Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Despliegue de una Red Móvil Ad-Hoc tolerante a fallos en entornos marinos

Grado en Ingeniería Mecánica

ALUMNO: Guillermo López Porto-Andión

DIRECTOR: Rafael Asorey Cacheda

CURSO ACADÉMICO: 2015-2016

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Despliegue de una Red Móvil Ad-Hoc tolerante a fallos en entornos marinos

Grado en Ingeniería Mecánica

Intensificación en Tecnología Naval

Cuerpo General

Universidade Vigo

RESUMEN

Este trabajo fin de grado expone la utilidad de una red mallada tolerante a fallos en el ámbito de la Escuela Naval Militar y más concretamente en las Lanchas de Instrucción. Para ello, se analizan los conocimientos necesarios para conseguir el funcionamiento de este tipo de redes. También se analizan los equipos necesarios para el despliegue y se detalla toda la configuración para lograr el objetivo. Al tratarse de un entorno militar y de comunicaciones relacionadas con información clasificada es preciso analizar los riesgos de seguridad para el sistema y cómo minimizarlos. El resultado final es una red, tal y como se ha descrito, que opera a bordo de las Lanchas de Instrucción y que proporciona un servicio de Internet y de un servicio interno de transmisión de información con almacenamiento persistente como principal característica, permitiendo no perder la información que se envía a nodos que están fuera de la zona de cobertura. La red se ha probado en navegación y se han analizado sus fortalezas y debilidades con la intención de continuar mejorándola y desarrollándola en el futuro.

PALABRAS CLAVE

Red mallada, almacenamiento persistente, redes marítimas, redes inalámbricas, redes seguras.

AGRADECIMIENTOS

En primer lugar, quiero agradecer a mi tutor su permanente disponibilidad para resolver cualquier duda durante la elaboración del trabajo y su apoyo diario para solucionar los contratiempos.

También quiero agradecer a mi novia, a mi hermana y a mis padres su apoyo, que ha hecho posible que esté en el último curso de la carrera y haya elaborado el Trabajo de Fin de Grado.

Por otro lado, me gustaría dar las gracias a Manuel Marín López por la información facilitada sobre su Trabajo de Fin de Grado.

Por último, quiero dar las gracias a la Escuela Naval Militar, por autorizar las pruebas a bordo de las Lanchas de Instrucción.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción

En la actualidad, las redes informáticas se han convertido en un medio esencial para la transmisión y recepción de información entre distintos puntos. Tanto es así, que muchas de las grandes empresas a nivel mundial dependen de ellas en aspectos esenciales como pueden ser el control de sus ventas, la compartición de conocimientos o el establecimiento de grupos de trabajo a distancia. Claro está, que estas son redes que trabajan en un ambiente favorable y siempre, dentro de la cobertura, pero no debemos obviar, que muchas otras se encuentran en condiciones mucho más complejas y están sometidas a una alta probabilidad de fallo e incluso de pérdida de información en el proceso de transporte.

El concepto de red tolerante a fallos, nos permite buscar una solución a este inconveniente. Mediante esta innovación, los nodos de la red serán capaces de almacenar los datos que no han podido ser enviados por un error, ya sea por la falta de cobertura o por el reinicio del sistema, de modo que una vez se recuperen las capacidades iniciales se envíe la información al nodo destinatario.

Las Fuerzas Armadas, haciendo especial hincapié en las unidades que se encuentran desplegadas por el mundo, ya sea por tierra, por mar o por aire, son uno de los principales usuarios de las comunicaciones a nivel mundial. Tanto su estructura de mando como el resto de subconjuntos derivados necesitan de un medio para transmitir órdenes y hacer que se cumplan. Esto no es sencillo porque a lo largo de los años se han ido construyendo múltiples sistemas de comunicaciones muy heterogéneos que no permiten seguir una línea conjunta. Además, como es el caso de España, al unirse a un organismo compuesto por varios países como es la Organización del Tratado del Atlántico Norte, ha tenido que añadir a sus unidades nuevos circuitos que alejan mucho más a sus ejércitos de conseguir un sistema de comunicaciones conjunto.

Por otro lado, los ambientes en los que se despliegan las Fuerzas Armadas obligan a usar comunicaciones muy robustas y seguras que eviten la pérdida de la información que debe llegar a su destino y que dificulten al enemigo realizar ataques de manipulación y robo de información con éxito.

Si existiese una red común tolerante a retardo y segura entre unidades, permitiría a los distintos buques, vehículos o estaciones en tierra comunicarse sabiendo que la red será capaz de entregar la información en el primer momento en el que sea posible y que mientras no pueda hacerlo, no perderá los datos que el resto de unidades necesitan recibir. Además dadas sus múltiples aplicaciones podría sustituir a muchas de las redes desplegadas en las Fuerzas Armadas, consiguiendo así una mayor eficiencia en la comunicación, una disminución del gasto de establecimiento y mantenimiento de

redes, un aumento de la seguridad, pues la variedad de redes puede hacer más vulnerable a todo el sistema, y un aumento de la interoperabilidad combinada y conjunta.

1.2 Objetivo

La Escuela Naval Militar es el centro de formación de los futuros oficiales de las Fuerzas Armadas y por ello debe buscar la excelencia en todos los ámbitos en los que esté a su alcance. En ella, los alumnos reciben una formación naval, militar y universitaria. Es de esperar que la mejora del adiestramiento de las damas y caballeros alumnos sea una tarea común y un reto tanto para sus profesores como para ellos mismos.

La formación naval que reciben se imparte desde dos puntos básicos, el teórico, inculcado en las aulas de navegación, meteorología y maniobra, entre otras, y el práctico, que se enseña principalmente a través del Simulador de Navegación y las Lanchas de Instrucción.

Las Lanchas de Instrucción consisten en una recreación, con una eslora de 20,5 metros y una manga de 4,9 metros, de los buques que los alumnos tendrán que maniobrar cuando estén destinados en la flota. En estas pequeñas aulas flotantes, se forma al alumno desde que entra en primer curso, hasta tercero. El Aspirante de primero recibe un adiestramiento desde el punto de vista de un marinero, aprendiendo a adujar estachas, a lanzar guías, a llevar la caña, a hacer funciones de serviola y a apuntar en la crónica. El Aspirante de segundo, ocupa puestos en el radar, en la carta, en la maniobra, en máquinas y en comunicaciones. Por último, los Guardiamarinas de primero ocupan puestos de oficial de guardia en puente, de oficial de comunicaciones, de oficial de derrota y de oficial de maniobra.

La formación en el ámbito de las comunicaciones navales a bordo de las Lanchas de Instrucción tiene algunas carencias. La principal es que, en muchas ocasiones, los alumnos emplean los circuitos con falta de rigor, debido a que usan las expresiones que han aprendido de memoria o interpretan las publicaciones de manera errónea. Cómo no siempre es factible escuchar las comunicaciones en alto en el puente, no es posible ni para los Guardiamarinas, ni para el Comandante realizar correcciones a sus subordinados.

Por otro lado, en ocasiones se pueden producir malentendidos por el circuito de comunicaciones, ya sea por el mal funcionamiento del mismo o por una orden mal transmitida. Cómo se trata de alumnos en formación, estos errores se pueden dar frecuentemente y podrían producir situaciones en las que se ponga en jaque la seguridad en la navegación. Por ello, debe buscarse una solución.

Otra forma de mejorar el adiestramiento de los alumnos, sería evitar el uso del Servicio Móvil Naval. De esta manera, el oficial de guardia no podrá recibir información por otras vías que no sean las de su propia preparación. Así aprenderá a ser mucho más autosuficiente y la preparación de la salida a la mar se volverá prioritaria. Sin embargo, si esto se llevase a cabo, los comandantes no tendrían una red coordinación en la que dar directrices y eso podría ser peligroso o incluso podría generar situaciones de desorden en algunos ejercicios.

Durante las semanas de instrucción y adiestramiento, puede ser necesario programar ejercicios mientras se navega e incluso realizar planeamientos para simular combates contra otras unidades. Al tener que hacerlo en navegación resulta más complicado si no existen los medios adecuados para compartir la información. Por otro lado, si se pudiese acceder a Internet para obtener datos meteorológicos precisos y actualizados u otra información útil de la zona de operaciones, los ejercicios se volverían mucho más dinámicos.

Todos estos requisitos estarían al alcance de las Lanchas de Instrucción si se elaborase una red que pudiese gestionar conversaciones entre cada uno de los nodos y que permitiese el envío de archivos y el acceso a Internet en un medio en el que pueden producirse grandes retardos e interrupciones en las comunicaciones. No hay que perder de vista que se está hablando de nodos en movimiento. Además, tendría que tratarse de una red con estrictas medidas de seguridad.

Este proyecto presenta el despliegue de una red móvil *ad-hoc* tolerante a fallos para enlazar las Lanchas de Instrucción entre sí y con la Escuela Naval, permitiendo dotarla de servicio de chat, de herramientas transferencia de archivos y de acceso a Internet. Todo ello con la pertinente seguridad, pues hay que ser conscientes de que la información manejada por las Fuerzas Armadas solo puede transmitirse a través de medios que garanticen, al menos en gran medida, la confidencialidad, la integridad, la autenticidad, el no repudio y la disponibilidad.

De forma más simplificada, los objetivos de este proyecto son:

- Despliegue de la red móvil *ad-hoc* tolerante a fallos.
- Prueba de la red en navegación y corrección de fallos e incompatibilidades
- Iniciar la implantación definitiva de la red a bordo de las lanchas de instrucción.
- Análisis y aplicación de medidas de seguridad.
- Transferencia de trazas NMEA a través de la red.
- Elaboración de un túnel que permita monitorizarla desde un cliente en tierra.

1.3 Organización de la memoria

El resto de la memoria está organizada como se describe a continuación:

- En el capítulo 2 se presenta un estado del arte que analiza la tecnología de las redes tolerantes a fallos e introduce otros conceptos relacionados con el ámbito del TFG, como las redes móviles *ad-hoc*, la seguridad o los túneles virtuales de comunicación.
- El capítulo 3 describe todo el desarrollo realizado para conseguir el despliegue de la red tolerante a fallos en las Lanchas de Instrucción.
- El capítulo 4 presenta las pruebas diseñadas para validar el despliegue y los resultados obtenidos.
- El capítulo 5 contiene las conclusiones del trabajo realizado y propone varias líneas futuras para continuar este trabajo.
- Finalmente, se han añadido varios anexos con información complementaria relacionada con este TFG.

2 ESTADO DEL ARTE

2.1 Descripción de la red tolerante a fallos

2.1.1 Introducción

A medida que avanzan las tecnologías se plantean nuevos retos en el mundo de las comunicaciones y la informática. En algunos ámbitos, como el espacial, el submarino, o en algunos casos, el terrestre, es necesario construir redes que permitan la transmisión de información en ambientes en que la desconexión, el alto retardo o la interrupción de la comunicación son más que probables. De este modo, aparecen las redes que hoy conocemos como *Delay / Disruption Tolerant Networks.*

Desde el punto de vista de la informática, la aparición de esta nueva tecnología implica la creación de una nueva capa, conocida como capa de paquete, situada por encima de la capa de transporte y por debajo de la de aplicación. Los nodos que la forman, nodos DTN, están dotados de una memoria que les permite almacenar temporalmente información en caso de que se produzca una interrupción de la conexión. Cuando un nodo DTN envía la información a otro y este le notifica la recepción, la responsabilidad de entrega queda delegada al siguiente. Además, es posible solicitar al nodo receptor una confirmación de la recepción de los datos. Se trata de un sistema fiable, apoyado por una adecuada y flexible gestión de nombres de los integrantes de la red que facilita la entrega de la información.

Los protocolos de Internet no funcionan correctamente en ambientes como los descritos porque se basan en una comunicación entre extremos que se inicia y finaliza sin contar con la posibilidad de interrupciones de comunicación. Se trata de protocolos estáticos con dificultades para adaptarse a situaciones cambiantes. Cuando hablamos de DTN hablamos de flexibilidad y de una forma de proceder que no necesita encontrar un camino de principio a fin directo. Puede variar el tamaño de los mensajes que transmite y funciona con distintas formas de nombrar y organizar los nodos. Además, es capaz de almacenar la información hasta que los datos llegan al nodo destinatario. También mantiene un nivel de seguridad adecuado para diferentes tipos de información. Por eso es necesario que las aplicaciones que emplea vayan en consonancia con el funcionamiento de los nodos DTN y deben estar diseñadas para minimizar los tiempos de ida y vuelta, para soportar fallos de la red e incluso reinicios y para indicar a la red la importancia de la información que se va a transmitir. Si se diese el mismo trato a toda la información que se transmite se producirían errores porque hay paquetes que por su naturaleza necesitan ser prioritarios para el correcto funcionamiento de las comunicaciones.

2.1.2 Arquitectura de la DTN

Las aplicaciones DTN emplean mensajes de longitud arbitraria llamados ADU, unidades de datos de aplicación, que a su vez se dividen en uno o más paquetes. Tienen dos o más bloques que llevan información sobre el destino de los datos o parámetros de la aplicación. Una característica muy particular de este sistema es que los paquetes se pueden fragmentar en cualquier punto de la red y ensamblarse más adelante. Es esencial la figura de los EID, identificadores de puntos de destino, a la hora de indicar de dónde viene y hacia dónde va la información. Este aspecto se analizará más adelante.

Para conseguir la eficacia de la que presume este tipo de red en la entrega de información, los paquetes deben incluir, entre otros datos, un sello temporal, un indicador de tiempo de vida, un indicador de tipo de servicio y la longitud. De este modo es mucho más fácil para la capa DTN la toma de decisiones a la hora de elegir por dónde van a enviarse los paquetes a través de la red, especialmente en situaciones en que la red se encuentre especialmente sobrecargada. De hecho, si en ese momento no es una buena idea transmitir, los datos pueden quedar almacenados en el nodo en cuestión hasta que se genere una conexión idónea.

Los puntos de destino DTN sirven de referencia para saber que un paquete se ha recibido y están compuestos de un determinado número de nodos DTN. El MRG, mínimo grupo de recepción, es el mínimo número de nodos del punto de destino DTN que tienen que recibir sin errores el paquete para que se considere que ha sido entregado correctamente. Los MRG pueden estar compuestos de un nodo o de varios, y un nodo puede pertenecer a dos o más MRG. Por otro lado, la etiqueta que define los destinos DTN, se llama EID, y está escrita en lenguaje URI, recurso uniforme de identificación. Este lenguaje se emplea para generar etiquetas de nombres o direcciones para una gran variedad de utilidades y nos permite detectar si una etiqueta está referida a un nodo, *unicast*, a algunos nodos, *anycast* o a todo un grupo de nodos, *multicast*. Los EID permiten saber cuál es el MRG de un destino DTN y cada nodo debe tener una EID que le identifique solamente a él. Por otro lado, esta nomenclatura se utiliza para que las aplicaciones puedan solicitar recibir los ADU destinados a un EID concreto, de hecho esto suele estar configurado de forma permanente mediante registros, así no se pierde al producirse fallos o reinicios del sistema. A mayores, los EID pueden reservar una parte para tareas de encaminamiento o diagnóstico de funcionamiento.

En Internet, cuando se realiza una petición a un servidor se sabe que está vinculado a una dirección y que esa relación se va a mantener de manera estática, es decir, ese servidor no va a aparecer de repente en otro lugar del mundo. Por ello, podemos decidir enviar a esa dirección sin que haya razones para pensar que se pueda producir un fallo en la entrega. Si se hiciese lo mismo en una red establecida en un ambiente complejo en el que se pudiesen producir fallos, desconexiones o interrupciones de cualquier tipo no funcionaria, pues esas dificultades modificarían el camino que la información puede seguir para llegar a su destino. Es por eso que los EID deben ser interpretados en el momento en que se va a transmitir porque así ya no obtendremos un error al intentar enviar por un camino preestablecido [1].

Para llegar a entender el funcionamiento de la red DTN es necesario entender primero cómo funciona *multicast*, *anycast* y *unicast* (Figura 1-1) [2]:

- *Multicast* es un método de envío de paquetes a un grupo de direcciones que deben estar previamente subscritas a un grupo del mismo nombre mediante un mensaje IGMP que además de servir para indicar que el cliente pertenece a ese grupo, también sirve para indicar al encaminador que ese equipó recibirá ese tipo de paquetes y que debe dirigir esos datos hacia él.

- *Anycast* es un tipo de direccionamiento que busca entregar los paquetes a un nodo cualquiera de un grupo. El no seleccionado será el que tenga menor coste según la topología de la red.
- En el caso de *unicast*, los paquetes son dirigidos y entregados a una única dirección.

Es muy diferente el funcionamiento de *multicast* en una red DTN que en Internet, porque en el segundo, si se quiere recibir paquetes de una dirección *multicast*, es tan sencillo como registrarse en ese grupo. En el caso de las redes DTN, un nodo puede querer recibir paquetes *multicast* y no poder porque todavía no exista una conexión que le permita recibir la información, por eso, será necesario que la red pueda almacenar la información y enviarla al nodo que no que no pudo recibirla en el momento.

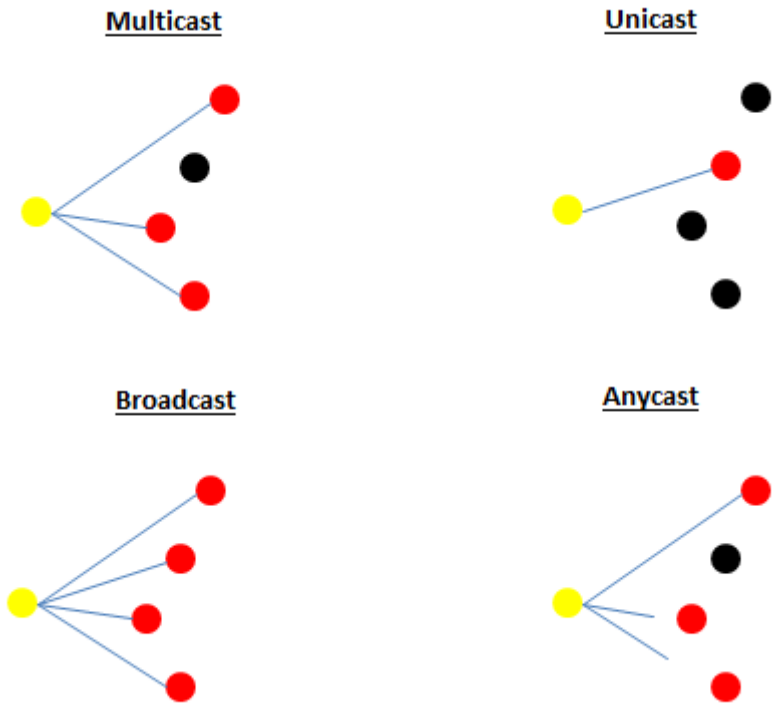


Figura 1-1 Ejemplos de topologías *unicast, anycast, multicast* y *broadcast*.

2.1.3 Clases de tráfico

La arquitectura DTN descrita en [1] emplea clasificación del tráfico para establecer prioridades. Esta clasificación se basa en la urgencia con que las aplicaciones necesitan que se entreguen sus mensajes, por lo que son estas las que indican la clase y el tiempo de vida de los paquetes. Esto implica que haya que organizar y separar los tipos de información mientras esperan para ser enviados. Se distinguen tres tipos de tráfico: *bulk*, normal y *expedited*. El tráfico tipo *bulk* es el de menor prioridad. De hecho, ninguno de los paquetes con esta clasificación se enviará hasta que todos los demás que tengan la misma fuente y el mismo destino ya hayan sido transmitidos. El tráfico tipo normal es aquel que tiene prioridad sobre el tráfico tipo *bulk*. Por último, el tráfico tipo *expedited* es el de mayor prioridad por lo que se enviará antes que los tipos anteriores.

Gracias a esta clasificación y al tiempo de vida indicado por las aplicaciones es más sencillo que se dé un mejor tratamiento a aquellos paquetes que lo necesitan. Sin embargo, debe notarse que estas prioridades garantizan la diferenciación del tráfico de una misma fuente, pero no necesariamente de fuentes diferentes.

2.1.4 Fragmentación y ensamble

Uno de los pilares de la eficiencia en una red DTN es el proceso de fragmentación y unión de los paquetes durante su tránsito desde la fuente hasta el destino. Así se consigue que aquellos paquetes que no han sido completamente enviados no tengan que retransmitirse y que se aproveche al máximo todas las conexiones. Podemos distinguir dos formas de llevar a cabo este proceso, la fragmentación proactiva y la reactiva. En la primera, los paquetes que debe enviar el nodo son fragmentados en paquetes menores previamente al envío. Al llegar al destino los paquetes fragmentados se vuelven a unir, dando lugar a los paquetes originales y estos a su vez a los mensajes de aplicación. Este tipo de fragmentación se usa cuando se conocen las cantidades de información que se van a enviar. En la fragmentación reactiva es diferente, pues los paquetes se envían y si la transmisión no se completa, la propia capa DTN se encarga de marcar los paquetes como fragmentados, con lo cual, el resto de nodos conocerá el estado de ese paquete y lo transmitirá como un paquete normal hasta que se ensamble posteriormente. Además, el nodo inicial, el que solo envió una parte de los datos, sabrá que debe de enviar el resto en cuanto se establezca una conexión válida.

