ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

EVALUACIÓN DEL DESEMPEÑO DE LA HERRAMIENTA ns-3 EN AMBIENTES INALÁMBRICOS BAJO EL ESTÁNDAR IEEE 802.11

RICARDO JAVIER MORENO CADENA

SANGOLQUÍ – ECUADOR

2012

CERTIFICACIÓN

Certificamos que el presente proyecto de grado denominado: “EVALUACIÓN DEL DESEMPEÑO DE LA HERRAMIENTA ns-3 EN AMBIENTES INALÁMBRICOS BAJO EL ESTÁNDAR IEEE 802.11”, ha sido desarrollado en su totalidad por el señor RICARDO JAVIER MORENO CADENA y ha sido orientada bajo nuestra dirección.

Atentamente,

Ing. Román Lara C.	Ing. Gonzalo Olmedo C.
DIRECTOR	CODIRECTOR

RESUMEN

En el presente documento se realiza una explicación sobre el estándar IEEE 802.11 sobre el cuál el siguiente proyecto de investigación será elaborado. Se menciona también una comparación respecto a un simulador similar al utilizado, *Network Simulator ns-2*, esta comparación permitirá tomar parámetros específicos para analizar el desempeño del simulador propuesto, *ns-3*, para su estudio bajo ambientes inalámbricos mediante la realización de simulaciones en varios ambientes de simulación. Por último se realizará un análisis de los principales parámetros de desempeño de la herramienta *ns-3*, lo cual permitirá obtener un amplio análisis que llevará a obtener las conclusiones y recomendaciones obtenidas después de realizar el presente proyecto de investigación.

DEDICATORIA

El presente proyecto lo dedico con todo cariño y amor a toda mi familia, en especial a mis padres, Maribel y Jorge, así como a mis hermanos Estefy y David, los amo a todos y que siempre estuvieron apoyándome desde que puse mi primer pie en la universidad hasta ahora que estoy dando mi último paso en esta prestigiosa institución, superando varios obstáculos pero al final logrando el objetivo que fue culminar este proyecto.

A mis abuelitos, Mami Bachi y Papi Jorge, Victorita y Panchito, quienes con sus consejos y apoyo me ayudaron, para poder lograr este tan anhelado objetivo que era terminar mi proyecto de tesis y llegar a ser un profesional.

A esa persona tan especial, Kary, que también me apoyó desde antes de iniciar este proyecto, dándome aliento y apoyo para lograr terminar el mismo. Te Amo mi amorcito.

A todos mis amigos, a quienes a muchos los tengo desde que estudiamos juntos en el colegio y que ahora continúan apoyándome en todo.

AGRADECIMIENTO

Agradezco ante todo a Dios, por haberme dado la vida. A mis padres por haberme apoyado durante todo este largo camino dándome la educación necesaria llena de conocimiento y valores para poder llegar a ser la persona que ahora soy, logrando guiarme por el camino correcto para saber como afrontar los duros momentos que nos puede presentar la vida y cómo sobrellevarlos para poder siempre salir adelante.

A mis hermanos con quiénes he compartido todo este tiempo, pasando gratos momentos durante la realización de este proyecto, gracias por su apoyo, comprensión y ánimos. Los quiero mucho.

A mis profesores que durante todo mi paso por la universidad me impartieron todas sus enseñanzas las cuales fueron aprovechadas durante la realización de este proyecto. En especial al Ingeniero Román Lara y al Ingeniero Gonzalo Olmedo quienes en principio fueron mis profesores y después supieron guiarme durante la realización de este proyecto.

En general, a todos mis familiares y amigos que siempre se preocuparon por llenar sus expectativas como estudiante y ahora como profesional.

PRÓLOGO

Las Redes de Nueva Generación han desarrollado nuevas tecnologías que se han implementado en estos últimos años a nivel mundial, en el Ecuador son pocas las tecnologías de Nueva Generación que se utilizan y se aprenden a desarrollar en las aulas de los centros de investigación y centros académicos. Es por eso que se han desarrollado herramientas de simulación para dichas tecnologías y topologías de redes de nueva generación, entre estas herramientas se encuentra el Simulador de Redes *ns-3*.

El simulador de redes *ns-3* posee importantes características aplicativas a nivel educacional, profesional y en el campo de la Investigación. El uso de programas de simulación, ha despertado el interés de muchos investigadores profesionales y estudiantes que se han involucrado con nuevas herramientas para desarrollar nuevos estudios, esto pasa con el simulador *ns-3*, es un software de muy poca difusión y poco conocido en nuestro medio, por lo que es importante dentro de los procesos de investigación de nuevos simuladores de redes el desarrollar e innovar técnicas de simulación con diversas redes a tratar.

La investigación y el desarrollo de ésta herramienta ha estimulado la realización del presente trabajo de tesis, la cual se ha introducido en la manipulación del software de manera detallada y específica. Siendo una herramienta muy práctica en el campo de la educación e investigación.

ÍNDICE DE CONTENIDOS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO

STA.- (*Station*) Estación inalámbrica fija o móvil, elemento indispensable para la formación de topologías inalámbricas.

MPDU.- (*MAC Protocol Data Unit*). Consiste en un número variable de bits transmitidos a la velocidad indicada en el sub-campo *Signal*.

MSDU.- (*MAC Service Data Unit*) Es el servicio de unidad de datos que recibe desde el control de enlace lógico una pila de protocolos para guardarlos dentro de la DLL.

SA/TA.- (*Source Address / Transmitter Address*) Direcciones Lógicas de los dispositivos inalámbricos tanto del dispositivo fuente como del dispositivo destino.

AP.- (*Access Point*) También conocido como un punto de acceso. Es un dispositivo utilizado en redes inalámbricas de área local (WLAN - Wireless Local Area Network), El *Access Point* es responsable dentro de una red inalámbrica de crear una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando esté configurado y tenga los permisos necesarios.

RA.- (*Receiver Address*) Direccionamiento lógico de un dispositivo de recibe información.

BSSID.- (*Basic Service Set Identifier*) Dirección única que identifica al Router/AP que crea la red Wireless.

LLC.- (*Logical Link Control*) Control de enlace lógico, que define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores.

PDU.- (*Protocol Data Unit*) Unidades de datos de protocolo, utilizadas para el intercambio entre unidades disparejas, dentro de una capa del Modelo OSI.

FCS.- (*Frame Control Sequence*) Campo de la trama IEEE 802.11 utilizado para verificar si la transmisión se ha llevado a cabo correctamente, es decir, los bits que recibe el receptor no se han alterado respecto a los enviados por el emisor.

ESSID.- (*Extended Service Set Identifier*): Nombre único de hasta 32 caracteres para identificar a la red Wireless. Todos los componentes de la misma red WLAN deben usar el mismo.

SSID.- (*Service Set Identifier*): Es un nombre incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres que la mayoría de las veces son alfanuméricos (aunque el estándar no lo especifica, así que puede consistir en cualquier carácter). Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

CAPÍTULO 1

INTRODUCCIÓN

1.1 ANTECEDENTES

El *Network Simulator ns-3* es un simulador nuevo, que maneja ciertas similitudes a su antecesor, el *ns-2*, sin sustituirlo, ambos manejan aplicaciones similares trabajando con los protocolos de comunicación más utilizados a nivel de redes inalámbricas y cableadas además son de distribución masiva al ser totalmente gratuitos, no son compatibles entre ellos y su método de programación es distinta, el *ns-3* maneja una programación basada en C++ y también se lo puede hacer utilizando lenguaje Python [1], a diferencia del ns-2 que maneja una programación propia para ficheros tipo OTcl.

Network Simulator en su versión 2 permite realizar simulaciones de varios tipos de redes, cableadas, inalámbricas, satelitales, etc., pero debido a su tipo de programación y el desarrollo de nuevos simuladores su utilización se ha reducido considerablemente especialmente en el área de la investigación y desarrollo de nuevos módulos para redes mencionadas anteriormente. El simulador *ns-3* pretende ampliar su estudio en estas áreas para mejorar implementaciones reales en base a la simulación más cercana a resultados reales.

La Escuela Politécnica del Ejército, ha desarrollado proyectos de investigación bajo el simulador ns-2 en el área de las comunicaciones inalámbricas bajo el estándar IEEE 802.11, redes AD-HOC, comunicaciones cableadas bajo protocolos TCP, UDP, entre otros. Tomando en cuenta estos estudios, el presente proyecto pretende presentar análisis similares a los ya

realizados tomando en cuenta las nuevas herramientas que presenta el simulador ns-3.

1.2 OBJETIVO

El objetivo del presente proyecto es evaluar el desempeño de la herramienta de simulación *ns-3* en ambientes inalámbricos bajo el estándar IEEE 802.11, tomando en cuenta estudios previos de los estándares para elegir el ideal durante la realización del proyecto, con el fin de conocer su funcionamiento y comportamiento durante la implementación de las redes utilizando el simulador.

También se busca realizar la implementación de las mejores topologías con el fin de obtener aquellas que permitan dar un mejor funcionamiento y desempeño a las redes de acuerdo al tipo de estándar utilizado, mediante la evaluación del desempeño de las redes inalámbricas implementadas utilizando herramientas de análisis de paquetes de comunicación, así como la utilización de otras que permitan visualizar el funcionamiento de las redes, logrando obtener resultados más precisos de *throughput*, *delay* y análisis de paquetes enviados, recibidos y perdidos durante las transmisiones realizadas en cada escenario de simulación.

1.3 ESTÁNDAR IEEE 802.11

El estándar IEEE 802.11 elegido para el presente proyecto, presenta variaciones durante su implementación. Hay que tomar en cuenta el alcance del proyecto para realizar los estudios previos a las simulaciones a ser efectuadas. Para nuestro caso, el Estándar IEEE 802.11 será configurado para topologías de corto alcance, estudios bajo ambientes fijos, móviles y fijo – móvil. Lo cual permitirá obtener resultados en los tres escenarios de manera que este estudio pueda ser aplicado a futuro en ambientes a larga distancia, ambientes mixtos y estudios más avanzados con una red híbrida entre los estándares IEEE 802.11 e IEEE 802.16.

Las principales ventajas de utilizar este estándar inalámbrico se resumen en las siguientes acotaciones.

- Es un estándar muy conocido, el más utilizado a nivel mundial y el mejor para realizar estudios de investigación de éste tipo. Se requiere un estándar inalámbrico bastante estable que permita realizar pruebas con el simulador, a fin de encontrar resultados satisfactorios muy aproximados a la realidad.

- La utilización de este estándar bajo el simulador *ns-3,* permite manejar las herramientas del simulador en su totalidad, gracias a las actualizaciones del software se puede variar los parámetros de simulación, obteniendo mejores resultados.

