAD EN EQUIPOS INALÁMBRICOS	21
2.10 LICENCIAS Y REGULACIONES	22
2.11 PERMISO DE TORRES DE ANTENAS	22
CAPITULO 3	24
3. SOLUCION PROPUESTA	24
3.1 DISEÑO DE LA SOLUCION PROPUESTA.....	25
3.2 IMPLEMENTACION	33
CAPITULO 4	38
4. RESULTADOS Y ANALISIS	38
4.1 Análisis del estado del sistema anterior a la implementación	38
4.2 Análisis del estado del sistema posterior a la implementación.....	39
4.2.1 Pruebas de conectividad	41
CONCLUSIONES Y RECOMENDACIONES.....	46
CONCLUSIONES	46
RECOMENDACIONES	47
BIBLIOGRAFIA	48
ANEXOS	52

INDICE DE ILUSTRACIONES

Ilustración 1 Representación gráfica de zona de Fresnel con un bloqueo parcial [28]	12
Ilustración 2 Conector LOCHSOEL RJ45 [29]	15
Ilustración 3 TUBERIA BX 1/2 [29]	15
Ilustración 4 NANOBEAM GEN2 [31]	16
Ilustración 5 Patrón de Radiación de NanoBeam Gen2 [31]	17
Ilustración 6 SECTOR AIRMAX PRISM AC [32]	17
Ilustración 7 Diagrama de flujos de la metodología de la solución propuesta	24
Ilustración 8 Diagrama de bloques de la solución propuesta	27
Ilustración 9 Conexión entre el equipo receptor y la unidad naval	28
Ilustración 10 Diagrama de expansión de la intranet	30
Ilustración 11 Simulación de los enlaces WLAN desde Torre COMACO hasta 7 muelles	31
Ilustración 12 Simulación de enlace WLAN desde Torre COMACO hasta el muelle 5	32
Ilustración 13 Primer punto de conexión	34
Ilustración 14 Torre Principal	34
Ilustración 15 Ubicación de equipos receptores	35
Ilustración 16 Protección del cableado	35
Ilustración 17 Ubicación de la caja de conexiones	36
Ilustración 18 Prueba de funcionamiento del cableado	36
Ilustración 19 Unidades en las que se llevó a cabo la implementación	37
Ilustración 20 Punto de acceso al interior del submarino Shyri	37
Ilustración 21 Equipo transmisor antes de la implementación	38
Ilustración 22 Equipo receptor en la unidad antes de la implementación	39
Ilustración 23 Barrido de frecuencias en la banda 5GHz	40
Ilustración 24 Esquema de conectividad para el submarino Shyri	40
Ilustración 25 Ping hacia los servidores DNS 8.8.8.8	41
Ilustración 26 Vista de la página principal de Google en el computador al interior del submarino	42
Ilustración 27 Imágenes de navegación Web al interior del submarino	42
Ilustración 28 Prueba ping realizada en el pc de control de la red	44
Ilustración 29 Historial de conexión y latencia del enlace	44

INDICE DE TABLAS

Tabla 1	Parámetros básicos del estándar IEEE 802.22 [29]	13
Tabla 2	Características físicas del UTP CAT6A [30]	14
Tabla 3	Especificaciones de Potencia y frecuencia de NanoBeam Gen2 [31]	16
Tabla 4	Especificaciones de potencia y frecuencia de Prism 5AC Gen 2 [32]	18
Tabla 5	Equipos de los enlaces actuales de microondas	26
Tabla 6	Prueba de velocidad en CPE-CORESM	26
Tabla 7	Coordenadas de Muelles y Torre	30
Tabla 8	simulación de cobertura con software de Ubiquiti	32
Tabla 9	Estado del enlace y parámetros básicos	43
Tabla 10	Resultados del monitoreo del enlace	43

CAPITULO 1

1. INTRODUCCIÓN

La Armada del Ecuador es un organismo estatal cuya misión es proteger la soberanía e integridad de los mares bajo su jurisdicción. Proteger las actividades, recursos e infraestructura en las aguas, así como coadyuvar al desarrollo de los recursos marítimos del país y la seguridad integral. Salvaguardar el uso y desarrollo del poder marítimo y ejercer las competencias de la administración marítima nacional, promover los intereses marítimos a fin de promover la defensa, la seguridad y el desarrollo nacional, así como la paz regional e internacional. [1]

Un departamento importante dentro de la institución es DIRTIC [2]. Su misión es planificar, gestionar y evaluar el desarrollo e integración de proyectos y recursos telemáticos alineados al plan de comunicaciones.

DIRTIC posee un centro físico de operaciones localizado en el recinto militar de la ciudad de Guayaquil que tiene por nombre base naval sur. Precisamente en las oficinas de la Dirección General de Materiales. Este se encarga de la gestión de las comunicaciones dentro de la base. Consecuentemente es el departamento que maneja la red de internet de la base y gestiona la seguridad de la información que allí se maneja. Sin embargo, existe un inconveniente de comunicación relativo a las unidades navales que se encuentran acoderadas en los muelles de la base. Estas unidades actualmente no cuentan con conexión a internet.

Por este motivo, el presente proyecto pretende solucionar el problema presentado, de forma eficiente, eficaz y económica. Otorgando un enfoque principal en la gestión de la red y el manejo seguro de la información, reduciendo el riesgo de comprometer la integridad de las unidades navales.

1.1 DEFINICIÓN DEL PROBLEMA

En la base de la armada ubicada en el sur de Guayaquil, se encuentran acoderadas diferentes unidades a flote. En las mismas se desarrollan diferentes tipos de actividades militares según su cronograma de operación. La comunicación del personal a bordo con los diferentes departamentos de la institución se realiza mediante Internet. Inicialmente las embarcaciones accedían a la Red Naval de Datos y al Internet mediante radioenlaces WIMAX, que consistían en la instalación de 1 equipo CPE-CLIENTE en cada unidad, los cuales apuntaban hacia la torre principal del centro de operaciones de DIRTIC. Los barcos situaban una MICROESTACION WIMAX con la cual se conectaban y gestionaban varios CPE-CLIENTE. [1]

Sin embargo, los equipos del sistema implementado fueron deteriorándose por falta de mantenimiento y por operar en un ambiente para el que no están diseñados. Esto ocasionó que la MICROSTACION WIMAX quede fuera de servicio, lo que generó que todos los enlaces hacia los clientes queden inhabilitados y por ende sin acceso a Internet y a la red naval de datos.

Como parte de la gestión para la adquisición de múltiples herramientas y equipamiento, DIRTIC en el 2018 adquirió 06 dispositivos marca UBIQUITI de la serie M5 para radioenlaces. Estos equipos en un principio no fueron concebidos para dar conectividad a las unidades a flotes, sino para dar conectividad a los edificios dentro de la base naval sur.

Dada la necesidad de conexión a Internet en las unidades navales, dichos dispositivos de la marca UBIQUITI de la serie M5 fueron ubicados en su momento de la siguiente manera: 1 en la torre principal de la DIRTIC, 4 en diferentes unidades navales.

La solución de radioenlace instalada y configurada por personal de DIRTIC presenta limitaciones. Esto se debe a que la línea de vista en los equipos depende del nivel de la marea. Por otra parte, el equipo utilizado como AP (NANOBEAM M5) es un equipo CPE, esto causa condiciones que coartan el límite en el ancho de banda requerido para la correcta transferencia de datos. En los diferentes enlaces el tráfico de datos en estas circunstancias es máximo de 3 a 5 Mbps [3]. Dichos

equipos y enlaces son monitoreados por un software de gestión de la propia marca UBIQUITI. Actualmente cuentan con este tipo de enlace las unidades BESGUA, CORESM, FRAMOR Y FRAPAL [4].

Debido a esto, los tripulantes optaron por contratar un servicio de internet de un proveedor particular, realizando pagos mensuales tal y como lo realiza cualquier cliente individual. Sin embargo, el reglamento de la institución militar estipula que se prohíbe la contratación de empresas externas para proveer internet a una unidad naval. Esto debido a que se puede comprometer la seguridad de la información militar que allí se maneja, la misma que es catalogada como información de alta confidencialidad [4].

1.2 JUSTIFICACION

El proyecto busca presentar un diseño y una implementación de la expansión de la intranet de la Armada del Ecuador, hacia las unidades navales acoderadas en los muelles de la Base Naval Sur. La finalidad del proyecto es solucionar problemas de conectividad en las embarcaciones para la comunicación con la red interna de la institución. Priorizando la seguridad de la información y teniendo en cuenta los factores ambientales en el lugar de instalación de los equipos. Esto sin olvidar los posibles incidentes que puedan ocurrir en el sitio, tales como: corrosión, durabilidad, dureza de los materiales, los cambios en las mareas y las maniobras de preparación al momento de salir a navegar.

El proyecto es de suma importancia ya que este nos permite tener un manejo y monitoreo constante de la red. Así es posible administrar el segmento de red que pertenece a cada unidad naval, lo cual permite alcanzar una comunicación optimizada. Además, se puede gestionar las páginas web que la institución no considere apropiado que los tripulantes puedan visitar en horarios laborales, esto incluye redes sociales, servicios de streaming y entretenimiento e incluso páginas con contenido para adultos. Esto lo convierte en un sistema muy flexible, económico y rentable para el cliente.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Diseñar e implementar la expansión de la red interna de la Armada, para otorgar un método de conexión a los tripulantes que laboran dentro de las unidades navales acoderadas en los muelles de la base naval sur. Otorgándole a los tripulantes la capacidad de interacción con la red de internet de forma segura y apropiada.

1.3.2 OBJETIVOS ESPECIFICOS

Determinar los puntos adecuados para la ubicación de las antenas del radioenlace.

Detallar la topología del segmento de red necesario para lograr la conectividad con los usuarios finales.

Efectuar la configuración inicial de los equipos utilizados en la red y de esta forma brindar seguridad a la información que transita por la misma.

Optimizar la comunicación entre distintos departamentos para llevar a cabo diferentes operaciones militares.

1.4 ESTADO DEL ARTE

La falta de conexión a internet dentro de un barco ha sido un constante problema el cual ha encontrado distintas soluciones a lo largo del tiempo, dichas soluciones resuelven varios conflictos específicos para los requerimientos de embarcaciones diferentes.

Un servicio de internet marítimo de alta velocidad es presentado en [5], ofrece un servicio de internet marítimo de alta velocidad (hasta 100Mbps) para diferentes tipos de embarcaciones, con cobertura disponible en todo el medio marítimo esto mediante el uso de tecnología satelital VSAT. Cabe mencionar que este servicio tiene un alto valor económico que debe ser cancelado cada mes.

Por otra parte, la empresa BOAT SECURITY ofrece una solución a la que ellos llaman Boat net. Esta consiste en la implementación de un enrutador con antenas GSM y Wifi de alta ganancia, dicho dispositivo utiliza 2 tarjetas SIM y conexión 4G [6]. El enrutador trabaja como un puerto de acceso inalámbrico cuando está en un puerto, ya que se conecta a una red de internet cercana para proporcionar internet a la embarcación. Cuando la misma sale a navegar utiliza conexión 4G por medio de las tarjetas SIM, pero esta depende de la ubicación de las torres de comunicaciones que se encuentren en tierra. [7] La cobertura de las redes celulares sobre el océano llega hasta 15km de distancia en casos favorables.

Podemos notar que la solución de la empresa BOAT SECURITY [6] y la presentada en la conferencia IEEE 2018 dependen de una red celular externa, las cuales en nuestro caso no es óptima por motivos de seguridad militar.

Un estudio [7] presenta una solución similar a la anteriormente mencionada, con la diferencia que esta utiliza tecnología Long range (LR) Wi-Fi [8]. Dicha tecnología se utiliza como backhaul para conectar las redes de acceso Wi-Fi de los barcos de forma inalámbrica a la red 4G LTE en tierra.

Soluciones diferentes son mostradas en el artículo [9] y en el trabajo [10] , estas proponen el uso y diseño de un sistema de auto tracking de alta precisión, para que las antenas de las embarcaciones establezcan enlaces de comunicaciones con radio bases que se encuentren mejor posicionadas. Estas propuestas conllevan trabajos adicionales de electrónica y prototipado.

En Latinoamérica de forma más concreta en Perú, [11] se han realizado trabajos que indican la implementación de sistemas de comunicaciones externas para embarcaciones [12]. Si bien estos sistemas de comunicaciones son capaces de enviar distintos tipos de datos, no se descarta el uso de sistemas similares para la conexión a una red privada por internet.

Aunque existen diferentes tecnologías que pueden ser usadas para proveer comunicación y conexión a internet para embarcaciones [13], nos indica que la mejor manera para brindar seguridad informática a los datos que se manejen en una red de internet se debe llevar a cabo mediante enlaces satelitales INMARSAT [14].

[15] Se menciona que el Servicio de Telecomunicaciones de la Armada de Colombia, es ampliamente utilizado en la red de telecomunicaciones fijas extraterritorial. El mismo permite la transmisión de tráfico de información en todo el país, y el primer gran avance de esta red hasta la fecha es la introducción de SNTDM, ya que este sistema es capaz de enviar documentos y mensajes.

De acuerdo con la Universidad Nacional de Colombia y un estudio realizado por sus alumnos, el sistema horizontal incluye los cables, terminales, tuberías, cables de hardware y latiguillos necesarios para dar servicio a cada estación de trabajo [16]. El sistema horizontal se instala entre las zonas de los buques denominadas “salas de radio” y la “zona de trabajo”.

ANSI/TIA/EIA 1005 es aquella regla utilizada en los Fundamentos de Telecomunicaciones para Instalaciones Industriales, siempre que MASTERCUBOX [17] cuente con una instalación industrial que contenga equipos que requieran una conexión Ethernet para su correcto funcionamiento.

Se determina la importancia de saber en qué banda de frecuencia se está operando, las condiciones climáticas del área donde se realizará y las especificaciones del equipo a utilizar [18].

INOCAR cuenta con una plataforma de predicción de los tipos de mareas según el puerto, fecha y hora estimada. También edita una publicación cada 6 meses de pronósticos de mareas que incluye un calendario de datos de mareas, y elevaciones asociadas a un nivel de referencia conocido como MLWS. Según este se realiza un Spring Average en los momentos más importantes para la navegación ecuatoriana, y los puertos que se encuentran en el top 20 del País. [19]

[20] Se muestra que la salinidad medida en el Estero del Muerto fue de 24 % en la superficie, mientras que, en la subsuperficie se incrementó a 25% en las estaciones 1AE y 4AE al norte y sur del Estero Caracol. Para referenciar, el agua de mar es aquella que se considera agua salina y se encuentra en todos los océanos del planeta, otro nombre es agua de mar euhalino. Su salinidad oscila entre el 30 y el 35%. El agua salobre es un área con salinidad de 0.5 a 29%, el Estero del Muerto se clasifica como agua salobre. [21]

[22] Analiza la propagación de RF en un maniquí salino para caracterizar la pérdida de señal a través del espacio libre. Esto se realiza al variar la distancia entre las antenas transmisora y receptora y el tipo y tamaño de las antenas, para encontrar la potencia recibida más alta a la potencia transmitida más baja.

Los cruceros están tratando de minimizar los costos mediante el uso de sistemas híbridos, los cuales combinan una conexión satelital costosa con Internet en tierra de bajo costo, dando acceso a múltiples servicios integrados en la misma red. [23] Además, evita los siguientes riesgos de seguridad: ataque de control de ruta, ataque de mantenimiento de ruta, ataque de inundación, ataque de sumidero, espionaje y ataque de agujero de gusano, entre otros.

1.5 ALCANCE

El trabajo tiene por finalidad diseñar e implementar una red para proveer internet a las unidades navales acoderadas en los muelles de la base naval sur, mediante el uso de un enlace punto-multipunto. Priorizando la gestión de los datos a bordo de modo seguro.

El enlace punto-multipunto transmite la información mediante wifi, desde una torre principal hacia los postes de alumbrado eléctrico donde se encuentran los equipos receptores, de esta forma se establece una conexión remota a la red de internet que conecta a toda la base sur, y a la misma con las diferentes bases que se encuentran en el país.

Establecer la conexión desde la torre principal permite el manejo correcto de la información, así como la restricción al acceso a ciertas páginas web y contenido explícito en línea, el cual no sea considerado apropiado para las labores del personal militar a bordo.