Las principales diferencias entre los dos métodos de fragmentación y ensamble son que el método proactivo opera previamente al envío de los paquetes mientras que el reactivo lo hace a posteriori, que el método reactivo necesita el apoyo de protocolos que pueden no estar disponibles, por lo que no siempre es una opción, y que la fragmentación reactiva es más problemática a la hora de usar firmas digitales y códigos de autenticación.

Debe resaltarse la importancia, para la circulación de los paquetes a través de la red, de la sincronización temporal de los nodos DTN. Sirve tanto para identificar los paquetes y fragmentos, como para encaminar a través de nodos predichos y programados, como para no rechazar paquetes de forma errónea y como para la expiración del registro de aplicaciones. Como analizaremos más adelante, debe haber un nodo que sirva de referencia temporal al resto de nodos o todos los nodos deben corregir sus tiempos a través de un servidor de Internet para que el sistema funcione [1].

2.1.5 Fiabilidad y transferencia de custodia

En ocasiones, las aplicaciones pueden necesitar una determinada fiabilidad en el envío de los paquetes, por ello es necesario un procedimiento que permita asegurarse de que llegan a su destino. Este sistema se conoce como transferencia de custodia y se describe en [1].

Cuando una aplicación quiere que se emplee el mecanismo de custodia de paquetes debe seleccionarlo en las opciones de envío, sin embargo, eso no garantiza que el nodo fuente tenga la capacidad de custodiar pues puede no estar habilitada o incluso no convenirle usarla en ese momento, ya sea por razones de congestión o de cualquier otra índole. Cuando un nodo acepta la custodia de un paquete, la capa DTN genera una señal conforme se ha producido este hecho y la envía al EID del actual custodio, contenido en el primer bloque del paquete. Además, se le indica al custodio cual es el EID al que debe reenviar el paquete. Así, queda patente la importancia de la capa DTN y de los protocolos subyacentes para que este sistema de transferencia de custodia funcione.

Por otro lado, es clarificador entender, que el uso de este método lleva a la aparición de un sistema de encaminamiento de los paquetes bastante complejo, porque la información debe pasar de custodio a custodio y eso, a veces implica incluso alejarse del propio destino que se pretende alcanzar para poder llegar hasta él posteriormente. Por otro lado, si la fuente, no tiene capacidad de custodia el paquete atravesará varios nodos hasta que encuentre uno que la tenga.

Un inconveniente que puede surgir durante la implementación de este sistema es que aparezca un camino unidireccional en la red, con lo cual, no sea posible, un vez se ha aceptado la transferencia, devolver la señal conforme se procede a custodiar la información. Si eso ocurriese, se generaría un informe de estado indicando que el paquete ha expirado cuando en realidad no es correcto, de hecho, el paquete seguiría el camino hacia su destino. La manera de disminuir el problema es activar la opción

de informe de paquete enviado, que se explicará a continuación, de modo que si la siguiente ruta es unidireccional se informe de la situación.

2.1.6 Opciones de entrega e informes de estado

Una vez explicadas las clases de tráfico, deben entenderse las diferentes opciones de entrega de los paquetes expuestas en [1], que además pueden combinarse entre sí según solicite la aplicación en cuestión para los nodos a través de los que envíe sus mensajes. Se distinguen ocho opciones de entrega de paquetes entre las que encontramos las siguientes: solicitud de transferencia de custodia, solicitud de aceptación de custodia del nodo fuente, informe de un paquete entregado, informe de paquete recibido por la aplicación, informe de paquete recibido, informe de aceptación de custodia de un paquete, informe de reenvío de un paquete e informe de paquete borrado.

- La opción de solicitud de transferencia de custodia se emplea para que los paquetes sean enviados con gran fiabilidad, de modo que se use un protocolo de transmisión de confianza mediante el que la custodia y la obligación de envío de los paquetes se vaya transfiriendo entre varios nodos denominados custodios.
- La solicitud de aceptación de la custodia por parte del nodo fuente sirve para que las aplicaciones puedan exigir a los nodos custodiar los paquetes que van a transmitir, porque en caso de no ser posible, la capa de aplicación no podría confiarles el paquete.
- El informe de paquete entregado, se usa para que al entregar el mensaje de aplicación se genere un informe de estado de paquete entregado al destino previsto.
- El informe de paquete recibido por la aplicación busca que se genere un informe de estado cuando la aplicación recibe el paquete y afirma que lo ha recibido.
- El informe de paquete recibido está pensado como método de diagnóstico y consiste en la generación de un informe de estado cuando un paquete llega a su destino.
- El informe de custodia de paquete aceptada también tiene funciones de diagnóstico y genera un informe de estado, llamado señal de custodia, cuando los paquetes son aceptados usando el procedimiento de custodia.
- En el caso del informe de reenvío de paquete, se genera un mensaje de estado, a modo de diagnóstico, del reenvío de un paquete hacia otro nodo.
- Por último, el informe de paquete borrado, también con fines de comprobación, genera un mensaje de estado cuando se borra un paquete de un nodo.

Si la seguridad está habilitada en la red, aparecen, a mayores, tres opciones de entrega:

- Requisito de confidencialidad: convierte al ADU en un secreto para todos excepto para la fuente y para el grupo del EID de destino.
- Requisito de autenticación: permite proteger varios campos del mensaje.
- Requisito de detección de errores: permite que las alteraciones en los campos de los bloques de un paquete, no modificables, sean apreciables con una alta probabilidad.

Al igual que el protocolo IP tiene los mensajes ICMP, la capa de paquetes DTN tiene también su propio tipo de mensajes de estado y de errores, los BSB. Estos mensajes reciben el nombre de registros administrativos y se dividen en informes de estado de paquetes y en indicadores de custodia. No tienen por qué ser enviados al EID del que partieron, sino que se dirigen, según el tipo de mensaje, al EID encargado específicamente de su recepción.

2.1.7 Los bloques de un paquete DTN

Un paquete DTN, tal y como se expone en [3], se compone de un bloque principal obligatorio (Figura 2-2) un bloque opcional de carga útil y un conjunto de bloques que pueden ser añadidos por diversas razones. Por ser el más importante, nos centraremos en describir el bloque principal, dentro del que destacan por su importancia el sello temporal, la vida útil, definida por una variación temporal desde el momento en que el paquete fue creado, el indicador de clase de servicio, que también indica las opciones de entrega, el EID del primer emisor del paquete, el EID de destino, el EID al que se envían los informes de estado y el EID del custodio del paquete. No es trivial entender que el sello temporal se basa en el momento en que una aplicación solicitó el envío del ADU. Además, también incluye un número de secuencia que hace ese paquete único para cada ADU originado desde la misma fuente.

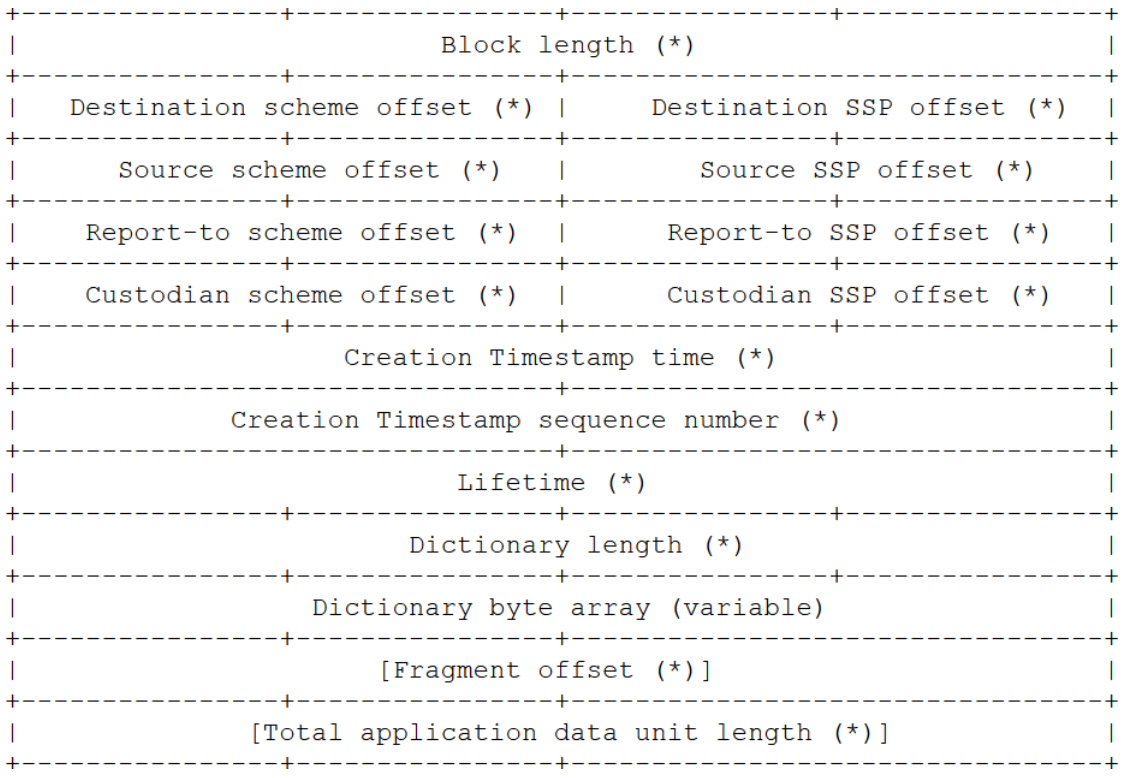


Figura 2-2 Bloque principal DTN [3].

El bloque de la carga útil (Figura 2-3) está formado por cuatro apartados: el campo del tipo de bloque, el campo de los *flags* de control, el de longitud del bloque y el de la carga útil propiamente dicha.

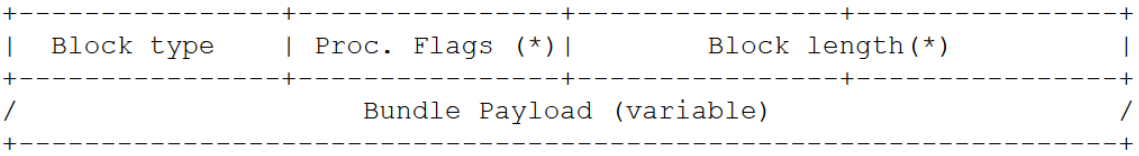


Figura 2-3 Bloque de la carga útil [3].

En el caso de los bloques que se añaden a mayores del bloque principal y del bloque de la carga útil, no es tan sencillo como en los anteriores porque la información contenida en estos no tiene por qué poder ser procesada por los nodos a través de los que el paquete va a circular. Por eso es necesario que el paquete esté configurado para que los puntos que atraviese puedan reenviarlo sin procesar el bloque en cuestión, hasta llegar a un nodo que sí pueda y deba interpretarlo.

2.1.8 Tipos de conexiones en la red

Basándose en su modo de funcionamiento y en la necesidad o no de realizar alguna acción para que tengan lugar, la referencia [1] describe una serie de conexiones que engloban, en gran medida, las diferentes posibilidades que pueden aparecer en la red. Entre ellas encontramos:

- Las conexiones persistentes: son aquellas que sin necesidad de realizar ninguna acción, se mantienen siempre disponibles.
- Las conexiones bajo demanda: se diferencian de las anteriores en que necesitan una acción que las inicie, sin embargo, una vez esa acción se produce, actúan como conexiones persistentes.
- Las conexiones intermitentes programadas: se caracterizan por estar configuradas para producirse en un momento temporal.
- Las conexiones intermitentes oportunistas: son aquellas que no se esperan, de hecho, aparecen en cualquier momento y pueden volver a desaparecer. Un ejemplo podría ser un dron con software DTN instalado que le permita actuar como un nodo, que comienza a volar dentro de la zona de cobertura de la red DTN de las lanchas de instrucción. Podría llevar información desde una lancha a otra si entre ellas no existe enlace.
- Las conexiones intermitentes previstas: son aquellas de las que no se tiene certeza de que vayan a poder utilizarse, sin embargo, basándonos en un registro de conexiones anteriores y en algunos datos más, es posible contar con ellas. De hecho, sería posible incluso planear rutas utilizando esta información.

2.1.9 Congestión y control de flujo en la capa DTN

Se entiende congestión por el estado de un nodo que no es capaz de gestionar los datos que recibe y control de flujo por la acción de evitar que una fuente envíe paquetes a un receptor a una velocidad superior a la que es capaz de gestionarlos. Se concluye por lo tanto, que si el control de flujo se realiza desde los receptores hacia las fuentes es posible solucionar, al menos en parte, la congestión.

La principal unidad de medida de congestión en la red, tal y como se explica en [1], es el almacenamiento persistente, que en un estado de congestión se encontrará en el límite de capacidad. La propia capa de paquete debe gestionarse ante estos inconvenientes y puede hacerlo de varias maneras. En primer lugar, un nodo en situación de congestión debe eliminar aquellos paquetes almacenados que hayan expirado, aunque eso ya es algo que debería hacer constantemente. Otra opción, para aquellos nodos que suelan aceptar peticiones de custodia, en caso de estar llegando al límite de capacidad, pueden eliminar esa opción temporalmente, aunque no está claro en qué momento el nodo debe tomar esa decisión. Como último recurso, puede tomar la decisión de eliminar aquellos paquetes de los cuales no haya aceptado la custodia, aunque no hayan expirado. Esto último ya es considerado una medida drástica. Debe notarse la importancia de que la capa de paquetes tenga en cuenta los protocolos de capas inferiores y se apoye en ellos para una correcta gestión de la congestión.

Es importante saber que este punto, englobado en el conjunto de características que describen la red tolerante a fallos, todavía tiene un largo camino por recorrer, por lo que se esperan grandes avances en un futuro próximo.

2.1.10 Túnel DTN

Se trata de una posibilidad muy interesante aunque quizás poco refinada todavía. Un ejemplo claro para entender los túneles en redes DTN sería una red como la que se está desplegando en este proyecto, con acceso a Internet. Supongamos que por encontrarse fuera de la cobertura del nodo o nodos que lo proporcionan, no fuese posible que un cliente tuviese servicio de Internet. La solución

sería configurar un túnel que permitiese que las conexiones TCP/IP de Internet fuesen a través de la red DTN a pesar de tratarse de un protocolo diferente. Así, algunos servicios como el correo y el Whatsapp, que no necesitan un envío inmediato de la información, podrían funcionar gracias al reenvío y almacenamiento de los nodos DTN, ya que estos son capaces de almacenar los datos hasta que haya una conexión disponible hacia el destino. Sí que es cierto que una llamada telefónica o un video en *streaming* no podrían funcionar debido al retardo que habría en la transmisión de datos desde la puerta de enlace hasta el nodo receptor. De todas formas, como ya se indicó, se trata de una tecnología en desarrollo y tiene todavía muchos aspectos que mejorar [1].

2.2 Seguridad

2.2.1 Introducción

La capa de paquete DTN se encuentra sobre la capa de transporte y por lo tanto sobre la capa de IP, por eso una red de este tipo es capaz de operar entre diferentes infraestructuras. Esto puede implicar que no todos los nodos de la red sean de confianza, pues una red privada podría emplear nodos públicos para transmitir información. En muchas ocasiones, como es el caso que nos ocupa, estas redes se utilizarán para transmitir información sensible y eso requiere un elevado nivel de seguridad [4].

Es lógico pensar que no todos los nodos de la red tienen que soportar protocolos de seguridad. Sin embargo, sí deben existir algunos nodos encargados de este aspecto para poder tratar correctamente la información que no debe estar al alcance de personas externas.

Como ya se ha explicado, los paquetes de la red tolerante a fallos se componen de una serie de bloques, dentro de los cuales, se incluyen los que están a cargo de la seguridad y que son generados e interpretados por los diferentes nodos seguros de la red DTN. Pero antes de continuar con la seguridad deben quedar claros una serie de conceptos básicos:

- Los nodos seguros generan bloques que añaden a los paquetes de la red.
- Los nodos seguros son los únicos que pueden elaborar e interpretar esos bloques.
- No es lo mismo un nodo fuente de un paquete que un nodo fuente de un bloque de seguridad de ese paquete. Aunque un nodo A sea fuente de un paquete, si un nodo B le añade un bloque de seguridad, será el nodo B el nodo fuente de ese bloque de seguridad.
- Los bloques de seguridad no tienen por qué tener el mismo destino que el resto del paquete. Es decir, si un nodo A envía un paquete a un nodo C, a través de un nodo B, puede ser que uno de los bloques de seguridad tenga como destinatario un nodo D y otro bloque de seguridad un nodo E.
- Los bloques deben enviarse en el mismo orden en que se reciben.
- Si un bloque de seguridad circula a través de un nodo no seguro, este debe ser capaz de retransmitirlo a pesar de no poder interpretarlo y no borrarlo o intentar modificarlo.
- Mantener el orden de los bloques es esencial para que se lleven a cabo todas las acciones que les permitan llegar a su destino.

2.2.2 Bloques de seguridad

Las seguridad en las redes tolerantes a fallos, que sigue lo descrito en la referencia [4], cuenta con cuatro tipos de bloques de seguridad: el bloque de autenticación de paquete, BAB, el boque de integridad de la carga útil, PIB, el bloque de confidencialidad de la carga útil, PCB y el bloque de seguridad de extensiones, ESB.

El BAB es el último bloque en ser calculado y se ocupa de mantener la integridad y la autenticidad de los paquetes en un salto, entendiendo por salto la transmisión de un paquete desde un nodo seguro a

otro nodo seguro, aunque atraviese otros que no lo sean. El PIB tiene como tarea mantener la autenticidad y la integridad de la carga útil, desde la fuente generadora del PIB hasta la fuente receptora del mismo, aunque los nodos intermedios que posean las claves, también podrán comprobar el bloque. EL PCB se genera en la fuente del mismo tras haber cifrado la carga útil del paquete. Por último el ESB, como su propio nombre indica, tiene como misión dotar de seguridad aquellos bloques distintos del bloque principal y la carga útil.

Todos los bloques de seguridad mencionados siguen el estándar de estructura de paquete del documento [3].

Dado que los bloques de seguridad tienen la mayoría de los campos en común, una forma de simplificar la parte de campos de datos específicos de cada tipo de bloque sería crear un bloque de seguridad abstracto (ASB) en el que se especificarían los campos presentes o no en el resto de bloques.

2.3 Redes móviles *ad-hoc*

2.3.1 Funcionamiento y utilidad

La capa DTN opera sobre una red móvil *ad-hoc* (MANET, *Mobile Ad-hoc Network*) [5]. Se trata de una red mallada y como tal, permite el multisalto. Es decir, se puede transmitir información mediante un enlace inalámbrico a nodos situados a más de un salto en la topología de la red, gracias a un protocolo de encaminamiento específico. Este concepto es una evolución del modo IBSS (*Independant Basic Service Set*) de las redes inalámbricas. La característica que diferencia a la MANET del resto de redes malladas es que permite una topología cambiante, de forma que los enlaces puedan establecerse y romperse constantemente. Se descarta el concepto de un encaminador central que gestione todo el tráfico de la red porque ahora todos los nodos pueden enviar, recibir y encaminar. Debido a su fácil despliegue, sencillo mantenimiento, alta escalabilidad y bajo coste, así como su capacidad para adaptarse a las situaciones cambiantes de los nodos, se considera que esta red es idónea para entornos militares. Reúne, por lo tanto, todas las características necesarias para ser una buena base para la capa DTN.

Un aspecto destacado en las MANET es su compatibilidad con los protocolos de Internet. Así, pueden proporcionar este servicio a todos los nodos de la red.

2.3.2 Protocolos de encaminamiento

Las MANET necesitan utilizar protocolos de encaminamiento distintos a los de las redes convencionales [5]. Los nodos de este tipo de red necesitan actualizar sus tablas de encaminamiento para gestionar las rutas entre los integrantes. Los protocolos de encaminamiento pueden ser reactivos, proactivos, híbridos y con calidad de servicio.

Los protocolos reactivos establecen la ruta entre nodos en el momento en que se necesita enviar información, en vez de mantener constantemente las tablas actualizadas. Las ventajas de este sistema son que evita la saturación del canal, no envía mensajes constantemente para mantener las tablas actualizadas y ahorra energía. La desventaja es que cada vez que se transmite es necesario esperar a que se establezca la ruta.

Los protocolos proactivos mantienen las tablas de encaminamiento constantemente actualizadas. Se renuevan periódicamente y cada vez que se producen cambios en la topología de la red. Las ventajas de este tipo de protocolos son que necesitan poco tiempo para el establecimiento de la conexión porque los nodos conocen las rutas de antemano y que el uso de los recursos es bastante estable. Sin embargo, los mensajes de control afectan al ancho de banda del canal y el consumo de energía es mayor.