- El estudio a pesar de que pretende ser sencillo, requiere de un estudio previo del simulador y del estándar que se va a aplicar bajo el mismo, lo cual es una motivación para la utilización del software *ns-3* ya que no se han registrado estudios anteriores a éste con la profundidad que se lo realiza. El estándar IEEE 802.11 es el ideal para iniciar un estudio con un simulador nuevo como el presentado a continuación. Los ambientes a ser simulados son sencillos, pero los resultados mostrarán las capacidades del simulador para lograr obtener datos muy cercanos a la realidad, con márgenes mínimos bajos de error.

CAPITULO 2

FUNDAMENTO TEÓRICO

2.1 EL SIMULADOR NS-3

La principal diferencia que el usuario familiarizado con el software de simulación *ns-2* encuentra durante el paso de éste al *ns-3* es la forma de escoger el lenguaje de programación en base a *scripts*. En *ns-2* todo código se lo realiza mediante un script en formato OTcl y los resultados que arrojan estas simulaciones pueden ser visualizadas utilizando herramientas gráficas incluidas en el simulador *ns-2* como es el *Network Animator*, o también conocido como nam.[1]. El simulador ns-3, está escrito en su mayor parte en lenguaje C++, adicionalmente el lenguaje Python también es un aporte para el desarrollo de este simulador. En el ns-3 actualmente se generan archivos de tipo *.pcap*, los cuales pueden ser leídos o interpretados por varios programas de captura de paquetes, entre los más usados podemos destacar al programa *Wireshark*.

Hay que tomar en cuenta también algunas similitudes que tienen, por ejemplo ambos están basados en objetos C++ y algunos códigos realizados en *ns-2* han sido llevados al *ns-3*. Adicionalmente, en el desarrollo de este estudio analizaremos algunas diferencias entre estos dos simuladores y las ventajas y desventajas que conllevan su utilización y funcionamiento.

El simulador *ns-3* contiene todos los modelos que posee el simulador *ns-2* y actualmente maneja aún más modelos de propagación, modelos inalámbricos, protocolos de comunicación, entre otros. Estas ventajas han permitidos que la

utilización del simulador *ns-3* vaya en aumento incorporando nuevas funciones y demostrando mayor capacidad de simulación con respecto al *ns-2.*

El simulador *ns-3* se ha basado en el trabajo de *Mathieu Lacage* en el simulador *yans* (*Yet Another Network Simulator*) [2], durante el cual se identificaron en *ns-2* un conjunto de fallos de diseño que fueron factores suficientes para iniciar el desarrollo de un nuevo simulador. Entre estos fallos destacaban la falta de versatilidad, debido básicamente a la dependencia entre los modelos (acoplamiento), el deficiente uso de las técnicas de programación orientada a objetos y el rígido acoplamiento entre C++ y OTcl.

El proyecto *ns-3* es un desarrollo que inició en junio de 2006 y está planificado que el estudio y ampliación de su código base se extienda hasta 2012, por las características y las grandes expectativas que *ns-3* ha creado en la comunidad. [2]

2.2 ORGANIZACIÓN DEL SOFTWARE NS-3

El simulador *ns-3,* se basa en el principio de que maneja simulaciones de eventos, esto quiere decir que son sucesos instantáneos que pueden cambiar el estado del sistema. Dichos eventos se manejarán durante este estudio pero de manera discreta, un sistema discreto se presenta cuando las variables de estado cambian solo en un conjunto discreto de puntos en el tiempo, su comportamiento se caracteriza por una secuencia finita o infinita de estados delimitados por eventos que ocurren de manera asíncrona.

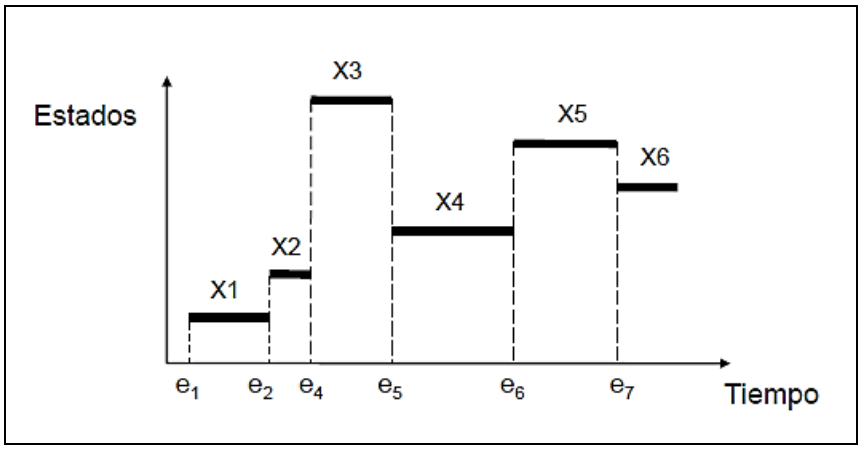


Figura. 2.1. Representación de un Sistema de Eventos Discretos

Las simulaciones y modelos inalámbricos que se manejan en el simulador *ns-3* son desarrollados e implementados bajo los lenguajes de programación descritos.

El código fuente para *ns-3* se encuentra organizado en el directorio principal */src*, este esquema es descrito en la Tabla 2.1. A continuación se presenta el proceso que realiza *ns-3* para la comunicación entre los módulos presentes en el simulador.

Tabla. 2.1. Organización del Software ns-3 [3]

ANÁLISIS			
AUXILIAR			
ENRUTAMIENTO	INTERNET-PILA	DISPOSITIVOS	APLICACIONES
NODO		MOVILIDAD	
GENERAL	SIMULACIÓN		
NÚCLEO			

Es importante conocer los contenidos que tiene el simulador, para su desarrollo y un práctico manejo en la utilización del mismo, por lo que es necesario conocer la ubicación de sus directorios y qué nos ofrece cada uno de ellos.

En primer lugar, el núcleo de simulación se lleva a cabo en el directorio *src/core* y la base se utiliza para construir el motor de simulación *src/simulator*. Los paquetes son los objetos fundamentales en un simulador de red y se ejecutan en *src/packet*. Estos tres módulos de simulación por sí mismos están destinados a formar un núcleo genérico de simulación que puede ser utilizado por diferentes tipos de redes, no basados en Internet. Los módulos anteriores de *ns-3* son independientes de la red y modelos específicos de dispositivos. [3]

En el tercer nivel se encuentran los más importantes a nivel de topología de red que son los módulos de Nodo y Movilidad. Los primeros serán contenidos en *DevicesContainers,* los cuales serán los responsables de guardar todos los datos configurados en los nodos o dispositivos inalámbricos que forman parte de la red, así mismo para el control de Movilidad de los mismos se manejan módulos específicos que catalogan a los nodos como fijos o móviles dentro de la red.

Dos tipos de Dispositivos de Redes especiales están diseñados para apoyar a la configuración de la red diferentes etapas de la simulación. Estos trabajan conjuntamente con los modelos asociados a Internet, incluida la API de sockets utilizados por las aplicaciones de Internet.

Finalmente se tienen los auxiliares y el análisis, que contienen comandos fundamentales para que el Núcleo pueda desarrollar las aplicaciones configuradas en los niveles superiores.

2.3 LA HERRAMIENTA DE SIMULACIÓN NS-3

Fundamentalmente el simulador *ns-3* es un sistema muy similar al que presenta C++, así mismo los objetos pueden ser declarados o instanciados siguiendo las mismas reglas, *ns-3* posee algunas características adicionales a los objetos que se maneja tradicionalmente en los lenguajes de programación. En resumen algunos patrones de diseño incluidos en el manejo orientado a objetos,

separación o distinción entre interface e implementación y patrón de diseño para una interface pública no virtual. [4]

El licenciamiento del simulador *ns-3* es de tipo GNU GPL v2 (GNU – *General Public Licence*), la cual es una licencia creada por la *Free Software Foundation* en 1989, año en la que se publicó la primera versión, y se encuentra orientada principalmente a proteger la libre distribución, modificación y uso de software, declarando que el software cubierto por ésta licencia es software libre y protegerlo de intentos de apropiación que restrinjan de libertades a los usuarios. [4]

Sistema Operativo: Sistemas POSIX (*Portable Operating System Interface Unix*) como GNU/Linux, BSD, OS X y Microsoft Windows (con *Cygwin* o *MinGW*) [5]

Código: C++, aproximadamente unas 500000 líneas de código desarrolladas en C++ y *Python*. En el futuro se prevé que también se pueda desarrollar prototipos de protocolos utilizando Python.

Protocolos Inalámbricos [6]

- 802.11a: El desarrollo original implementa completamente 802.11a en modo infraestructura (AP/cliente) y ad-hoc (el código lo hereda de *yans*)

- 802.11b: Presentado por Guangyu Pei y Tom Henderson en el proyecto Wns3-2009 (2009 *Workshop on ns-3*)

- 802.11e: De los dos tipos de acceso que contempla HCF (*Hybrid Coordination Function*) *ns-3* implementa EDCA (*Enhanced Distributed Channel Access*) y se encuentra en desarrollo el soporte para HCCA (*Controlled Access*)

- 802.11g: Implementaciones varias bajo el modo g. Actualmente también se encuentran estudios de desarrollo para otras variaciones de infraestructura.

Nodos multi-interfaz: La herramienta es muy versátil, es posible añadir tantas interfaces como se desee, de la tecnología que sea, en cada nodo.

Encaminamiento: Si la simulación no está orientada a pruebas específicas de encaminamiento, por simplicidad se emplea una tabla de enrutamiento centralizada y única (objeto *GlobalRouteManager*). Además, existen implementaciones para encaminamiento estático (tanto para *unicast* como *multicast*), OLSR (*Optimized Link State Routing*) y AODV (*Ad-hoc On-Demand Distance Vector*).

Nivel físico configurable: En las interfaces inalámbricas las características del canal son configurables:

Pérdida de paquetes: Soportada, a partir del cálculo del SNR y la BER (en función de la modulación empleada).

SNR/BER externo: Como en el resto de simuladores no existe esta opción, se tendría que implementar.

Posibilidad de aislamiento entre estaciones: No se contempla.

Soporte para larga distancia en 802.11: Soportado, *ACKTimeout* y *SlotTime* son parámetros configurables.

Simulaciones distribuidas: No soportado en este momento, aunque es uno de los objetivos del simulador desde el inicio y está prevista como tarea para el GSC-2009 (*Google Summer of Code*).

Simulación de aplicaciones/protocolos reales: No soportado, aunque se está trabajando para ofrecer una API similar a la de los *sockets* BSD para facilitar el desarrollo de aplicaciones para *ns-3*. Por otra parte, está en desarrollo portar NSC a *ns-3*, lo que permitiría usar implementaciones reales del protocolo TCP (con el objetivo de, al menos, poder simular con el *kernel* de Linux).