1.6 METODOLOGÍA

La implementación de la red tiene un enfoque en ambientes exteriores que poseen un alto nivel de salinidad, ocasionando que el manejo de los elementos con los que se trabaja posea una protección y acreditación específica para estos lugares. De lo contrario la implementación de la red no funcionará correctamente por mucho tiempo.

Por otra parte, la tecnología del proyecto se basa en modelos de propagación para exteriores, con la facilidad de que en todo momento se busca una línea de vista entre los dispositivos transmisores y receptores.

Por tal motivo se selecciona un equipo transmisor que posee una antena sectorial con una cobertura de 45°, con esta abarcamos todo el perímetro del puerto donde acoderan los barcos. Los equipos receptores son nanobeamg5, estos son ideales ya que se adaptan a las condiciones de trabajo, el ancho de banda con el que operan es lo suficientemente amplio para las conexiones en las unidades.

Además de la implementación y la instalación física de los equipos, se realizará la configuración de estos y el manejo de la red, incluyendo sus restricciones de uso desde el switch principal. De esta forma se controla el tráfico de la red de las diferentes VLANs y se asegura la información mediante el cifrado de los mensajes.

CAPITULO 2

2. MARCO TEORICO

En esta sección del proyecto se definen las bases teóricas que se utilizan en el desarrollo de la solución ofertada. Los conocimientos más relevantes para comprender son principio de Huygens, zona de Fresnel, interferencia, estándar IEEE 802.11, seguridad de una red y sus amenazas. Así mismo, es necesario conocer lo elementos utilizados en la implementación del proyecto, NanoBeam Gen2, Access point Sector Airmax Prism ac, y el protocolo de seguridad con el que trabajan WAP2.

Debido al sector donde se aplica el proyecto es correcto conocer los permisos, regulaciones y licencias que se deben seguir para llevar a cabo una implementación sin inconvenientes.

2.1 PRINCIPIO DE HUYGENS

Este concepto estipula que un punto onda frontal es el resultado de la combinación de todos los puntos de frentes de ondas secundarias circulares [24]. Este principio por ende se convierte en un método por el cual es posible predecir con precisión por dónde y cómo será la propagación de una onda.

2.2 INTERFERENCIA

Por interferencia se puede entender a la superposición no deseada entre señales de radiofrecuencia [25]. Esto ocasiona que las comunicaciones entre dispositivos como celulares, radio, televisión e internet, no se realice de forma correcta o en casos extremos los equipos queden totalmente incomunicados.

Se conocen dos tipos de interferencias, interferencias constructivas e interferencias destructivas [26]. Las interferencias constructivas ocurren cuando dos pulsos se superponen, y la magnitud de la onda de la señal es igual a la suma de las magnitudes de ondas de dos señales distintas. Mientras que las interferencias

destructivas ocurren cuando dos pulsos se superponen, y la magnitud de la onda de la señal es igual a la cancelación parcial de las magnitudes de ondas de dos señales distintas. [27]

Los equipos que son comercializados en la actualidad y que forman parte de los diferentes sistemas de comunicaciones, deben estar preparados para el manejo de diferentes interferencias, las cuales pueden provenir de distintas fuentes. Las fuentes de interferencias cotidianas que con mayor frecuencia se presentan son:

- Sistemas de comunicación cercano.
- Instalación eléctrica cercana.
- Dispositivos no regulados.

Un sistema de comunicación cercano hace referencia a aquellos equipos que transmiten señales en distintas frecuencias, de las cuales comúnmente no se tiene una regulación aplicada de forma correcta.

La instalación eléctrica cercana se refiere a líneas de transmisión y distribución para servicios de televisión por cable, líneas telefónicas o equipos eléctricos alrededores de los equipos de transmisión.

Los dispositivos no regulados se definen como aquellos equipos de comunicación para el consumidor, como teléfonos (fijos/móviles) y dispositivos de acceso inalámbrico que aún no han sido aprobados o registrados por el gobierno del país [27]. En este caso, ARCOTEL es la entidad encargada de homologar dichos aparatos de comunicaciones. Para que eso suceda los dispositivos deben cumplir con distintos parámetros y requerimientos según se considere necesario.

2.3 LINEA VISUAL

Mayormente conocido como línea de vista o LOS, este concepto es sencillo de entender si se lo interpreta como un rayo de luz visible. En el caso de las telecomunicaciones y la propagación de ondas el concepto se puede volver un poco más complicado por los factores que influyen. Se puede resumir como un camino sin obstáculos entre los dispositivos transmisores y emisores. [28]

Para dispositivos de radiofrecuencias, se debe precautelar su ubicación y el ambiente donde se instalarán. Es recomendado transmitir en sitios donde no

interfieran grandes estructuras. A su vez, es prioritario evitar arreglos donde intervengan grandes cantidades de metal, ya que se el sistema se vería propenso a reflejar la señal y por tal se puede llegar a la cancelación de la señal que se desea transmitir.

Algunos aspectos que se consideran en la instalación de equipos de comunicaciones para que exista una correcta LOS son: la altura, las pruebas y el nivel de señal [29]. La altura de los equipos será una distancia tal que se pueda prevenir un tráfico abundante de objetos (autos/personas). Si no se elige una altura correcta, la señal puede verse distorsionada y la calidad de las comunicaciones será muy mala

El nivel de señal depende de la potencia de los equipos y de la ubicación de estos. Es recomendable hacer un estudio de factibilidad previo a la instalación de cualquier equipo. Las pruebas se deben realizar cuando se lleva a cabo la configuración inicial. Esto se realiza para evitar inconvenientes con la condición de la señal de transmisión. En caso de presentarse algún problema la solución se ejecutará de forma inmediata.

2.4 ZONA DE FRESNEL

Este concepto se define como, el area limitada por los confines donde las ondas de la señal transmitida llegan desde el transmisor al receptor, con la misma fase de la señal original.

La teoría de Fresnel estipula que existen diferentes zonas de Fresnel en función de las fases de la señal, esto sucede gracias a la presencia de la difracción que sufren las ondas electromagnéticas debido a las partículas de aire que se encuentran en el ambiente [29].

La primera zona de Fresnel es aquella en donde la fase tiene un valor de 180° y esta se asemeja a una elipse. La siguiente zona es aquella donde la fase tiene un valor de 360° , esta tiene la forma de un elipsoide que contiene en su interior al elipsoide correspondiente a la primera zona de Fresnel. Es posible obtener diferentes zonas de Fresnel y lo que diferencia a todas ella es la obstrucción permitida. En radiocomunicaciones se considera la curvatura de la tierra y la obstrucción máxima recomendada es de un 20%.

La fórmula para encontrar las zonas de Fresnel que se mencionan es definida según la ecuación 1.

$$r_n = \sqrt{\frac{n\lambda d_1 d_2}{d_1 + d_2}} \quad (1)$$

r_n = Corresponde al diámetro de la n -ésima región de Fresnel

d_1 = Distancia considerando como referencia el transmisor

d_2 = Distancia considerando como referencia el receptor

λ = Longitud de onda

Si bien existen muchas zonas de Fresnel, n zonas tal como lo indica la fórmula, se debe trabajar solo con la primera zona de Fresnel, ya que la contribución a partir de la segunda región ya es negativa.

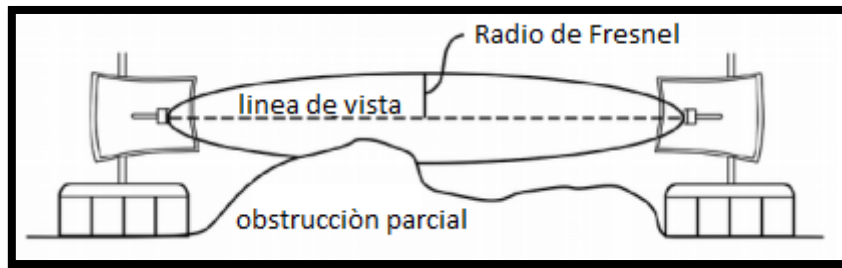


Ilustración 1 Representación gráfica de zona de Fresnel con un bloqueo parcial [30]

En la ilustración 1 podemos observar que la línea de vista entre un equipo transmisor y un equipo receptor está libre, mientras que en la primera zona de Fresnel se observa un pequeño obstáculo. La teoría recomienda que la zona de Fresnel esté libre de estorbos al igual que la línea de vista. Sin embargo, en la práctica un pequeño obstáculo dentro de la primera Zona de Fresnel no afecta significativamente.

2.5 ESTANDAR IEEE 802.11

Fácilmente conocido por ser el estándar de comunicación que utilizan todas las redes de comunicaciones inalámbricas de área local (WLAN). Es el estándar diseñado para obtener una conexión de banda ancha, con comunicación

inalámbrica de larga distancia. Los métodos utilizados en IEEE 802.11 para determinar el espectro incluyen geolocalización y detección de espectro [31].

En este proyecto se analizará el método de detección de espectro, este se trata de observar el espectro y determinar qué canales están desocupados para que la transmisión sea permitida.

De esta forma, en las redes 802.11 se puede determinar en qué canal se puede transmitir, y cambiar a un nuevo canal no utilizado si alguno está ocupado con transmisiones autorizadas. Se trabaja con una arquitectura de red punto-multipunto, en este caso la estación base es la que determina y monitorea quien accede a la red en cada instante.

El estándar se utiliza para sistemas que definen que los usuarios posean una velocidad de descarga cercano a 1.5Mbps, lo que supone que se pueden conectar diversos usuarios simultáneamente. A continuación, podemos observar los parámetros básicos en los que trabaja el estándar IEEE 802.11

Tabla 1 Parámetros básicos del estándar IEEE 802.22 [29]

Parámetros básicos	IEEE 802.11
Radio de cobertura	3km
Capacidad del canal	18 Mb/s
Capacidad del usuario	1,5 Mb/s - 384Kb/s
Ancho de Banda del Canal	6,7,8 MHz

2.6 ELEMENTOS DE IMPLEMENTACIÒN

Para llevar a cabo un estudio, diseño e implementación de algún sistema de comunicaciones, es necesario tener en consideración los componentes físicos que forman parte importante de la estructura de la red. De estos depende el funcionamiento idóneo del sistema y la gestión económica del mismo.

2.6.1 CABLE UTP CAT 6A

Este proyecto requiere el uso de cables con características especiales debido al ambiente de trabajo, el tipo de cable es el UTP CAT6A. Este es utilizado para el transporte de datos, considerado de alto rendimiento, trazado para rapidez de transferencia de hasta 10 GB por segundo [32].

Dichos cables admiten el uso de protocolos concurrentes con clase EA para implementar equipos 10GBASE-T. De igual forma el cable trabaja con rangos de frecuencia de hasta 500MHz, a su vez es compatible con equipos que utilicen POE y POE+.

Tabla 2 Características físicas del UTP CAT6A [30].

	Cat. 6E FTP y PE		
Numero de pares	4		
Conductor	cobre solido (clase 1)		
Aislamiento	HDPE		
Alambre de drenaje	cobre estañado		
Pantalla	Papel Al		
Revestimiento exterior	Polietileno de baja densidad (LDPE)	LSZH	LSZH
Color	Negro	Azul	Azul Claro

2.6.2 CONECTORES Y ADAPTADORES

De forma similar al cable utilizado, es necesario un tipo de adaptador especial por el area de instalación y por la seguridad de los equipos, teniendo en consideración las diferentes actividades que en la locación se realizan.

El tipo de conector manejado esta oportunidad corresponde al conector LOCHSOEL RJ45 con certificación IP65. Esta protección garantiza impermeabilidad y resistencia al oxido, el cual se puede producir por los efectos de la salinidad. El acople blindado mantiene la continuidad del escudo ofreciendo protección contra interferencias EMI/RFI, por lo cual se garantiza la transmisión de datos en ambientes hostiles. La Ilustración 2 es una referencia visual de la composición de los conectores utilizados en el proyecto.



Ilustración 2 Conector LOCHSOEL RJ45 [29]

2.6.3 TUBERIA FLEXIBLE BX

La tubería BX se puede observar en la ilustración 3, es una protección utilizada para cables eléctricos, cables ethernet o fibra óptica. Es ideal para ambientes donde se realicen actividades que impliquen altas vibraciones, trabajos con elementos afilados. Brinda protección contra golpes, agresiones mecánicas involuntarias y corrosión.



Ilustración 3 TUBERIA BX 1/2 [29]

2.7 NANOBEAM GEN2 (RECEPTOR)

Se trata un poderoso terminal CPE de alto rendimiento, el cual compone un radio Wifi dedicado para su gestión remota, cuenta con seguridad contra descargas, resiste 450 Mbps reales TCP/IP [3].

Promete 19 dBi de ganancia, y su operación se encuentra en el rango de frecuencias de 5150 – 5875 MHz. También tiene un puerto Gigabit Ethernet 10/100/1000. La ilustración 4 es una referencia visual de la apariencia del dispositivo utilizado en la implementación, mientras que en la ilustración 6 observamos el patrón de radiación del equipo mencionado. En la tabla 3 podemos observar las especificaciones de potencia y frecuencia de NanoBeam Gen2, estas son obtenidas desde el Datasheet del equipo.



Ilustración 4 NANOBEAM GEN2 [31]

Tabla 3 Especificaciones de Potencia y frecuencia de NanoBeam Gen2 [31]

Frecuencia de Operación							
Mundial	5150-5875						
USA	U-NII-1: 5150-5250	U-NII-2A: 5250-5350 MHz			U-NII-3: 5725-5850 MHz		
Gestión de Radio (MHz)							
Mundial	2412-2472						
USA	2412-2462						
NBE-5AC-Gen2 Potencia de Salida: 25dBm							
Especificaciones de Potencia TX				Especificaciones de Potencia RX			
Modulación	Tasa de datos	Avg TX	Tolerancia	Modulación	Tasa de datos	Avg TX	Tolerancia
Airmax ac	1x BPSK (1/2)	25 dBm	± 2dB	Airmax ac	1x BPSK (1/2)	-96dBm	± 2dB
	2x QPSK (1/2)	25 dBm	± 2dB		2x QPSK (1/2)	-95dBm	± 2dB
	2x QPSK (1/4)	25 dBm	± 2dB		2x QPSK (1/4)	-92dBm	± 2dB
	4x 16QAM (1/2)	25 dBm	± 2dB		4x 16QAM (1/2)	-90dBm	± 2dB
	4x 16QAM (1/4)	25 dBm	± 2dB		4x 16QAM (1/4)	-86dBm	± 2dB
	6x 64QAM (2/3)	24 dBm	± 2dB		6x 64QAM (2/3)	-83dBm	± 2dB
	6x 64QAM (3/4)	23 dBm	± 2dB		6x 64QAM (3/4)	-77dBm	± 2dB
	6x 64QAM (5/6)	22 dBm	± 2dB		6x 64QAM (5/6)	-74dBm	± 2dB
	8x 256QAM (3/4)	21 dBm	± 2dB		8x 256QAM (3/4)	-69dBm	± 2dB
	8x 256QAM (5/6)	20 dBm	± 2dB		8x 256QAM (5/6)	-65dBm	± 2dB

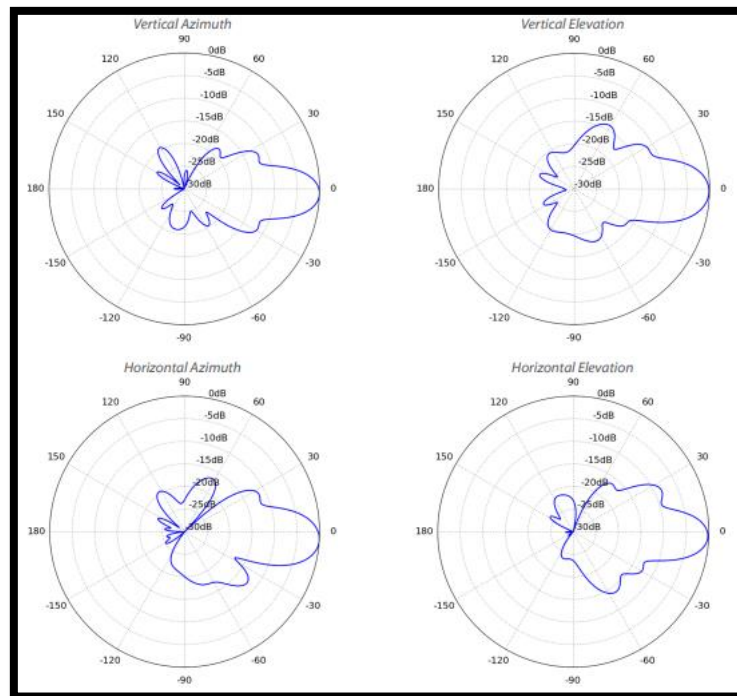


Ilustración 5 Patrón de Radiación de NanoBeam Gen2 [31]

2.8 SECTOR AIRMAX PRISM AC (EMISOR)



Ilustración 6 SECTOR AIRMAX PRISM AC [32]

El Access Point radio base Ubiquiti RP-5AC-Gen2 posee procesador Atheros MIPS 74kc y memoria RAM de 128Mb. Es un punto de acceso resistente diseñado principalmente para trabajar en estaciones base Wi-Fi. Opera en la frecuencia de 5GHz, trabaja en un rango de más de 50 Kilómetros, fundamentalmente elaborado para trabajos con enlaces PtP y PtMP, utilizada con un patrón de radiación sectorial

a 45°. [33] Las especificaciones de este equipo se obtienen directamente del Datasheet que entrega el fabricante y se visualizan en la tabla 5.