Por último, los protocolos con calidad de servicio buscan que se establezcan conexiones que garanticen unos requisitos mínimos. Hay que tener en cuenta que esto no siempre es posible en una

MANET y que el no alcanzar los mínimos no debe ser un impedimento para el funcionamiento de la red.

2.3.3 Optimized Link State Routing Protocol

OLSR (*Optimized Link State Routing Protocol*) es de un protocolo de encaminamiento proactivo ideado por T.Clausen y P. Jacquet en noviembre de 1998. Utiliza un método llamado retransmisión multipunto por inundación [5]. Consiste en seleccionar un conjunto de nodos vecinos llamados *Multipoint Relay,* encargados de realizar la inundación *broadcast,* aumentando así la eficiencia en el proceso. De este modo, no disminuye tanto el ancho de banda y se consigue que los paquetes lleguen igualmente a todos los nodos de la red. Se ha comprobado que cuanto mayor es la red en la que se aplica este protocolo, más beneficios se obtienen en comparación a un método de inundación normal. Se debe destacar que OLSR no encamina tráfico, sino que actualiza las tablas de encaminamiento.

El protocolo tiene una estructura modular con un núcleo central. Por lo tanto, al protocolo se le pueden añadir complementos que amplían su funcionamiento básico. El núcleo se divide en las siguientes partes:

- Formato de los paquetes y reenvío.
- Estado de enlace.
- Detección de enlaces y nodos vecinos.
- Selección y señalización *Multipoint Relay*.
- Difusión de mensajes de control.
- Cálculo de caminos.

Destaca la importancia de los mensajes de control HELLO, encargados del estado de enlace, detección de nodos vecinos y señalización de las retransmisiones *Multipoint Relay*. Por último, los mensajes TC (*Topology Control*) son los encargados de la transmisión de la topología de la red, los mensajes MID (*Multiple Interface Declaration*) de indicar la presencia de nodos con múltiples interfaces y los HNA (*Host Network Association*) de indicar la presencia de interfaces no OLSR.

2.4 Proyecto de referencia: El Internet interplanetario

Las conexiones interplanetarias, según se describe en [6] y en [7], son un gran reto intelectual y económico para el mundo aeroespacial. Se trata de una ambiente sometido a grandes retardos, errores de *bits* y múltiples desconexiones, haciendo muy difícil que los datos transmitidos lleguen a su destino. Por un lado, mientras que los tiempos en una red terrestre de bajo retardo son del orden de milisegundos, como podría ser el caso del servicio de Internet proporcionado a la mayoría de las casas, el retardo, en el camino de ida, de una transmisión a la Luna sería de casi dos segundos y el retardo de una transmisión a Marte sería de ocho minutos A este aspecto hay que sumarle los errores en los bits transmitidos, producidos por la radiación solar y las desconexiones ocurridas por la interposición de cuerpos celestes en medio de la línea de visión de las dos antenas.

La NASA, y más concretamente los científicos Kevin Gifford, Adrian Hook y Karen Tuttle, están llevando a cabo una serie de experimentos en colaboración con la Estación Espacial Internacional y otras estaciones en tierra que tiene como finalidad llegar a establecer una red interplanetaria similar a Internet pero, en este caso, tolerante a fallos. Esta red sería capaz de conectar la Estación Espacial Internacional con robots, con estaciones terrestres y llegar incluso a sostener infraestructura en la superficie de otros planetas.

Los experimentos con la red interplanetaria consisten en utilizar este tipo de infraestructura en los CGBA-4 y CGBA-5, que son instrumentos genéricos de bioprocesado para establecer las condiciones idóneas de realización en el espacio de una gran variedad de experimentos. Los científicos manejan estos instrumentos desde la Tierra y permiten monitorizar las pruebas y experimentos durante la

misión espacial. Instalándoles el *software* DTN y comprobando el funcionamiento desde la Tierra se pueden extraer importantes conclusiones y planificar mejoras. Por otro lado, la red DTN también debe transmitir telemetría desde la Estación Espacial Internacional hasta una estación en tierra situada en Boulder, *downlink*, con la correspondiente confirmación automática de la entrega de los paquetes, *uplink*.

El primer experimento sobre se realizó en julio de 2009 y consistió en el envío de imágenes desde el CGBA-5 a la tierra a través de un satélite, sin conocer el estado de los enlaces de subida y bajada. Se comprobó que a pesar de las interrupciones de la comunicación, que duraron varios minutos, el CGBA-5 volvió a realizar la transmisión de custodia de los datos después de un determinado tiempo de espera. Por ello, se concluyó que la prueba del protocolo de la red tolerante a interrupciones había sido un éxito. En un segundo experimento, el CGBA-5 envió datos de telemetría a la tierra través de la red no DTN, y los mismos datos a través de la DTN. En este caso, en un periodo de tres días, la media de recepciones redundantes en la DTN fue muy inferior. La NASA espera aumentar el despliegue de la red, llegando a estar compuesta por dos nodos espaciales, el CGBA-4 y el CGBA-5, y dos nodos en tierra. Con ellos se pretende iniciar la investigación en el campo de la transferencia de custodia en una sola dirección y en el del encaminamiento basado en el estado de los nodos cercanos.

Si hay algo que se puede concluir de este proyecto, es que la NASA necesita el protocolo DTN para completar sus misiones en la Luna, Marte y a donde quiera que la lleve el paso del tiempo, pues facilita la investigación realizada por humanos y robots. La DTN aporta unas características que no puede facilitar otro tipo de red y que son vitales para soportar las duras condiciones del ambiente interplanetario. Por otro lado, el hecho de que la NASA necesite desplegar una DTN es beneficioso para la evolución de este tipo de redes, ya que gracias a los medios de la agencia se podrán realizar experimentos que mejoren su funcionamiento para aplicarse posteriormente en otros ámbitos.

2.5 IBR-DTN

2.5.1 Introducción

IBR-DTN es un *software* que implementa la pila de protocolos de la arquitectura DTN. La capa que este *software* gestiona está basada en [3] y sus protocolos de seguridad en [4]. Permite encaminamiento mediante conexiones estáticas, reenvío a través de los nodos descubiertos, encaminamiento *Epidemic* con *bloomfilter*, que utiliza una estructura probabilística de datos para indicar si un nodo está presente en la red o no, encaminamiento por inundación, menos eficiente, y encaminamiento *PRoPHET*, que se explicará a continuación. Además, tal y como describe en la arquitectura DTN, emplea almacenamiento persistente en la memoria de los dispositivos para tolerar reinicios y fallos del sistema.

Este *software* proporciona una capa de comunicación que se asienta sobre la capa de transporte y, por tanto, también sobre la capa de red. Por eso necesita funcionar sobre los protocolos subyacentes como son: TCP/IP, UDP/IP, IPND, entre otros.

Adicionalmente, IBR-DTN proporciona una serie de aplicaciones que se explican más adelante, demostrando la potencialidad de este tipo de redes.

2.5.2 Descubrimiento de nodos y encaminamiento

Para entender la manera en que los nodos descubren a sus vecinos en la red para posteriormente intercambiar las listas de los vecinos de cada nodo es necesario explicar brevemente el funcionamiento de IPND (*IP Neighbor Discovery*) [8], que es un método de descubrimiento de vecinos a través de IP. Los nodos usan el IPND para conocer la existencia, disponibilidad y dirección de otros nodos. Consiste en la escucha y envío de mensajes UDP, llamados “beacons”, que sirven a los nodos para anunciarse. Los mensajes se envían mediante *unicast, multicast* o *broadcast* e incluyen el EID de los

equipos, permitiendo así establecer conexión con ellos. Una vez se establece la conexión es posible intercambiar los DHT.

El funcionamiento de IPND se apoya sobre tablas *hash* distribuidas, DHT. Una tabla *hash* consiste en un índice que poseen todos los pares que conforman una red y que permite la búsqueda del nodo con el que se pretende establecer una conexión. De este modo se evita la necesidad de designar un nodo central que posea la información para enlazar con el resto de pares porque de ser así, si el nodo central falla o está fuera de cobertura, la red dejaría de funcionar.

Otra cuestión relevante de las DTN es el encaminamiento. IBR-DTN proporciona un mecanismo denominado PRoPHET, que es el elegido en este TFG. Se trata de un protocolo de encaminamiento que funciona por probabilidad, usando el historial de encuentros y la transitividad. La transitividad implica que si un elemento se relaciona con otro y ese otro con un tercero, entonces el primero y el tercero también se relacionan. Es una ligera modificación del protocolo *Epidemic*, que comprueba que todos los nodos de la red tienen todos los mensajes. *PRoPHET*, a través de estimaciones de probabilidad, consigue aumentar la eficiencia y evita la inundación innecesaria de la red.

3 DESARROLLO

3.1 Configuración

3.1.1 Objetivo

En este apartado se expone el método utilizado para conseguir el objetivo de desplegar la red. Se explica la configuración de los equipos al detalle y se comentan las dificultades encontradas, así como las soluciones adoptadas y otras alternativas posibles.

3.1.2 Descripción de los equipos que forman la red

Las antenas seleccionadas para desplegar la red son las siguientes: la Ubiquiti Nanostation M2 (Figura 3-1), la Ubiquiti Bullet Titanium M2 Hi Power (Figura 3-2) y la Ubiquiti Picostation 2HP (Figura 3-3). La Nanostation M2 es el nodo de tierra y por lo tanto, a través del que se provee el servicio de Internet a toda la red. Las Ubiquiti Bullet Tintanium M2 son las que se instalan en las lanchas como nodos DTN-OLSR. Por último, las Ubiquiti Picostation 2 son los puntos de acceso inalámbricos para los equipos de la red interna de las Lanchas de Instrucción.

La Nanostation M2 [9] es un punto de acceso de alto rendimiento y bajo coste. Contiene mejoras en la latencia, caudal y escalabilidad con respecto a otros equipos similares. Por otro lado, está preparada para funcionar en exteriores, incluyendo una carcasa que permite cubrir el espacio en el que se encuentran los pines de conexión de los cables Ethernet. Su procesador es el Atheros MIPS 24KC de 400 MHz, tiene una memoria SDRAM de 32 MB y 8 MB de memoria *flash*. Utiliza una fuente de energía de 24 voltios y 0,5 amperios y su polarización es lineal dual. Por último, cabe recalcar que la sujeción se realiza mediante bridas fijas a un volumen cilíndrico.

Figura 3-1 Nanostation M2.

La Ubiquiti Bullet Titanium M2 Hi Power descrita en [10], junto con la antena omnidireccional de Alfa Network de 2,4GHz y 15dBi constituye un tipo de dispositivo con un diseño adecuado para exteriores, gracias a la calidad del aluminio y a la carcasa preparada para soportar condiciones ambientales adversas. Además, incluye varias tiras hidrófugas que se enroscan en las zonas comprometidas para evitar su deterioro. Tiene una potencia de hasta 600 mW y su capacidad de recepción mejora con respecto a la versión anterior, la Bullet M. Tiene un peso de 196 g, un procesador Atheros MIPS 24KC de 400 MHz, una memoria SDRAM de 32 MB y 8 MB de memora *flash* y una alimentación similar a la de la Nanostation M2. Todo ello la convierte en un dispositivo adecuado para enlaces a larga distancia y permite una gran personalización de su uso. Con respecto a la instalación, la sujeción se realiza mediante anclajes atornillados a un volumen cilíndrico.

Figura 3-2 Ubiquiti Bullet M2.

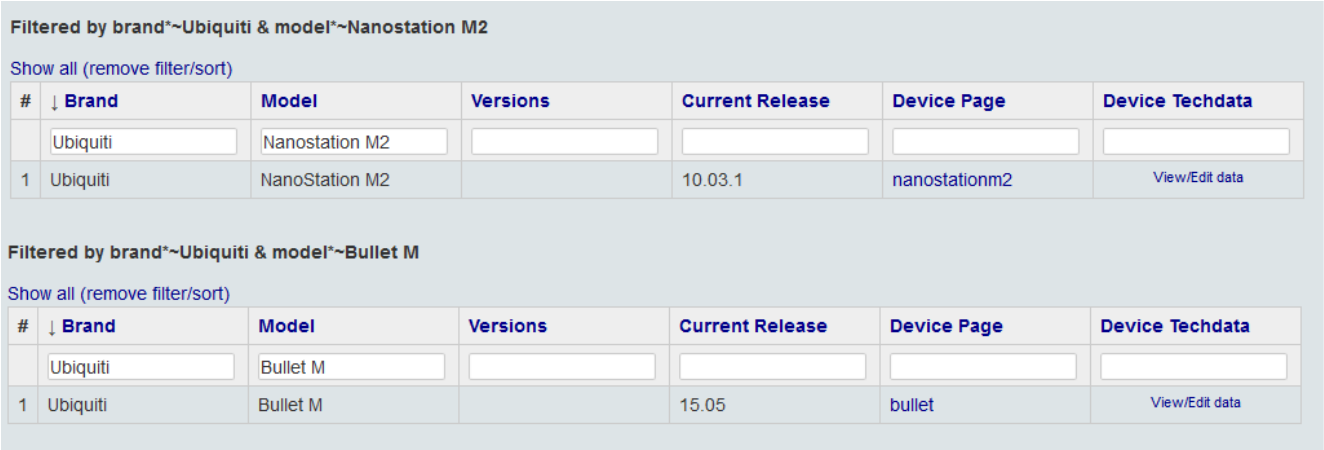
La Ubiquiti Picostation 2HP caracterizada en [11], junto con la antena RP-SMA 6dBi constituye un potente y eficaz punto de acceso gracias al procesador Atheros AR2316 SOC, MIPS 4KC de 180MHz. Cuenta con una memoria SDRAM de 32 MB y una memoria *flash* de 8 MB, puede llegar hasta una potencia de 29 dBm y tiene una sensibilidad de -95dBm. El alcance es de 500 m, aproximadamente, más que suficiente para hacer la función de punto de acceso en las Lanchas de Instrucción, y necesita una alimentación de 12 V y 1 A, efectuándose la alimentación a través de cable Ethernet. Por último, cabe destacar que está preparada para operar en exteriores gracias a la cubierta protectora de las tomas Ethernet. Con respecto a la instalación, cuenta con dos tipos de anclaje, atornillado o embridado a una superficie cilíndrica.

Figura 3-3 Picostation 2HP [11].

3.1.3 Descarga del sistema operativo de los puntos de acceso

El sistema operativo instalado en los puntos de acceso se puede descargar en la referencia [12]. Para averiguar qué sistema operativo se debe instalar se introducen los datos de los dispositivos en la tabla de *hardware* de la página (Figura 3-4) y se accede al apartado en el que se indican las versiones disponibles para cada uno. Para tomar una decisión adecuada es preciso tener en cuenta qué se pretende conseguir, siendo en este caso el despliegue de una red tolerante a fallos que emplea el *software* IBR-DTN. Este *software* solo es compatible con algunos sistemas operativos por lo que habrá que seleccionar uno que tenga una arquitectura que no produzca fallos al instalar IBR-DTN y que sea válido al mismo tiempo para cada punto de acceso.

A continuación se separan los caminos de los tres tipos de dispositivo que se usan en este proyecto. El primero emplea el sistema operativo “openwrt-ar71xx-generic-ubnt-nano-m-squashfs-factory.bin”, el segundo, el “openwrt-ar71xx-generic-ubnt-bullet-m-squashfs-factory.bin” y el tercero, el “openwrt-15.05-ath25-ubnt2-pico2-squashfs.bin”.



Filtered by brand*~Ubiquiti & model*~Nanostation M2

Show all (remove filter/sort)

#	↓ Brand	Model	Versions	Current Release	Device Page	Device Techdata
	Ubiquiti	Nanostation M2				
1	Ubiquiti	NanoStation M2		10.03.1	nanostationm2	View/Edit data

Filtered by brand*~Ubiquiti & model*~Bullet M

Show all (remove filter/sort)

#	↓ Brand	Model	Versions	Current Release	Device Page	Device Techdata
	Ubiquiti	Bullet M				
1	Ubiquiti	Bullet M		15.05	bullet	View/Edit data

Figura 3-4 Tabla de *hardware* de Openwrt [12].

3.1.4 Instalación de Openwrt

La instalación de Openwrt con un ordenador que use Ubuntu puede realizarse de dos maneras: a través del sistema operativo del punto de acceso, Air OS, que viene instalado de fábrica o a través de una conexión TFTP. Si se escoge la primera opción, lo que deberemos hacer es acceder, a través de la dirección IP 192.168.1.20, al interfaz gráfico que proporciona el sistema operativo y seleccionar la opción "Browse", dentro del apartado del sistema operativo, para indicar desde nuestro ordenador el *software* que hayamos elegido para el punto de acceso en cuestión. En caso de elegir la opción de TFTP, habrá que descargar el paquete en nuestro ordenador escribiendo en el terminal el comando "sudo apt-get install tftp". A continuación, tendremos que iniciar el modo TFTP de la antena, presionando el botón de "Reset" desde justo antes de conectar la antena a la alimentación hasta que se aprecien luces LED parpadeando en color rojo. Una vez hecho, se empleará un cable Ethernet para establecer una conexión local entre el ordenador y la antena de forma que se pueda iniciar la instalación. Es muy importante tener claro que este cable se conectará en la clavija LAN del adaptador PoE y no a la toma PoE, *Power on Ethernet*, que será la que conectará directamente con el punto de acceso para darle alimentación. Para establecer la conexión se configurará el interfaz *eth0* de nuestro ordenador con una IP que se encuentre dentro de la misma subred que emplea la antena para comunicarse. Una opción sería 192.168.1.254, teniendo en cuenta que nos encontramos en la subred 192.168.1.0/24. A continuación se procederá a enviar el archivo mediante TFTP (Figura 3-5). Si esta operación se desarrolla correctamente la instalación se realizará de manera inmediata en la antena, luego se reiniciará y ya será posible acceder a la interfaz gráfica de Openwrt.

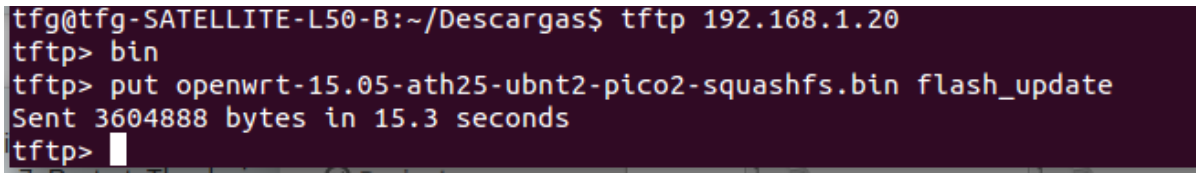


Figura 3-5 Instalación con TFTP.

Un aspecto importante que se deberá conocer sobre TFTP es que será útil en caso de que se produzca un error en la instalación, pues es un método válido para restablecer el sistema de la antena. Sin embargo, el primer procedimiento de carga del *firmware* mencionado no sería posible en caso de fallo de la instalación. Durante la instalación del sistema operativo en la antena sectorial (Nanostation M2) se produjo esta situación y fue necesario realizar la recuperación mediante TFTP. El proceso es igual, pero antes del comando "put" es necesario ejecutar la orden "trace" en el terminal, a lo que

responderá, "packets tracing on", que es lo que permitirá que los paquetes lleguen a su destino y puedan instalarse a pesar de que el software instalado esté dañado. A mayores, el comando "flash_update" se tendrá que omitir.

Un inconveniente muy común a la hora de realizar la instalación ocurre en el momento de configurar manualmente la IP del interfaz *eth0*. Como sabemos, Ubuntu cuenta con un gestor de las conexiones, llamado *Network Manager*, que tomará decisiones por nosotros y, en ocasiones, cuando realicemos una configuración manual la modificará. Si esto sucede, habrá que asegurarse de que el Network Manager está en modo manual y si no es así, habrá que modificarlo. Si a pesar de la comprobación el fallo persiste, se puede desinstalar Network Manager y manejar las conexiones con el terminal.

3.1.5 Instalación del protocolo de encaminamiento OLSR

Dado que el sistema operativo ha cambiado, la IP del punto de acceso también, pasando a ser 192.168.1.1. Como ya habíamos configurado nuestro interfaz Ethernet en la subred 192.168.1.0/24, solo tendremos que abrir el navegador y teclear la IP en cuestión para acceder a la interfaz gráfica. Para asegurarnos de que va a funcionar podemos ejecutar un comando *ping* a esta dirección, comprobando de este modo que recibimos respuesta del dispositivo.

Para instalar el protocolo de encaminamiento, se deben descargar los paquetes indicados en [13], pero tal y cómo está conectado el punto de acceso en este momento no es posible. Para modificar la conexión, accederemos en la interfaz gráfica a la pestaña "Network" y una vez dentro editaremos la interfaz *eth0*. En la pestaña "General Setup", que es la primera en aparecer, podremos ver que *eth0* está configurado con una IP estática 192.168.1.1 y una máscara de red 255.255.255.0. Para realizar los cambios oportunos seleccionaremos en la pestaña de "Static Address" la opción "DHCP client", presionaremos el botón "Switch Protocol" y guardaremos la configuración. Si no se da la orden de cambiar el protocolo antes de guardar los cambios, el protocolo no se modificará y el punto de acceso no tendrá acceso a Internet.