Modo de emulación: Soportado, una simulación *ns-3* puede enviar datos a través de redes reales a otros nodos de simulación *ns-3*.

Modo de comandos/GUI: Por el momento todas las operaciones se hacen por línea de comandos. No hay herramientas gráficas, aunque están en desarrollo aplicaciones que permitirán visualizar simulaciones a través de un GUI.

Uno de los objetivos declarados de *ns-3* es replicar a largo plazo el éxito de *ns-2* respecto a la enorme cantidad de código externo. *ns-3* dispone de varias listas de correo (para desarrolladores y usuarios), y aunque el tráfico sea más bajo que el de su predecesor, los desarrolladores principales son muy activos a la hora de responder.

El simulador *ns-3* es un simulador que recoge el testigo de *ns-2* en sus mejores aspectos (licencia libre, desarrollo abierto, colaboración amplia de la comunidad académica) a la vez que trata de superar las carencias y fallos de diseño (ampliamente compartidos por su comunidad de usuarios) de una herramienta con veinte años de historia. La cantidad de documentación en forma de tutoriales, detalles de la API, artículos, etc., con la que cuenta es un elemento a destacar.

2.4 ESTRUCTURA DE UN SCRIPT

Antes de analizar la estructura de un *script* desarrollado con el simulador de programación *ns-3*, se debe hacer una breve descripción de lo que es un *script*. “Los *scripts* son un conjunto de instrucciones generalmente almacenadas

en un archivo de texto que deben ser interpretados línea a línea en tiempo real para su ejecución, se distinguen de los programas, pues deben ser convertidos a un archivo binario ejecutable para correrlos.” [7]

Los *scripts* pueden estar embebidos en otro lenguaje para aumentar las funcionalidades de este, como es el caso los *scripts* PHP o *Javascript* en código HTML.

A continuación se especificará la estructura y funcionamiento de cada sección que conforma un *script*, para esto se tomará como ejemplo un *script* previamente desarrollado y probado para su ejecución.

Texto Estándar

En la primera línea del *script* se debe especificar el estilo de codificación que se utilizará en el código fuente. Ésta línea es la siguiente:

```
/* -*- Mode:C++; c-file-style:”gnu”; indent-tabs-mode:nil; -*- */
```

Adicionalmente se especifica información acerca de la licencia de distribución del software *ns-3*, aquí se indica que se utiliza una licencia GNU *General Public Licence versión 2*.

```
* This program is free software; you can redistribute it and/or modify
* it under the terms of the GNU General Public License version 2 as
* published by the Free Software Foundation;
*
* This program is distributed in the hope that it will be useful,
* but WITHOUT ANY WARRANTY; without even the implied warranty of
* MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
See the GNU General Public License for more details.
```

```
* You should have received a copy of the GNU General Public License
* along with this program; if not, write to the Free Software
* Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 US
```

Módulos de Inclusión

La manera correcta de iniciar la escritura del código es realizando la declaración de los módulos de inclusión.

```
#include "ns3/core-module.h"
#include "ns3/simulator-module.h"
#include "ns3/node-module.h"
#include "ns3/helper-module.h"
```

Si accedemos al código fuente de éstos archivos (../../build/debug/ns3) nos daremos cuenta que el contenido de éstos archivos de inclusión incluyen todos los archivos de inclusión pública en sus respectivos módulos.

Definición de nombres en *ns-3*

La siguiente línea en el script a ser desarrollado es la declaración de nombres.

```
using namespace ns3;
```

El proyecto *ns-3* que se vaya a realizar se lo inicia con la declaración *ns3*. Ésta declaración permite realizar un manejo más global de las variables incluso, para integrar funciones de otros códigos.

Registros o Notas

La siguiente línea del *script*, es la siguiente:

```
NS_LOG_COMPONENT_DEFINE ("FirstScriptExample");
```

Se utiliza ésta parte del código como un espacio conveniente para indicar los procesos que siguen la documentación del denominado espacio *Doxygen* que maneja el *ns-3* enfocado en el manejo de registros (*logging*).

La principal función de ésta sentencia es la de indicar o registrar los procesos que realiza la simulación mediante mensajes de error, de advertencia, desconocidos, de información, de descripción de funciones, entre otros.

Función Principal

La declaración de la función principal en el programa tendrá la siguiente sintaxis:

```
int
main (int argc, char *argv[])
{
```

Es similar a la manera de iniciar un programa en lenguaje C++ en la que se necesita de alguna manera definir una función principal la cual será la primera en ser ejecutada.

Se debe tomar en cuenta que en el instante que se ha iniciado la escritura del código, también se debe ubicar las especificaciones sobre los registros (logging) para que se pueda dar información de la simulación durante su ejecución. La sintaxis para los registros se los puede realizar tal como se muestra

en el siguiente ejemplo, en el cual se realiza una transferencia de paquetes de comunicación cliente – servidor.

```
LogComponentEnable("UdpEchoClientApplication", LOG_LEVEL_INFO);
LogComponentEnable("UdpEchoServerApplication", LOG_LEVEL_INFO);
```

Clases para el diseño de topologías

Existe una gran cantidad de clases que se utilizan en el simulador las cuales permiten realizar los procesos de declaración de variables, tipos de comunicaciones que se van a realizar, redes de datos a ser configuradas, protocolos de comunicaciones, etc.

Las principales clases y más utilizadas se listan a continuación:

- *NodeContainter*
- *PointToPoint Helper*
- *NetDeviceContainer*
- *InternetStackHelper*
- *Ipv4AddressHelper*

Aplicaciones

Existe una gran cantidad de aplicaciones que se pueden realizar mediante la implementación de un *script* en el cual se manejan protocolos de comunicaciones y diferentes formas de transmisión de datos. Las aplicaciones que más se maneja en los diferentes simuladores de redes de datos son las más

conocidas UDP y TCP cuando se realiza una comunicación sencilla punto a punto, en la Figura 2.2 se describen las aplicaciones que generalmente utiliza el simulador *ns-3* . [8]

El propósito principal de las aplicaciones es proporcionar una manera uniforme para iniciar y detener las solicitudes durante el proceso de simulación.

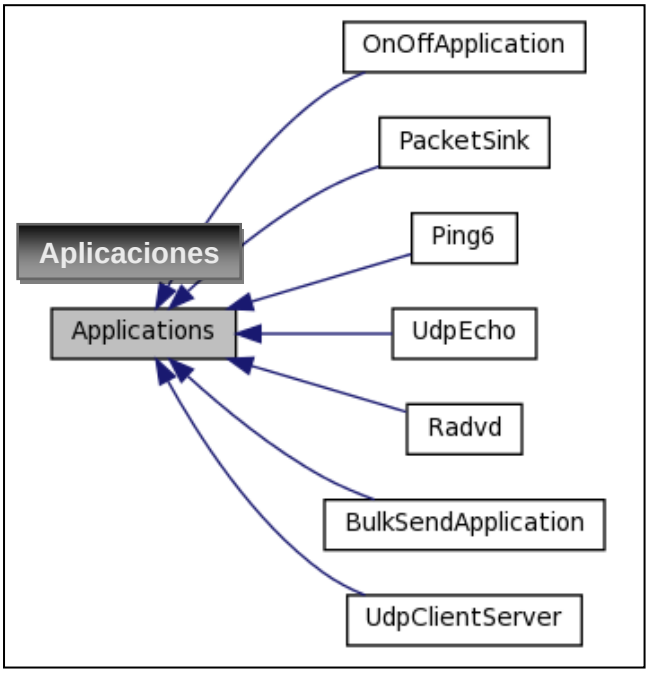


Figura. 2.2. Diagrama para Aplicaciones

Simulador

En este punto lo que se busca es realizar, propiamente la ejecución del programa que se ha escrito previo diseño de la red a ser simulada.

La ejecución del programa se lo debe hacer utilizando la siguiente función global:

```
Simulator::Run ();
```

Lo que hará el sistema cuando lea ésta instrucción será ejecutar todas las tareas programadas que se indican a lo largo del script realizado, siempre siguiendo el orden en que han sido ubicados los eventos para la ejecución de la simulación.

Después de que todos los eventos han sido ejecutados en su totalidad, y no existe ningún evento adicional a ser ejecutado, el sistema regresa a la sentencia de ejecución *Simulator::Run ();* realiza una limpieza total del sistema llamando a la función global:

Simulator::Destroy

Esta función auxiliar permite destruir todos los objetos auxiliares que hayan sido creados durante la simulación y que luego sean considerados como “elementos basura”.

2.5 CÓDIGO FUENTE DE NS-3

Los códigos fuente del simulador *ns-3* se pueden encontrar en la página principal del simulador: *http://code.nsnam.org/ns-3-dev* ésta es una opción que se maneja para desarrolladores que desean ingresar a formar parte del equipo de desarrollo de nuevas herramientas que podría soportar el simulador *ns-3*. Es muy importante el realizar trabajos que puedan ser analizados y posteados por los principales representantes de la página principal del simulador *ns-3* ya que dichos trabajos pueden ser publicados en la página principal en la sección de *examples* que maneja dicha página.

El código fuente del simulador, generalmente se ubica, después de que ha sido instalado en un ordenador en el directorio *src*, accediendo a éste directorio se puede manipular todo el programa simulador, ejecutando nuevas pruebas e

incluso cambiando scripts previamente desarrollados para el uso de aplicaciones específicas.

2.6 ANÁLISIS DEL ESTÁNDAR IEEE 802.11 [9]

La especificación IEEE 802.11 (ISO/IEC 8802-11) es un estándar internacional que define las características de una red de área local inalámbrica (WLAN). Wi-Fi (*Fidelidad inalámbrica)*, (5) es el nombre de la certificación otorgada por la *Wi-Fi Alliance*, anteriormente WECA (*Wireless Ethernet Compatibility Alliance*), grupo que garantiza la compatibilidad entre dispositivos que utilizan el estándar 802.11.

El estándar 802.11 establece los niveles inferiores del modelo OSI para las conexiones inalámbricas que utilizan ondas electromagnéticas, por ejemplo:

- La capa física ofrece tres tipos de codificación de información.
- La capa de enlace de datos compuesta por dos subcapas: control de enlace lógico (LLC) y control de acceso al medio (MAC)

La capa física define la modulación de las ondas de radio y las características de señalización para la transmisión de datos mientras que la capa de enlace de datos define la interfaz entre el bus del equipo y la capa física, en particular un método de acceso parecido al utilizado en el estándar Ethernet, y las reglas para la comunicación entre las estaciones de la red. En realidad, el estándar 802.11 tiene tres capas físicas que establecen modos de transmisión alternativos.