Tabla 4 Especificaciones de potencia y frecuencia de Prism 5AC Gen 2 [32]

Frecuencia de Operación							
Mundial	5150-5875						
USA	U-NII-1: 5150-5250		U-NII-2A: 5250-5350 MHz			U-NII-3: 5725-5850 MHz	
Gestión de Radio (MHz)							
Mundial	2412-2472						
USA	2412-2462						
NBE-5AC-Gen2 Potencia de Salida: 25dBm							
Especificaciones de Potencia TX				Especificaciones de Potencia RX			
Modulación	Tasa de datos	Avg TX	Tolerancia	Modulación	Tasa de datos	Avg TX	Tolerancia
Airmax ac	1x BPSK (1/2)	28 dBm	± 2dB	Airmax ac	1x BPSK (1/2)	-96dBm	± 2dB
	2x QPSK (1/2)	28 dBm	± 2dB		2x QPSK (1/2)	-95dBm	± 2dB
	2x QPSK (1/4)	28 dBm	± 2dB		2x QPSK (1/4)	-92dBm	± 2dB
	4x 16QAM (1/2)	28 dBm	± 2dB		4x 16QAM (1/2)	-90dBm	± 2dB
	4x 16QAM (1/4)	28 dBm	± 2dB		4x 16QAM (1/4)	-86dBm	± 2dB
	6x 64QAM (2/3)	28 dBm	± 2dB		6x 64QAM (2/3)	-83dBm	± 2dB
	6x 64QAM (3/4)	27 dBm	± 2dB		6x 64QAM (3/4)	-77dBm	± 2dB
	6x 64QAM (5/6)	26 dBm	± 2dB		6x 64QAM (5/6)	-74dBm	± 2dB
	8x 256QAM (3/4)	24 dBm	± 2dB		8x 256QAM (3/4)	-69dBm	± 2dB
	8x 256QAM (5/6)	22 dBm	± 2dB		8x 256QAM (5/6)	-65dBm	± 2dB

2.9 SEGURIDAD PARA REDES DE TELECOMUNICACIONES

La seguridad de una red se reduce a la protección de la información contenida en la misma, protegiéndola de factores externos como ciberdelincuentes, o algún tipo de programa maligno. [34] El nivel de riesgo depende de la información que se esté transmitiendo o almacenando, la información se considera sensible cuando se trata de centros médicos, centros militares, municipios, datos de gobierno, etc.

Los programas malignos son aplicativos de ciberdelincuentes que tienen diferentes resultados, básicamente son programas informáticos que no queremos encontrarlos. Sin embargo, las técnicas de ejecución de estos ataques informáticos son muy ingeniosos, entre estos, los puntos de acceso con el fin de capturar a la víctima objetivo, el phishing en el uso del correo electrónico, entre otros métodos que permiten el acceso a la información. [35]

2.9.1 TIPOS DE PROTOCOLOS

En la capa de Aplicación del modelo Open System Interconnections (OSI), se encuentran protocolos que se necesitan para la gestión y administración de la Intranet, tales como:

- FTP: admite el intercambio de archivos entre sistemas principales de forma directa. [36]
- DNS (Domain Name System): es una disposición del nombre en la red TCP/IP de internet. [37] Por norma una empresa u organización cuenta con un dominio único para poder nombrar a las plataformas que contiene, como: correo electrónico, plataformas de trabajo, páginas webs institucionales, entre otros.
- DHCP (Dynamic Host Configuration Protocol): asigna automáticamente un host de Protocolo Internet con su dirección IP y Gateway. [38] Es el típico protocolo para asignar y configurar la ip de un dispositivo que forma parte de una red, ya sea en dispositivos finales, como en las vlans para acceso a usuarios recurrentes.
- HTTP: admite el intercambio de información o de archivos de tipo XML, HTML o pdf. Esto se realiza para su propio funcionamiento en la World Wide Web tal como HTML o CSS para su maquetación. [39]
- TELNET: es un protocolo que establece la comunicación estándar de dispositivos finales. Mediante la emulación de una terminal remota le permite al usuario iniciar sesión en un sistema principal externo. [40] Su principal uso es como iniciador de una sesión remota, lo que se utiliza para la administración por la línea de comando de un dispositivo final desde su servidor de internet.
- SSH: Brinda la opción de un ingreso remoto a un portal web, mediante un canal que ofrece seguridad donde la información se encuentra protegida. [41] La parte cifrada es una de las diferencias que la convierten en un protocolo de comunicación necesario para la protección de una red, brindándole seguridad a una red insegura. El control sobre direccionamiento de puerto con SSH, es la característica más importante para la administración de puertos de usuarios de este protocolo, ya que su acceso remoto a usuarios finales estará con protección de una clave SSH.
- Putty es un cliente SSH y TELNET, es de código libre para Windows. Sus siglas son Pu: Puerto Único TTY: Teletipo, como resultado significa el Teletipo de Puerto

Único. [42] Tiene diversas características, como: control en direccionamiento de puertos con SSH y soporte para conexiones de puerto serie local.

2.9.2 TIPOS DE AMENAZAS EN LA RED

Programa maligno. - Aquí se agrupan los diferentes tipos de amenazas en la red, donde encontraremos: virus, troyanos, gusanos, rasonware, DDos, Rootkits, Puertas traseras, entre otros. [43] [44]

Wardriving. - Cuando se intenta conectar u obtener información de una red Wifi en movimiento, dentro de un vehículo o en cualquier otro medio de transporte se lo puede denominar Wardriving. [45] Con la ayuda de otras herramientas se puede crear una especie de radar wifi con localización por medio del GPS.

2.9.3 SOLUCIONES EN SEGURIDAD

VPN es una de las soluciones más versátiles que existe para una red extensa, esto debido al cifrado de los datos y la subdivisión para su administración. [46] Para la creación de una VPN se debe considerar la categoría en la que esta va a operar, ya que esta categoría se debe adaptar a los estándares de la empresa, por ejemplo: VPN con seguridad que generen confianza, VPN basadas en el cliente al borde de la web, VPN de red interna o subcontratada. [47]

FIREWALL puede ser un equipo físico o un software, ya sea que este se ubique en una puerta de enlace de servidores o para la filtración de paquetes. [48] Las prácticas de protección de información se las realiza en los puntos de acceso a lo largo de la red, para la protección de puntos de acceso se utilizan softwares o hardware llamados Firewall, los que sirven para el monitoreo y control de una red empresarial o una red troncal. [49]

SOPHOS es una empresa encargada de brindar protección contra programas malignos, mediante equipos y servicios para usuarios finales o redes en general. [50] Su último lanzamiento en equipos firewall cuenta con un chip de siguiente generación. Posee una arquitectura Xstream particular dedicada a descifrar, inspeccionar y acelerar aplicaciones en vista de un ataque cibernético. [51]

2.9.4 SEGURIDAD EN EQUIPOS DEL NÚCLEO DE LA RED.

Los equipos principales de información en una empresa deben estar en un cuarto de comunicaciones. Deben contar con su respectiva seguridad como controles de acceso en puertas, ya sea con una llave única, o con biométricos de alta tecnología, como reconocimiento facial, o sensor de huella dactilar. [52] Esta habitación debe estar con temperatura de máx. 24 grados centígrados.

En el cuarto de comunicaciones se encuentran los servidores con la información de mensajería por correo, o programas de dominios asociados a las aplicaciones institucionales. Se prioriza el aseguramiento de puertos en equipos conmutadores desde la interfaz de administración del equipo, con el fin de mitigar ataques en las subredes en modo de área. Un ataque en capa 2 del modelo OSI es un ejemplo de los peligros ya mencionados, por eso se recomienda utilizar las listas de control de accesos (ACL) siempre depuradas y monitoreadas para tener un control de los usuarios y sus permisos de acción. [53]

2.9.5 SEGURIDAD EN EQUIPOS INALÁMBRICOS

Una vez se aseguran las puertas principales al usuario final, se le recomiendan ciertos parámetros para el uso de navegación en internet y protección para evitar la violación a la información. Para los Access point que se usan para expandir la cobertura de la intranet, existen las contraseñas para las redes inalámbricas que se las representan con el protocolo WPA2. [54]

Como parte del refuerzo en una WLAN [55], existen 3 tipos de protocolos: WEP, WPA, WPA2 y WPA3. Wired Equivalent Privacy (WEP) tiene un nivel de cifrado muy leve por lo que no se utiliza, está basado en un algoritmo llamado RC4. [56]

Wifi Protected Access (WPA) van detectando vulnerabilidades en el algoritmo de cifrado, a esto se debe su evolución y migración de un protocolo de WPA a WPA2. WPA2 es el protocolo que recomienda utilizar la IEEE. [54]

2.10 LICENCIAS Y REGULACIONES

En Ecuador existen diversas regulaciones para el establecimiento de radioenlaces, estas dependen de la zona en la que se va a llevar a cabo el trabajo y la región del espectro radioeléctrico en el que se va a operar.

El control y manejo del espectro radioeléctrico es competencia de ARCOTEL. Para realizar trabajos de este tipo, es necesario presentar una solicitud donde se pueda verificar que se cumple con todos los requisitos que requeridos por ARCOTEL. Además, es necesario pasar por un proceso evaluatorio a cargo de la misma agencia [57].

El trámite de registro de los radioenlaces no es necesario en esta ocasión, ya que se trabaja únicamente con las bandas radio industriales científicas y médicas o mejor conocidas como bandas ISM. En Ecuador estas bandas corresponden a las frecuencias de 2.4GHz y 5GHz [58].

2.11 PERMISO DE TORRES DE ANTENAS

La instalación de torres de comunicaciones ya sean estas, radio bases, celulares o de telecomunicaciones en general, están reguladas bajo la ley No.29022, la cual se conoce como Ley Orgánica de Telecomunicaciones. La misma en su art. 3 dispone “Promover el despliegue de redes e infraestructura de telecomunicaciones que incluyen audio, video y similares, bajo el cumplimiento de normas técnicas, políticas nacionales y regulación de ámbito nacional relacionadas con el ordenamiento de redes, soterramiento y mimetización” [59].

Debido a la ley ya mencionada, se entiende que los permisos para un nuevo asentamiento de una torre de radio en el Ecuador corresponden a un procedimiento de aprobación automática, siempre y cuando el solicitante presente una lista de requisitos, entre estos se encuentran:

- Instrumento de Gestión Ambiental.
- Autorización DGAC.
- Autorización expuesta por parte del ministerio de Cultura.
- Normas Técnicas que será aplicadas para su comprobación por ARCOTEL.

- Certificado para proponer una nueva región Natural Protegida o sus Zonas de Amortiguamiento ecológico.

El instrumento de Gestión Ambiental hace referencia a la presentación de una ficha técnica, la cual se utiliza como herramienta para llevar a cabo la gestión ambiental exigida por ley. Así mismo, es requerida una declaración de impacto ambiental donde se estipule el cálculo de radiaciones ionizantes y no ionizantes. La ubicación de la torre y su impacto en las áreas naturales donde se planea levantar la estructura.

La dirección General de Aviación Civil requiere brindar su autorización a razón de tener conocimiento de los parámetros de la torre, con la finalidad de restringir correctamente los límites de altura en los vuelos que crucen por la región, esto en afán de evitar accidentes e inconvenientes en la planificación de vuelos con aeródromos cercanos en la zona. Por ley es necesario el certificado del SERNAMP para evitar la intervención en áreas protegidas [57].

La autorización del ministerio de Cultura es necesaria para comprobar que no existan restos arqueológicos en la ubicación, y evitar que ciertos bienes culturales (monumentos o patrimonios) se vean afectados.

Se deben cumplir con las normas técnicas de ubicación

- (i) La torre no se puede ubicar a menos de 100 metros de otras estaciones SGNER.
- (ii) Si la torre se ubica a 500 metros de cualquier Estación SGNER; por obligación la torre deberá constar de una altitud de al menos 20 metros.
- (iii) Si la torre se colocará a una distancia desde 500 hasta 1,500 metros de una Estación de referencia, la altitud máxima permitida se obtendrá mediante la ecuación 2.

(la altura de la Estación SNGER cercana) + (0.052407779la distancia de separación). **(2)**

CAPITULO 3

3. SOLUCION PROPUESTA

La solución propuesta a la problemática planteada está dividida en dos etapas: El diseño de la solución para todas las unidades a flote atracadas en los muelles. La implementación de dos puntos de red para las unidades a flote en el muelle 5.

Antes de idear la solución, se recolecta la mayor cantidad de información ofrecida por DIRTIC. Esto incluye el estado de la infraestructura y las necesidades a cumplir con los objetivos del problema. Una vez se tenga noción acerca del funcionamiento de la red Naval, se realiza la inspección de los equipos y estaciones de trabajo que intervienen en la solución. Se logró idear una solución que consta con distintos módulos que le brindan una estructura a la misma. Estos módulos son parte del bloque inicial que se observa en la ilustración 7.

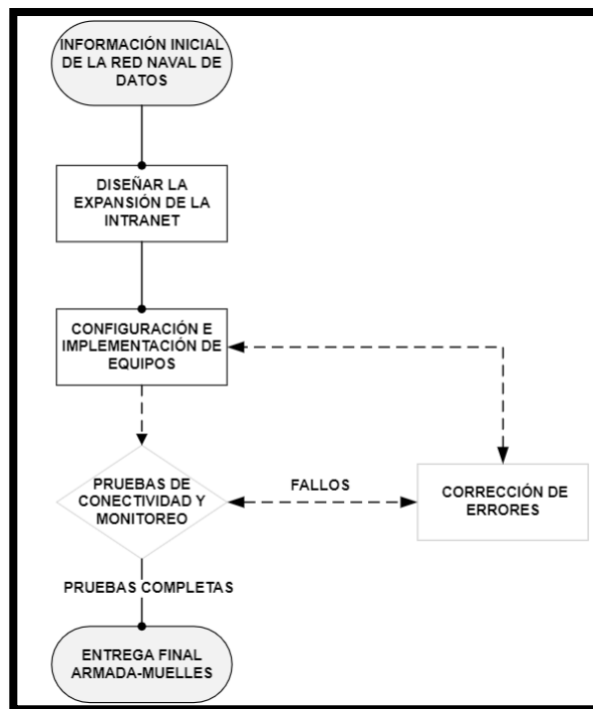


Ilustración 7 Diagrama de flujo de la solución propuesta

La primera etapa de la solución consiste en el diseño de una red que satisfaga las necesidades del proveedor. En esta ocasión, las necesidades que posee DIRTIC para sus clientes que son las unidades a flote.

La segunda etapa de la solución trata de la implementación de un segmento del diseño de la red, mediante los equipos provistos por DIRTIC y en conjunto con diversos materiales obtenidos por los autores de este proyecto. Con el fin de garantizar una correcta implementación de la solución propuesta, se realizan pruebas de conectividad y monitoreo de los equipos implementados.