Si todo lo anterior se hizo según los pasos indicados la siguiente tarea será enchufar el cable conectado en la toma LAN de la antena a una toma Ethernet con acceso a Internet. De esta manera, el punto de acceso recibirá a través del protocolo DHCP una IP que le permitirá acceder a los servidores de descarga de paquetes para Openwrt. Sin embargo, durante este proceso pueden surgir algunos inconvenientes, como es el caso del fallo en la configuración de los DNS o la falta de puerta de enlace a la *web* en las tablas de encaminamiento de la antena. Más adelante se expondrá cómo se deben afrontar.

A partir de este momento se puede establecer una conexión con el punto de acceso mediante protocolo SSH. Esta conexión se realizará por cable Ethernet en el puerto 22, por lo que previamente se debe comprobar que en la pestaña "System" de la antena, en el apartado de administración, se encuentra seleccionado este puerto para SSH. La conexión se establece a través del terminal mediante el comando "ssh root@IPpunto_de_acceso" (por ejemplo "ssh root@192.168.1.26" si la IP del punto de acceso es 192.168.1.26).

Tal y como se expone en la referencia [14], el protocolo SSH (Figura 3-6) permite acceder a máquinas remotas a través de la red y controlarlas mediante una serie de comandos, así mismo, cifra la sesión de conexión haciendo imposible que un atacante pueda robar las contraseñas. Cuando se establece la primera conexión se registra la clave RSA, tal y como se puede ver en la Figura 3-6, de modo que en las próximas conexiones con esa máquina la huella tendrá que coincidir o se considerará que estamos siendo víctimas de un ataque. Así, queda garantizado que no se nos redirigirá a un nodo malintencionado cuando estemos realizando la conexión.

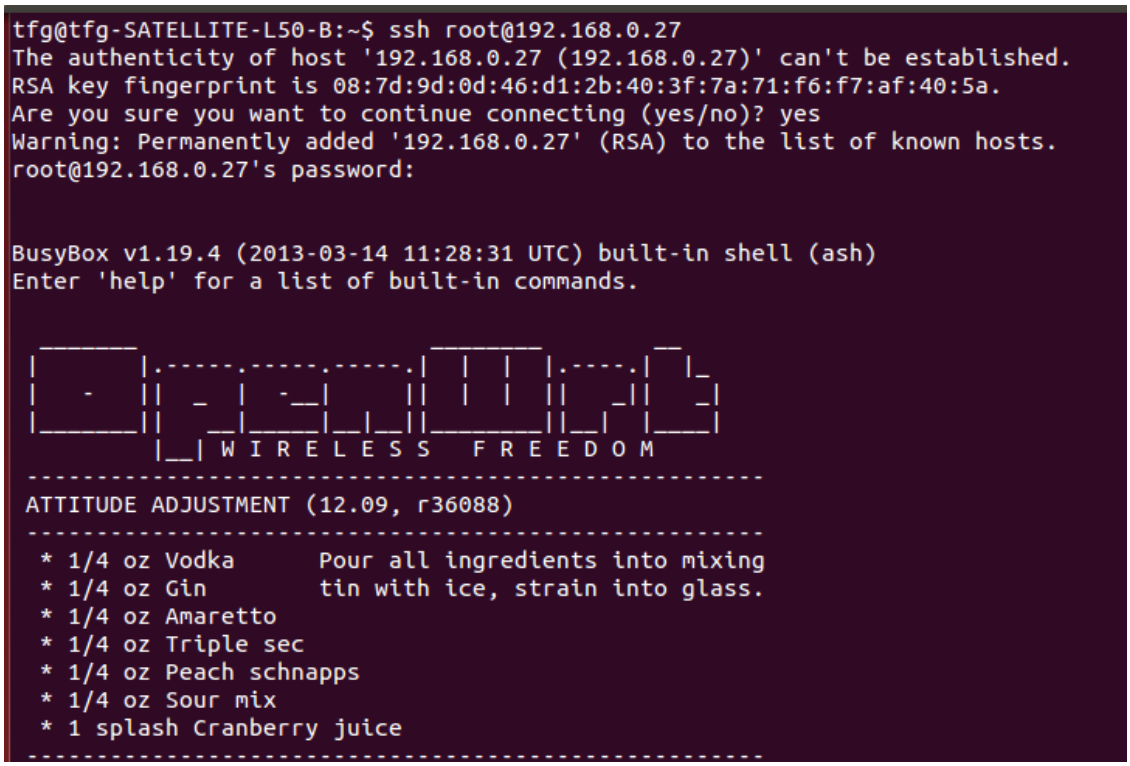


Figura 3-6 Conexión SSH.

Llegados a este punto analizaremos los fallos de establecimiento de la conexión a Internet. En primer lugar, sabremos que existe un error si al intentar hacer un ping desde la antena a una página como www.google.es se obtiene una señal de error ICMP. Para distinguir de qué fallo se trata realizaremos un *ping* a una dirección de servidores de Google, por ejemplo “ping 8.8.8.8”. Si no obtenemos respuesta sabremos que no se ha incluido la información del encaminador en la tabla de encaminamiento del punto de acceso. Para solucionarlo, tendremos que introducir una ruta por defecto con el comando “sudo route add default gw IP”, siendo la dirección IP que figura en el comando la del encaminador de la red que se esté usando. Una vez solventado volveremos a hacer un *ping* a la misma página y en caso de volver a recibir un error ICMP se accederá al archivo “resolv.conf”, que se encuentra en la carpeta “/etc”, a través de los comandos “cd /etc” y “vi resolv.conf”. Será necesario usar la opción “vi” porque no estará instalado aún el comando “nano”, que tiene un funcionamiento mucho más sencillo para el usuario. Tendremos que editar el archivo cambiando la dirección del servidor DNS 127.0.0.0 por la de un servidor de Google, de forma que lo escrito en el documento sea “nameserver 8.8.8.8”. Al finalizar, la página de Google debería responder al *ping* y eso significará que el punto de acceso ha encontrado ruta hacia Internet y es capaz de enlazar los servidores de nombres adecuados.

Entender el protocolo ICMP facilita mucho la conectividad de las máquinas. ICMP pertenece al conjunto de protocolos de Internet y sobre todo se encarga de enviar mensajes de error cuando se produce algún fallo o contratiempo en algún proceso IP, por lo que se puede decir que su principal función es de diagnóstico y control. Los paquetes ICMP se dirigen a la fuente originadora y eso permite que se pueda analizar el fallo. Por ejemplo, si efectuamos un *ping*, que es una herramienta que permite comprobar la comunicación entre una máquina local y una o varias máquinas remotas usando un mensaje de petición *Echo ICMP*, y recibimos un mensaje ICMP de destino inalcanzable, sabremos que existe un problema para enlazar los dos extremos de la conexión. En el caso de realizar un *traceroute*, los mensajes ICMP nos permitirán saber si el paquete ha alcanzado o no su destino y en el caso de haberlo hecho, cuántos saltos ha dado para llegar al punto final. Los paquetes ICMP se encapsulan dentro de un datagrama IP por lo que no se garantiza su entrega, pero sí que se tratan como un tipo de mensaje especial.

Los principales mensajes ICMP que pueden generarse son los siguientes [15]:

- Fuente saciable: se produce porque los paquetes enviados a una máquina disminuyen su velocidad porque su búfer está lleno o llegando al límite.
- Redirecciones: se dan cuando se están enviando paquetes a un encaminador para comunicarse con una máquina pero hay una ruta más adecuada a través de un encaminador diferente.
- Tiempo excedido: se usa para indicar a la fuente que el tiempo de vida ha llegado a cero.
- Sello temporal: se usa para la sincronización de tiempo.
- Solicitud de dirección de máscara: lo envía normalmente un cliente a un encaminador para obtener una adecuada máscara de subred.
- Destino inalcanzable.
- Petición y solicitud Echo.

El primer paso para iniciar la instalación de los paquetes OLSR es escribir en el terminal el comando "opkg update" para que el gestor de paquetes *opkg* actualice la lista de paquetes disponibles. La siguiente orden que se dará será la siguiente: "opkg install luci luci-ssl nano pciutils luci-app-olsr lucí-app-olsr-services luci-app-olsr-viz olsrd olsrd-mod-arprefresh olsrd-mod-bmf olsrd-mod-dot-draw olsrd-mod-dyn-gw olsrd-mod-dyn-gw-plain olsrd-mod-httpinfo olsrd-mod-mdns olsrd-mod-nameservice olsrd-mod-p2pd olsrd-mod-pgraph olsrd-mod-secure olsrd-mod-txtinfo olsrd-mod-watchdog". Así, se instalarán todos los paquetes necesarios para el funcionamiento de la red mallada (Tabla 3-1) y también otros como "nano" que facilitan el uso del terminal y la configuración.

olsrd 0.6.1-3		
Name	**Size**	**Description**
olsrd	108257	OLSR (Optimized Link State Routing) daemon
olsrd-mod-dyn-gw-plain	2902	Dynamic internet gateway plain plugin
olsrd-mod-bmf	12106	Basic multicast forwarding plugin, dependece: `kmod-tun`
olsrd-mod-httpinfo	23831	Small informative web server plugin
olsrd-mod-quagga	5848	Quagga plugin
olsrd-mod-dyn-gw	4348	Dynamic internet gateway plugin
olsrd-mod-txtinfo	6201	Small informative web server plugin
olsrd-mod-nameservice	11511	Lightweight hostname resolver plugin
olsrd-mod-dot-draw	4233	Dot topology information plugin
olsrd-mod-mdns	5648	Multicast DNS plugin
olsrd-mod-watchdog	2316	Watchdog plugin
olsrd-mod-arprefresh	2703	Kernel ARP cache refresh plugin
olsrd-mod-p2pd	8066	Peer to Peer Discovery plugin
olsrd-mod-secure	9710	Message signing plugin to secure routing domain

Tabla 3-1 Paquetes OLSR [12].

3.1.6 Configuración de OLSR

En este apartado se expone de forma detallada la configuración del protocolo de encaminamiento. Esta configuración puede realizarse a través del interfaz gráfico LuCi o mediante una conexión SSH a la antena que se quiera configurar. Para simplificar la configuración, se decidió que la mejor opción era hacerlo a través del interfaz gráfico LuCi por ser un entorno más confortable para el usuario.

Para conectarnos al punto de acceso tendremos que conocer su dirección IP, por lo que habrá dos situaciones diferentes según la configuración que le hayamos dado al dispositivo. Si tiene una IP estática, sabremos de antemano cuál es su dirección IP, pero no si está en modo DHCP y, por lo tanto, será necesario averiguarlo. Una opción muy sencilla para solucionar este inconveniente es usar un programa como AngryIP, que permite conocer la dirección que se le ha asignado a un nuevo equipo conectado a la red LAN del lugar de trabajo. Por otro lado, al acceder a la dirección IP de algunos encaminadores se presenta un esquema de los equipos conectados a la red. Por ello, conociendo la dirección MAC del *hardware*, es decir, la dirección de capa de enlace, podremos averiguar cuál es la dirección IP que se le ha asignado.

Cuando se haya establecido la conexión, el primer paso es habilitar el servidor *web* de forma que el sistema operativo sea capaz de iniciarlo cada vez que el sistema arranque. Esta operación se realiza en el terminal mediante los siguientes comandos: en primer lugar, "/etc/init.d/uhttpd enable" para habilitarlo, en segundo lugar, "/etc/init.d/uhttpd start" para iniciarlo, y por último "reboot" para asegurarse de que al reiniciar todos los sistemas funcionan correctamente. Seguidamente accedemos al interfaz gráfico de la antena a través del navegador web, eso nos permitirá ver una imagen general del estado de la antena. Accederemos a la pestaña "System" y dentro del apartado "General Settings" le daremos nombre al punto de acceso en la casilla "Host", sin olvidar guardar y aplicar los cambios al final del proceso. Dentro del apartado "Administration" que se encuentra en la pestaña "System". En ella, tendremos que modificar la configuración de acceso SSH activando la casilla que permite el acceso desde clientes de otras redes. Así, una vez que OLSR esté funcionando se podrá acceder al punto de acceso desde otros nodos vecinos.

El siguiente paso será añadir una nueva interfaz, pues por defecto solo existe el interfaz LAN. Tras acceder a la configuración del interfaz, se le da nombre, en este caso "wlan0" por tratarse de un interfaz para conexión no cableada, y se clasifica como una red inalámbrica con dirección IP estática. Al aceptar los cambios, el sistema operativo permitirá seleccionar los parámetros de la red, pero para tomar decisiones correctas es preciso tener claro algunos conceptos. Para elegir qué rango IP vamos a dedicar a cada interfaz de red debemos tener en cuenta las subredes que pretendemos interconectar porque para que se produzca el encaminamiento entre ellas, sus IP no pueden encontrarse dentro del mismo rango. Por ejemplo, si un equipo tiene una dirección IP 192.168.1.2 que pertenece a la red 192.168.1.0/24 y pretende conectarse a otro equipo de otra red que tiene el mismo rango IP, no se producirá el encaminamiento y no será posible esta conexión. En nuestro caso, las subredes con las que se enlazará serán del tipo 10.X.0.0/16, siendo X el número de lancha multiplicado por 10, por lo que la red que hemos seleccionado para los nodos OLSR es la 192.168.2.0/24. Poniendo como ejemplo Lancha1, seleccionaremos una IP 192.168.2.10 con una máscara de red 255.255.255.0 y guardaremos los cambios. El resto de antenas variarán el último número de su dirección según el número de lancha, es decir, Lancha2 tendrá una dirección 192.168.2.20 perteneciente a 192.168.2.0/24

Para que el OLSR pueda funcionar, los parámetros del interfaz inalámbrico deben estar adecuadamente seleccionados y por eso lo próximo será acceder al apartado "WIFI" dentro de la pestaña "Network" para editar los datos que ahí figuran. En la configuración del dispositivo se elegirá el canal 3 (2,422 GHz) y una potencia de transmisión de 10 dBm para las pruebas, aunque luego deberá incrementarse al valor máximo. Indicaremos el nombre de la red mallada "NW-MESH", seleccionaremos el modo *ad-hoc* y le asignaremos el interfaz *wlan0* que ya habíamos configurado. Así, solo quedará guardar los cambios y posteriormente ponerla en funcionamiento. Por último, en la pestaña "Advanced settings", seleccionaremos el modo 802.11g y el código de país.

Los errores más comunes en este apartado, que impedirán la conectividad de los nodos OLSR, son debidos a una diferencia en la selección de las frecuencias de los nodos y a un nombramiento distinto y por lo tanto erróneo del enlace no cableado.

El hecho de haber configurado todos los parámetros no implica que el protocolo de encaminamiento sepa que interfaz utilizar para comunicarse, así que se tendrá que indicar. En el apartado "Services", al final de la página, aparece la opción de añadir un interfaz OLSR. Se seleccionará esta opción y se indicará que emplee *wlan0*.

Los *plugins* también se deben activar y configurar (Figura 3-7). Por ello, habrá que acceder al apartado de *plugins* de OLSR y asegurarnos de que así es. Como mínimo tendrán que estar activados los siguientes: "olsrd_arprefresh.so.0.1", "olsrd_dyn_gw.so.0.5", "olsrd_httpinfo.so.0.1", "olsrd_txtinfo.so.0.1" y "olsrd_dyn_gw_plain.so.0.4". Si se activa el *plugin* de servicio de nombres hay que configurarlo. Se accederá a su edición y se añadirán las siguientes casillas de parámetros: nombre, donde indicaremos el nombre que el protocolo envía al resto de nodos para adjuntar las tablas de encaminamiento, intervalo, que es la frecuencia con la que el nodo anuncia su nombre al resto de los nodos, el tiempo de validez, que es el periodo durante el que el nodo considera válido un mensaje de este tipo, el "sighup_pid_file", que permite enviar una señal al "dnsmasq" para indicar que el nodo ha modificado su tabla de nombres y que debe rehacer su archivo de nodos, y el "name_change_script", que permite mantener una base de datos actualizada aunque se produzcan cambios en las tablas de nombres.

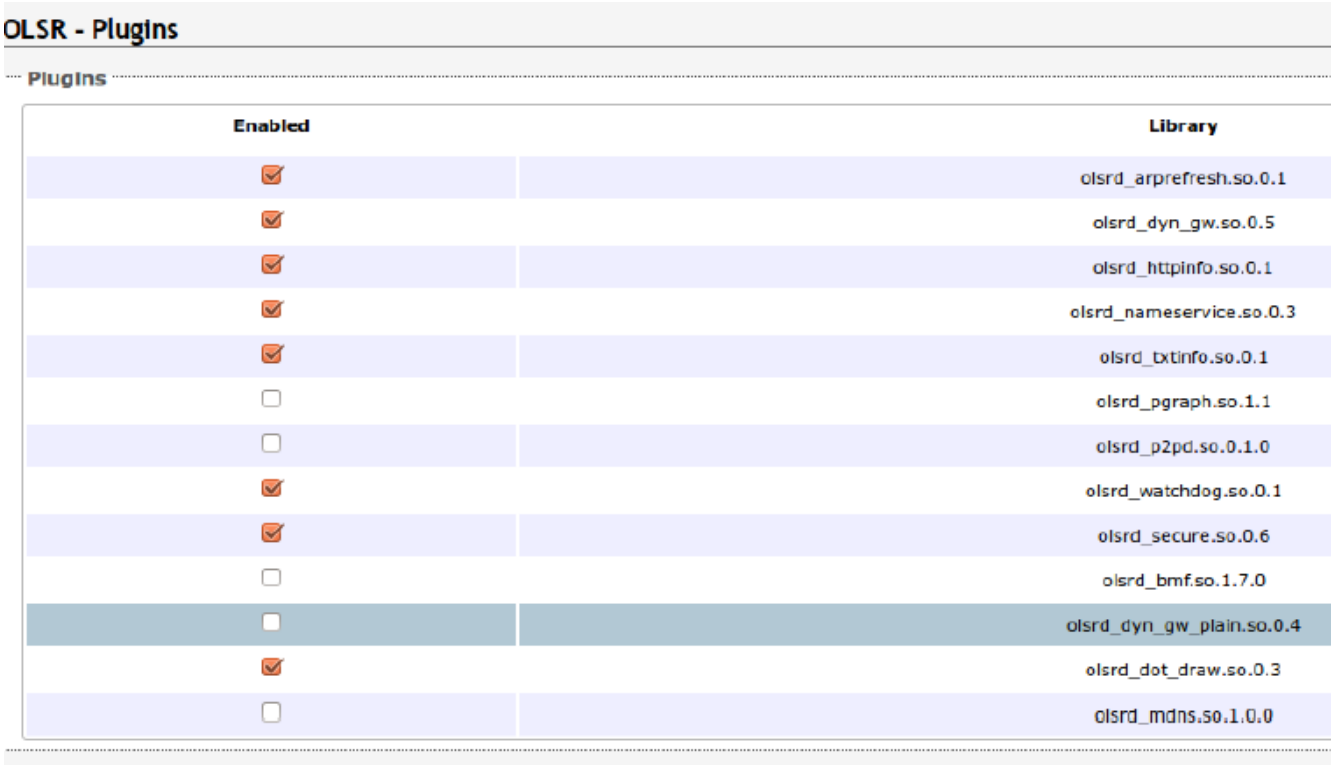


Figura 3-7 Complementos OLSR.

Dado que nos encontramos en una red privada, la configuración del cortafuegos de los nodos de las Lanchas de Instrucción será muy sencilla. Los dos interfaces se encontrarán dentro de la zona local y se permitirá *forwardings*, *inputs* y *outputs* para el funcionamiento del protocolo de encaminamiento. Por otro lado, en el nodo terrestre habrá que deshabilitar el *forwarding* hacia la red de la ENM del

tráfico *multicast* para evitar inundar esta red con el tráfico *multicast* que utilizan tanto OLSR como la red DTN.

A estas alturas, si se accede al apartado de OLSR dentro de la pestaña "Status", ya deberíamos de poder ver reflejado cualquier nodo vecino que aparezca dentro de la cobertura de la antena. Pero la configuración va más allá, pues para este proyecto no llega con tener conectados los nodos, sino que es necesario que sea posible la conexión entre redes externas a OLSR. Es decir, si un ordenador está conectado a la red interna de una lancha, debe poder establecer enlace con otro equipo que esté en la red interna de otra lancha. Para eso se utilizan los mensajes de asociación de redes externas a OLSR, mensajes HNA, que se encargan de anunciar las redes conectadas a los nodos que emplean el protocolo. Para configurar los nodos accederemos al apartado de "HNA", dentro de la pestaña "Services", y añadiremos la red correspondiente. Por ejemplo, el nodo OLSR Lancha4 con IP en *wlan0* 192.168.2.40 tendrá que anunciar la red interna 10.4.0.0/16. De este modo, todos los equipos que estén dentro de ese rango IP podrán conectarse a cualquier punto de la red. En la Tabla 3-2 se detalla la relación de las IP de la red.