Tabla. 2.2. Capas del Modelo OSI para conexiones inalámbricas

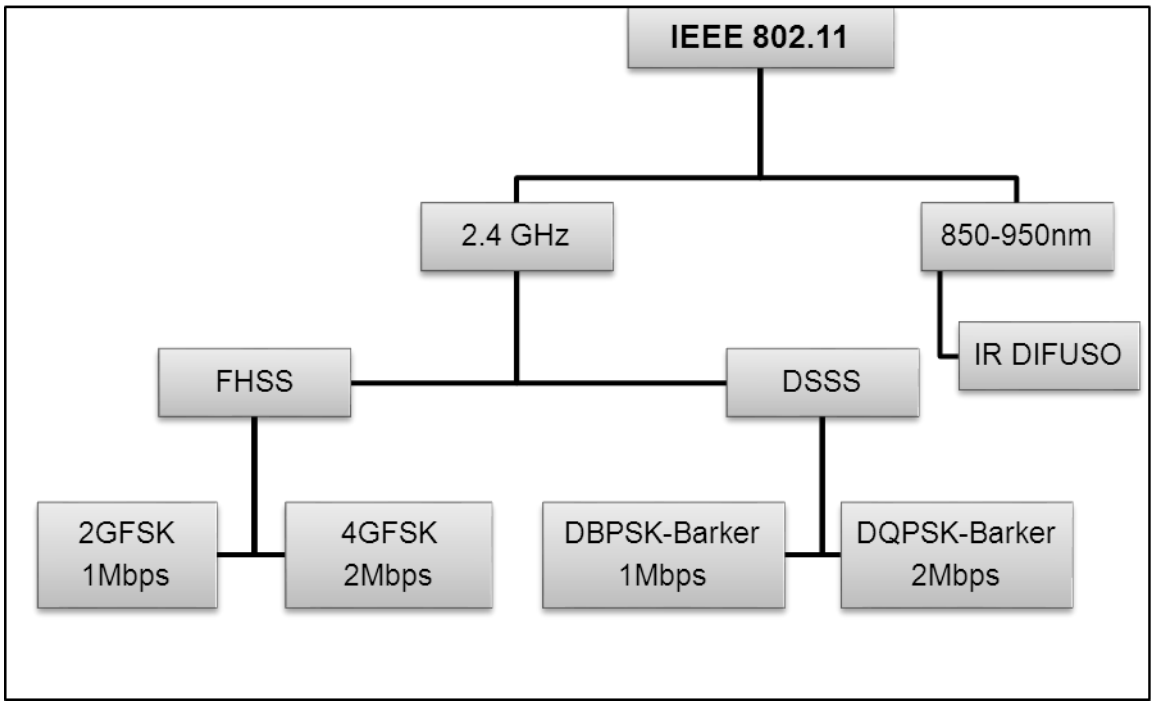
Capa de enlace de datos (MAC)	802.2
	802.11
Capa física (PHY)	DSSS | FHSS | Infrarrojo

2.6.1 La Capa Física

La capa física de cualquier red y específicamente de las redes inalámbricas, define la modulación y la señalización características para la transmisión de datos.

El estándar IEEE 802.11 define tres posibles opciones para la elección de la capa física, cada una con sus características principales y aplicaciones durante su respectivo funcionamiento:

Tabla. 2.3. Diagrama descriptivo de la capa física del 802.11 y sus extensiones



La definición de tres capas físicas distintas se debe a la necesidad del usuario para realizar una implementación mucho más sencilla que otra, tomando en cuenta el costo que resulta de realizar una implementación más compleja que otra, al igual que las prestaciones y fiabilidad que da al usuario. No obstante, es previsible, que al cabo de un cierto tiempo se puede obtener una clara preponderancia en el mercado de alguna de éstas opciones.

Antes de analizar cada opción que brinda la capa física, se debe analizar el medio por el cual estas tecnologías mantienen un funcionamiento operativo. De las tres opciones presentadas, dos emplean las radiofrecuencias, la bada estrecha y la banda ancha, también conocida como espectro ensanchado, siendo ésta última la más utilizada.

En mayo de 1985, y tras cuatro años de estudios, el FCC (*Federal Communications Comission*), la agencia Federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas IMS (*Industrial, Scientific and Medical*) 902 – 928 MHz; 2,400 – 2,4835 GHz; 5,725 – 5, 850 GHz a las redes inalámbricas basadas en espectro ensanchado. (9) Entre ellas, el IEEE 802.11 incluye en su especificación las frecuencias en torno a 2,4GHz que se habían convertido ya en el punto de referencia a nivel mundial.

La tecnología de espectro ensanchado utiliza todo el ancho de banda disponible, en lugar de utilizar una portadora para concentrar la energía a su alrededor. Posee características que le hacen sobresalir sobre otras tecnologías de radiofrecuencias, por ejemplo excelentes propiedades en cuanto a inmunidad a interferencias y a sus posibilidades de encriptación, a diferencia de las tecnologías que utilizan banda estrecha, tal es el caso de las comunicaciones que utilizan microondas.

Existen dos tecnologías que utilizan el espectro ensanchado, estas son: Espectro Ensanchado por Secuencia Directa – DSSS y Espectro Ensanchado por Salto de Frecuencia – FHSS.

Espectro Ensanchando por Secuencia Directa (*Direct Sequence Spread Spectrum* – DSSS)

La norma IEEE 802.11 establece la codificación de los datos transmitidos utilizando la tecnología DSSS (*direct-sequence spread-spectrum*). Dicha codificación trabaja tomando la corriente de datos (ceros y unos) y modulándolos con un segundo patrón: la secuencia de "*chipping*" (secuencia binaria aleatoria que presenta propiedades aleatorias parecidas a las del ruido) este patrón de bits redundante es muy utilizada para “esparcir” la velocidad de transmisión y por lo tanto el ancho de banda. En el estándar 802.11 esta secuencia es conocida como "código *Barker*" (también llamado código de dispersión o *PseudoNoise*), consiste en una secuencia de 11 bits (ejemplo: 10110111000). La corriente de datos básica y el código de Barker se aplican a una operación lógica OR para generar una serie de datos llamados "chips". Cada bit es codificado con el código Barker de 11 bits, representado en la Figura 2.3. La sección de RF del *Wireless* genera una portadora de 2,4GHz (banda de 2,4 GHz a 2,483 GHz) y modula señal usando una variedad de técnicas. Solo los receptores a los que el emisor haya enviado previamente la secuencia podrán recomponer la señal original. Además, al sustituir cada bit de datos a transmitir, por una secuencia de 11 bits equivalente, aunque parte de la señal de transmisión se vea afectada por interferencias, el receptor aún puede reconstruir fácilmente la información a partir de la señal recibida. [10]

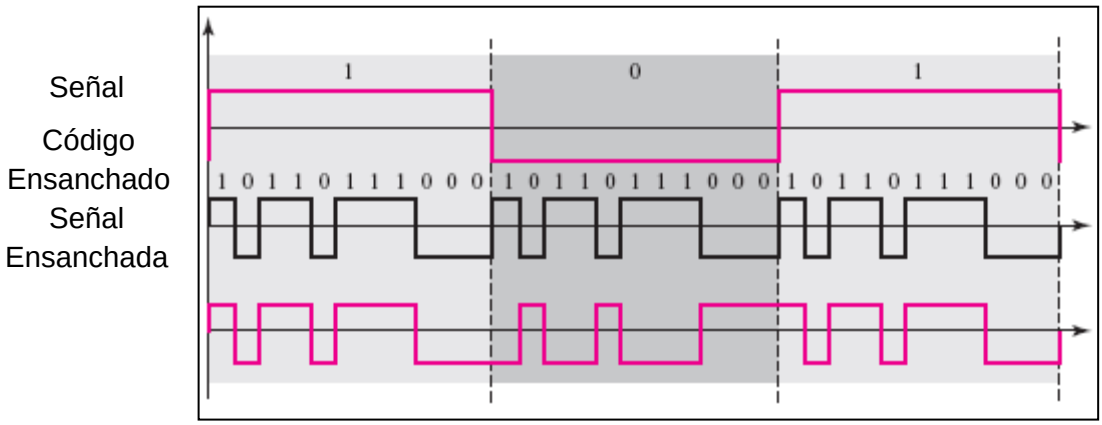


Figura. 2.3. Codificación de la Información mediante la secuencia de Barker [11]

Una vez aplicada la señal de chip, el estándar IEEE 802.11 ha definido dos tipos de modulación para la técnica de espectro ensanchado por secuencia directa (DSSS), la modulación DBPSK (*Differential Binary Phase Shift Keying*) y la modulación DQPSK (*Differential Quadrature Phase Shift Keying*), que proporcionan una velocidad de transferencia de 1 y 2 Mbps respectivamente. [11]

En el caso de Estados Unidos y Europa la tecnología DSSS utiliza un rango de frecuencias que va desde los 2,4 GHz hasta los 2,4835 GHz, lo que permite tener un ancho de banda total de 83,5 MHz. Este ancho de banda se subdivide en canales de 5 MHz, lo que hace un total de 14 canales independientes, aunque hay que tener en cuenta que el número de canales disponibles depende del ancho de banda ubicado por las agencias nacionales de regulación. Cada país está autorizado a utilizar un subconjunto de estos canales. En configuraciones donde existan más de una celda, estas pueden operar simultáneamente y sin interferencias siempre y cuando la diferencia entre las frecuencias centrales de las distintas celdas sea de al menos 30 MHz, lo que reduce a tres el número de canales independientes y funcionando simultáneamente en el ancho de banda total de 83,5 MHz. Esta independencia entre canales nos permite aumentar la capacidad del sistema de forma lineal. [11]

La técnica de DSSS podría compararse con una multiplexación en frecuencia debido a que la potencia de transmisión de equipos de radio está regulada por los organismos oficiales de Comunicaciones y limitada a 30 dBm (1 watt EIRP: *equivalent isotropically radiated power*), el único factor que puede cambiar es el rango. Por lo tanto, en dispositivos 802.11, a medida que el usuario se aleja del equipo de radio (*Access Point*), este último se adapta a dicha condición y usa un mecanismo menos complejo y más lento de codificación para transmitir datos.