Como se observa en la ilustración 7, se destina una sección de corrección de errores. En caso de ser necesario, esta se desarrolla posterior a la instalación de los equipos en las ubicaciones dispuestas en las áreas correspondientes según el diseño de la topología. Esta sección es utilizada para corregir los fallos presentados en el enlace.

Una vez finalizadas las pruebas de funcionamiento, en conjunto con personal de DIRTIC y los usuarios finales, se socializan los resultados de las etapas de la solución propuesta. A su vez, se consideran las mejoras que se pueden implementar con el diseño realizado, con la finalidad de que todas las unidades a flote dispongan de un punto de red en el muelle correspondiente.

3.1 DISEÑO DE LA SOLUCION PROPUESTA

En la etapa primera de la solución propuesta se presenta el diseño de una red WLAN. La tecnología base de la red está basada en el estándar IEEE 802.11ac y en el uso de la Red Naval de Datos para proporcionar el servicio de internet.

Este diseño, determinará la solución óptima para el problema presentado, estableciendo un punto de red en cada muelle. Dicho punto de acceso será de uso exclusivo para la unidad a flote más cercana atracada al muelle. Así mismo, se considera que pueden atracar hasta máximo 3 unidades por muelle, con miras al futuro estar en la capacidad de brindar los servicios de la Red a los usuarios de todas las unidades a flote.

DIRTIC en mejora de la calidad de servicio de enlaces microondas de los muelles en la base naval sur, tras pasar por la tecnología WiMAX y luego hacer pruebas con equipos de bajo rendimiento de tecnología Wifi, ha realizado la compra de equipos ubiquiti con características definidas.

Dichos equipos implementados en las diferentes tecnologías fueron instalados en la torre del COMACO y sobre las unidades a flote que se encuentran en la tabla 5. Los equipos en el enlace WLAN actual operan en la banda de 5 [GHz], se muestra en la tabla 5 los equipos que trabajan en dicha banda.

Tabla 5 Equipos de los enlaces actuales de microondas

Nº	UBICACION	EQUIPO	MARCA	MODELO	SERIAL
1	TORRE DEL COMACO	AP	UBIQUITI	NBE-M5-19	0418D6AAB2F2
2	CORESM	CPE	UBIQUITI	NBE-M5-19	0418D6AAB2F3
3	FRAPAL		UBIQUITI	NBE-M5-19	0418D6AAB2F4

Como argumento del problema, en la tabla 6. se muestran las velocidades de navegación de la antena CPE destinada para la unidad CORESM que es inferior 5 Mbps afectando la calidad de servicio en los usuarios finales.

Tabla 6 Prueba de velocidad en CPE-CORESM

PRUEBA DE VELOCIDAD	DESCARGA [Mbps]		SUBIDA [Mbps]	
	ACTUAL	PROMEDIO	ACTUAL	PROMEDIO
CORESM	1.9	1.9	1.9	3

En la ilustración 8, podemos identificar los diferentes componentes que forman parte del diseño propuesto para el desarrollo de la solución propuesta.

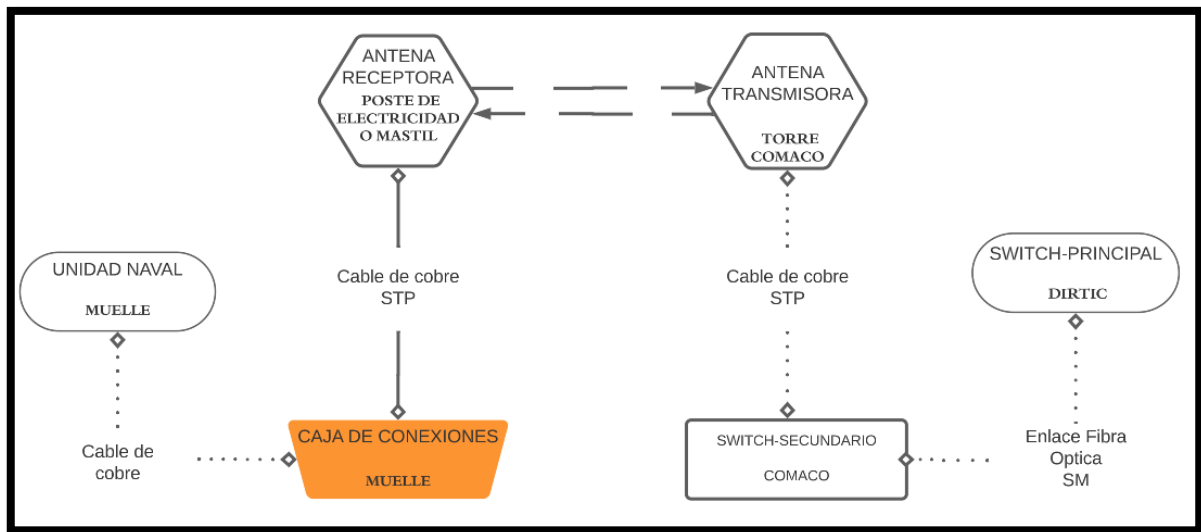


Ilustración 8 Diagrama de bloques de la solución propuesta

Desde las oficinas de DIRTIC inicia la infraestructura de la intranet que se empleara en este desarrollo. Se extiende hacia la torre del COMACO mediante un enlace de fibra óptica Monomodo con un transceptor de hasta 1 [Gbps].

El área de cobertura que tendrá la red aproximadamente es de 7 [Km²]. Dicha área tiene los siguientes límites cardinales: al norte la “Coop. Nueva de octubre”, al sur con el barrio Sandino 4, al oeste con el estero del muerto, y al este con el barrio “12 de octubre”. La elevación del lugar en promedio es de 11 m.s.n.m

Se tomaron las mediciones de las ubicaciones de los puntos donde se ubican los equipos, utilizando un GPS modelo Garmin 1000. Posteriormente dichos puntos se utilizarán para visualizar el funcionamiento del segmento red, en un software de monitoreo, obteniendo así lecturas precisas.

El AP se encuentra ubicado a 50 [m] de altitud en la torre del COMACO, en coordenada geográfica (latitud y longitud) -2.26444, -79.900281. Esta se tomará en cuenta para el diseño de la WLAN propuesta, este dato se menciona en la tabla 7.

Como se muestra en la Ilustración 9. desde la antena CPE se traza el recorrido hasta un punto de red en una caja de conexiones en los muelles, utilizando cable STP CAT6.

Para proteger de la corrosión se utilizan conectores rugerizados. En la caja de conexiones se deja un conector hembra para cada unidad correspondiente. Máximo se tiene previsto que hallan 3 unidades a flote en el mismo muelle.

El cable desde la antena CPE hasta el PoE de la misma antena no puede exceder los 80 metros. El cable desde la caja de conexión hasta el PoE es responsabilidad de la unidad a flote, así como el equipo que se provee para el uso de la RND e Internet.

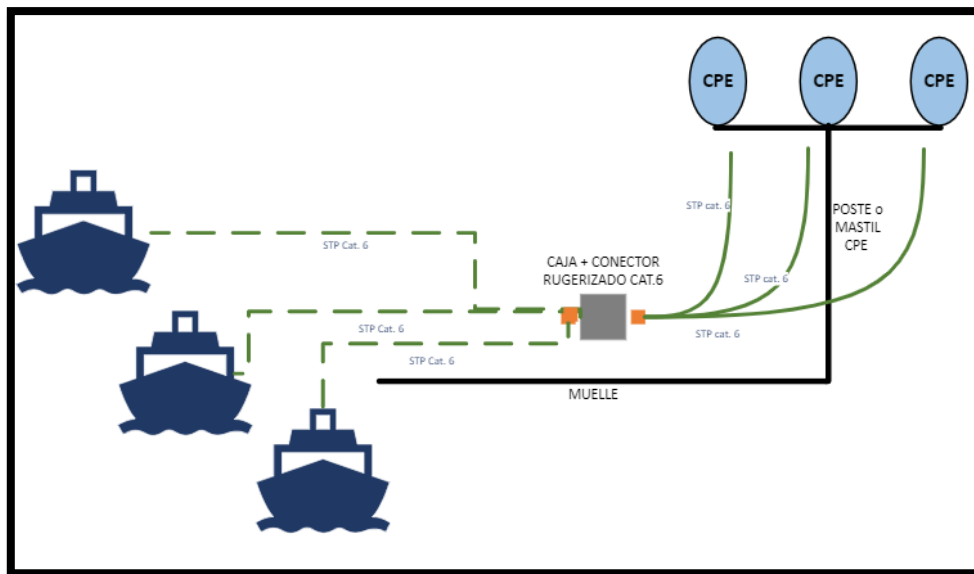


Ilustración 9 Conexión entre el equipo receptor y la unidad naval

Muelle 1. Las coordenadas geográficas (latitud y longitud) de este muelle son: - 2.262399, -79.908996.

Se considera que atracan 3 unidades. La distancia desde el poste de electricidad hasta el punto donde se pretende ubicar la caja de conexiones es de 33 metros.

Resultado de la inspección en las unidades, se recomienda utilizar el poste de energía como parte del mástil de las 3 antenas para cada unidad a flote respectivamente.

Muelle 3. Las coordenadas geográficas (latitud y longitud) de este muelle son: - 2.261646, -79.909634.

Existen 3 unidades a flote que atracan en este muelle. Resultado de la inspección en las unidades, se recomienda utilizar un mástil únicamente para posicionar los 3 equipos para cada unidad a flote respectivamente.

Evitando los 38 metros de cable de par trenzado STP que necesitaría la tercera unidad atracada en el muelle para su cableado interno, logrando ofrecer los servicios.

Muelle 4. Las coordenadas geográficas (latitud y longitud) de este muelle son: - 2.26123, -79.910009.

Este muelle cuenta con el mismo tipo de unidades que el muelle 3. Sin embargo, la distancia entre el muelle y el poste de electricidad es mayor que la del muelle 3. Por lo que se recomienda utilizar un mástil únicamente para ubicar los equipos de las unidades a flote.

Muelle 5. Las coordenadas geográficas (latitud y longitud) de este muelle son: - 2.261317, -79.910559.

En este muelle atracan 2 unidades a flote, y la distancia es mencionada en la tabla 7. Se utiliza el poste de electricidad como parte del mástil de los 2 equipos correspondientes a cada unidad a flote. El resultado de la simulación en este muelle será de gran ayuda para la implementación de los respectivos enlaces.

Muelle 6. Las coordenadas geográficas (latitud y longitud) de este muelle son: - 2.262577, -79.911383.

En este muelle se encuentra un tipo de unidad a flote de gran tamaño, por lo que se sugiere utilizar un mástil para la antena correspondiente. Todo esto para evitar el movimiento del equipo CPE, lo que puede causar Interferencia Inter Simbólica (ISI). En la actualidad el equipo CPE se ubica en un mástil sobre la unidad a flote, en la parte superior de la misma. En la sección de monitoreo y corrección de errores con ayuda del software se evidenciará el resultado del fenómeno multipaso.

Muelle 8. Las coordenadas geográficas (latitud y longitud) de este muelle son: - 2.263331, -79.911589. La distancia del muelle es muy extensa, donde se sugiere utilizar un mástil que soporte una antena CPE para dicha unidad.

Muelle 9. Las coordenadas geográficas (latitud y longitud) de este muelle son: - 2.264617, -79.91186.3. Al igual que el muelle 8, la distancia es mencionada en la tabla 7, se sugiere utilizar un mástil designado a la unidad correspondiente que soporte la antena CPE.

Tabla 7 Coordenadas de Muelles y Torre

RADIO AP - MUELLES CPE		DISTANCIA MUELLE-POSTE ELECTRICIDAD	COORDENADAS
M U E L L E	1	33	-2.262399, -79.908996
	3	38	-2.261646, -79.909634
	4	45	-2.26123, -79.910009
	5	31	-2.261317, -79.910559
	6	36	-2.262577, -79.911383
	8	50	-2.263331, -79.911589
	9	50	-2.264617, -79.911863
AP	1	N/P	-2.26444, -79.900281

El diagrama de red está representado por la ilustración 10, en esta se reflejan las direcciones de gestión para la antena y dirección de usuarios finales, datos del enlace de radiofrecuencia, equipos disponibles y sobre todo un esquema general del diseño de red inalámbrica.

La banda sugerida es de 5 [GHz]. Sin embargo, hay que aprovechar el rango de frecuencias que tienen los equipos para elegir el canal con menor interferencia. Para esto se realiza con un barrido de frecuencias desde el equipo transmisor mencionada en la sección 2.8, este puede ser evidenciado en la ilustración 24 en el capítulo 4.

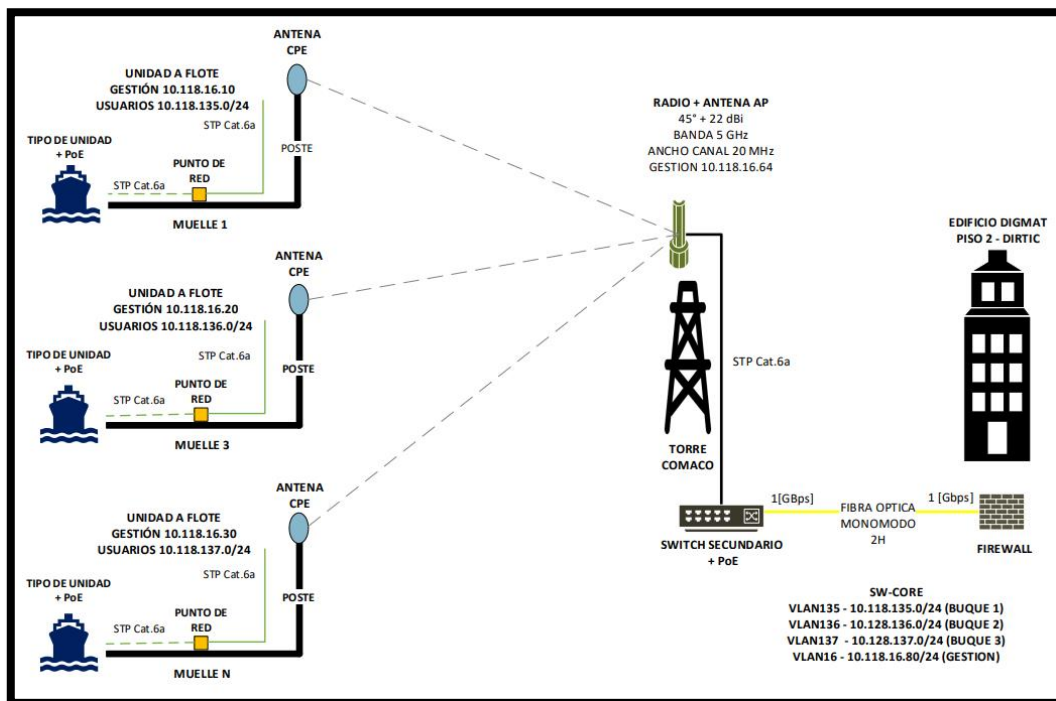


Ilustración 10 Diagrama de expansión de la intranet

DIRTIC asigna el direccionamiento ip para un acoplamiento a la intranet existente, la red de gestión es 10.118.16.64 mascara 255.255.255.0 para los enlaces WLAN hacia las unidades a flote.

Los usuarios utilizarían la IP: 10.118.137.0 mascara 255.255.255.0 como se muestra en la Ilustración 10 del muelle N. Debido a la sensibilidad de los datos, los direccionamientos IP y asignación de usuarios, será provisto DIRTIC.

Para tener una mejor apreciación de la WLAN se realiza una simulación de los enlaces propuestos como se observa en la Ilustración 11. Los equipos mencionados en la sección 2.7 corresponden al equipo CPE (Equipo Local Cliente) y en la sección 2.8 se encuentra el equipo transmisor denominado AP (Punto de Acceso) y sus respectivas características.

Para esto se utiliza el software de Ubiquiti que es una herramienta didáctica y precisa, donde analiza la orientación de las antenas, zona de Fresnel, alcance de los equipos, velocidad de transmisión estimada, etc.