Nombre antena	**WLAN0**	**LAN**
Lancha1 (Bullet M2)	192.168.2.10	10.1.0.1
Lancha1 (Picostation2)	-	10.1.0.5
Lancha2 (Bullet M2)	192.168.2.20	10.2.0.1
Lancha2 (Picostation2)	-	10.2.0.5
Lancha3 (Bullet M2)	192.168.2.30	10.3.0.1
Lancha3 (Picostation2)	-	10.3.0.5
Lancha4 (Bullet M2)	192.168.2.40	10.4.0.1
Lancha4 (Picostation2)	-	10.4.0.5
Sectorial (Nanostation M2)	192.168.2.50	10.5.0.1
DRON (Picostation M2)	192.168.2.60	10.6.0.1

Tabla 3-2 Organización a nivel IP de la red.

3.1.7 Acceso a Internet

Para proporcionar Internet a toda la red mallada habrá que conectar una de las antenas, a través de cable Ethernet, a una toma con servicio de Internet para que el propio OLSR sea capaz de anunciar la conexión. Si se accede a la tabla de redes anunciadas aparecerá una red identificada como 0.0.0.0 y máscara de red 0.0.0.0. Sin embargo, que anuncie la red no quiere decir que sea capaz de llevar a cabo el encaminamiento, pues las IP utilizadas en la red mallada son IP privadas, no públicas. Para que se produzca el encaminamiento es necesario activar el IP *masquerading* en el nodo terrestre. De ese modo se consigue que se traduzcan las IP privadas de la red a IP públicas para realizar peticiones a servidores de Internet. El mismo proceso tiene lugar al revés para que los clientes de la red privada reciban las respuestas a sus peticiones.

Para comprobar que la red tiene acceso a Internet con normalidad solo tendremos que conectarnos a una de las antenas que no esté directamente conectada a una toma con servicio de Internet. Tras comprobar que OLSR está funcionando con un *ping* a la IP de la *wlan0* del punto de acceso que anuncia la conexión a Internet, realizaremos un *ping* a los servidores de Google, por ejemplo a la

dirección 8.8.8.8. Si recibimos respuesta quiere decir que el encaminamiento funciona y que la red se anuncia correctamente. Si aun así no es posible acceder al contenido de la *web*, es muy probable que haya un error en la configuración de los DNS. Una solución válida aunque temporal, sería modificar el archivo "resolv.conf" y añadir los DNS, pero de ser así, habrá que revisar la configuración y comprobar que todo se ha realizado correctamente de cara a usos posteriores.

Si la prueba se está llevando a cabo en la red de la Escuela Naval Militar, no se recibirá respuesta al *ping* porque el tráfico de este tipo está bloqueado.

3.2 Instalación y configuración de IBR-DTN

3.2.1 Instalación de IBR-DTN

Para que la instalación de IBR-DTN no generase errores fue necesaria, en el paso de selección del sistema operativo del punto de acceso, la búsqueda de una arquitectura compatible que permitiese el funcionamiento de este *software*. La arquitectura seleccionada fue "ar71xx, Attitude Adjustment 12.09". En consecuencia, el *software* IBR-DTN tendrá que compartir estas características con el sistema operativo para poder funcionar. Por lo tanto, al acceder a [16] habrá que elegir la descarga correcta entre las siguientes opciones: arquitectura "x86, Backfire 10.03.1", arquitectura "ar71xx, Backfire 10.03.1", arquitectura "x86, Attitude Adjustement 12.09" o "ar71xx, Attitude Adjustment 12.09".

Para instalar los paquetes se accede al terminal y se establece una conexión SSH con el punto de acceso. A continuación, se accede a la carpeta "/etc" y con el comando "nano" se edita el archivo "opkg.conf". En el editor se tendrá que añadir la siguiente línea de código: "src/gz ibrdtn http://jenkins.ibr.cs.tu-bs.de/download/openwrt/repository/attitude_adjustment/ar71xx/packages/". Así es como se indica al instalador, "opkg", a dónde debe acceder para obtener los paquetes que se necesitan. Tras guardar los cambios con la tecla F2, se ejecuta "opkg update" para que se actualice la lista de paquetes disponibles, incluyendo los del nuevo enlace. Si no se ha producido ningún error, tras ejecutar el comando "opkg install ibrdtnd" debería instalarse todo el *software* necesario. Los siguientes pasos ya serían de configuración.

3.2.2 Configuración de IBR-DTN

La configuración que se ha decidido adoptar en la DTN se ha aplicado usando la herramienta "uci" y modificando el archivo de configuración de IBR-DTN que se encuentra en "/etc/config/ibrdtn". En la Figura 3-8 se puede ver cuáles son los parámetros básicos de funcionamiento que se han tenido en cuenta y cómo se han configurado.

```
config daemon 'main'
        option logfile '/tmp/ibrdtn.log'
        option errfile '/tmp/ibrdtn.err'
        option routing 'prophet'
        option forwarding 'yes'

config daemon 'safemode'
        option forwarding 'no'
        option storage '64M'
        option maxblock '16M'


config daemon 'storage'
        option engine 'simple'
        option blobs '/tmp/ibrdtn/blobs'
        option bundles '/tmp/ibrdtn/bundles'

config daemon 'discovery'

config daemon 'tcptuning'

config network
        option type 'tcp'
        option port '4556'
        option global 'yes'
        option interface 'bmf0'
```

Figura 3-8 Parámetros básicos funcionamiento.

Para empezar a configurar, primero hay que asegurarse de que el complemento "olsr-mod-bmf" está activado porque el sistema nunca llegará a funcionar si no existe un sistema que gestione el tráfico *multicast* a través de OLSR. Tras comprobarlo, se tendrá que añadir al archivo de configuración el nuevo interfaz que crea el complemento, *bmf0*, que es el interfaz *multicast* de la red mallada. En principio, el sistema de encaminamiento utilizado será *PRoPHET*, explicado en [17].

```
config daemon 'dht'
        option port '9999'
        option enable_ipv6 'no'
        option ignore_neighbour_informations 'no'
        option allow_neighbour_announcement 'yes'
        option allow_neighbours_to_announce_me 'yes'
        option bootstrap 'yes'
```

Figura 3-9 DHT.

Con respecto a la actualización de las tablas de nodos alcanzables, IBR-DTN tiene dos formas de encontrarlos, a través de Internet o a través de métodos de descubrimiento locales. Para el método de Internet se emplea el DHT de Bittorrent y se permite gestionar los EID mediante direcciones de la capa de convergencia. Para ello, debe habilitarse la opción "bootstrap" tal y como se aprecia en la Figura 3-9. Por otro lado, para que funcione el descubrimiento de nodos de forma local, deben habilitarse las opciones "dht_allow_neighbour_announcement" y "dht_allow_neighbours_to_announce_me", y desactivarse "dht_allow_neighbours_to_announce_me".

```
config daemon 'timesync'

        option synchronize 'yes'
        option reference 'no'
```

Figura 3-10 Sincronización de tiempos.

Lo siguiente será la sincronización de tiempos (Figura 3-10), ya que si los nodos no están sincronizados, los paquetes serán rechazados por no concordar los sellos temporales. Por un lado, si Internet funciona, los nodos se sincronizarán en tiempo usando el servidor, sin embargo, como se trata de una red tolerante a fallos, deberá funcionar con ausencia del mismo, dotando a las lanchas de instrucción de una gran autonomía. La forma de hacerlo es configurando uno de los nodos como referencia temporal y dando la orden al resto de que empleen esa referencia para sincronizarse. Otra opción para la sincronización podría basarse en utilizar la señal GPS de las Lanchas de Instrucción. Esta última opción ofrece la ventaja de que cada una de las embarcaciones puede ajustar su reloj sin necesidad de comunicarse con nadie.

```
config 'static-connection'
        option uri                      dtn://Sectorial
        option address          192.168.2.50
        option port                     4556
        option protocol         udp
        option immediately      no


config 'static-connection'
       option uri                       dtn://Lancha3
       option address           192.168.2.30
       option port                      4556
       option protocol          udp
       option immediately       no

config 'static-connection'
       option uri                       dtn://Lancha4
       option address           192.168.2.40
       option port                      4556
       option protocol          udp
       option immediately       no

config 'static-connection'
       option uri                       dtn://Lancha2
       option address           192.168.2.20
       option port                      4556
       option protocol          udp
       option immediately       no

config 'static-connection'
       option uri                       dtn://Lancha1
       option address           192.168.2.10
       option port                      4556
       option protocol          udp
       option immediately       no
```

Figura 3-11 Conexiones estáticas.

Dado que en esta red se conocen las direcciones IP de todos los nodos que la conforman, es beneficioso para todo el sistema indicar a todos los equipos con IBR-DTN instalado, quiénes son sus vecinos y bajo que IP van a ser localizados. De este modo, se simplifica el intercambio de información a la hora de localizar a los vecinos. La forma de hacerlo es utilizando conexiones estáticas, como se puede ver en la Figura 3-11. En cualquier caso, esto último no es necesario para un correcto funcionamiento de la DTN.

3.3 Configuración de los puntos de acceso de las Lanchas de Instrucción

La señal inalámbrica que emiten los nodos OLSR permite que los nodos se conecten entre ellos. Sin embargo, esa red no emplea el mismo lenguaje que los dispositivos habituales. Por ello, aunque figure entre las redes inalámbricas la detección de un ordenador o un teléfono móvil, no es posible conectarse a no ser que el dispositivo sea un nodo OLSR. Como uno de los intereses de este proyecto es que las lanchas tengan capacidad de acceso a Internet de forma inalámbrica, es necesario instalar un punto de acceso adicional por lancha que proporcione este servicio. La forma en que se ha decidido configurar estos puntos de acceso se conoce como "bridged AP" y la forma de hacerlo se desarrolla en [12]. Este tipo de punto de acceso permite extender las capacidades de los nodos OLSR, de modo que serán ellos los que proporcionen la conectividad IP pero a través de estos puntos de acceso. Además, con este sistema no será necesaria ninguna modificación para la configuración del tráfico *multicast*.

El modo puente (Figura 3-12) consiste en unir dos redes a nivel de enlace de forma transparente para los nodos de ambas redes, por ejemplo una red Ethernet con una inalámbrica.

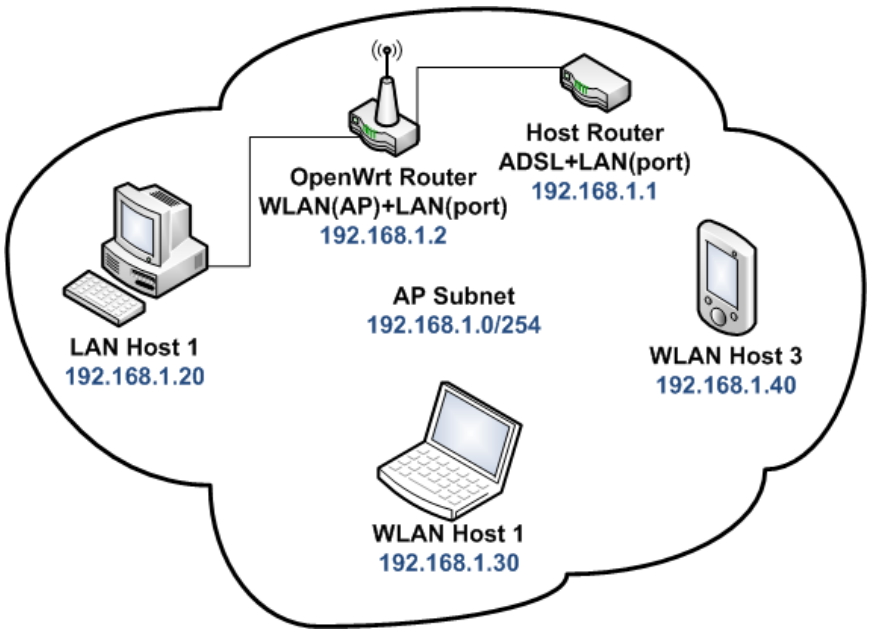


Figura 3-12 Modo "bridge" [12].

En este caso, con ánimo de aplicar y poder ilustrar un método distinto para configurar, todo el proceso se ha llevado a cabo a través de una conexión SSH. Este proceso consiste en modificar ficheros e introducir los nuevos parámetros de los interfaces de red. En este caso, se modificaron los archivos "/etc/config/network" y "/etc/config/wireless" (Figuras 3-13 y 3-14, respectivamente).

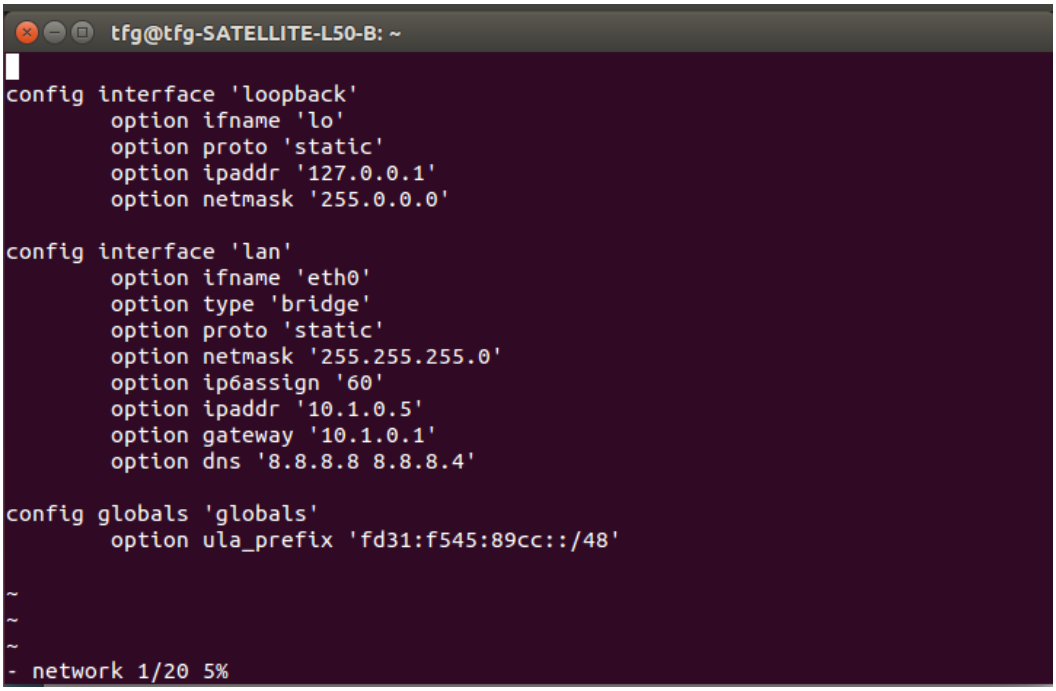


Figura 3-13 Contenido del archivo "/etc/config/network".

El interfaz *eth0* tiene asignada una IP que pertenece a la subred anunciada por el nodo OLSR con el que enlaza. De este modo, se establece la conectividad entre la "Picostation 2" y la "Bullet M2". En modo *bridge*, el encaminador encargado de direccionar el tráfico será el nodo OLSR y, por eso, la Picostation 2 solo necesita proporcionar la capacidad inalámbrica. Para indicar la ruta del tráfico desde el punto de acceso hacia el encaminador se debe indicar el *bridge* en el *eth0* de la "Picostation 2" y fijar como puerta de enlace la LAN del encaminador, que en el ejemplo será 10.1.0.1.

Figura 3-14 Contenido del archivo "/etc/config/wireless".

El interfaz debe configurarse en modo punto de acceso y hay que añadirle seguridad para evitar que terceros, como otros buques navegando en la zona, puedan acceder a la red mallada. En este caso, se usa "wpa psk2" con clave compartida. En un futuro podría llegar a configurarse "WPA Enterprise" o algún sistema equivalente, de forma que todo el personal deba acceder con usuario y clave.

Debe notarse, que dejar activado el sistema NAT hará que el punto de acceso no funcione correctamente.

3.4 Seguridad de la red

3.4.1 OLSR secure

Tal y como se explica en [18], "OLSR secure" es una extensión del protocolo de encaminamiento que utiliza la firma de paquetes, basada en claves simétricas, para aumentar la seguridad del protocolo. Lo cierto es que este sistema solo firma los mensajes de control de OLSR y no es suficiente para la seguridad del tráfico transmitido a través de la red. Este complemento implica también el intercambio de sellos temporales para evitar los ataques de reenvío de paquetes, ya que se puede detectar que en esos paquetes la diferencia de tiempos entre los nodos no coincide. La firma consiste en un *hash* elaborado mediante el algoritmo SHA-1 de la cabecera del paquete OLSR, de los mensajes presentes en el paquete, sin incluir la firma, de la cabecera, de la subcabecera, del sello temporal del mensaje de la firma y de la clave compartida.

La clave compartida se almacena en "/etc/config/olsrd_secure_key". Debe tenerse en cuenta que la clave tiene que ser igual en todos los nodos y que es importante proteger el acceso a este archivo para evitar que terceros puedan acceder a su contenido. Adicionalmente sería conveniente diseñar políticas para la actualización y difusión de claves que refuerce la seguridad del sistema.

"OLSR secure" se puede instalar con la aplicación "opkg" de Openwrt. Para simplificar el proceso en OLSR, recoge todo el tráfico de control que entra y sale y opera individualmente de forma que no afecta al funcionamiento del encaminamiento.

A pesar de la seguridad, si un atacante copiase varios mensajes de solicitud de intercambio de sellos temporales podría elaborar un ataque de denegación de servicio dirigiendo todos los mensajes a un nodo al mismo tiempo, dejándolo fuera de servicio. Sin embargo, un ataque así no sería fácil de ejecutar y solo afectaría a uno de los nodos, permitiendo que el resto de la red siguiese operativa.

3.4.2 Configuración del cifrado "WPA2 PSK" en la red MANET

Dado que la seguridad se considera primordial en este tipo de redes por su carácter militar, se estableció un cifrado adecuado para el canal de transmisión de datos. Sin embargo, esta tecnología en redes malladas se encuentra todavía en desarrollo, lo que reduce la eficiencia de las comunicaciones, por lo menos en esta versión del sistema operativo.

Tras las pruebas realizadas, se comprobó que con la versión actual del *software* los nodos no se conectaban. Sin embargo, utilizando la versión "Chaos Calmer" de OpenWRT, que se analiza más adelante, sí funcionaba pero se producían paros en las transmisiones y se optó por abandonar la implementación de este tipo de seguridad.

Por si en un futuro se mejorase la eficiencia de este cifrado en redes MANET, se expone la manera de hacerlo. En primer lugar, se debe eliminar el paquete "wpad-mini" ("opkg remove wpad-mini") e instalar el paquete "wpad" ("opkg install wpad"). A continuación, se procede a aplicar en todos los equipos OLSR la configuración de la Figura 3-15.

```
root@OpenWrt:~# uci set wireless.@wifi-iface[0].encryption=psk
root@OpenWrt:~# uci set wireless.@wifi-iface[0].key="your_password"
root@OpenWrt:~# uci commit wireless
root@OpenWrt:~# wifi
```

Figura 3-15 Configuración de "WPA2 PSK" en la red MANET OLSR.

Tras el reinicio del sistema los nodos deberían establecer conexiones entre ellos sin necesidad de realizar ninguna acción. Otra opción, si no funciona con el paquete "wpad", es instalar "hostapd" y "wpa_suplicant" y seguir los mismos pasos.

3.5 Cooperación entre proyectos

Como demostración de la interoperabilidad, se ha incluido el dron que forma parte del TFG titulado "Desarrollo de un sistema de control para UAV con capacidad ATOL en las lanchas de instrucción de la ENM" dentro de la red MANET como un nodo OLSR y con soporte para DTN. El dron lleva acoplado un punto de acceso Picostation M2 con una versión de Openwrt de arquitectura "ar71xx, Attiude Adjustment", adecuada para esa plataforma.

Además del punto de acceso, el dron lleva otros equipos instalados. Por tanto, debe hacerse una correcta distribución de IP. Lo primero que se hizo fue asignar a la interfaz LAN del punto de acceso la IP 10.6.0.1 y que anunciase a través de OLSR la red 10.6.0.0/16. De este modo, es posible acceder a los equipos del dron, como son la cámara de vídeo y la "Raspberry Pi" desde las redes internas de las Lanchas de Instrucción.

La Raspberry Pi es el ordenador que actúa como cerebro del dron. Con la integración en la red MANET (Figura 3-16) es posible enviar órdenes al mismo desde las lanchas, permitiendo distintas órdenes de manejo. Uno de los objetivos es permitir que el dron aterrice en la toldilla de las lanchas automáticamente. Por otro lado, el dron también aporta un servicio a la red, porque como nodo OLSR es capaz de facilitar los enlaces para dar conexión a Internet a los equipos de las lanchas y como nodo DTN facilita el envío de paquetes, pues al moverse a gran velocidad es capaz de transportar la información que lleva almacenada a lanchas que en ese momento no estén dentro de la cobertura del nodo que intenta enviarles un mensaje. Es decir, el dron contribuirá a aumentar el mallado de la red y, por tanto, la fortalecerá.