Para prevenir interferencias en redes trabajando con canales adyacentes, se los debe separar al menos 22 MHz, en la Figura 2.4 se presenta una configuración con separación de 25 MHz, entre las frecuencias centrales de los canales. Adicionalmente con una separación de 5 MHz de separación entre canales, las redes deben estar separadas por 5 números de canal. [11]

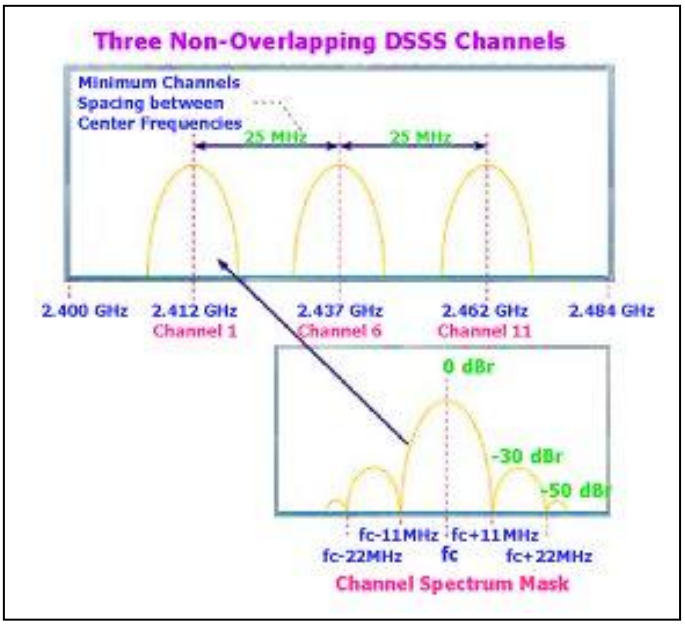


Figura. 2.4. Canalización para los sistemas 802.11 en DSSS

Espectro Ensanchando por Salto de Frecuencia (*Frequency – Hopping Spread Spectrum* – FHSS) [12]

El espectro ensanchado por salto de frecuencia es una técnica que consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamada *dwell time* e inferior a 400ms. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo. El orden de los saltos de frecuencia se determina según una secuencia pseudoaleatoria que tanto el emisor y el receptor deben conocer. Si se intentara interceptar la señal, sólo se conseguiría para unos pocos bits. Una transmisión en espectro ensanchado ofrece 3 ventajas principales:

- Las señales en espectro ensanchado son altamente resistentes al ruido y a la interferencia.

- Las señales en espectro ensanchado son difíciles de interceptar. Una transmisión de este tipo suena como un ruido de corta duración, o como un incremento en el ruido en cualquier receptor, excepto para el que esté usando la secuencia que fue usada por el transmisor.

- Transmisiones en espectro ensanchado pueden compartir una banda de frecuencia con muchos tipos de transmisiones convencionales con mínima interferencia.

Su principal desventaja es su bajo ancho de banda

El orden en los saltos en frecuencia se determina según una secuencia pseudoaleatoria almacenada en unas tablas, y que tanto el emisor y el receptor deben conocer. Si se mantiene la sincronización en los saltos de frecuencias se consigue que, aunque en el tiempo se cambie de canal físico, a nivel lógico se mantiene un solo canal por el que se realiza la comunicación. [13]

Esta técnica también utiliza la zona de los 2.4GHz, la cual se organiza en 79 canales con un ancho de banda de 1MHz cada uno. El número de saltos por segundo es regulado por cada país.

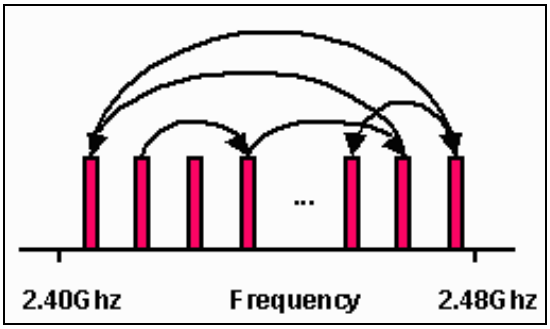


Figura. 2.5. Saltos de Frecuencia para FHSS

El estándar IEEE 802.11 define la modulación aplicable en este caso. Se utiliza la modulación en frecuencia GFSK (*Gaussian Frequency Shift Keying*), de dos niveles para una velocidad de 1 Mbps en la cual los niveles 0 y 1 se codifican como desviaciones de la frecuencia actual de la portadora, mientras que en la modulación de cuatro niveles para una velocidad de 2 Mbps cuatro desviaciones diferentes de la frecuencia central definen las 4 combinaciones de dos bits, estos datos se contemplan en la Tabla 2.4.

Tabla. 2.4. Espectro Ensanchado por Salto de Frecuencia

TASA DE DATOS	MODULACIÓN	TASA DE SÍMBOLOS	BITS/SÍMBOLO
1 Mbps	Dos niveles - GFSK	1 Msps	1
2 Mbps	Cuatro niveles - GFSK	1 Msps	2

En la revisión del estándar 802.11b, ésta velocidad también ha aumentado a 11 Mbps. La técnica FHSS sería equivalente a una multiplexación en frecuencia.

Tecnología de Infrarrojos [14]

Éste tipo de tecnología no es muy utilizada en el estándar IEEE 802.11, específicamente se lo ha utilizado y realizado trabajos de investigación bajo la variación 802.11r en la cual se destacan algunas características principales:

- Entornos muy localizados, un aula concreta, un laboratorio o un edificio.

- Modulaciones de 16-PPM y 4-PPM que permiten 1 y 2 Mbps de transmisión.

- Longitudes de onda de 850 a 950 nanómetros de rango.

- Frecuencias de emisión entre $3.15x10^{14}$ Hz y $3.52x10^{14}$ Hz

Las WLAN por infrarrojos son aquellas que usan el rango infrarrojo del espectro electromagnético para transmitir información mediante ondas por el espacio libre. Los sistemas de infrarrojos se sitúan en altas frecuencias, justo por debajo del rango de frecuencias de la luz visible. Las propiedades de los infrarrojos son, por tanto, las mismas que tiene la luz visible. De esta forma los infrarrojos son susceptibles de ser interrumpidos por cuerpos opacos pero se pueden reflejar en determinadas superficies. En la Figura 2.6 se ejemplifican algunas de las aplicaciones que utiliza esta tecnología.

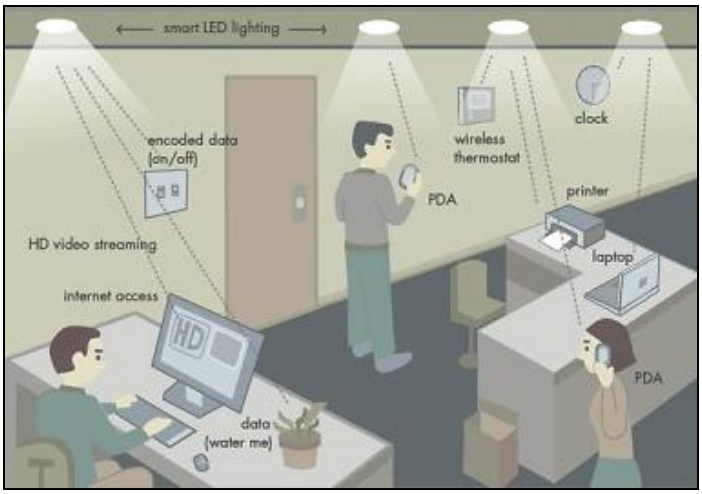


Figura. 2.6. Transmisión por Infrarrojos

De acuerdo al ángulo de apertura con que se emite la información en el transmisor los sistemas infrarrojos pueden clasificarse en sistemas de corta apertura, también llamados de rayo dirigido o de línea de vista (*line of sight, LOS*) y en sistemas de gran apertura, reflejados o difusos (*diffused*).

- Los sistemas infrarrojos de corta apertura, están constituidos por un cono de haz infrarrojo altamente direccional y funcionan de manera similar a los controles remotos de las televisiones: el emisor debe orientarse hacia el receptor antes de empezar a transferir información, limitando por tanto su funcionalidad. Resulta muy complicado utilizar esta tecnología en dispositivos móviles, pues el emisor debe reorientarse constantemente. Este mecanismo solo es operativo en enlaces punto a punto exclusivamente. Por ello se considera que es un sistema inalámbrico, pero no móvil, o sea que esta más orientado a la portabilidad que a la movilidad.

- Los sistemas de gran apertura permiten la información en ángulo mucho más amplio por lo que el transmisor no tiene que estar alineado con el receptor. Una topología muy común para redes locales inalámbricas basadas en esta tecnología, consiste en colocar en el techo de la oficina un nodo central llamado punto de acceso,

hacia el cual dirigen los dispositivos inalámbricos su información, y desde el cual ésta es difundida hacia esos mismos dispositivos.

- La dispersión utilizada en este tipo de red hace que la señal transmitida rebote en techos y paredes, introduciendo un efecto de interferencia en el receptor, que limita la velocidad de transmisión. Éste es uno de los factores que ha hecho que la tecnología infrarroja no sea muy utilizada bajo la norma 802.11.

La modulación utilizada en esta tecnología es la modulación conocida como Modulación por Posición de Pulso (*Pulse Position Modulation – PPM)* ésta técnica de modulación es el resultado de diferenciar y después rectificar la señal obtenida tras la modulación PDM de la señal inicial. La distancia entre dos pulsos representa la amplitud muestreada de la onda seno, con el primer pulso en la referencia de tiempo cero. La ventaja de éste sistema es que la potencia media del sistema es mucho menor que la requiere el sistema PDM, pero con el inconveniente de requerir un ancho de banda mayor. [15] En la Figura 2.7 se representa esta clase de modulación.

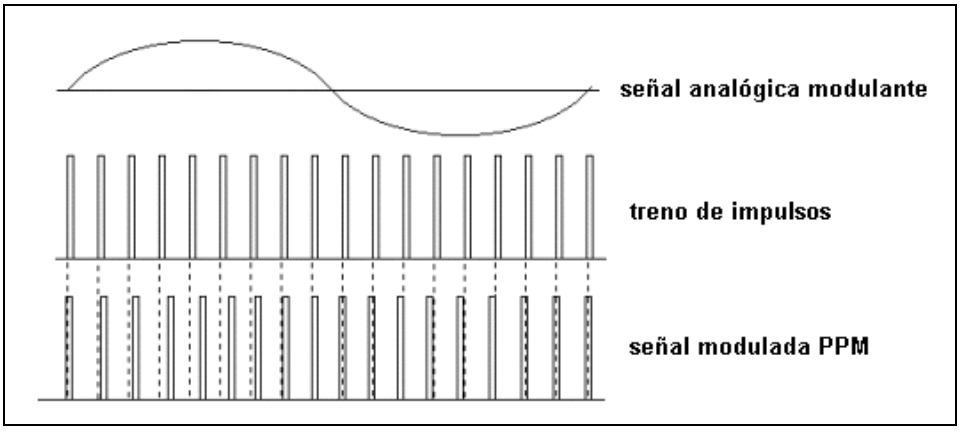


Figura. 2.7. Modulación PPM

Una red de área local o WLAN (*Wireless* LAN) utiliza ondas electromagnéticas (radio e infrarrojo) para enlazar (mediante un adaptador) los

equipos conectados a la red, en lugar de los cables coaxiales o de fibra óptica que se utilizan en las LAN convencionales cableadas (Ethernet, Token Ring, ...). [16]

2.6.2 La Capa Mac

Los diferentes métodos de acceso de IEEE 802.11 están diseñados según el modelo OSI y se encuentran ubicados en el nivel físico y en la parte inferior del nivel de enlace o subnivel MAC.