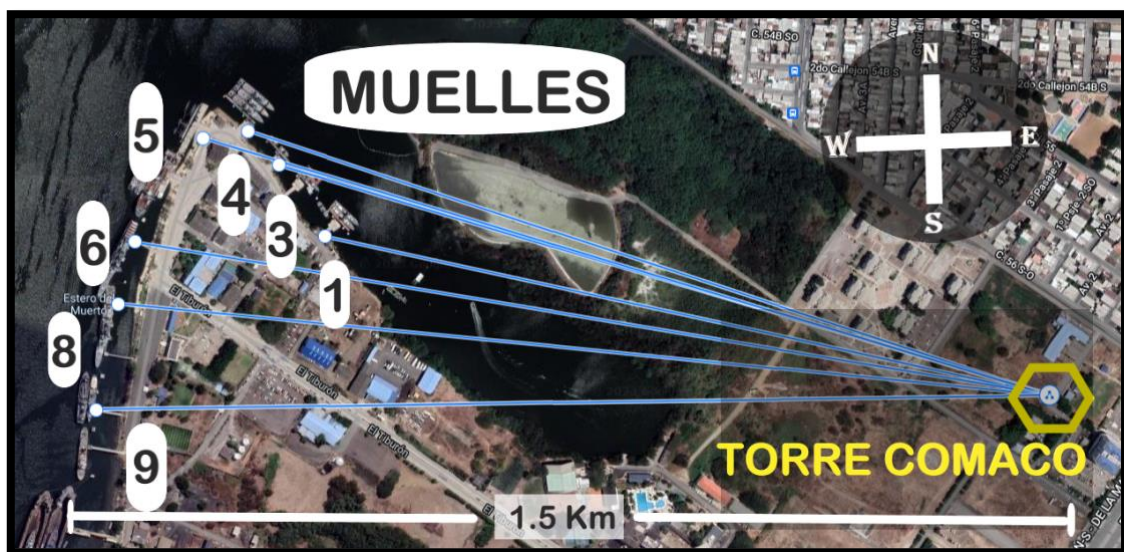


Ilustración 11 Simulación de los enlaces WLAN desde Torre COMACO hasta 7 muelles

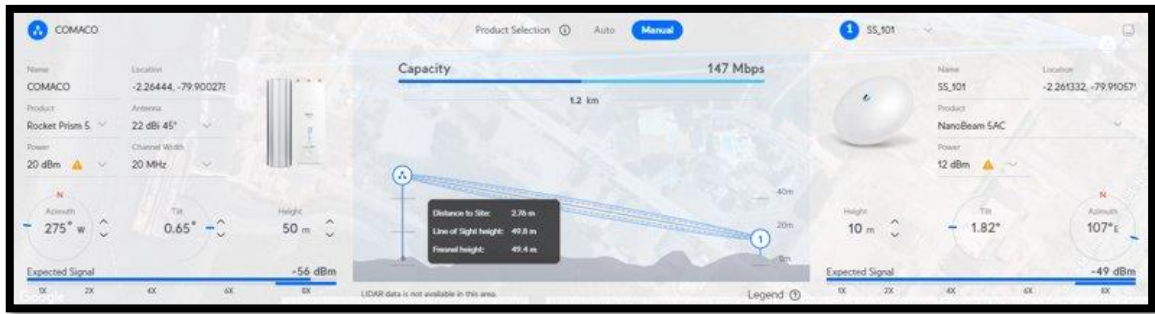


Ilustración 12 Simulación de enlace WLAN desde Torre COMACO hasta el muelle 5

La tabla 8 contiene los resultados obtenidos de la simulación tal como se observa en la ilustración 12. Este es el ejemplo del enlace para el muelle 5. De esta forma se obtienen los datos de orientación, azimuth, inclinación y altura de cada antena CPE ubicada en cada uno de los 7 muelles, ya sea del equipo de transmisión o recepción.

Tabla 8 simulación de cobertura con software de Ubiquiti

EQUIPO DE TRANSMISIÓN				
	COORDENADAS (Latitud y longitud)	ORIENTACIÓN	INCLINACION	ALTURA [m]
TORRE COMACO	-2.26444, -79.900281	275° W	0.65°	50
EQUIPO DE RECEPCIÓN				
# MUELLE	COORDENADAS (Latitud y longitud)	ORIENTACIÓN	INCLINACION	ALTURA [m]
1	-2.262399, -79.908996	103°E	2.71°	5
3	-2.261646, -79.909634	107°E	2.29°	5
4	-2.26123, -79.910009	108°E	2.03°	5
5	-2.261317, -79.910559	107°E	2.05°	5
6	-2.262577, -79.911383	100°E	2.12°	5
8	-2.263331, -79.911589	96°E	2.08°	5
9	-2.264617, -79.911863	89°E	1.9°	9

3.2 IMPLEMENTACION

En el diagrama de bloques de la ilustración 8 se pueden identificar los componentes necesarios para llevar a cabo la implementación mencionada en la ilustración 7. Se comienza estableciendo una conexión entre el Conmutador-PRINCIPAL ubicado en el edificio principal de la base, y el Conmutador- SECUNDARIO de la torre de control por medio de un enlace de fibra óptica.

Posteriormente, se procede a la instalación y configuración del equipo transmisor en la torre de comunicaciones COMACO (CAE). Se establece el enlace punto-multipunto con los equipos receptores en los postes de luz, los cuales están ubicados en los muelles cercanos a las unidades navales.

A continuación, en el cuarto de comunicaciones del edificio donde se encuentra el conmutador-Principal, se realizó la configuración de la red, esta pudo ser posible con el usuario y contraseña del jefe de DIRTIC. Aquí se pudo realizar la creación de las VLANs destinadas para el segmento de red a utilizar. De la misma manera se pudo habilitar los enlaces troncales en las VLANs, estos se basan en el estándar IEEE 802.1q para habilitar el tráfico entre ellas sin la necesidad de un enlace físico. Se habilitaron las direcciones IP a utilizarse en las unidades. Dado a que la configuración se realizó para operaciones militares, no es posible mostrar los comandos utilizados en esta etapa de la implementación.

Se muestran las especificaciones para el primer enlace el cual se utiliza de referencia para los demás. La configuración de los equipos se realizó mediante el UISP, el cual es un software de configuración y monitoreo propio de los equipos de la marca UBIQUITI.

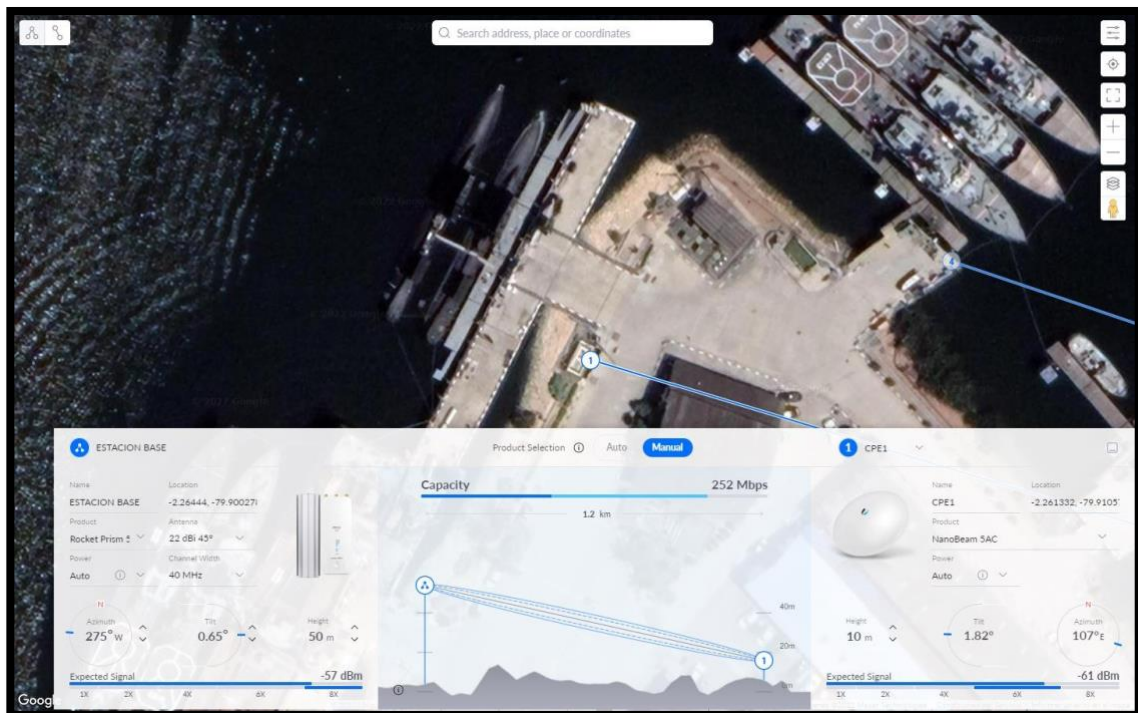


Ilustración 13 Primer punto de conexión

En la ilustración 14, se observa la torre principal de la base donde se ubica el equipo transmisor, de igual forma se muestra la ubicación de los equipos receptores ubicados en el muelle 5. Estos equipos son los correspondientes para las dos unidades en las cuales se llevará a cabo la implementación. Dichas unidades son 2 submarinos bautizados Shyri y Huancavilca



Ilustración 14 Torre Principal



Ilustración 15 Ubicación de equipos receptores

Como se muestra en la ilustración 16, el cableado pasa a través de un ducto cajón ubicado a un costado de los muelles. Se usa la manguera corrugada BX mencionada en el capítulo 2 sección 2.6.3 como medida de protección.

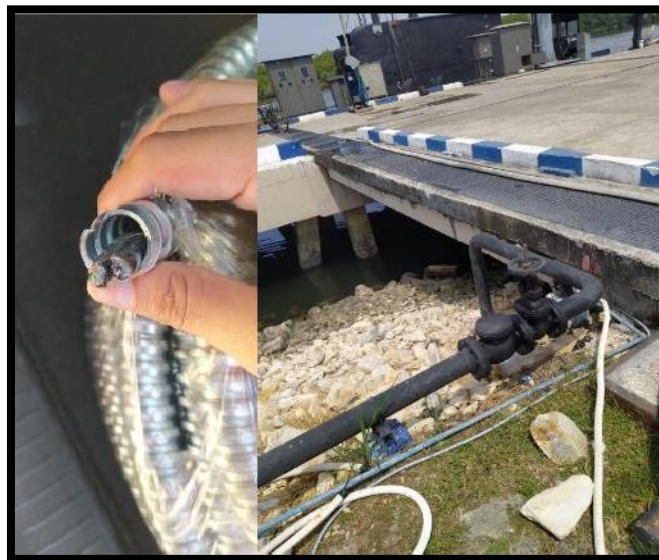


Ilustración 16 Protección del cableado

Al extremo de cada cable se instalaron los conectores rugerizados, un extremo se conecta a los equipos receptores y otro extremo se ubica en una caja de conexiones en el muelle que protegerá los puntos de red,

esto se visualiza en la ilustración 17. Esto con la finalidad de que las unidades se conecten y se desconecten según sus requerimientos. La caja mencionada cuenta con la certificación para trabajar en ambientes salinos.



Ilustración 17 Ubicación de la caja de conexiones

Para evitar algún inconveniente con la instalación de los cables, se llevó a cabo una prueba de continuidad luego de la instalación de los conectores. Como se muestra en la ilustración 18 la prueba se llevó a cabo utilizando la herramienta Wire Tracker. Esta prueba resultó exitosa y nos brinda la seguridad que el empalmado de los conectores se realizó correctamente



Ilustración 18 Prueba de funcionamiento del cableado

Con la finalidad de comprobar el funcionamiento óptimo del primer enlace, se obtuvieron los permisos para ingresar a una unidad a realizar pruebas de conectividad, en este caso la unidad es el submarino Shyri la cual se muestra en la Ilustración 19



Ilustración 19 Unidades en las que se llevó a cabo la implementación

En el interior de la unidad se pudo observar el AP marca Cisco, este se utiliza para dar señal de internet a todos los tripulantes en su interior. Se procedió a realizar su configuración según las especificaciones que se desean, se llevó a cabo su direccionamiento según lo estipulado por DIRTIC. Esto puede ser evidenciado en la ilustración 20.



Ilustración 20 Punto de acceso al interior del submarino Shyri

Posterior a la configuración del equipo mencionado se llevó a cabo una prueba de conectividad para comprobar su funcionamiento. Dicha prueba puede ser evidenciada en la sección Resultados y Análisis de este documento.

CAPITULO 4

4. RESULTADOS Y ANALISIS

Continuando con la secuencia lógica de los demás capítulos, en este apartado se lleva a cabo la muestra de los resultados que corresponden a la parte de implementación del proyecto. Así mismo, se lleva a cabo el análisis de diferentes variables de interés. Esto con la finalidad de demostrar el correcto funcionamiento de proyecto.

4.1 ANÁLISIS DEL ESTADO DEL SISTEMA ANTERIOR A LA IMPLEMENTACIÓN

El diseño provisional que se encontraba trabajando con limitaciones en la base militar, constaba con el uso de un sistema CPE-Cliente como equipo transmisor. La ilustración 21 corresponde a la vista desde el equipo utilizado como transmisor hacia los muelles, el cual se encontraba instalado en la torre CAE a una altura de 35 metros, de forma tal que exista una línea de vista solamente con algunas de las unidades navales.



Ilustración 21 Equipo transmisor antes de la implementación

De forma similar en las unidades a flote se encontraba instalado un equipo CPE-cliente en el lugar más alto de la embarcación para realizar el enlace con el equipo transmisor ubicado en la torre CAE, el CPE-cliente de la unidad tenía conexión directa con el rack principal de datos del barco. La ilustración 22 muestra el equipo receptor ubicado en lo más alto de una unidad naval, en la parte baja se visualiza una porción del muelle, además, se observa el soporte del equipo deteriorado por las condiciones donde está ubicado.

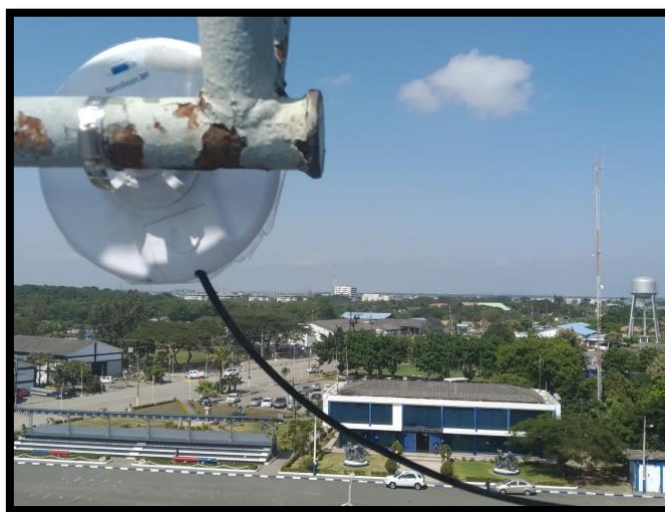


Ilustración 22 Equipo receptor en la unidad antes de la implementación

4.2 ANÁLISIS DEL ESTADO DEL SISTEMA POSTERIOR A LA IMPLEMENTACIÓN

La implementación de los nuevos equipos y su ubicación en las nuevas locaciones nos permite un enlace de comunicaciones más estable con respecto al sistema anterior ya mencionado.

La configuración de estos, ayudan a evitar las pérdidas de paquetes, facilitan el manejo y control del segmento de red, fortalecen la seguridad del tráfico que circula por la misma logrando una protección contra distintas amenazas.

Un aspecto importante de la configuración de los equipos que forman parte de este segmento de red es la frecuencia en la que estos trabajan. Para determinar que la configuración fue adecuada se llevó a cabo un barrido de frecuencias. Si bien se trabaja en la banda de 5GHz (Banda no licenciada) es óptimo conocer las frecuencias menos saturadas para mejorar la calidad de transmisión.

En la ilustración 23, se muestran las frecuencias escaneadas con los equipos de transmisión mencionados en la sección 2.7. en la banda de 5 [GHz] en el rango de 5.18 - 5.70 [GHz]. Resultado de este análisis se tiene que el mayor rango de frecuencias disponibles empieza en 5.3 [GHz] hasta 5.6 [GHz]. Por tal motivo dicho rango de frecuencias fue el elegido para la operación de los equipos.