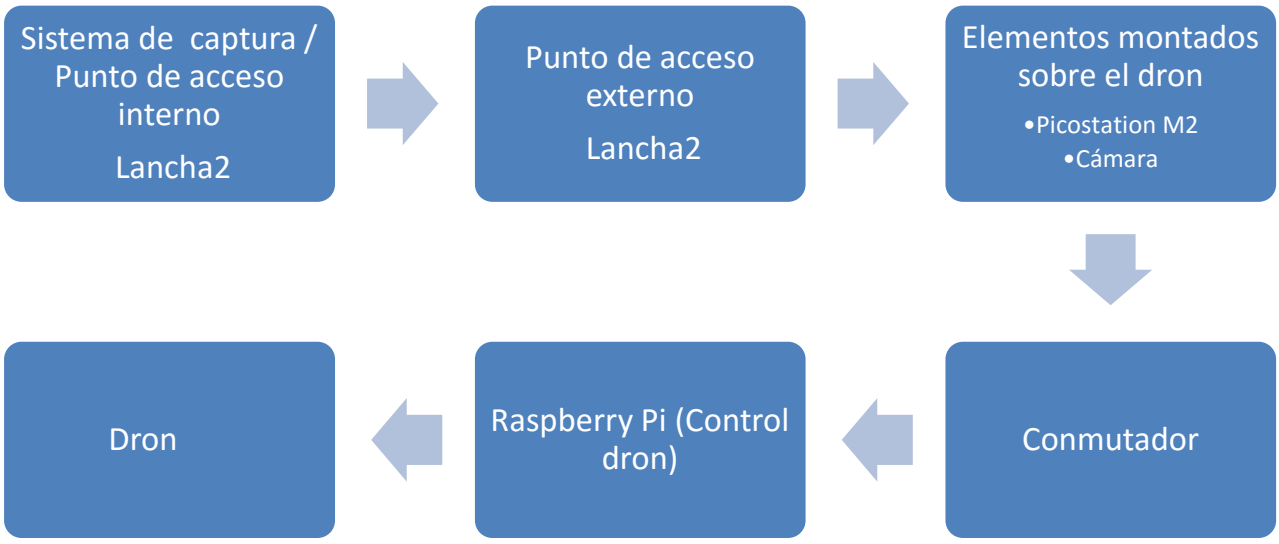


Figura 3-16 Arquitectura de la conexión del dron.

Este ejemplo de interoperabilidad es solo una pequeña demostración de todas las posibilidades que ofrece, pues una red como esta podría llegar a gestionar una gran parte de las comunicaciones internas de la escuela y vincularse con muchos otros proyectos en un futuro.

3.6 Encaminamiento del tráfico de mensajes NMEA

Con la intención de permitir la circulación del tráfico NMEA a través de la red, se ha implementado un *software* de captura en una "Raspberry Pi". Este pequeño ordenador, con una IP 10.1.200.1 y una máscara de red 255.255.0.0, se encuentra conectado al conmutador de las Lanchas de Instrucción, elemento que concentra todas las trazas NMEA del sistema y se encarga de capturar y transformar este tráfico, de naturaleza *broadcast*, y de convertirlo en *unicast*. Esto es posible gracias a la aplicación "socat" y a la configuración del *script* "socat_lanchas" que se encuentra en "/usr/bin" (Figura 3-17). No se debe olvidar iniciar el proceso en "/etc/rc.local". De este modo, el tráfico se puede analizar en tierra o utilizar en el dron.

```
#!/bin/ash

while true;
  do /usr/bin/socat UDP4-RECVFROM:10021,broadcast,range=172.31.0.0/16 UDP4-DATAGRAM:10.1.1.1:10021;
done
```

Figura 3-17 Contenido del archivo "socat_lanchas".

Los estándares NMEA definen una interfaz y un protocolo para comunicación entre instrumentos del medio marino, como pueden ser los GPS, las ECDIS y los radares. Las siglas NMEA, National Marine Electronics Association, se refieren a la entidad que gestionó la elaboración de este estándar y que lo extendió por el mundo. Distinguimos NMEA 0183 y NMEA 2000, siendo el segundo una actualización mucho más avanzada del primero. Gracias a este protocolo, es posible que un radar o cualquier otro instrumento de navegación reciba datos de otros equipos para satisfacer en mayor medida la experiencia del usuario.

3.7 Chaos Calmer

Tras poner a prueba el sistema operativo Openwrt de Attitude Adjustment y comprobar que funcionaba correctamente se decidió probar un sistema más reciente, como es el caso de la versión "Chaos Calmer" de "Openwrt".

La prueba del sistema operativo consistió en instalarlo en cuatro "Ubiquiti Bullet M2", que no habían sido utilizadas todavía. Se descargó el *software* de [12] y se instaló. A continuación se repitieron los mismos pasos que para el sistema anterior. Sin embargo, fue necesario eliminar algunos paquetes de *software* para que cupiese todo en la memoria del punto de acceso, pues "Chaos Calmer" ocupa más que el sistema anterior. Eso dificultó la configuración en algunos casos porque algunos programas como el editor de textos "nano", ya no estaban disponibles. Los paquetes que se incluyeron en la instalación se pueden ver en la Figura 3-18.

```
root@OpenWrt:~# opkg install ibrdtnd ibrdtn-tools luci pciutils luci-app-olsr lu
ci-app-olsr-services olsrd-mod-arprefresh olsrd-mod-bmf olsrd-mod-dot-draw olsrd
-mod-dyn-gw olsrd-mod-httpinfo olsrd-mod-secure olsrd-mod-txtinfo olsrd-mod-watc
hdog
```

Figura 3-18 Paquetes instalados con "opkg" en la versión "Chaos Calmer".

Una vez configurado y probado con éxito el encaminamiento OLSR se procedió a configurar la DTN. Una vez hecho, se comprobaron algunas mejoras con respecto al sistema operativo anterior. Entre ellas, se pudo comprobar que es posible configurar IBR-DTN en la interfaz *wlan0*, en vez de en

bmf0, consiguiendo así que el funcionamiento del sistema se vea mucho menos forzado, pues el interfaz *bmf0* debe estar dedicado exclusivamente a tráfico *multicast*.

3.8 Túnel VPN

Con la intención de poder operar la red desde cualquier punto remoto de forma segura, por ejemplo el CUD, se instaló un servidor de túneles VPN en el nodo en tierra de la red MANET. Para las pruebas, se utilizó como cliente un portátil con sistema operativo Ubuntu. El método empleado para elaborar el túnel se explica en el Anexo I, que a su vez está basado en la referencia [12]. Cabe señalar que la red del servidor VPN configurado en el nodo en tierra es 10.8.0.0/24.

4 VALIDACIÓN DEL FUNCIONAMIENTO DE LA RED MANET-DTN

4.1 Prueba de aplicaciones IBR-DTN en tierra

El *software* DTN instalado permite llevar a cabo una serie de acciones de envío y recepción de información, que una vez llevadas a la práctica demuestran con creces el buen funcionamiento y las enormes posibilidades del *software* instalado. Entre ellas encontramos: "dtnping", "dtnsend" y "dtnrecv", "dtnstream", "dtninbox", "dtnoutbox" y "dtntrigger". Todas ellas han sido probadas tanto en una situación básica como en una más compleja en la que se simulan fallos del sistema para comprobar que el concepto "red tolerante a fallos" se cumple.

La primera prueba que se realizó fue con la aplicación "dtnping" (Figura 4-1). La situación consistía en una conexión, a través de cable al punto de acceso "Lancha2" y una conexión a través del interfaz *wlan0* a al nodo en tierra. Primero, se inició IBR-DTN e el nodo en tierra y en "Lancha2", indicando que se emplearía el interfaz *bmf0*. El modo de hacerlo es iniciar una conexión SSH con cada dispositivo e introducir en el terminal la orden "/etc/init.d/ibrdtn start". Tras confirmar que OLSR detecta al nodo vecino y que IBR-DTN ha arrancado correctamente, se realiza una comprobación de la conexión mediante una un ping a la dirección *multicast* 224.0.0.1 y se comprueba que se están enviando y recibiendo paquetes. A continuación, en el terminal del nodo en tierra se ejecuta un "dtnping" dirigido a la "Lancha2" con el comando "dtnping dtn://Lancha2/echo", de modo que quede indicado a quien se dirige. Si no hay errores de conexión se debería recibir la respuesta al "dtnping" con un retardo de milisegundos. En ese momento, se debe acceder mediante SSH al nodo en tierra y se procede a parar IBR-DTN con el comando "/etc/init.d/ibrdtn stop". Acto seguido, se vuelve a iniciar de modo que se simula una desconexión de la DTN. Si IBR-DTN funciona correctamente, el "dtnping" que no llegó a su destino a causa de la desconexión no debería perderse y alcanzar su objetivo cuando el sistema se reinicie. Este comportamiento fue el observado en la prueba llevada a cabo.

Figura 4-1 Ejemplo de funcionamiento de "dtnping".

Las herramientas "dtnsend" y "dtnrecv" (Figura 4-2) se emplean para mandar archivos desde un nodo DTN a otro y presentar su contenido en pantalla. La prueba en la que se utilizaron consistió en crear un archivo llamado "sendFile" con la frase "IBR-DTN is great" como contenido y enviarlo. Para ello, se accede a través de una conexión SSH a las dos dispositivos y se ejecuta en "Lancha2" la orden de registrarse como receptor mediante el comando "dtnrecv --name dtnReceiver" y en el nodo en tierra la orden de enviar el archivo al receptor usando el comando "dtnsend dtn://Lancha2/dtnReceiver sendFile". Así, una vez se haya transferido el archivo aparecerá la frase "IBR-DTN is great" en el terminal de "Lancha2". Como ya se adelantó en la introducción de este apartado, se hizo lo mismo pero generando una desconexión en mitad del proceso y el resultado fue satisfactorio.

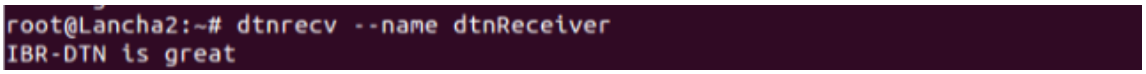


Figura 4-2 Ejemplo de funcionamiento de "dtnrecv".

Las herramientas "dtninbox" y "dtnoutbox" están pensadas para compartir archivos de forma automática. Para la prueba, se prepara el mismo enlace a los dispositivos que en el resto de pruebas y se establece la conexión SSH. Primero, se crea una carpeta de recepción en "Lancha2" con el nombre "inboxFolder" (Figura 4-3) usando el comando "mkdir". En el mismo terminal en que se crea ese directorio se ejecuta el comando "dtninbox inboxReceiver inboxFolder/". Así, se indica que en esta carpeta se reciben los mensajes del otro nodo DTN. Luego, creamos la carpeta de salida en el nodo en tierra con el nombre "outboxFolder" y mediante el comando "dtnoutbox outboxSender outboxFolder/ dtn://Lancha2/inboxReceiver" indicamos que todo lo que se guarde en esa carpeta será enviado a "Lancha2". La aplicación "dtnoutbox" (Figura 4-4) informará cuando se borre, envíe o añada un archivo. Después, se crean algunos archivos en la carpeta de salida y se comprueba que se detectan y envían automáticamente. Así mismo, se lleva a cabo una desconexión de IBR-DTN en "Lancha2" y se comprueba que los archivos se envían igualmente cuando se inicia de nuevo el sistema.

Figura 4-3 Ejemplo de funcionamiento de "dtninbox".

```
root@Sectorial:~# dtnoutbox outboxSender outboxFolder/ dtn://Lancha2/inboxReceiver
-- dtnoutbox --
file found: file1
file found: file2
files sent: file1 file2
file removed: file1
file removed: file2
file found: file1
files sent: file1
```

Figura 4-4 Ejemplo de funcionamiento de "dtnoutbox".

4.2 Despliegue provisional de la red en el entorno marítimo

Una vez comprobado el funcionamiento del *software* sobre los dispositivos escogidos, llega el momento de realizar pruebas en el entorno de trabajo final, las Lanchas de Instrucción y la Escuela Naval Militar.

Para llevar a cabo la instalación en sus correspondientes áreas fue necesario el uso de bridas y sujeciones metálicas. El nodo en tierra se instaló con bridas, entre la primera y la segunda planta, en la escalera de incendios norte del Cuartel de alumnos Almirante Francisco Moreno para cubrir la mayor parte de la ría de Pontevedra. Las antenas omnidireccionales se instalaron con las sujeciones metálicas en la escala de acceso al puente alto de las Lanchas de Instrucción porque era la zona en la que más sencilla era la instalación y, además, garantizaba una amplia cobertura. Por último, los puntos de acceso para la red interna también van situados en el puente alto porque en esa posición no se requiere aumentar la cantidad de cable Ethernet para conectarlos con las antenas omnidireccionales. Por otro lado, el hecho de estar en el puente alto permite al punto de acceso, repartir su cobertura de manera homogénea, ya que se trata de una posición bastante neutra.

En cuanto al cableado, se necesitó una gran cantidad de cable Ethernet. En concreto, ocho cables de tres metros, un cable de cuatro metros y cinco cables cortos. Los cables de tres metros se emplearon para la alimentación de los cuatro puntos de acceso de la red MANET y de los cuatro puntos de acceso de la red interna. Estos cables se extienden desde el puente alto hasta el C.I.C., Centro de Información para el Combate, de la lancha, a través de los portillos que se encuentran en el mismo. Dentro del C.I.C., hay una regleta conectada a uno de los enchufes de 220V y en ella están conectados los cables de alimentación de los dos dispositivos del puente alto. Esos cables de alimentación conectan con el adaptador PoE y este a su vez, con los cables Ethernet de alimentación de los puntos de acceso. De esta forma, los puntos de acceso de la red MANET ya tienen energía y son capaces de enlazar entre ellas mediante el protocolo de encaminamiento OLSR. Sin embargo, la red todavía no tiene acceso a Internet y los puntos de acceso de la red interna no están conectados con los de la red MANET. Para ello, es preciso conectar la toma LAN del adaptador PoE de cada punto de acceso de la red MANET con la misma toma del adaptador PoE del punto de acceso de la red interna.

Para habilitar el acceso a Internet es necesario poner a funcionar el nodo de tierra. Lo primero es asegurarse de que el interfaz *eth0* está usando DHCP para poder configurar una IP de la red de cuartel. Después se debe conectar el cable de alimentación a una toma de corriente y el otro extremo al adaptador PoE. También, a la toma LAN del adaptador se deberá enchufar el cable que a su vez enlazará con la red del cuartel. Por suerte, los estudios del cuartel ya tenían conexión con la red del Centro Universitario de la Defensa por lo que no fue necesario realizar ningún cambio para acceder a Internet. Ahora, solo faltaría proporcionar corriente al nodo en tierra conectando el cable Ethernet de cuatro metros, por un extremo, a la toma principal del dispositivo y, por otro, a la toma PoE del adaptador.

La forma de revisar que la instalación de la red ha funcionado es conectarse a uno de los puntos de acceso de las lanchas. Bastará con aproximarse a una de las ellas y buscar en cualquier dispositivo, ya sea un móvil o un ordenador, la red interna en cuestión. Llegados a este punto tendremos que ser capaces de acceder a Internet desde cualquier dispositivo.

En cualquier caso, que funcione la red OLSR no es suficiente. Para saber si IBR-DTN está operando, el primer paso es acceder mediante conexión SSH a los nodos DTN de la red. Lo siguiente es iniciar el demonio en los nodos y realizar un "dtnping" desde cada uno de ellos al resto. Si no se genera ningún error que impida el funcionamiento, querrá decir que la instalación y configuración es la apropiada

4.3 Primera prueba a bordo de las Lanchas de Instrucción

La primera prueba consistió en una comprobación de la conectividad entre nodos, tanto funcionando como nodos OLSR como utilizando la nueva capacidad de la DTN. En la prueba, que se realizó durante una de las salidas a la mar semanales, se desplegaron los siguientes dispositivos: el nodo en tierra, situado en la escalera de incendios del Cuartel Almirante Francisco Moreno, y dos puntos de acceso de la red MANET de las lanchas, uno situada en la lancha Guardiamarina Salas y otro situado en la Guardiamarina Rull.

La preparación fue muy sencilla a pesar de que todavía no se había autorizado la instalación permanente. Se emplearon regletas a modo de alargadores y se conectaron los puntos de acceso a la alimentación. La instalación comenzó a las 13:40 y finalizó a las 14:25, siendo la salida a la mar a las 14:50.

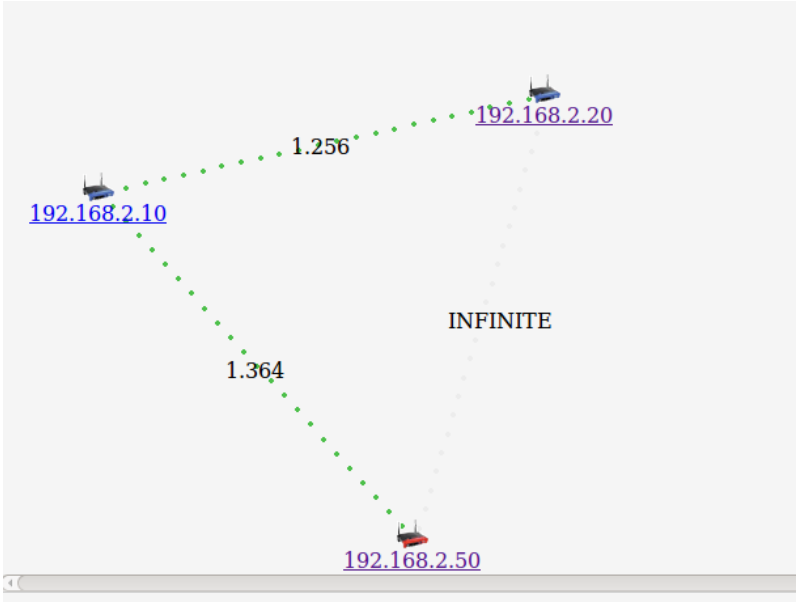


Figura 4-5 Ejemplo del estado la red MANET durante las pruebas.

Mientras comenzaba la maniobra de desatraque se hizo una prueba de conectividad y se pudo apreciar que había enlace entre los puntos de acceso de la red MANET y que el nodo en tierra aparecía como detectado pero con coste de enlace infinito porque se posicionó de forma que la prioridad fuese cubrir la zona de fuera de la ría de Pontevedra (Figura 4-5). A mayores, había edificios en el medio. A medida que nos fuimos separando del muelle Almirante Vierna, en el que estábamos atracados, comenzó a aparecer un coste de 16 en la conexión con el nodo en tierra pero al dirigirnos hacia el este se volvió a perder, pues esa zona no estaba dentro de la cobertura y ninguna otra lancha se encontraba

dentro de ella para poder retransmitir. Entre tanto, se inició IBR-DTN en todos los nodos y se enviaron "dtnping" para comprobar el funcionamiento de la DTN. Debe quedar constancia de que el resultado de las pruebas fue satisfactorio. Después, al poner rumbos de componente oeste, mejoró el coste del enlace con el nodo en tierra (Figura 4-6) y se probó con éxito el acceso a Internet. Sin embargo, a los pocos minutos de realizar las primeras pruebas, la otra lancha de la prueba se averió y no fue posible seguir contando con ella para el resto del experimento. El nodo en tierra continuó funcionando y permitiendo el acceso a Internet hasta que se desconectó por un fallo de alimentación.

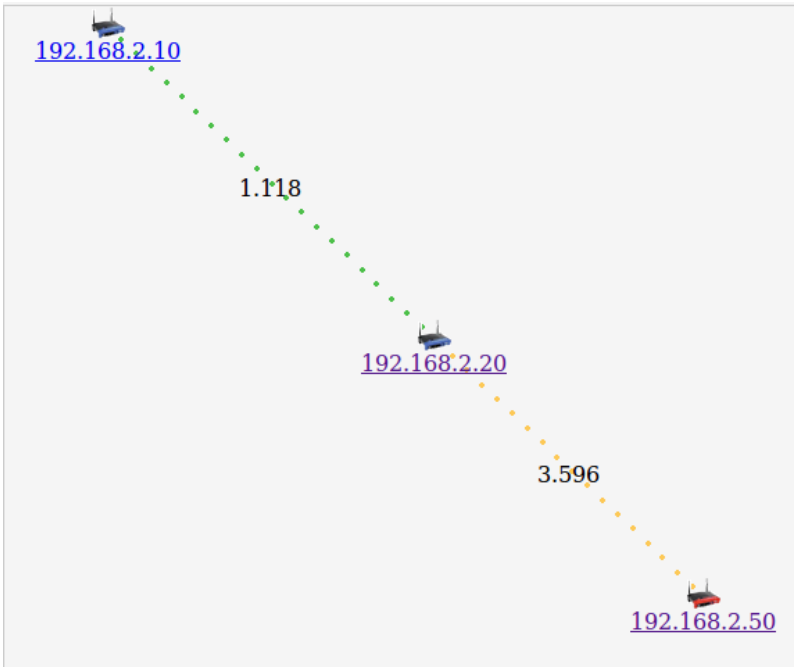


Figura 4-6 Ejemplo del estado la red MANET durante las pruebas.