MAC se define como un subnivel inferior, provee el acceso compartido de las tarjetas de red al medio físico, es decir, define la forma en que se va a acceder al medio físico empleado en la red para el intercambio de datos. Adicional, se realiza un control en aspectos tales como sincronización y algoritmos del sistema de distribución, que se define como el conjunto de servicios que precisa o propone el modo infraestructura. [17]

El estándar 802.11 define en su capa de control de acceso al medio (*Medium Access Control – MAC*) una serie de funciones para realizar las operaciones propias de las redes inalámbricas. La capa MAC se encarga, en general, de gestionar y mantener las comunicaciones entre estaciones 802.11. La capa MAC tiene que coordinar el acceso a un canal de radio compartido y utilizar su capa Física (PHY) para detectar la portadora y proceder a la transmisión y recepción de tramas. [17]

Un adaptador de red cliente tiene que obtener primero el acceso al medio antes de poder transmitir tramas. El medio es una canal de radio compartido. El estándar 802.11 define dos formas de acceso al medio representadas en la Figura 2.8.

- La función de coordinación distribuida (DCF)

- La función de coordinación puntual (PCF).

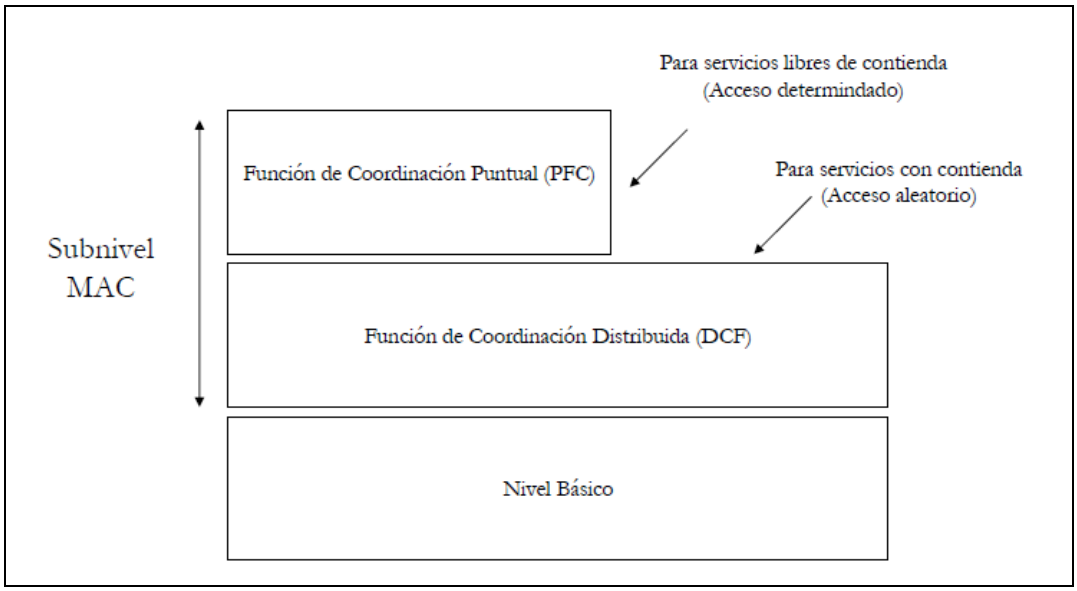


Figura. 2.8. Descripción de la Arquitectura MAC

Función de Coordinación Distribuida (*Distributed Coordination Function – DCF*) [17]

Se define a la Función de Coordinación Distribuida, como la funcionalidad que determina, dentro de un conjunto básico de servicios (BSS), cuándo una estación puede transmitir y/o recibir unidades de datos de protocolo a nivel MAC a través del medio inalámbrico. En el nivel inferior del subnivel MAC se encuentra la función de coordinación distribuida y su funcionamiento se basa en técnicas de acceso aleatorias de contienda por el medio. El tráfico que se transmite bajo esta funcionalidad es de carácter asíncrono ya que estas técnicas de contienda introducen retardos aleatorios y no predecibles ni tolerados por los servicios síncronos.

Características de DCF

- Utiliza como protocolo de acceso al medio al Acceso múltiple con prevención de colisiones – MACA (*Multiple Access with Collission Avoidance*)

- Reconocimientos necesarios ACKs, provocando retransmisiones si no se recibe la información.

- Utiliza el campo *Duration/ID* que contiene el tiempo de reserva para transmisión y ACK. Esto quiere decir que todos los nodos conocerán cuando el canal vuelve a quedar libre.

- Implementa fragmentación de datos.

- Concede prioridad entre tramas, utilizando la técnica de espaciado entre trama (IFS)

- Soporta Broadcast y Multicast sin ACKs.

Protocolo de Acceso al Medio CSMA/CA y MACA

El algoritmo básico de acceso a este nivel es muy similar al implementado en el estándar IEEE 802.3 y se le conoce como CSMA/CA. Este algoritmo funciona como se describe a continuación:

1.- Antes de transmitir información a una estación debe analizar el medio, o canal inalámbrico, para determinar su estado (libre / ocupado).

2.- Si el medio no está ocupado por ninguna otra trama la estación ejecuta una acción adicional llamada espaciado entre tramas (IFS).

3.- Si durante este intervalo temporal, o bien ya desde el principio, el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transacción actual antes de realizar cualquier acción.

4.- Una vez finalizada esta acción, como consecuencia del medio ocupado la estación ejecuta el algoritmo de *Backoff*, según el cual se determina una espera

adicional y aleatoria escogida uniformemente en un intervalo llamado ventana de contienda (CW). El algoritmo de *Backoff* nos da un número aleatorio y entero de ranuras temporales (slot time) y su función es la de reducir la probabilidad de colisión que es máxima cuando varias estaciones están esperando a que el medio quede libre para transmitir.

5.- Mientras se ejecuta la espera marcada por el algoritmo de *Backoff* se continúa escuchando el medio de tal manera que si el medio se determina libre durante un tiempo de al menos IFS esta espera va avanzando temporalmente hasta que la estación consume todas las ranuras temporales asignadas. En cambio, si el medio no permanece libre durante un tiempo igual o superior a IFS el algoritmo de *Backoff* queda suspendido hasta que se cumpla esta condición.

Cada retransmisión provocará que el valor de CW, que se encontrará entre Cwmin y CWmax se duplique hasta llegar al valor máximo. Por otra parte, el valor del slot time es de 20 μseg.

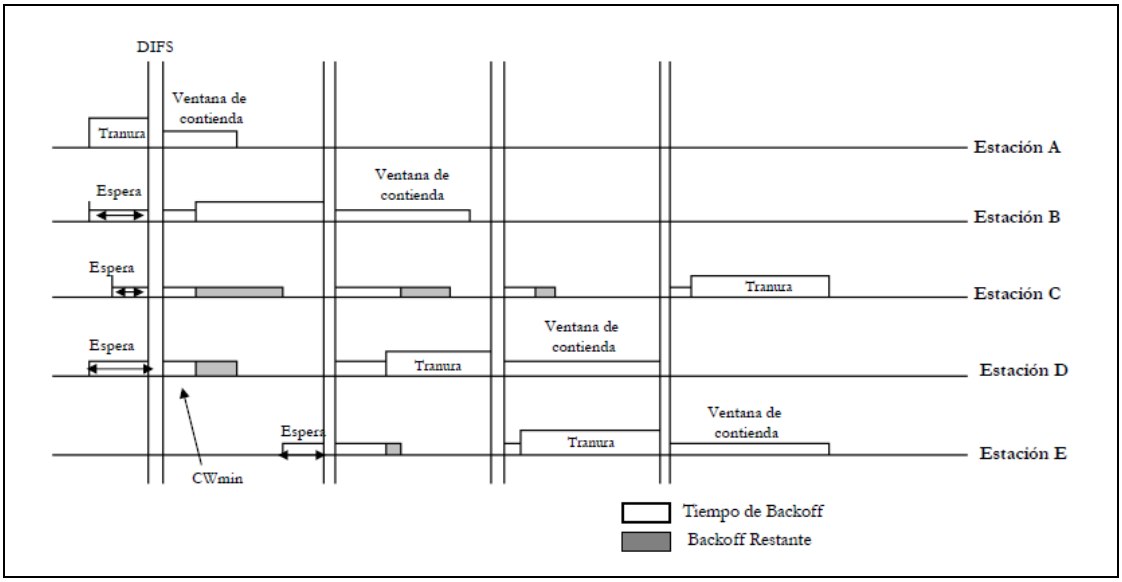


Figura. 2.9. Descripción del funcionamiento de acceso CSMA/CA

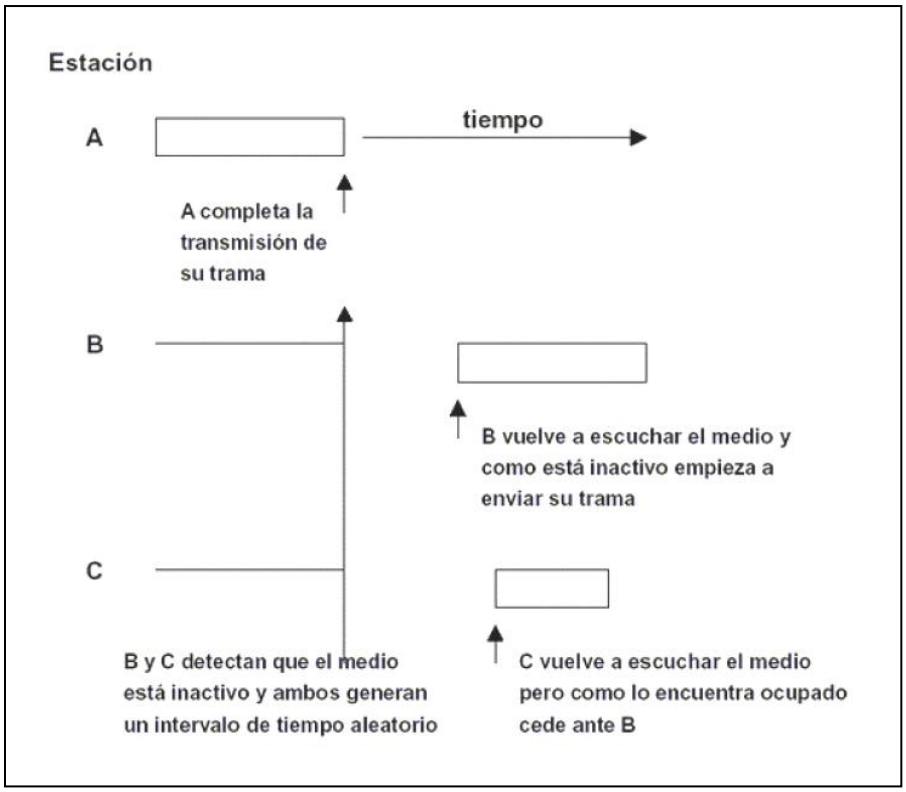


Figura. 2.10. Determinación de disponibilidad del canal

Sin embargo, CSMA/CA en un entorno inalámbrico presenta una serie de problemas que se intentan resolver con alguna modificación. Los dos principales problemas que podemos detectar son:

- Nodos ocultos. Una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo que no escucha.