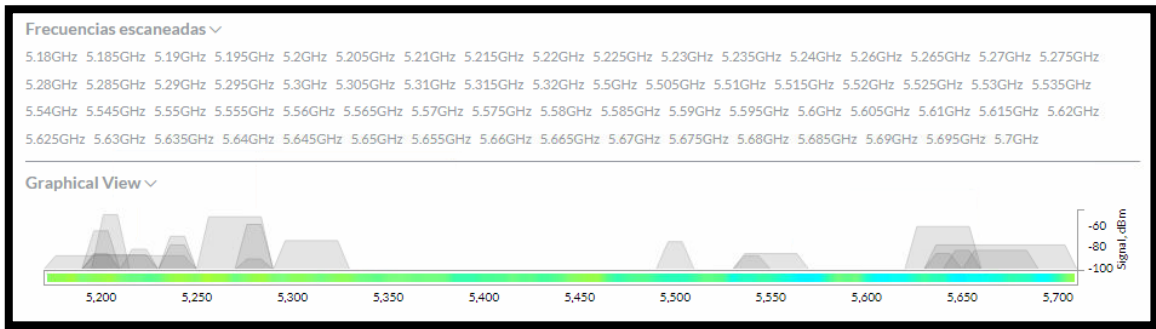


Ilustración 23 Barrido de frecuencias en la banda 5GHz

En nuestra implementación, los enlaces prioritarios estipulados por el cliente han sido los correspondientes a los 2 submarinos acoderados en los muelles de la base sur (Shyri y Huancavilca). Para efectos de una mejor comprensión en las pruebas que se muestran en este documento se utiliza de referencia los resultados que se obtuvieron de las pruebas realizadas en el submarino Shyri. Siendo así, el esquema de conectividad como se muestra en la ilustración.

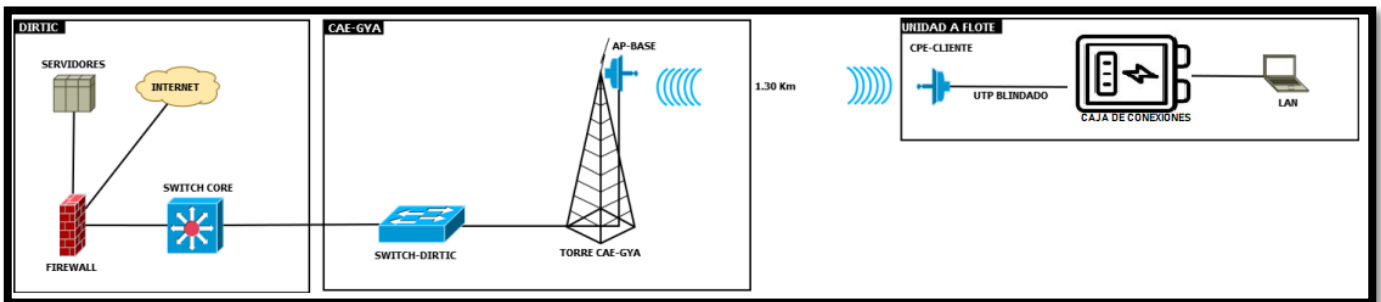
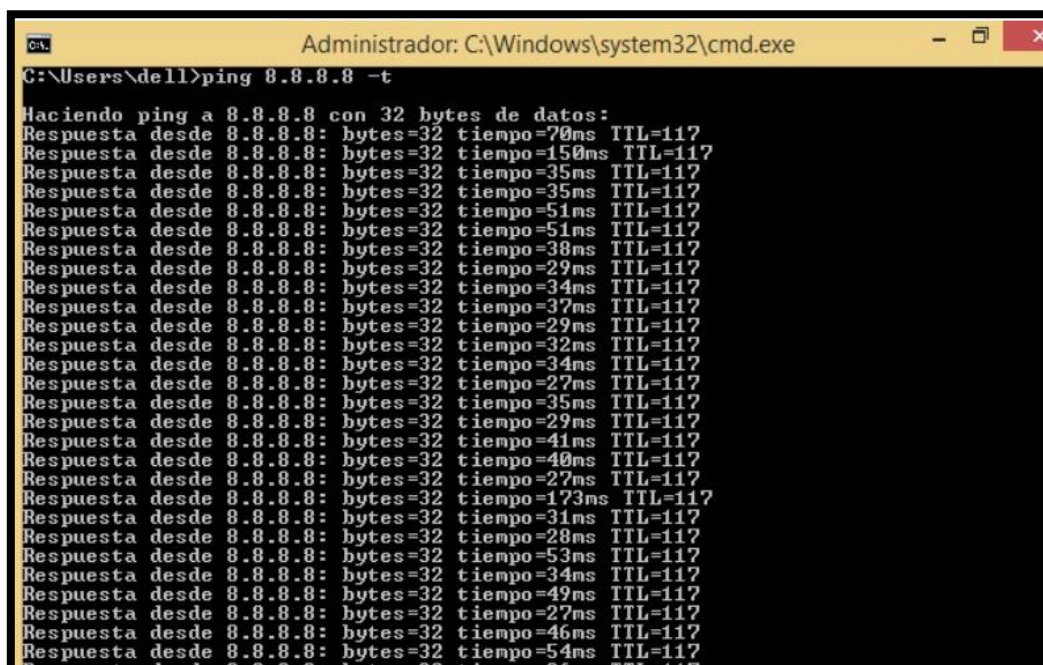


Ilustración 24 Esquema de conectividad para el submarino Shyri

4.2.1 PRUEBAS DE CONECTIVIDAD

Dado la configuración de la red, es posible realizar pruebas de conectividad y funcionamiento tanto en el interior de las unidades como desde las oficinas de DIRTIC. En el interior del submarino con el equipo receptor encendido nos conectamos vía wifi a la red LAN de la unidad la cual es manejada por el Access Point de su interior.

Una vez tenemos acceso a la red LAN de la unidad y dadas todas las configuraciones que se mencionaron en el capítulo anterior, en este punto deberemos tener acceso a la Red naval de Datos y por consiguiente a internet. Es decir que podremos navegar por la web. Basados en esto realizamos una prueba ping a una dirección ip en línea, para comprobar que la conexión desde la unidad hacia internet es exitosa. En esta ocasión usamos la dirección de los servidores DNS de Google la cual es 8.8.8.8. Como se observa en la ilustración 25 la respuesta es exitosa y con un tiempo de respuesta bajo. Analizando estos datos obtenemos que el tráfico de datos desde la unidad es adecuado y lo suficientemente rápido para navegar por internet sin inconvenientes.



```
C:\Users\dell>ping 8.8.8.8 -t
Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=70ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=150ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=51ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=51ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=38ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=29ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=34ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=37ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=29ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=32ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=34ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=27ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=29ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=41ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=40ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=27ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=173ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=31ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=28ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=53ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=34ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=49ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=27ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=46ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=54ms TTL=117
```

Ilustración 25 Ping hacia los servidores DNS 8.8.8.8

Se determinó por medio de la terminal de un computador, que la prueba fue exitosa y no hubo perdida de paquetes. Posteriormente desde el mismo

computador, se ingresó a un navegador web para observar de forma visual la conexión a internet desde el submarino. Esto puede ser visualizado en la ilustración 26. Cabe mencionar que desde el interior de la unidad se pudo navegar por distintas páginas web, entre ellas el portal aula virtual de la universidad visualizada en la ilustración 27, e incluso se llevó a cabo una videollamada por WhatsApp con el personal militar que trabaja en DIRTIC.

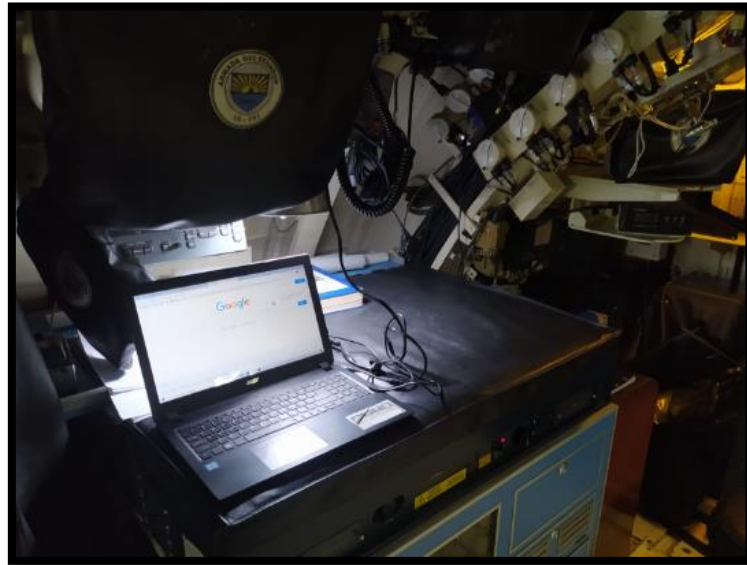


Ilustración 26 Vista de la página principal de Google en el computador al interior del submarino

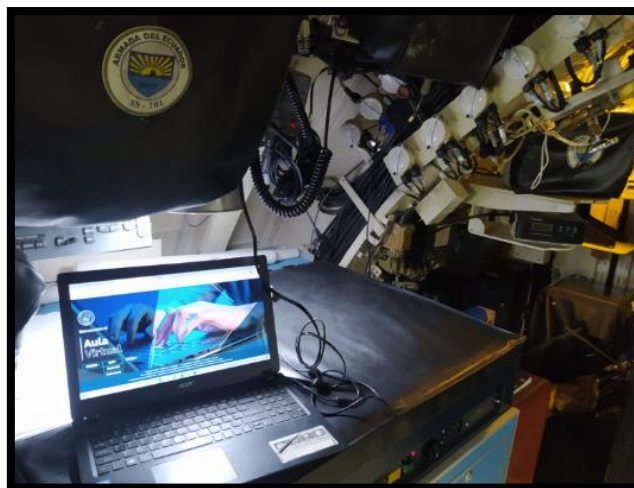


Ilustración 27 Imágenes de navegación Web al interior del submarino

Una gran ventaja que tenemos al utilizar equipos de la marca Ubiquiti es que esta cuenta con un software de monitoreo en tiempo real. Por medio de dicho software

es posible conocer el estado de los equipos, el estado del enlace y realizar pruebas de conectividad directamente desde las oficinas de DIRTIC.

El programa es muy completo y nos muestra una amplia variedad de datos y variables tal como se observa en la imagen anterior. Sin embargo, para facilitar la comprensión lectora y hacer énfasis en datos de variables relevantes los datos recaudados de las pruebas se pueden visualizar en la siguiente tabla.

Tabla 9 Estado del enlace y parámetros básicos

AP DIRTIC						
TIPO	ESTADO	MAC ADDRESS	NOMBRE DEL DISPOSITIVO	MODELO	ULTIMA IP	LATENCIA
CPE-CLIENTE	ACTIVO	E0:63:DA:D2:1F:9D	CPE-SS-101	NanoBeam 5AC	10.128.61.49	1ms

Tabla 10 Resultados del monitoreo del enlace

ESTADO DEL ENLACE			
DISTANCIA	1.20 KM		
FRECUENCIA	5690 MHz		
ANCHO DE BANDA	20 MHz		
AP-DIRTIC		CPE-SS-101	
POTENCIA TX	24 dBm	POTENCIA TX	11 dBm
NIVEL DE RUIDO	-88 dBm	NIVEL DE RUIDO	-92 dBm
SNR	21 dB	SNR	28 dB

De la tabla 10 podemos conocer el estado del enlace el cual se encuentra activo al momento de realizar la prueba, eso quiere decir que la unidad se encontraba acoderada en el muelle y conectada a la red de la base.

En caso de que la unidad se encuentre navegando observaríamos que el estado del enlace sería inactivo. De igual forma podemos observar la distancia a la que se encuentran los dos equipos que forman el enlace, su frecuencia de trabajo de 5690MHz y el ancho de banda del canal 20MHz.

De los equipos podemos obtener diferentes lecturas individuales como se observa, la potencia de transmisión, el nivel de ruido y el SNR, con estos datos es posible deducir que el enlace es muy estable y la transferencia de datos será adecuada para las necesidades del cliente.


```
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 172.17.26.21:
  Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\Users\Carlos Galan>ping 10.128.61.49 -t

Haciendo ping a 10.128.61.49 con 32 bytes de datos:
Respuesta desde 10.128.61.49: bytes=32 tiempo=11ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=10ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=43ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=14ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=14ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=17ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=16ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=9ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=53ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=27ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=23ms TTL=63

Estadísticas de ping para 10.128.61.49:
  Paquetes: enviados = 11, recibidos = 11, perdidos = 0
    (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 9ms, Máximo = 53ms, Media = 21ms
Control-C
^C
```

Ilustración 28 Prueba ping realizada en el pc de control de la red

En la ilustración 28, observamos la prueba de ping realizada desde un computador en las oficinas de DIRTIC hacia el equipo receptor. De los resultados obtenidos podemos notar que no existen perdidas de paquetes y que tiene un tiempo de respuesta bajo, esto nos indica que el enlace implementado es estable.

Por último, se observa que la ilustración 29 que muestra el historial de latencia del enlace, remarcando como fecha importante el 17 de noviembre, esta fue la fecha donde el nuevo sistema entro en funcionamiento.

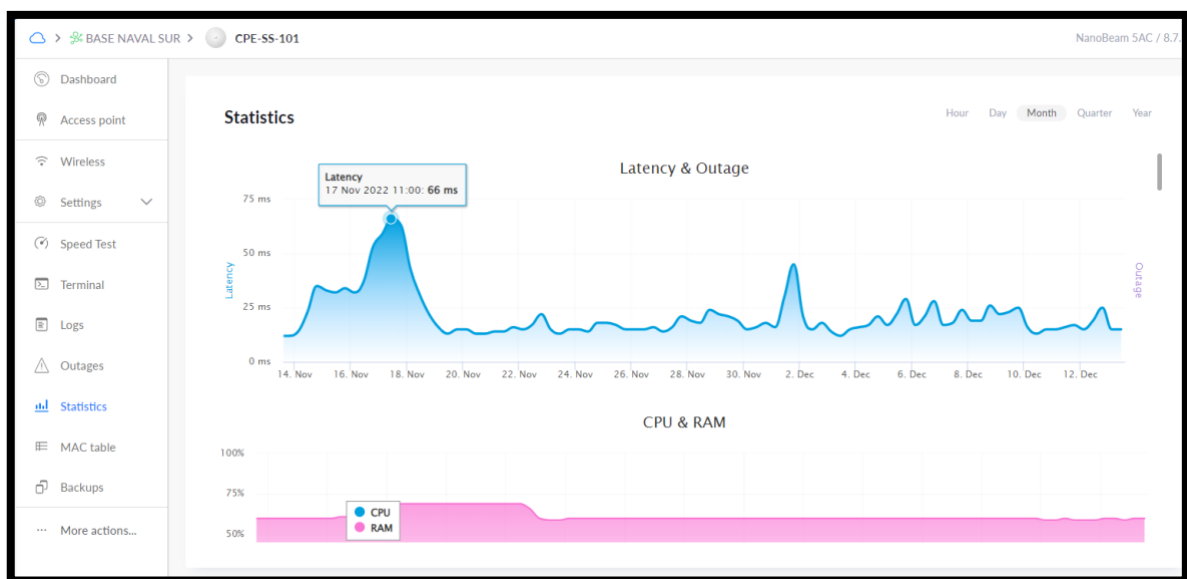


Ilustración 29 Historial de conexión y latencia del enlace

De esta grafica se muestra un nivel de latencia relativamente bajo. Es necesario aclarar aquellos picos que se observan en la gráfica, los cuales corresponden probablemente a momentos en los que la unidad naval, se tuvo que conectar y desconectar por un periodo de tiempo debido a alguna actividad realizada.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Mediante la simulación que se verifica en la sección 3.1 ilustración 12 y las mediciones de las potencias de recepción de los equipos que se indican en la tabla 10, se pudo determinar las ubicaciones adecuadas designadas para los CPE-Clientes. Estas localizaciones aseguran línea de vista constante entre los puntos de los enlaces, reduciendo la pérdida de paquetes en el tráfico de datos del segmento de red con relación al sistema que se encontraba implementado anteriormente. Estos lugares, inclusive permiten evitar la mala manipulación de los equipos por parte del personal militar no capacitado.
- Tal como se puede observar en el capítulo 3, se diseñó la topología del segmento de red implementado, el cual se detalla en la ilustración 10. De esta forma, se facilita el crecimiento de la red permitiendo agregar nuevos dispositivos en caso de que se requieran en un futuro. Además, se simplifica la detección de fallas y daños de equipos o infraestructura, sin afectar al funcionamiento de los demás equipos que trabajan en la red.
- Al conocer que la información que transita por la red es de carácter militar, sensible y prioritaria, se configuraron los equipos priorizando la seguridad contra posibles amenazas. Para alcanzar este objetivo se ejecutaron los protocolos que se detallan en las secciones 2.9.1 y 2.9.3. Como resultado se asegura que la información se encuentra protegida contra las amenazas especificadas en la sección 2.9.2.
- Con los resultados que se especifican en la tabla 10 se comprobó la adecuada calidad de los canales de comunicación. Con estos podemos concluir que dada la relación señal ruido de 28 dB, acompañada de una potencia de recepción de 11dBm y un ancho de banda de canal de 20MHz, el tráfico de datos es adecuado para las necesidades del cliente. Así mismo, se observa en la ilustración 29 que el promedio del nivel de latencia del enlace es bajo, alrededor de 12 ms.