El resto de la salida se aprovechó para planear la posible instalación permanente de la red y para revisión de los resultados obtenidos.

4.4 Segunda prueba a bordo de las Lanchas de Instrucción

En esta prueba estaba previsto salir a navegar de nuevo en las Lanchas de Instrucción para poder realizar las pruebas definitivas de la red. Sin embargo, debido a las condiciones meteorológicas, tuvieron que probarse los equipos estando las unidades atracadas y con solo tres de ellas disponibles, además del nodo en tierra. Debe notarse que tanto "Lancha1", como "Lancha2", como "Sectorial", tenían IBR-DTN instalado, pero "Lancha4" no.

Al iniciar la prueba se corroboró que no se detectaba el nodo en tierra y como no era posible hacer las comprobaciones sin ese nodo fue necesario acceder a la escalera de incendios del Cuartel Almirante Francisco Moreno a modificar su posición. Después, se pudo ver que ya figuraba como detectada y con un coste asequible (Figura 4-7).

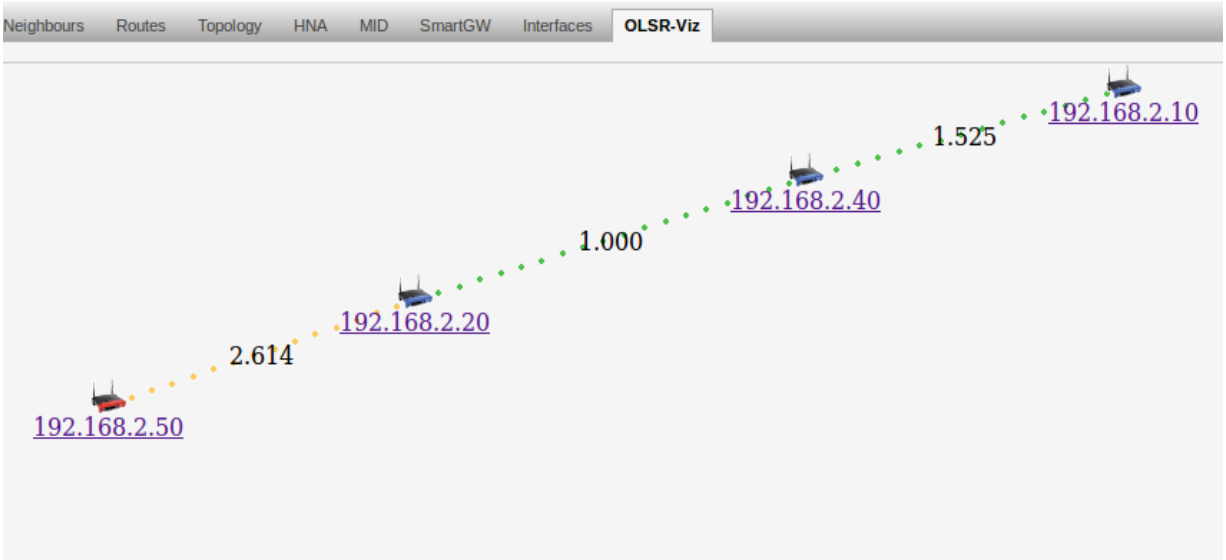


Figura 4-7 Ejemplo del estado la red MANET durante las pruebas.

A pesar de tratarse una prueba estática, sirvió para descubrir errores importantes en la configuración y corregirlos. En primer lugar, se observó que si el nodo seleccionado como referencia de tiempo no se encuentra en la red y además no hay servicio de Internet no se produce la sincronización. Entonces no es posible que los paquetes alcancen su destino sin ser rechazados. Esto implica tener que buscar un método diferente para que funcionen en todo momento porque esta red está pensada precisamente para la desconexión temporal de algunos nodos y si uno de ellos se reinicia y no tiene manera de sincronizarse, queda fuera de la red. Otro inconveniente descubierto fue la incapacidad de la red de reenviar los paquetes a nodos que no son vecinos directos y también para enviar a través de nodos no configurados con IBR-DTN.

En primer lugar, se autorizó el reenvío en el archivo de configuración del *software*, pero al comprobar que no era ese el único fallo se hicieron otras modificaciones. Lo primero que se corrigió en todos los puntos de acceso, en la archivo "/etc/sysctl.conf", fue la opción de descartar tráfico *broadcast* de control por parte del sistema operativo, que estaba bloqueado y por lo tanto no permitía el descubrimiento de nodos a dos saltos. Además, se añadieron rutas estáticas a los nodos ya conocidos. Sin embargo, algo seguía fallando, pues no era posible enviar información a través de un nodo sin IBR-DTN. Más tarde, se averiguó que este no tenía habilitado el complemento "olsr-mod-bmf" y, por tanto, no podía encaminar tráfico *multicast* para el descubrimiento de nodos (Figura 4-8).

```
root@Lancha1:~# tcpdump -i bmf0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on bmf0, link-type RAW (Raw IP), capture size 65535 bytes
19:53:35.204956 IP 192.168.2.30.4551 > 224.0.0.142.4551: UDP, length 37
19:53:39.550235 IP 192.168.2.30 > 224.0.0.22: igmp v3 report, 1 group record(s)
19:53:40.211489 IP 192.168.2.30.4551 > 224.0.0.142.4551: UDP, length 37
19:53:45.218262 IP 192.168.2.30.4551 > 224.0.0.142.4551: UDP, length 37
19:53:50.225526 IP 192.168.2.30.4551 > 224.0.0.142.4551: UDP, length 37
19:53:55.232472 IP 192.168.2.30.4551 > 224.0.0.142.4551: UDP, length 37
19:54:00.238939 IP 192.168.2.30.4551 > 224.0.0.142.4551: UDP, length 37
19:54:05.245589 IP 192.168.2.30.4551 > 224.0.0.142.4551: UDP, length 37
19:54:10.252208 IP 192.168.2.30.4551 > 224.0.0.142.4551: UDP, length 37
19:54:15.258896 IP 192.168.2.30.4551 > 224.0.0.142.4551: UDP, length 37
19:54:20.267189 IP 192.168.2.30.4551 > 224.0.0.142.4551: UDP, length 37
19:54:25.272749 IP 192.168.2.30.4551 > 224.0.0.142.4551: UDP, length 37
19:54:30.280435 IP 192.168.2.30.4551 > 224.0.0.142.4551: UDP, length 37
19:54:35.286298 IP 192.168.2.30.4551 > 224.0.0.142.4551: UDP, length 37
19:54:40.292297 IP 192.168.2.30.4551 > 224.0.0.142.4551: UDP, length 37
```

Figura 4-8 Análisis de tráfico *multicast* en el interfaz *bmf0* con la aplicación "tcpdump".

Una vez realizados todos los cambios, se generó artificialmente una situación en la que un nodo DTN transmitía un paquete a otro nodo DTN a través de un nodo que no lo era (Figura 4-9). Efectivamente, el resultado fue satisfactorio. Se utilizó el comando "traceroute" para comprobar que la información viajaba dos saltos en la capa IP y su utilizó "dtntracepath" para comprobar que la entrega era correcta (Figura 4-10). Se usó el mismo método entre tres nodos DTN y el reenvío fue satisfactorio.

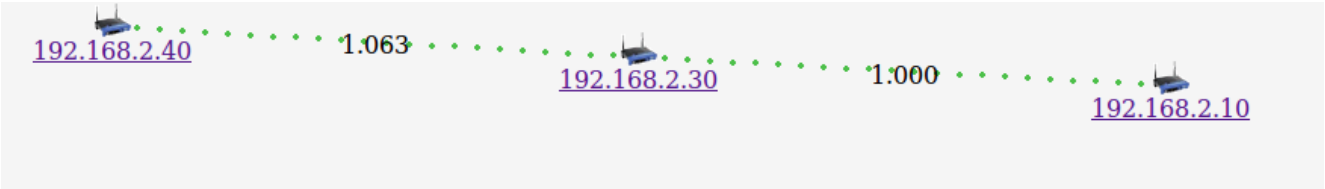


Figura 4-9 Situación de la prueba con nodo intermedio sin OLSR.

```
root@Lancha4:~# traceroute 192.168.2.10
traceroute to 192.168.2.10 (192.168.2.10), 30 hops max, 38 byte packets
 1  192.168.2.30 (192.168.2.30)  13.748 ms  9.360 ms  3.792 ms
 2  192.168.2.10 (192.168.2.10)  14.267 ms  13.332 ms  12.274 ms
root@Lancha4:~# dtntracepath dtn://Lancha1/echo
TRACE TO dtn://Lancha1/echo
   1: dtn://Lancha1/echo                                ECHO         100.72 ms
   2: dtn://Lancha1                                     delivery     127.40 ms

root@Lancha4:~#
```

Figura 4-10 Diferente forma de apreciar la ruta en la capa DTN y la capa IP.

4.5 Prueba final a bordo de las Lanchas de Instrucción

El objetivo de esta salida a la mar era confirmar el correcto funcionamiento del sistema en todos los ámbitos una vez solventados todos los errores detectados anteriormente.

Dado que una de las Lanchas de Instrucción continuaba averiada, una de los puntos de acceso no pudo formar parte de la red desplegada, con lo cual los integrantes eran "Lancha1", "Lancha2", "Lancha4" y "Sectorial". Todas ellos tenían instalado IBR-DTN y "Sectorial" era el encargado de proporcionar el acceso a Internet.

Durante la preparación para salir a la mar se comprobó el correcto funcionamiento del protocolo de encaminamiento, pudiendo observarse la adecuada conectividad de los tres nodos de las lanchas. Se realizaron "ping" y "dtnping" a un solo salto para comprobar que no se producían errores y todo se desarrolló según lo preestablecido.

Al salir a la mar se perdió la conectividad entre las unidades y eso generó un desconcierto debido a que las distancias alcanzadas debían ser muy superiores a las obtenidas. Se realizaron diversas pruebas y no se encontró el problema hasta que se descubrió que "Lancha2", la única con la que en ocasiones existía enlace, transmitía de forma adecuada pero "Lancha1" no. A raíz de los sucedido se decidió desmontar el transmisor de "Lancha1" y al hacerlo se comprobó que en su interior había una gran cantidad de humedad, incluso gotas de agua. Debido a la meteorología de los días pasados, las antenas que quedaron en las lanchas sin el transmisor acoplado habían acumulado humedad y la habían trasladado al transmisor. A continuación, se secó el interior del conector y tras comprobar los enlaces se restableció el funcionamiento habitual de la red (Figura 4-11). Con ánimo de cuidar los equipos, se hizo una limpieza de todos los conjuntos al llegar a tierra.

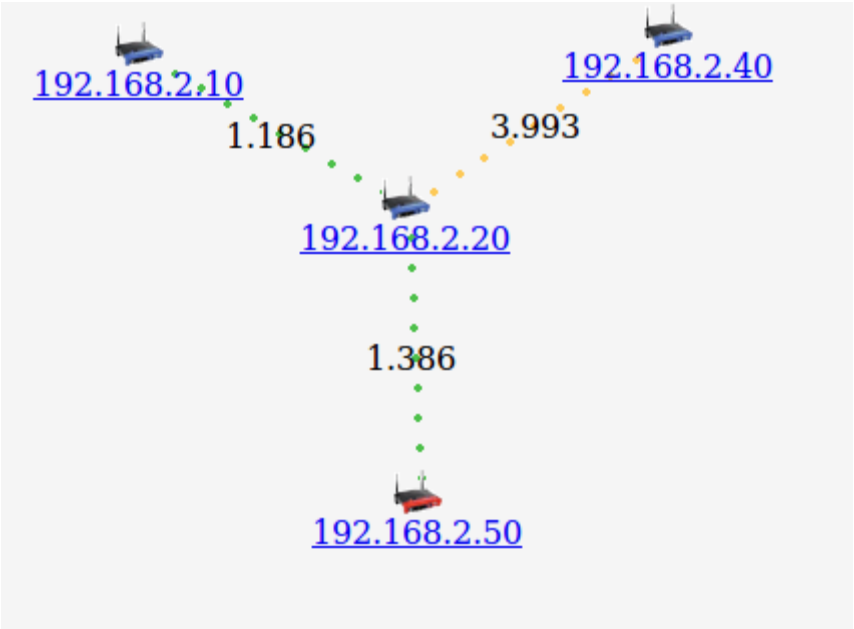


Figura 4-11 Situación tras la limpieza del transmisor en "Lancha1".

Una vez la conectividad volvió a su estado normal comenzaron las pruebas de la red. En primer lugar se realizaron "ping" y "dtnping" a nodos a un solo salto para asegurarse de que no se habían vuelto a generar complicaciones. Tras confirmar que eran efectivos se comprobó la conexión a Internet que resultó ser la deseada y se iniciaron las pruebas de la DTN (Figura 4-12).

```
root@Lancha4:~# /etc/init.d/ibrdtn start
running dtnd ... done
root@Lancha4:~#
```

Figura 4-12 Arranque del servicio DTN.

En primer lugar se realizó un "dtnping" a un nodo a dos saltos, desde "Lancha1" a "Sectorial" pasando por "Lancha2" y no se produjeron errores. Después, con la misma topología, se efectuó el mismo "dtnping" pero habiendo detenido previamente el servicio DTN de "Sectorial" y de "Lancha2", con un tiempo de vida de 30000 segundos. Lógicamente, en los primeros instantes, "Sectorial" no recibió los datos, así que se arrancó IBR-DTN en "Lancha2". Si la capa de paquete funciona correctamente, en ese instante "Lancha2" debería recibir la información y en el momento en que estuviese disponible "Sectorial", es decir, al arrancar el demonio tendría que enviársela. De hecho, así fue, al arrancar el sistema en "Sectorial" se recibió en "Lancha1" el asentimiento del primer paquete (Figura 4-13).

```
root@Lancha1:~# dtnping --lifetime 30000 dtn://Sectorial/echo
ECHO dtn://Sectorial/echo 64 bytes of data.
64 bytes from dtn://Sectorial/echo: seq=1 ttl=30000 time=13.72 s
64 bytes from dtn://Sectorial/echo: seq=2 ttl=30000 time=72.96 ms
64 bytes from dtn://Sectorial/echo: seq=3 ttl=30000 time=70.44 ms
64 bytes from dtn://Sectorial/echo: seq=4 ttl=30000 time=74.19 ms
```

Figura 4-13 Arranque del servicio DTN.

Por último, se aprovechó para probar la herramienta DTN que faltaba por poner a prueba, "dtnstream". Esta herramienta se puede utilizar para enviar datos tales como las trazas NMEA que generan los equipos de las Lanchas de Instrucción. En este caso se decidió enviar una página web aprovechando el servicio de Internet que proporcionaba la sectorial. Para ello se inició un receptor de datos con el comando "dtnstream -s streamReceiver" y un emisor con "wget -O - http://www.google.es | dtnstream -d dtn://Lancha1/streamReceiver -s streamSource" (se usó la página http://www.google.es como fuente de datos). Efectivamente, los datos de la página fueron transmitidos de un dispositivo al otro.

Con todo ello, quedó demostrado el buen funcionamiento de la red y las múltiples posibilidades que brinda a las unidades.

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones

Después de realizar todas las pruebas, si algo se ha podido apreciar es la funcionalidad del sistema y la gran cantidad de posibilidades que aporta a cualquier usuario. La red desplegada abre una nueva etapa para el adiestramiento de los alumnos a bordo de las Lanchas de Instrucción de la Escuela Naval Militar, que desde ahora podrán disfrutar de nuevas formas de desarrollar su trabajo a bordo. Algunas funciones como el *chat* o el sistema automático de compartición de archivos permitirán llevar a cabo ejercicios más complejos y aproximar mucho más al alumno a lo que encontrará más adelante en las unidades de la Armada.

Este proyecto ha conseguido alcanzar los objetivos previstos en la fase inicial y ha podido adelantar nuevos aspectos para el futuro. De forma más concreta, podemos decir que se ha conseguido probar con éxito el funcionamiento de la red y de sus herramientas, destacando la efectividad y utilidad del almacenamiento persistente de la capa DTN y el servicio de acceso a Internet. También, que se ha podido dar seguridad al sistema y se han dado grandes pasos en la instalación permanente de todo el conjunto, en colaboración con el Núcleo de Lanchas de la Escuela Naval Militar.

5.2 Líneas futuras

Si por algo se caracteriza este tipo de proyecto es por no tener un final. Las posibilidades de investigación y desarrollo de este tipo de red entre las Lanchas de Instrucción y la Escuela Naval Militar son muy variadas. Bien implementadas, pueden servir de gran ayuda al adiestramiento de las damas y caballeros alumnos, así como a sus profesores e instructores. Este trabajo ha sentado las bases de una línea futura muy amplia que puede ser continuada desde muchos puntos de vista

Se sabe que para un barco de guerra su sistema de combate es el elemento principal. Esta red permitiría mediante el desarrollo de pequeños programas, la creación de un sistema similar entre las Lanchas de Instrucción. Esto incluiría el empleo de trazas NMEA, que ya se ha gestionado en este proyecto, y su presentación por pantalla, un *chat* como el actual, con comandos “dtnsend” y “dtnrecv”, pero con un formato más amigable de cara al usuario, un sistema de intercambio de información como el que proporcionan los comandos actuales pero con un entorno gráfico y todas las opciones que nos permita el almacenamiento de nuestros dispositivos.

Otra mejora importante para implantar nuevas funcionalidades sería añadir memoria a los dispositivos porque con los paquetes instalados, el espacio disponible se ha visto reducido al mínimo. La solución es añadir una memoria externa, de forma que en el almacenamiento propio de los puntos de acceso solo queden instalados los paquetes básicos de funcionamiento. La memoria estaría

protegida de los agentes meteorológicos, pues la instalación definitiva permite que los equipos sensibles queden en el interior de la lancha. Una opción que ya se ha valorado para poder aumentar el espacio es establecer una configuración en modo *puente* entre el punto de acceso de la red MANET y la "Raspberry Pi" usada para capturar el tráfico NMEA, de forma que sea esta la encargada de almacenar todo los que no sean paquetes básicos.

Otra de las ambiciones futuras de este proyecto es la elaboración de un túnel de tráfico nativo a través de la red DTN, de modo que algunos tipos de información como pueden ser los correos electrónicos o cualquier tráfico prioritario, alcancen su destino a través de la DTN a pesar de que el encaminamiento normal haya dejado de funcionar. Esta tecnología está documentada en [16], sin embargo se encuentra en desarrollo y tiene algunos fallos por lo que habrá que esperar para poder instalarla.

Para aumentar la capacidad de la red, sería muy positivo instalar nodos de tierra en la zona de la dársena para que la cobertura de la ría de Pontevedra sea total. Así, los nodos tendrían servicio de Internet en todo momento, pues, actualmente, dada la posición del nodo de tierra, el enlace en la dársena no suele producirse, o por lo menos no con la calidad suficiente. Al proporcionar varias puertas de acceso habría que configurar el servicio "Smart Gateway" para que los nodos sean capaces de seleccionar la ruta que proporcione un mejor servicio.

Con la intención de facilitar la integración de dispositivos de la última generación de *Bluetooth* en la red, sería interesante migrar toda la red a IPv6. De esta forma, podrían añadirse con facilidad diversos tipos de sensores.

Por último, debido a que la seguridad en redes malladas todavía tiene evolucionar, no fue posible dar un nivel de seguridad tan completo a la red como el que se pretendía. Por tanto, sería beneficioso que a medida que la tecnología avance, los proyectos que se vayan sucediendo en relación a este tema actualicen esta capacidad en toda la red y en cada una de sus capas.

6 BIBLIOGRAFÍA

[1] N. W. Group, «Delay-Tolerant Networking Architecture,» Abril 2007. [En línea]. Available: https://tools.ietf.org/html/rfc4838. [Último acceso: 7 Enero 2016].

[2] D. E. Garcia, «Glosarioit,» 2003. [En línea]. Available: www.glosarioit.com. [Último acceso: 8 Enero 2016].

[3] D. T. N. R. Group, «Bundle Protocol Specification,» Diciembre 2006. [En línea]. Available: https://tools.ietf.org/html/draft-irtf-dtnrg-bundle-spec-08. [Último acceso: 25 Enero 2016].

[4] I. R. T. Force, «Bundle Security Protocol Specification,» Mayo 2011. [En línea]. Available: https://tools.ietf.org/html/rfc6257. [Último acceso: 1 Febrero 2016].

[5] M. M. López, «Despliegue de una red MANET entre lanchas de instrucción,» Pontevedra, 2015.

[6] K. Costello, «Página oficial de la NASA,» NASA, 5 Agosto 2015. [En línea]. Available: http://www.nasa.gov/mission_pages/station/research/experiments/730.html. [Último acceso: 25 Enero 2016].