- Nodos expuestos. Una estación cree que el canal está ocupado, pero en realidad está libre pues el nodo al que escucha no le interferiría para transmitir a otro destino.

La solución que propone el estándar 802.11 es MACA o *Multiple Access Collision Avoidance.* Según este protocolo, antes de transmitir el emisor envía una trama RTS (*Request to Send*), indicando la longitud de datos que quiere enviar. El

receptor le contesta con una trama CTS (*Clear to Send*), repitiendo la longitud. Al recibir el CTS, el emisor envía sus datos.

Los nodos seguirán una serie de normas para evitar los nodos ocultos y expuestos:

- Al escuchar un RTS, hay que esperar un tiempo por el CTS.
- Al escuchar un CTS, hay que esperar según la longitud.

La solución final de 802.11 utiliza MACA con CSMA/CA para enviar los RTS y CTS.

Espaciado entre tramas IFS

El tiempo de intervalo entre tramas se llama IFS. Durante este periodo mínimo, una estación STA estará escuchando el medio antes de transmitir. Se definen cuatro espacios para dar prioridad de acceso al medio inalámbrico.

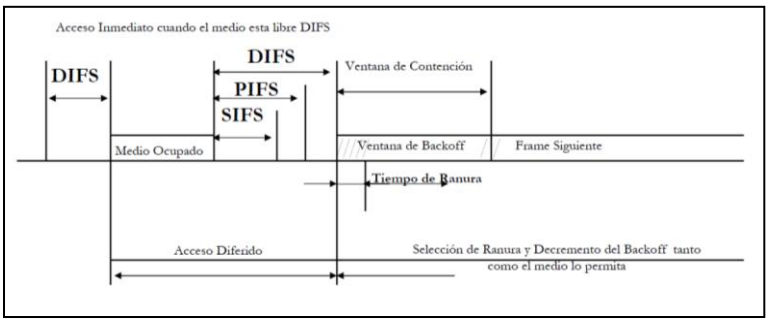


Figura. 2.11. Espaciado de Tramas IFS

- SIFS (*Short InterFrame Space*).- Este es el periodo más corto. Se utiliza fundamentalmente para transmitir los reconocimientos. También es utilizado para transmitir cada uno de los fragmentos de una trama.

También es utilizado por el PC o Point Control para enviar testigo a estaciones que quieran transmitir datos síncronos.

- PIFS (*PCF InterFrame Space*). Es utilizado por las STAs para ganar prioridad de acceso en los periodos libres de contienda. Lo utiliza el PC para ganar la contienda normal, que se produce al esperar DIFS.

- DIFS (*DCF InterFrame Space*). Es el tiempo de espera habitual en las contiendas con mecanismo MACA. Se utiliza para el envío de tramas MAC MPDUs y tramas de gestión MMPDUs.

- EIFS (*Extended InterFrame Space*). Controla la espera en los casos en los que se detecta la llegada de una trama errónea. Espera un tiempo suficiente para que le vuelvan a enviar la trama u otra solución. [17]

Conocimiento del medio

Las estaciones tienen un conocimiento específico de cuando la estación, tiene el control del medio porque está transmitiendo o recibiendo, para finalizar su periodo de reserva del canal. Esto se hace a través de una variable llamada NAV (*Network Allocation Vector*) que mantendrá una predicción de cuando el medio quede liberado.

Tanto al enviar un RTS como al recibir un CTS, se envía el campo *Duration/ID* con el valor reservado para la transmisión y el subsiguiente reconocimiento. Las estaciones que estén a la escucha modificarán su NAV según el valor de este campo *Duration/ID.*

En realidad, hay una serie de normas para modificar el NAV, una de ellas es que el NAV siempre se situará al valor más alto de entre los que se disponga.

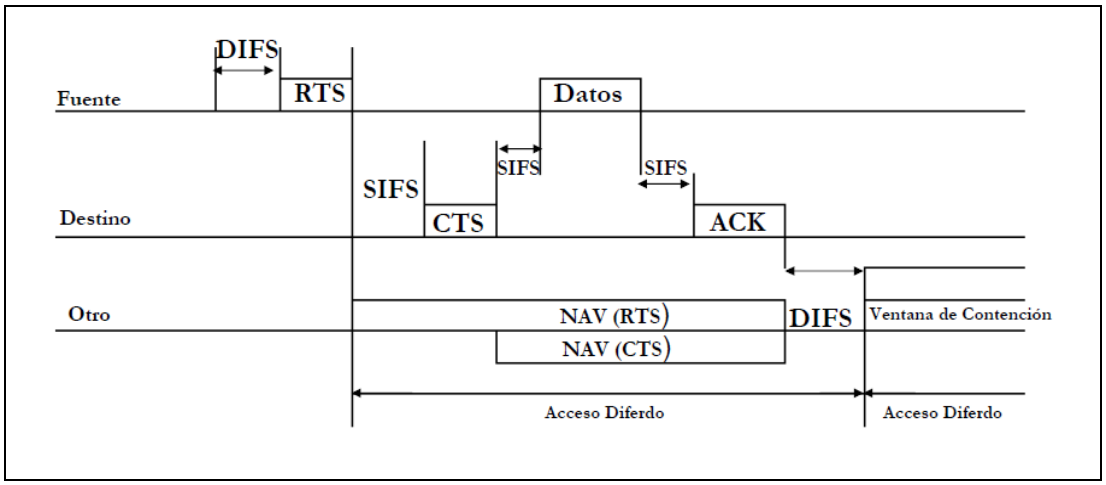


Figura. 2.12. Conocimiento del Medio

Función de Coordinación Puntual (*Point Coordination Function – PCF*)

Por encima de la funcionalidad DCF se sitúa la función de coordinación puntual PCF, asociada a las transmisiones libres de contienda que utilizan técnicas de acceso deterministas. El estándar IEEE 802.11, en concreto, define una técnica de interrogación circular desde el punto de acceso para este nivel. Esta funcionalidad está pensada para servicios de tipo síncrono que no toleran retardos aleatorios en el acceso al medio. [18]

Estos dos métodos de acceso pueden operar conjuntamente dentro de una misma celda o conjunto básico de servicios dentro de una estructura llamada *supertrama*. Un parte de esta *supertrama* se asigna al periodo de contienda permitiendo al subconjunto de estaciones que lo requieran transmitir bajo mecanismos aleatorios. Una vez finalizado este periodo el punto de acceso toma el medio y se inicia un periodo libre de contienda en el que pueden transmitir el resto de estaciones de la celda que utilizan técnicas deterministas. [18]

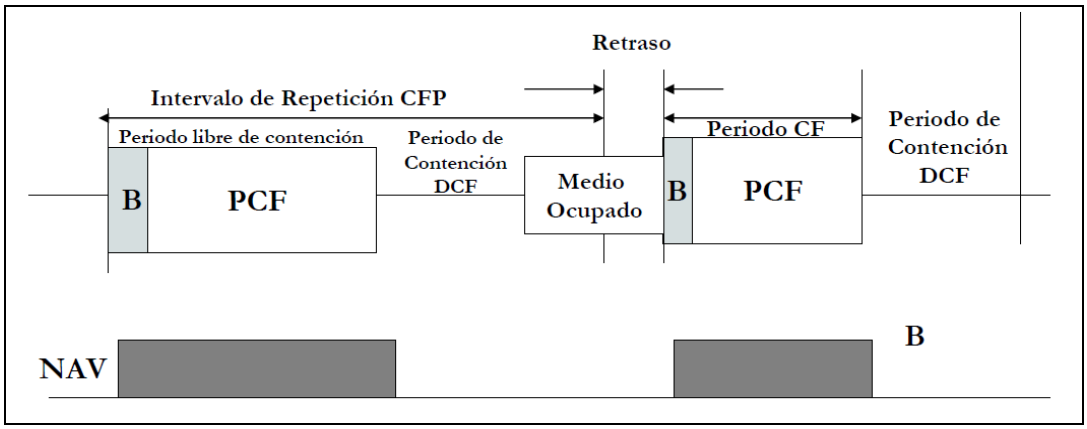


Figura. 2.13. Función de Coordinación Puntual

El funcionamiento de PCF es solamente compatible con el modo DCF, observando un funcionamiento transparente para las estaciones; de esta manera, una estación se asociará (se dará de alta en un modo infraestructural) de modo que pueda actuar en el periodo CFP, o por el contrario se situará su NAV según las indicaciones del punto de coordinación.

Existe un nodo organizador o director, llamado punto de coordinación o PC. Este nodo tomará el control mediante el método PIFS enviando un CF-Poll a cada estación que pueda transmitir un CFP, concediéndole poder transmitir una trama MPDU. El PC mantendrá una lista Poll (*pollable)* donde ubicará todos los datos de las estaciones que se han asociado al modo CF-Poll. La concesión de transmisiones será por riguroso listado y no permitirá que se envíen dos tramas hasta que la lista se haya completado. El nodo utilizará una trama para la configuración de la supertrama, llamada *Beacon*, donde se establecerá una *CFRate* o tasa de periodos de contienda. Pese a que el periodo de contienda se puede retrasar por estar el medio ocupado, la tasa se mantendrá en el siguiente periodo con medio libre.