RECOMENDACIONES

- Se recomienda instalar un transceiver para proveer internet que al menos tenga capacidad de 10/100 Mbps. Esto con la finalidad de evitar lentitud en el servicio, en el caso que todos los clientes se encuentren conectados al mismo tiempo.
- Dado que el segmento de red diseñado es para uso estrictamente laboral, se recomienda bloquear los permisos de navegación a diferentes páginas web que no sean utilizadas con fines laborales. Esto con la finalidad de evitar lentitud en el servicio usualmente debido al uso de plataformas de entretenimiento como redes sociales y video streaming.

BIBLIOGRAFIA

- [1] ARMADA DEL ECUADOR, «armada del ecuador,» [En línea]. Available: <https://www.armada.mil.ec/mision-1>. [Último acceso: 2022 10 30].
- [2] A. N. d. H. M. d. Ecuador, «issuu,» [En línea]. Available: https://issuu.com/anahimi/docs/historia_resumida_de_la_armada_part_afc0f61f3874b0/131#:~:text=La%20Dirtic%20realiza%20la%20gesti%C3%B3n,que%20cuenta%20la%20Armada%2C%20los.
- [3] UBIQUITI NETWORKS, *NanoBeam Gen2 Datasheet*, 2018.
- [4] D. d. t. d. l. i. y. c. Alex Tapia Chichande, «Informe de Necesidades DIGLOG,» Guayaquil, 2020.
- [5] Usail Maritime Communications, «usail,» 2022. [En línea]. Available: <https://www.usail.es/>. [Último acceso: 22 10 17].
- [6] BOAT SECURITY, «Boat security,» [En línea]. Available: <https://boatsecurity.com/seguridad-a-bordo/boat-net/>. [Último acceso: 2022 10 17].
- [7] D. R. V. P. S. A. M. V. R. a. V. R. S. N. Rao, «A novel solution for high speed internet over the oceans,» de *EEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops*, 2018.
- [8] LongShots SeattleWireless, 2018. [En línea]. Available: <https://archive.is/A78Ho>.
- [9] C. L. Y. Z. G. R. Z. W. Y. W. X. Ba, «A Novel Polarization and DOA Reliable Auto-Tracking,» *Multidisciplinary Digital Publishing Institute - MDPI*, 2022.
- [10] K. O. S. O. a. M. U. T. Yoshida, «Aerospace Research Central,» 2021. [En línea]. Available: <https://arc.aiaa.org/doi/pdf/10.2514/6.2003-5731>.
- [11] G. S. Aliaga, *Implementación e instalación de una antena satelital automática VSAT Intellian, en embarcaciones de la empresa Hayduk, para brindar servicio de datos de internet en altamar, en la empresa BMP Consulting SAC, Lima*, 2018.
- [12] G. R. VILLACORTA, *IMPLEMENTACIÓN DE UN SISTEMA DE TRANSMISIÓN DE DATOS SATELITAL PARA EMBARCACIONES PESQUERAS ANCHOVETERAS PARA OPTIMIZAR SU EFICIENCIA OPERACIONAL*, Lima, 2020.
- [13] R. G. Blanco., *INCIDENCIA DE LAS NUEVAS TECNOLOGÍAS EN LA SEGURIDAD DE LOS BUQUES*, España: Universitat Politecnica de Catalunya , 2018.
- [14] Cenautica, «Practicas de Radio,» 10 10 2022. [En línea]. Available: <http://www.practicasderadiocomunicaciones.com/Modules/Apuntes/tema18.aspx>.
- [15] M. V. Muñoz, «Revista Marina,» [En línea]. Available: <https://revistamarina.cl/revistas/2003/4/vasquez.pdf>.
- [16] «PUNTO SENCILLO CABLEADO HORIZONTAL CAT6A U/FTP,» Servicio Geologo Colombiano y Universidad Nacional de Colombia, [En línea]. Available: <https://www2.sgc.gov.co/centro-excelencia-geociencias/Bloque%201/Especificaciones%20tecnicas%20B1/11.%20INSTALACIONES%20DE%20VYD/11.%20INSTALACIONES%20VYD.pdf>.
- [17] C. F. V. PONCE, «DISEÑO DE UN SISTEMA DE COMUNICACIÓN PARA LA EMPRESA,» 2019. [En línea].

- [18] K. N. O. O. y. J. A. P. CHACÓN, «ELABORACIÓN DE GUÍA TÉCNICA PARA EL DISEÑO E,» 2018. [En línea].
- [19] «INOCAR,» INOCAR, 2022. [En línea]. Available: <https://www.inocar.mil.ec/web/index.php/productos/tabla-mareas>.
- [20] I. M. E. Amaguaña., «ESTUDIO DE IMPACTO AMBIENTAL EX ANTE "DRAGADO DE LOS MUELLES DE LA BASE NAVAL SUR DE LA CIUDAD DE GUAYAQUIL EN EL ESTERO CARACOL",» INSTITUTO OCEANOGRÁFICO DE LA ARMADA, Guayaquil, 2019.
- [21] «WIKIPEDIA,» OCTOBER 2022. [En línea]. Available: <https://es.wikipedia.org/wiki/Salinidad#:~:text=La%20salinidad%20del%20agua%20es%20una%20variabl e%20que,y%20mares%20metahalinos%20de%2036%20a%2040%20%E2%80%B0..>
- [22] IEEE, 2018. [En línea]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8438748>.
- [23] M. Sheraz, Internet of Ships: A Survey on Architectures, Emerging Applications, and Challenges, IEEE, 2020.
- [24] Rice University, «Open stax,» [En línea]. Available: <https://openstax.org/books/f%C3%ADsica-universitaria-volumen-3/pages/1-6-principio-de-huygens>. [Último acceso: 2022 11 27].
- [25] Federal Communications Commission, «FCC,» [En línea]. Available: <https://www.fcc.gov/consumers/guides/interferencia-de-senales-de-radio-tv-y-telefonicas#:~:text=La%20interferencia%20ocurre%20cuando%20se%20B1ales,completo%20la%20rec epci%C3%B3n%20de%20se%20B1ales..> [Último acceso: 2022 11 27].
- [26] M. Aviles, «interferencia y difraccion,» de *Física 2do Bachillerato*.
- [27] J. Butler, E. Pietrosevoli, M. Zennaro, C. Fonda, S. Okay, C. ". Aichele y S. Büttrich., Redes inalámbricas en los países en desarrollo, Copenhagen: Creative Commons Attribution, 2013.
- [28] ENACOM, «Enacom,» [En línea]. Available: https://www.enacom.gob.ar/-que-son-las-interferencias-_p376.
- [29] WNI MÉXICO S.A., «wni mexico wireless solution,» [En línea]. Available: https://www.wni.mx/index.php?option=com_content&view=article&catid=31:general&id=50:los. [Último acceso: 2022 11 28].
- [30] G. L. Hernández y J. L. L. Bonilla, «Metodología para el cálculo adecuado de las alturas de antenas en un radioenlace de microondas en Línea de Vista,» *Revista Electrónica Nova Scientia*, p. 12, 2013 9 4.
- [31] R. Telemática y J. A. C. d. Portillo, «IEEE 802.22, SUPER WI-FI.,» Ciudad Habana, Cuba, 2017.
- [32] Eland Cables, «ELAND cables,» 2022. [En línea]. Available: <https://www.elandcables.com/es/cables/lan-cat-5e-6-6a-cable#:~:text=Los%20cables%20de%20la%20categor%C3%ADa%206A%20son%20compatibles%20con%20rangos,y%20con%20PoE%20y%20PoE%2B.&text=Los%20cables%20de%20la%20Categor%C3%ADa%207%20son%20cables%20de%20muy,de%2>
- [33] u. networks, *Sector Airmax Prism ac Datasheet*, 2018.
- [34] IBM, «Definición de seguridad de red,» sitio web, 2022. [En línea]. Available: <https://www.ibm.com/es-es/topics/network-security>. [Último acceso: 2022].

- [35] AMBIT, «Tipos de Vulnerabilidades y Amenazas informáticas,» Blog , 10 11 2020. [En línea]. Available: <https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas>. [Último acceso: 2022].
- [36] IBM, «Protocolo de transferencia de archivos (File Transfer Protocol),» IBM, 03 03 2022. [En línea]. Available: <https://www.ibm.com/docs/es/aix/7.1?topic=protocols-file-transfer-protocol>. [Último acceso: 2022].
- [37] IBM, «Domain Name System (DNS) Overview,» IBM, 03 03 2021. [En línea]. Available: <https://www.ibm.com/docs/es/aix/7.1?topic=services-domain-name-system-dns-overview>. [Último acceso: 2022].
- [38] Microsoft, «Protocolo de configuración dinámica de host (DHCP),» 21 09 2022. [En línea]. Available: <https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top>. [Último acceso: 2022].
- [39] WIKIPEDIA, «Protocolo de transferencia de hipertexto,» 19 11 2022. [En línea]. Available: https://es.wikipedia.org/wiki/Protocolo_de_transferencia_de_hipertexto. [Último acceso: 2022].
- [40] IBM, «PROTOCOLO TELNET,» IBM, 03 03 2021. [En línea]. Available: <https://www.ibm.com/docs/es/aix/7.1?topic=protocols-telnet-protocol>. [Último acceso: 2022].
- [41] WIKIPEDIA, «Secure Shell,» 30 05 2022. [En línea]. Available: https://es.wikipedia.org/wiki/Secure_Shell. [Último acceso: 2022].
- [42] PuTTY, «PuTTY,» Organizacion, 2022. [En línea]. Available: <https://www.putty.org/>. [Último acceso: 01 12 2022].
- [43] WIKIPEDIA, «MALWARE,» enciclopedia web, 28 11 2022. [En línea]. Available: <https://en.wikipedia.org/wiki/Malware>. [Último acceso: 01 12 2022].
- [44] D. Harper., « "Etymology of malware.",» Online Etymology Dictionary. , 20 09 2018. [En línea]. Available: <https://www.etymonline.com/word/malware>. [Último acceso: 2022].
- [45] FORTINET, «Wardriving,» FORTINET, 2022. [En línea]. Available: <https://www.fortinet.com/resources/cyberglossary/wardriving>. [Último acceso: 30 11 2022].
- [46] KASPERSKY, «¿Qué es una VPN y cómo funciona?,» Pagina Web, 2022. [En línea]. Available: <https://latam.kaspersky.com/resource-center/definitions/what-is-a-vpn>. [Último acceso: 01 12 2022].
- [47] F. B. S. a. M. A. A. A. Jaha, « "Proper Virtual Private Network (VPN) Solution," ,» de *The Second International Conference on Next Generation Mobile Applications, Services, and Technologies*, 2008.
- [48] S. M. B. a. W. R. Cheswick, «Network firewalls,» de *IEEE Communications Magazine*, 1994.
- [49] FORTINET, «Firewall,» FORTINET, 2022. [En línea]. Available: <https://www.fortinet.com/resources/cyberglossary/firewall>. [Último acceso: 30 11 2022].
- [50] SOPHOS, «SOPHOS,» COMPANIA , 2022. [En línea]. Available: <https://www.sophos.com/es-es/company>. [Último acceso: 01 12 2022].
- [51] SOPHOS, «SOPHOS FIREWALL,» COMPANIA, 2022. [En línea]. Available: <https://www.sophos.com/es-es/products/next-gen-firewall>. [Último acceso: 01 12 2022].
- [52] DLACCESS, «MULTIBIOMÉTRICODEHUELLA,» 2022. [En línea]. Available: <https://www.dley.com.ec/producto/terminal-multibiometrica-con-reconocimiento-facial-con-luz-visible->

dactilar-y-contrasena-para-control-de-asistencia-y-
acceso/?attachment_id=14026&download_file=lmqhcoi7mhvv0.

- [53] IBM, «Listas de control de accesos (ACL) y reglas de nivel de vinculación de ACL,» ibm, 03 03 2021. [En línea]. Available: <https://www.ibm.com/docs/es/content-manager/8.5.0?topic=ac-access-control-lists-acls-acl-binding-level-rules>. [Último acceso: 04 12 2022].
- [54] M. M. S. D. a. B. S. Arash Habibi Lashkari, «"A survey on wireless security protocols (WEP, WPA and WPA2/802.11i),» de *2nd IEEE International Conference on Computer Science and Information Technology*, 2009.
- [55] wikipedia, «802.11,» Enciclopedia libre, 11 11 2022. [En línea]. Available: https://es.wikipedia.org/wiki/IEEE_802.11.
- [56] M. A. G. a. D. J. S. M. J. -I. Castillo-Velazquez, «Hardening as a best practice for WLAN Security Meanwhile WPA3 is released,» de *IEEE 39th Central America and Panama Convention (CONCAPAN XXXIX)*, Panama , 2019.
- [57] ARCOTEL, «Arcotel,» [En línea]. Available: <https://www.arcotel.gob.ec/requisitos-servicios-de-radiodifusion-sonora-television-para-medios-de-comunicacion-publicos-privados-y-comunitarios2/>. [Último acceso: 2022 11 29].
- [58] ARCOTEL, «RESOLUCIÓN ARCOTEL,» Quito, 2018.
- [59] M. d. t. y. d. l. s. d. l. informaciòn, *Acuerdo ministerial No 006-2018*, Quito, 2018.

ANEXOS

Configuración del equipo transmisor desde la plataforma propia de UBIQUITI

The image shows a screenshot of the Ubiquiti wireless configuration interface, divided into two main sections: 'Wireless Configuration' and 'Security'.