[7] B. Dunbar, «Página oficial de la NASA,» NASA, 12 Abril 2008. [En línea]. Available: http://www.nasa.gov/centers/marshall/news/background/facts/cgba.html. [Último acceso: 15 Enero 2016].

[8] N. W. Group, «DTN IP Neighbor Discovery (IPND),» 8 Noviembre 2012. [En línea]. Available: https://tools.ietf.org/html/draft-irtf-dtnrg-ipnd-02. [Último acceso: 8 Febrero 2016].

[9] U. Networks, «]NanoStationM & NanoStationlocoM Datasheet - Ubiquiti,» [En línea]. Available: https://dl.ubnt.com/datasheets/nanostationm/nsm_ds_web.pdf. [Último acceso: 2 Febrero 2016].

[10] U. Networks, «Data Sheet - Ubiquiti Networks,» [En línea]. Available: dl.ubnt.com/bm2hp_datasheet.pdf. [Último acceso: 2 Febrero 2016].

[11] U. Networks, «PicoStation2hp,» [En línea]. Available: https://dl.ubnt.com/pico2hp_ds.pdf. [Último acceso: 2 Febrero 2016].

[12] «Página web de Openwrt,» [En línea]. Available: www.openwrt.org. [Último acceso: 27

Diciembre 2015].

[13] A. Tønnesen., «Sitio web del protocolo OLSR,» [En línea]. Available: http://www.olsr.org/mediawiki/index.php/Main_Page. [Último acceso: 6 Enero 2016].

[14] M. I. o. Tecnology, «Red Hat Enterprise Linux 4: Manual de referencia,» Red Hat, Inc, 2005. [En línea]. Available: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html. [Último acceso: 20 Enero 2016].

[15] N. W. Group, «Internet Control Message Protocol,» Networking Work Group, Septiembre 1981. [En línea]. Available: https://tools.ietf.org/html/rfc792. [Último acceso: 2016 Enero 6].

[16] J. Morgenroth, «IBR-DTN,» Technische Universtiät Braunchsweig, 20 Julio 2013. [En línea]. Available: https://trac.ibr.cs.tu-bs.de/project-cm-2012-ibrdtn. [Último acceso: 2 Febrero 2016].

[17] D. R. Group, «Probabilistic Routing Protocol for Intermittently Connected Networks,» Internet Engeneering Task Force, 23 Noviembre 2012. [En línea]. Available: https://tools.ietf.org/html/draft-irtf-dtnrg-prophet-10#section-2.1. [Último acceso: 2 Febrero 2016].

[18] A. T. R. B. R. J. A. a. Ø. K. Andreas Hafslund, «Secure Extension to the OLSR protocol,» 2004. [En línea]. Available: www.olsr.org/docs/solsr_paper.pdf. [Último acceso: 11 Febrero 2016].

[19] D. J. W. A. S. Tanenbaum, Redes de Computadoras, México: Pearson, 2012.

[20] D. T. N. R. Group, «Delay Tolerant Networking TCP Convergence Layer Protocol,» 3 Noviembre 2008. [En línea]. Available: http://tools.ietf.org/html/draft-irtf-dtnrg-tcp-clayer-02. [Último acceso: 15 Febrero 2016].

[21] D. T. N. R. Group, «UDP Convergence Layers for the DTN Bundle and LTP Protocols,» 19 Noviembre 2008. [En línea]. Available: http://tools.ietf.org/html/draft-irtf-dtnrg-udp-clayer-00. [Último acceso: 14 Febrero 2016].

[22] K. Betke, «The NMEA 0183 Protocol,» Mayo 2000. [En línea]. Available: www.tronico.fi/OH6NT/docs/NMEA0183.pdf. [Último acceso: 29 Febrero 2016].

ANEXO I: TÚNEL VPN

El primer paso será instalar OpenVPN y el gestor de claves RSA en "Sectorial". Para ello, se actualiza "opkg" y se instalan los paquetes. A continuación, tal y como se indica en el la Figura A1-1, se construyen los certificados y claves.

```
build-ca
build-dh
build-key-server my-server
build-key-pkcs12 my-client
```

Figura A1-1 Elaboración de certificados y claves.

Las claves no tienen ningún tipo de utilidad si no se comparten con el cliente. Por eso, tendremos que enviarle los certificados y claves indicados en Figura A1-2. Además, será necesario copiar los archivos que se ven en la Figura A1-2 a la carpeta "/etc/openvpn". Puede que nuestro cliente no nos permita copiar en la carpeta "/etc/openvpn" por lo que habrá que enviarlos a otra y más adelante, con permisos de administrador, moverlos a esta.

```
cp /etc/easy-rsa/keys/ca.crt /etc/easy-rsa/keys/my-server.* /etc/easy-rsa/keys/dh2048.pem /etc/openvpn
scp /etc/easy-rsa/keys/ca.crt /etc/easy-rsa/keys/my-client.* root@CLIENT_IP_ADDRESS:/etc/openvpn
```

Figura A1-2 Certificados y claves compartidos.

En la Figura A1-3 se indica cómo se deber configurar la VPN dentro de las redes de nuestro dispositivo.

```
uci set network.vpn0=interface
uci set network.vpn0.ifname=tun0
uci set network.vpn0.proto=none
uci set network.vpn0.auto=1
```

Figura A1-3 Configuración de la red.

En la Figura A1-4 se indica como configurar el cortafuegos y en la Figura A1-5 cómo configurar las zonas del mismo. En la Figura A1-6 se indica cómo aplicar los cambios

```
uci add firewall rule
uci set firewall.@rule[-1].name=Allow-OpenVPN-Inbound
uci set firewall.@rule[-1].target=ACCEPT
uci set firewall.@rule[-1].src=*
uci set firewall.@rule[-1].proto=udp
uci set firewall.@rule[-1].dest_port=1194
```

Figura A1-4 Configuración del cortafuegos.

```
uci add firewall zone
uci set firewall.@zone[-1].name=vpn
uci set firewall.@zone[-1].input=ACCEPT
uci set firewall.@zone[-1].forward=ACCEPT
uci set firewall.@zone[-1].output=ACCEPT
uci set firewall.@zone[-1].network=vpn0
uci add firewall forwarding
uci set firewall.@forwarding[-1].src='vpn'
uci set firewall.@forwarding[-1].dest='wan'
```

Figura A1-5 Configuración de las zonas del cortafuegos.

```
uci commit network
/etc/init.d/network reload
uci commit firewall
/etc/init.d/firewall reload
```

Figura A1-6 Puesta en marcha de la nueva configuración.

Para terminar la configuración del servidor, solo queda modificar el archivo de configuración de OpenVPN (Figura A1-7). En él, se indican datos esenciales como son las rutas de los certificados, la red del servidor y el puerto que se usará para establecer la conexión. Debe notarse que en el túnel llevado a cabo en este proyecto, el archivo "dh2048.pem" recibió el nombre "dh1024.pem" debido a la diferente longitud del cifrado.

```
echo > /etc/config/openvpn # clear the openvpn uci config
uci set openvpn.myvpn=openvpn
uci set openvpn.myvpn.enabled=1
uci set openvpn.myvpn.verb=3
uci set openvpn.myvpn.port=1194
uci set openvpn.myvpn.proto=udp
uci set openvpn.myvpn.dev=tun
uci set openvpn.myvpn.server='10.8.0.0 255.255.255.0'
uci set openvpn.myvpn.ca=/etc/openvpn/ca.crt
uci set openvpn.myvpn.cert=/etc/openvpn/my-server.crt
uci set openvpn.myvpn.key=/etc/openvpn/my-server.key
uci set openvpn.myvpn.dh=/etc/openvpn/dh2048.pem
uci commit openvpn
/etc/init.d/openvpn enable
/etc/init.d/openvpn start
```

Figura A1-7 Configuración de OpenVPN.

Después, se procede a configurar el cliente. Lo primero será asegurarse de que en la carpeta "/etc/openvpn" del mismo se encuentran todos los archivos. A continuación, se indicará la puerta de

enlace con el servidor, que será la IP usada por el interfaz *eth0* del punto de acceso, junto con el resto de información que se detalla en la Figura A1-8.

```
dev tun
proto udp

log openvpn.log
verb 3

ca /etc/openvpn/ca.crt
cert /etc/openvpn/my-client.crt
key /etc/openvpn/my-client.key

client
remote-cert-tls server
remote SERVER_IP_ADDRESS 1194
```

Figura A1-8 Configuración de cliente OpenVPN.

Por último, se introducirá en el terminal el comando “openvpn --config conf.ovpn” y quedará iniciada la conexión.

ANEXO II: INSTALACIÓN PERMANENTE

Uno de los objetivos de este proyecto era la instalación permanente de la red en las Lanchas de Instrucción (Figura A2-1). Así, se deja constancia en este anexo de los avances conseguidos.

En primer lugar y lo más importante de todo es que la instalación permanente está autorizada y en proceso. Se ha decidido el lugar de la instalación y la forma en que se hará. Además, las estructuras que soportarán los puntos de acceso ya han sido encargadas al taller mecánico para su instalación.

Las bases consisten en un tubo hueco y curvado que conduce el cableado hacia el interior de la lancha. Además, cuenta con una placa soldada con cuatro agujeros para atornillar la Ubiquiti Bullet M2. Por otro lado, el anclaje a la superestructura también es atornillado e implica taladrar el techo de la lancha para pasar el cable.

Figura A2-1 Arquitectura de la red.

Los puntos de acceso de la MANET se situarán encima de la superestructura del puente en la banda de estribor (Figuras A2-2 y A2-3).

Figura A2-2 Posición futura de la antena.

Figura A2-3 Posición futura de la antena.

El cableado se conducirá a través de la base solicitada al taller y del techo técnico de las lanchas, descendiendo hasta la zona de equipos de estribor de los buques (Figura A2-4).

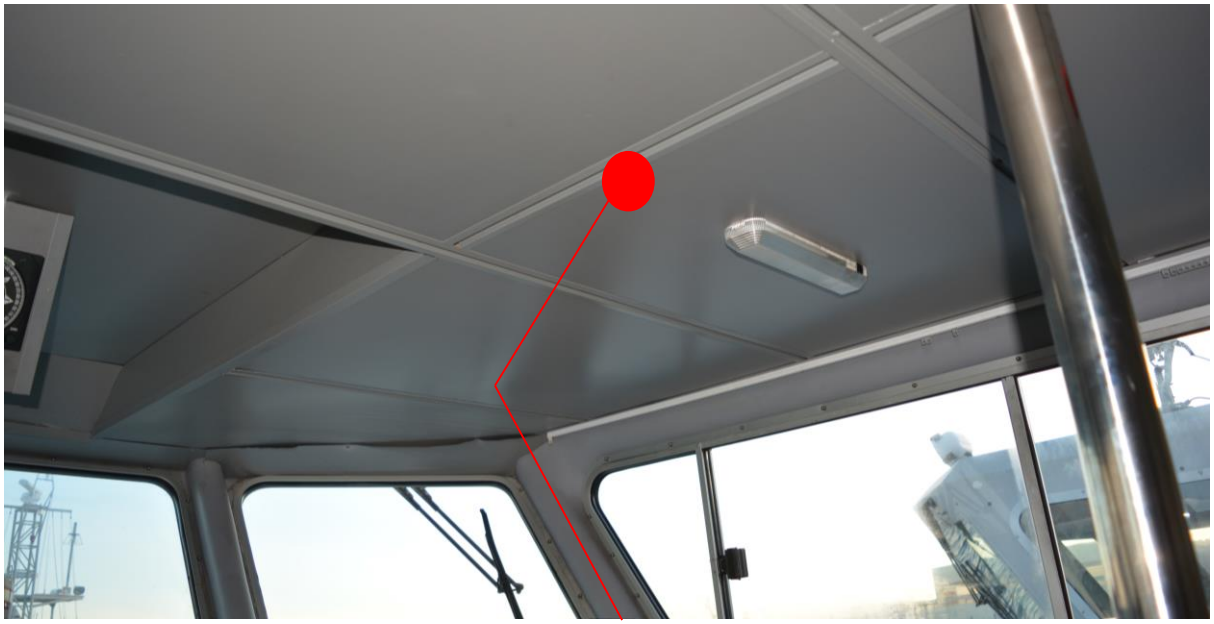


Figura A2-4 Posible disposición del cableado.

En el armario de madera (Figuras A2-5 y A2-6), que se encuentra bajo las consolas, es donde se colocarán los equipos sensibles como las “Picostation 2”, una “Raspberry Pi” para capturar el tráfico NMEA, un conmutador Ethernet, los adaptadores PoE de los puntos de acceso y una regleta de enchufes.

Figura A2-5 Armario de cableado.

Figura A2-6 Armario de cableado.

Figura A2-7 Concentrador de trazas.

El concentrador de trazas (Figura A2-7) se encuentra dentro del armario de cableado y es el elemento en el que se junta la información procedente de los instrumentos de navegación. Es ahí donde

habrá que conectar la Raspberry Pi para poder capturar el tráfico cuando se haga la instalación permanente.

ANEXO III: ARQUITECTURA DE LA RED

En la Figura A3-1 se esquematiza la arquitectura de la red desplegada.

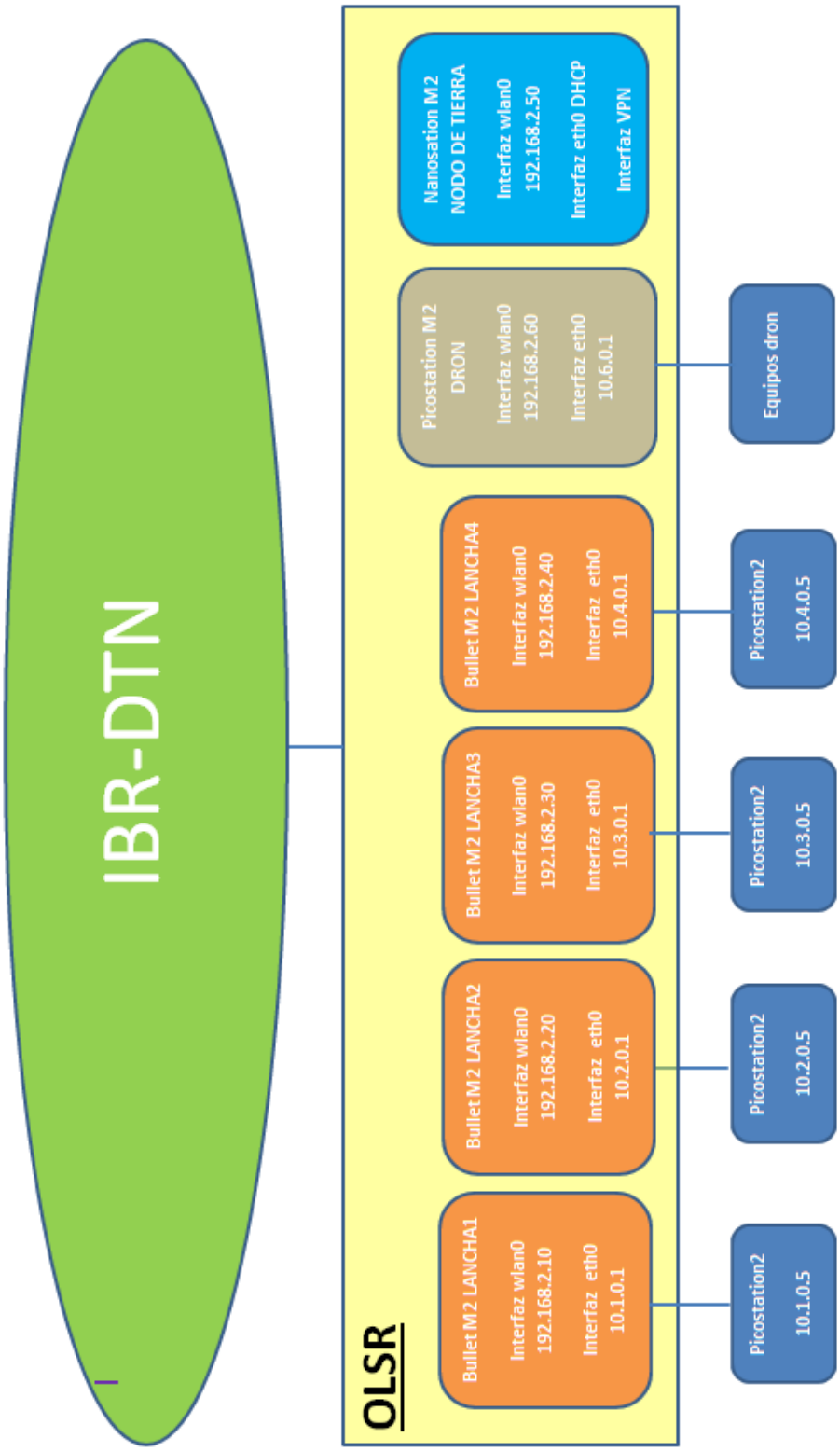


Figura A3-1 Arquitectura de la red.

ANEXO IV: RED DE INSTRUMENTOS DE LAS LANCHAS DE INSTRUCCIÓN

En la Figura A4-1 se presenta el esquema de los equipos de las Lanchas de Instrucción que se utilizó para decidir dónde instalar la Raspberry Pi que captura las trazas NMEA.

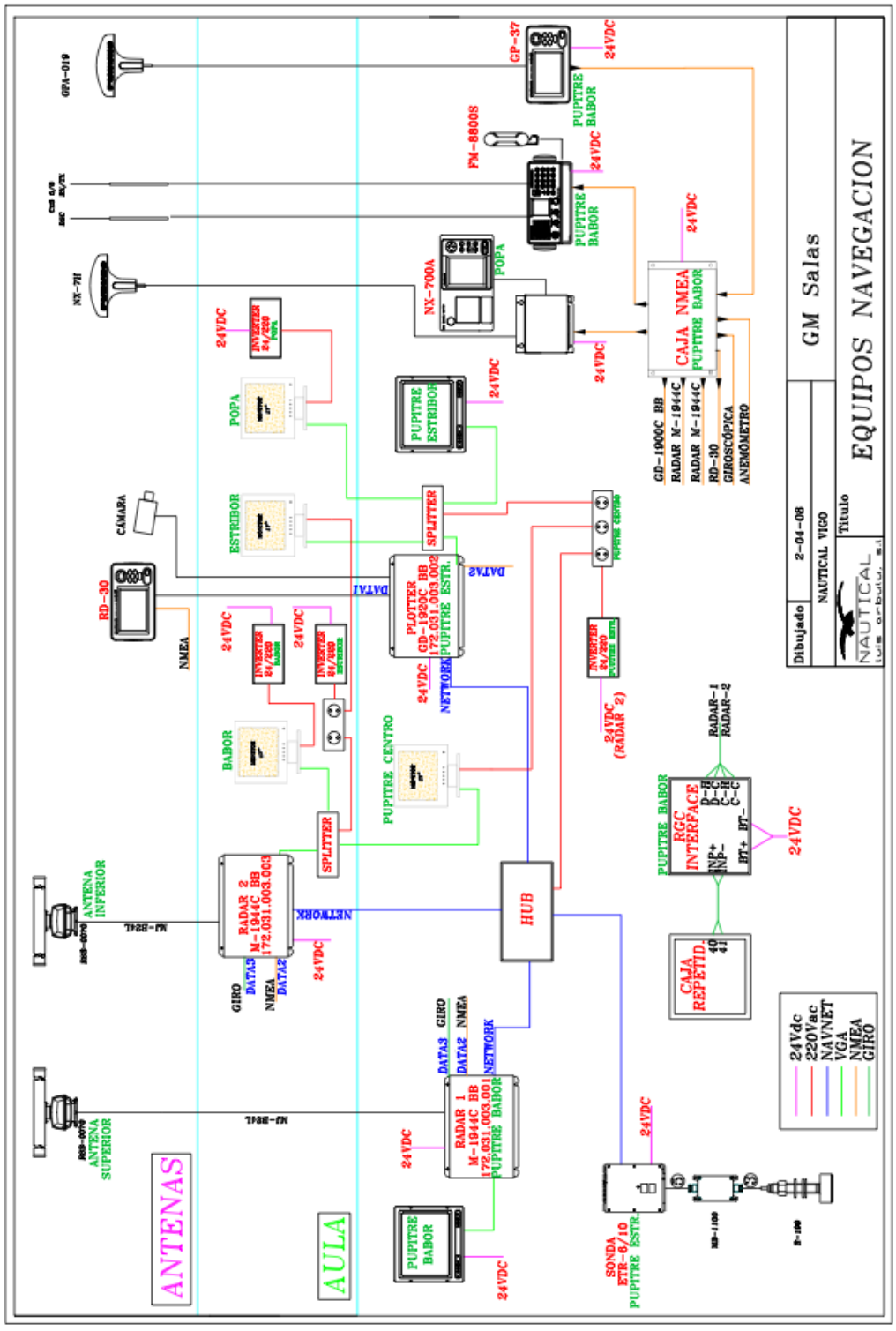


Figura A4-1 Red de instrumentos de las Lanchas de Instrucción.