Wireless Configuration - Basic Settings:

- Wireless Mode: Access Point P1MP aiMAX Mixed
- Antenna: AM-5AC22-45 - 22 dBi
- SSID: ARMADA-IW-DIRTIC
- Country: Netherlands
- Channel Width: 20 MHz
- Control Frequency Scan List, MHz:
- Calculate EIRP Limit:
- Antenna Gain: 22 dBi
- Cable Loss: 2 dBi
- Output Power: 24 dBi (range from -4 to 28)
- Auto Adjust Distance:

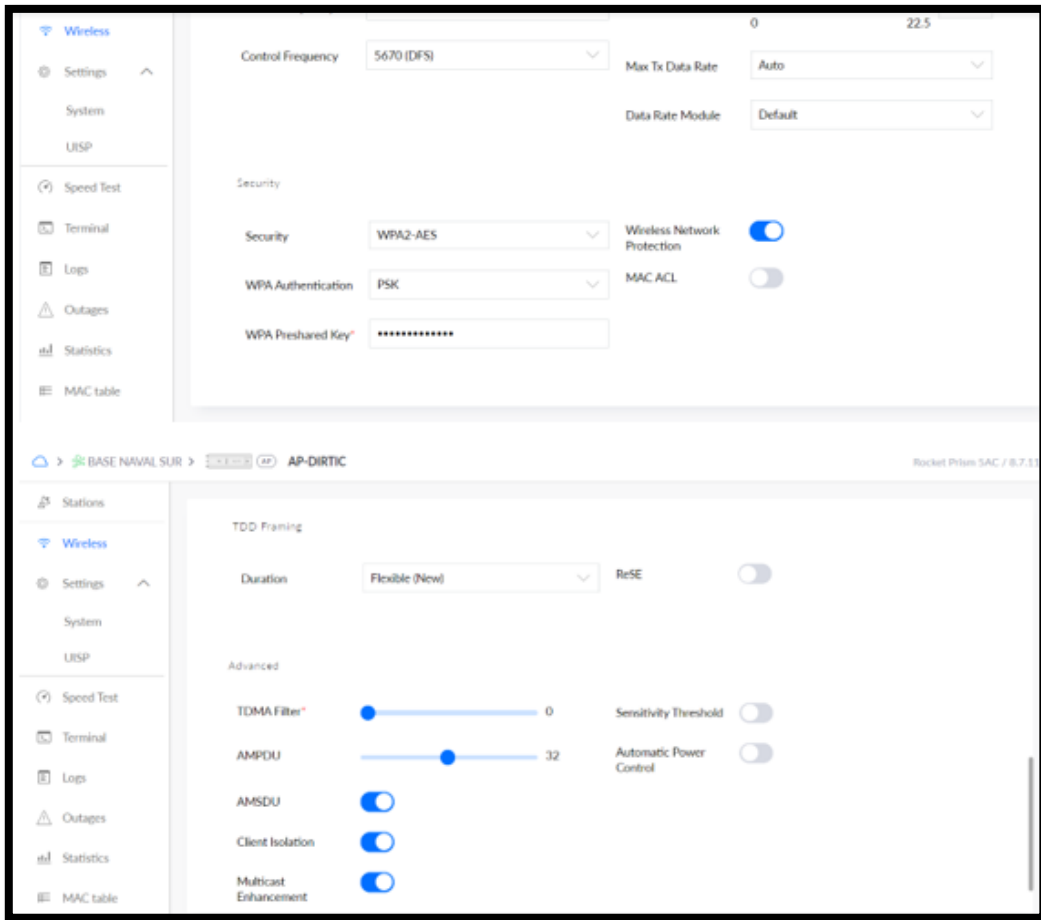
Wireless Configuration - Advanced Settings:

- Center Frequency: 5670 (DFS)
- Control Frequency: 5670 (DFS)
- Distance: 0.6 km (range from 0 to 22.5)
- Max Tx Data Rate: Auto
- Data Rate Module: Default

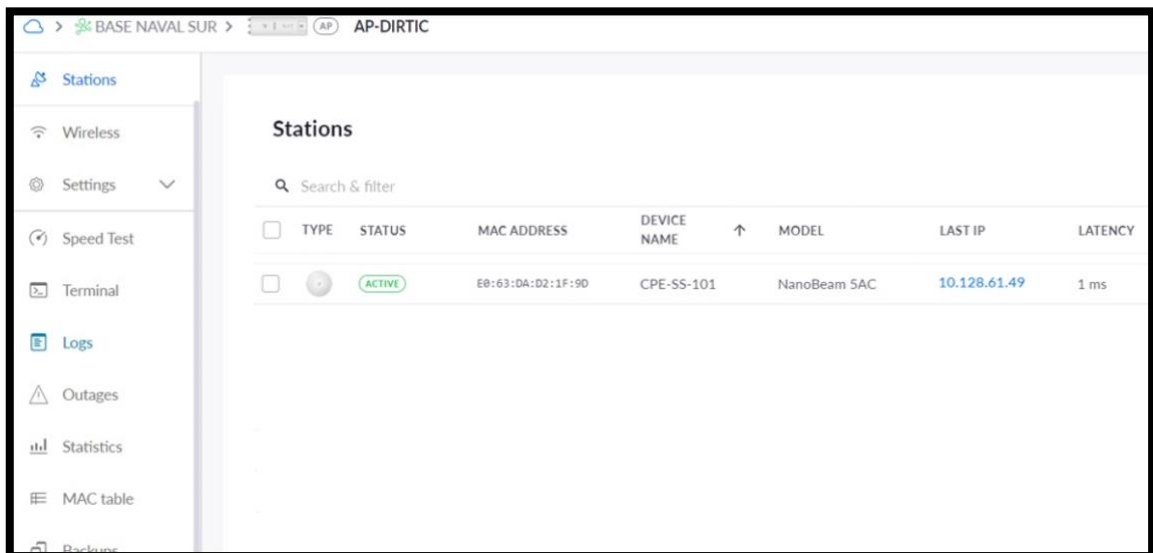
Security:

- Security: WPA2-AES
- WPA Authentication: PSK
- WPA Preshared Key: *****
- Wireless Network Protection:
- MAC ACL:

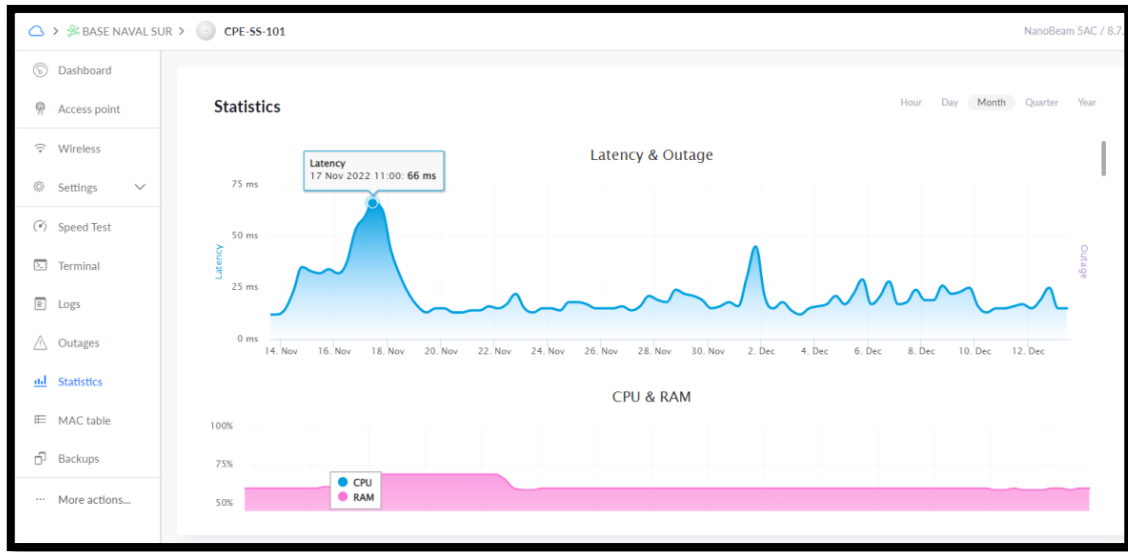
The interface includes a left-hand navigation menu with options like 'Wireless', 'Settings', 'System', 'URSP', 'Speed Test', 'Terminal', 'Logs', 'Outages', 'Statistics', and 'MAC table'. The top status bar shows 'BASE NAVAL SUR > AP-DIRTIC' and 'Rocket Pro 5AC (E7.1)'.



Estado del enlace



Historial de latencia



Datos del enlace



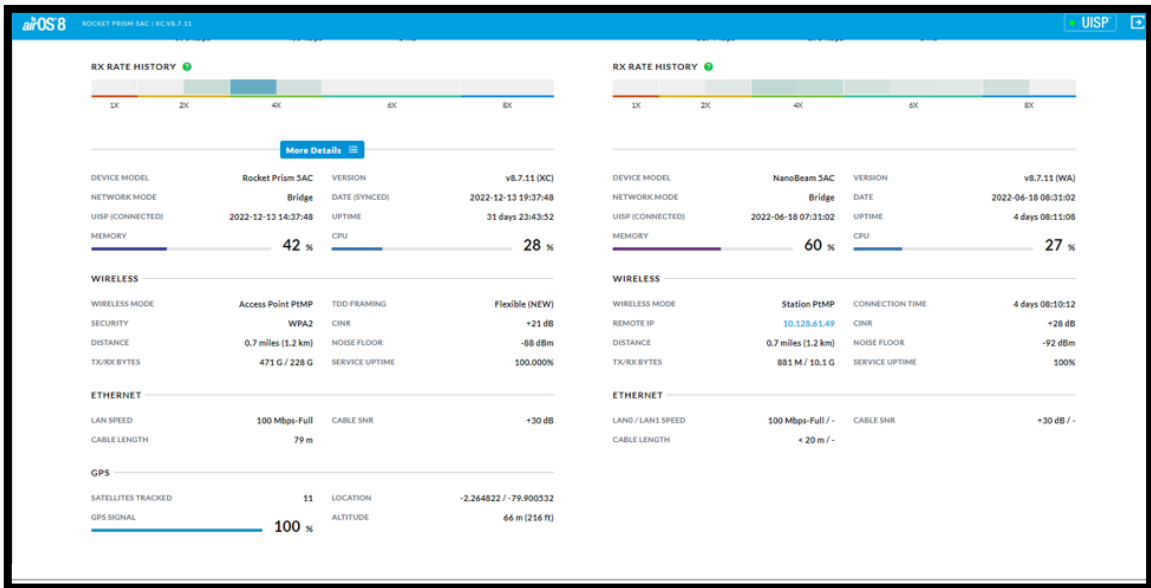
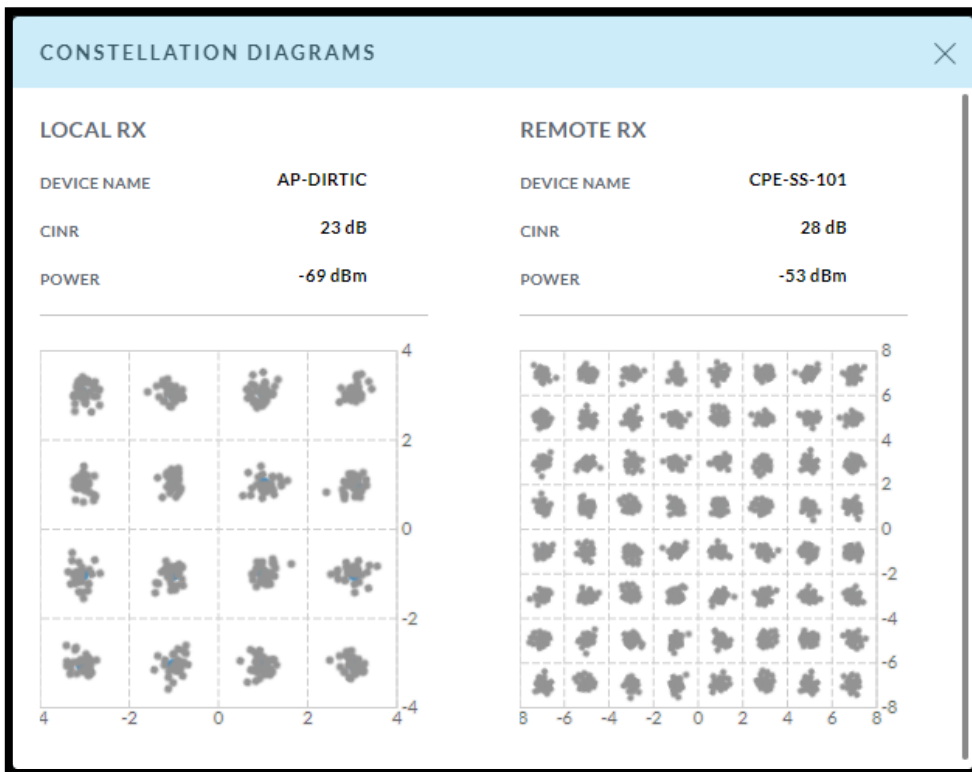
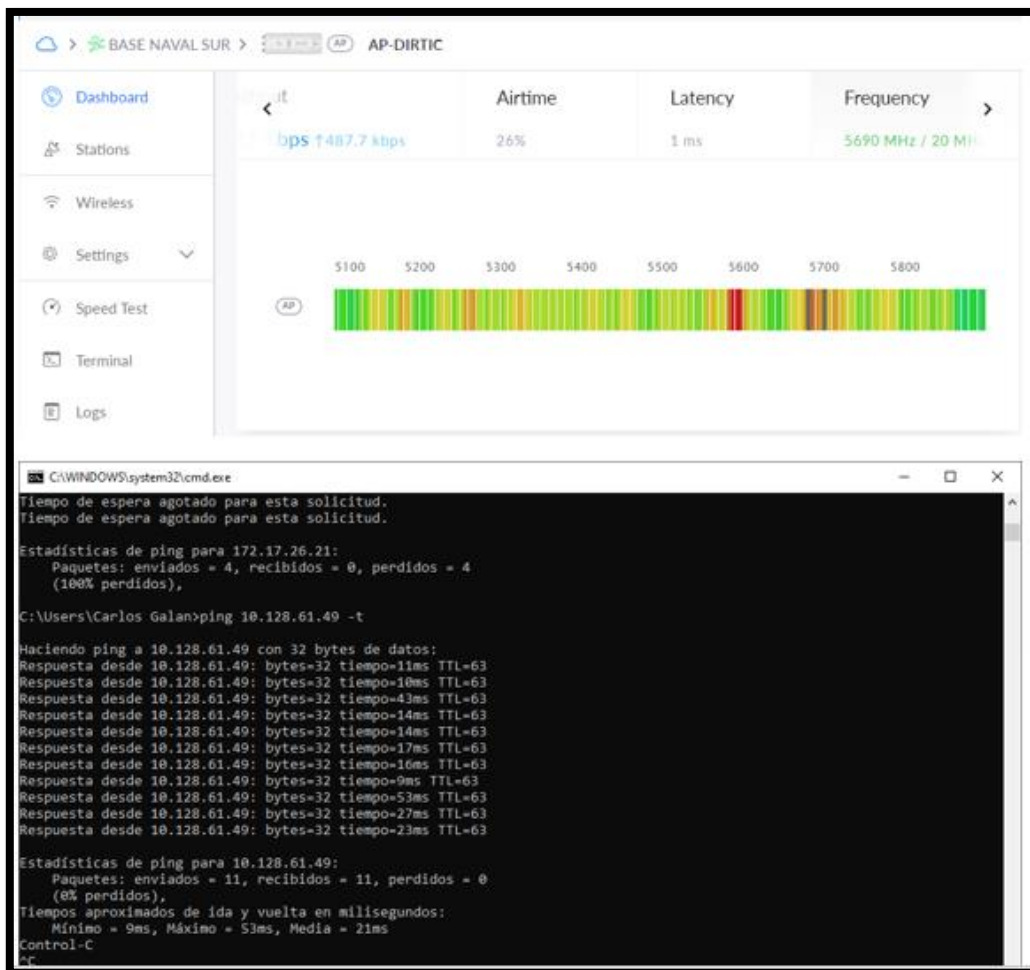


Diagrama de constelaciones



Ping desde el switch del edificio digmag



The image shows a network management interface for a device named 'AP-DIRTIC' at 'BASE NAVAL SUR'. The interface includes a sidebar with navigation options: Dashboard, Stations, Wireless, Settings, Speed Test, Terminal, and Logs. The main area displays performance metrics for a selected station 'it':

Station	Airtime	Latency	Frequency
it	bps 1487.7 kbps	26%	1 ms
			5690 MHz / 20 MHz

Below the metrics is a spectrum graph showing signal strength across a frequency range from 5100 to 5800 MHz. The graph displays a series of vertical bars in green and yellow, indicating signal activity.

Below the network interface is a Windows command prompt window showing the results of a ping test:

```
C:\WINDOWS\system32\cmd.exe
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 172.17.26.21:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
      (100% perdidos),

C:\Users\Carlos Galan>ping 10.128.61.49 -t

Haciendo ping a 10.128.61.49 con 32 bytes de datos:
Respuesta desde 10.128.61.49: bytes=32 tiempo=11ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=10ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=43ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=14ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=14ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=17ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=16ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=9ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=53ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=27ms TTL=63
Respuesta desde 10.128.61.49: bytes=32 tiempo=23ms TTL=63

Estadísticas de ping para 10.128.61.49:
    Paquetes: enviados = 11, recibidos = 11, perdidos = 0
      (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
      Mínimo = 9ms, Máximo = 53ms, Media = 21ms
Control-C
^C
```