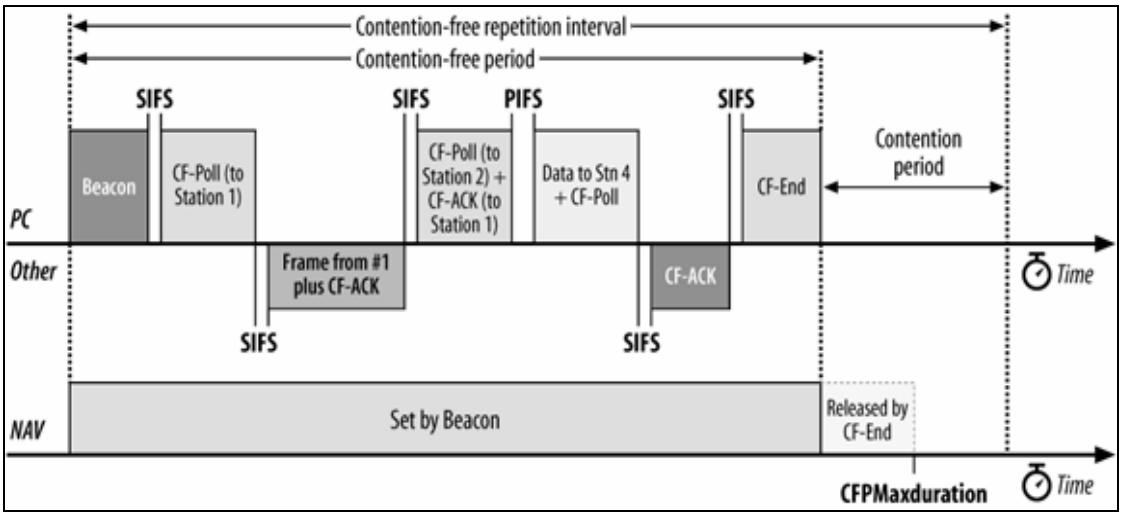


Figura. 2.14. Transmisión CF-Polls

Tal como se indica en la Figura 2.11, la transmisión de CF-Polls requiere de un tiempo de espera SIFS para el envío de las tramas y reconocimientos durante la transmisión. Adicionalmente, si una estación no aprovecha su CF-Poll se transmite al siguiente en el listado *Pollable.*

Las estaciones que no usen el CF, situarán su NAV al valor final del CF para después aplicar un *reset* para poder modificarlo en el periodo de contienda en igualdad de condiciones.

Un problema importante que se puede notar, es el traslape de redes inalámbricas que ocurre cuando varios sistemas con coordinación puntual comparten una tasa *CFRate* semejante. Una solución suele ser establecer un periodo de contienda entre PCs para ganar el medio esperando un tiempo DIFS + *BackOff* (1 – CW*min*) [19]

2.6.3 Formato de las tramas MAC

Las tramas MAC contienen los siguientes componentes básicos:

- Una cabecera MAC, que comprende campos de control, duración, direccionamiento y control de secuencia.

- Un cuerpo de trama de longitud variable, que contiene información específica del tipo de trama.

- Una secuencia *checksum (FCS)* que contiene un código de redundancia CRC de 32 bits.

Las tramas MAC se pueden clasificar según tres tipos:

- Tramas de datos. Son las encargadas de transportar la información de las capas superiores.

- Tramas de control. Entrega de tramas de datos entre estaciones.

    - Tramas *Request to Send* (RTS).- Reduce las colisiones en el caso de dos estaciones asociadas a un mismo punto de acceso pero mutuamente fuera de rango de cobertura. La estación envía una trama RTS para iniciar el diálogo de comienzo de transmisión de una trama.

    - Tramas *Clear to Send* (CTS).- Las estaciones utilizan tramas CTS para responder a una trama RTS para dejar el canal libre de transmisiones. Las tramas CTS contienen un valor de tiempo durante el cual el resto de las estaciones dejan de transmitir el tiempo necesario para transmitir la trama.

    - Tramas *Acknowledgement* (ACK).- Confirman la recepción de una trama. En caso de no llegar la trama ACK el emisor vuelve a enviar la trama de datos.

- Tramas de gestión. Permiten mantener comunicaciones a las estaciones inalámbricas.

  - Trama de autenticación.- El adaptador cliente inicia el proceso de enviando al punto de acceso una trama de autenticación que contiene su identidad en el campo de datos, el punto de acceso responde con otra trama de autenticación que indica si acepta o rechaza la conexión.

  - Trama de des-autenticación.- Es una trama que envía una estación a otra cuando quiere terminar las comunicaciones.

  - Trama de solicitud de asociación.- Es utilizada por una estación cliente para iniciar el proceso de asociación, es decir, indica al punto de acceso que reserve recursos (memoria) y realice la sincronización con la estación cliente.

  - Trama de respuesta de asociación.- Utilizada por los puntos de acceso para responder solicitudes de asociación.

  - Trama *Beacon* (baliza).- Un punto de acceso envía tramas *beacon* periódicamente para difundir su presencia y la información de la red, el SSID, etc. a las estaciones clientes en su radio de cobertura. [19]

  - Trama de solicitud de prueba.- Enviada por la estaciones para obtener información de otra estación, por ejemplo obtener una lista de puntos de acceso disponibles.

  - Trama de respuesta de prueba.- Es la respuesta de una estación a una solicitud, por ejemplo las tasas de transmisión.

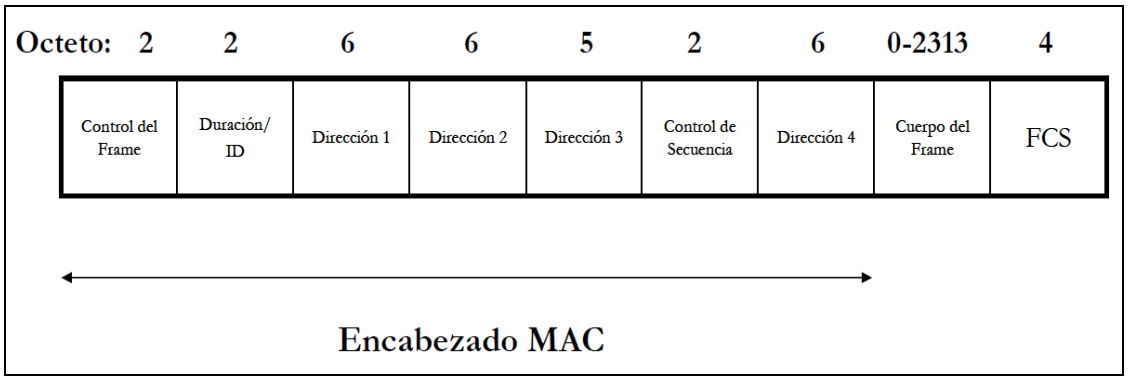


Figura. 2.15. Trama MAC Genérica

Los campos que componen esta trama son:

- Campo de control
- Duración / ID
- Campos de Dirección
- Campo de control de secuencia
- Cuerpo de la trama
- FCS

Campos de Control [20]

Los campos de control de trama tienen el siguiente formato:

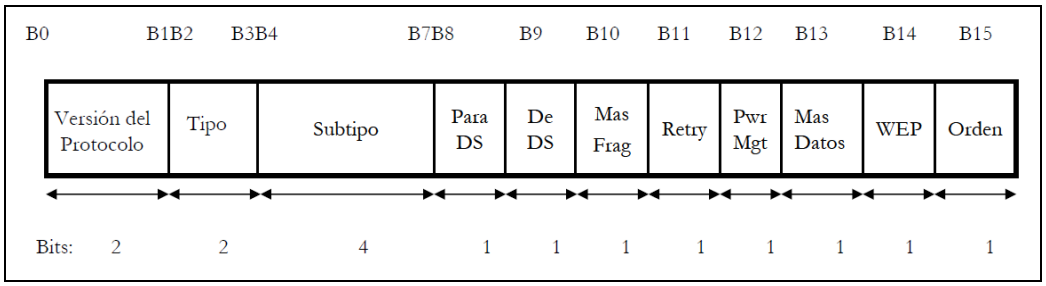


Figura. 2.16. Campos de Control de Trama

- Versión del Protocolo (*Protocol Version*): Indica la versión del protocolo. El valor por defecto que se toma en este campo es el "0".

- Tipo (*Type*): Indica el tipo de trama. Las tramas pueden ser de administración, datos o control, según la siguiente combinación:

Control:	01
Administración:	00
Datos:	10
Reservado:	11

- Subtipo (*Subtype*): Indica la función de la trama.

Tabla. 2.5. Tramas de Administración

Type Value	Type Description	Subtype Value	Subtype Description
00	Management	0000	Association request
00	Management	0001	Assocation response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message
00	Management	1010	Dissociation
00	Management	1011	Authentication

Tabla. 2.6. Tramas de Control y Datos

Type Value	Type Description	Subtype Value	Subtype Description
01	Control	1010	Power save - poll
01	Control	1011	Request to send
01	Control	1100	Clear to send
01	Control	1101	Acknowledgment
01	Control	1110	Contention-free (CF)-end
01	Control	1111	CF-end + CF-ack
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-poll (no data)
10	Data	0111	CF-Ack + CF-poll (no data)

- Para DS (*To DS*): Indica (valor = 1) si la trama está destinada al sistema de distribución o no. En redes ad-hoc el valor de este campo es “0”. El caso más complejo contempla el envío entre dos estaciones a través del sistema de distribución, esto se lo realiza ubicando el valor de “1” tanto al campo Para DS como al siguiente campo De DS.

- De DS (*From DS*): Indica (valor = 1) si la trama fue enviada desde el DS.

- Más Fragmentos (*MF*): Se activa si se usa fragmentación, o si la información es un fragmento de una MSDU (*MAC Service Data Unit)*

- *Retry* (RT): Indica (valor = 1) si la trama es una retransmisión de la trama anterior.

- *Power Management* (PM): Indica el modo de administración de potencia del emisor.

Modo Ahorro de energía	1
Modo activo	0

- *More Data* (MD)*:* Indica si el emisor o un punto de acceso cualquiera tiene más datos para enviar.

- WEP: Indica si la trama ha sido procesada (valor = 1) con el algoritmo de autenticación y encriptación WEP.

- *Order* (O): Si el valor = 1 indica que el servicio de entrega está en un orden estricto. [20]

Duración / ID

En tramas de tipo PS o *Power–Save* para dispositivos con limitaciones de potencia, contiene el identificador o AID de estación. En el resto, se utiliza para indicar la duración del periodo que se ha reservado una estación o el tiempo en el cual se utilizará el canal.

Campos de Dirección

Contiene direcciones de 48 bits donde se incluirán las direcciones de la estación que transmite, la que recibe, el punto de acceso origen y el punto de acceso destino.

El estándar IEEE 802.11 establece una diferenciación entre fuente y transmisor *(source and transmitter)* y entre destino y receptor *(destination and receiver)*.

6	6	5	2	6
Dirección 1	Dirección 2	Dirección 3	Control de Secuencia	Dirección 4

Figura. 2.17. Campos de Dirección de la trama MAC

La Dirección 1 identifica al receptor de la trama.

La Dirección 2 identifica al transmisor de la trama.

Para una red de infraestructura, se puede modelar una red de la siguiente manera tal como se muestra en la Figura 2.16.

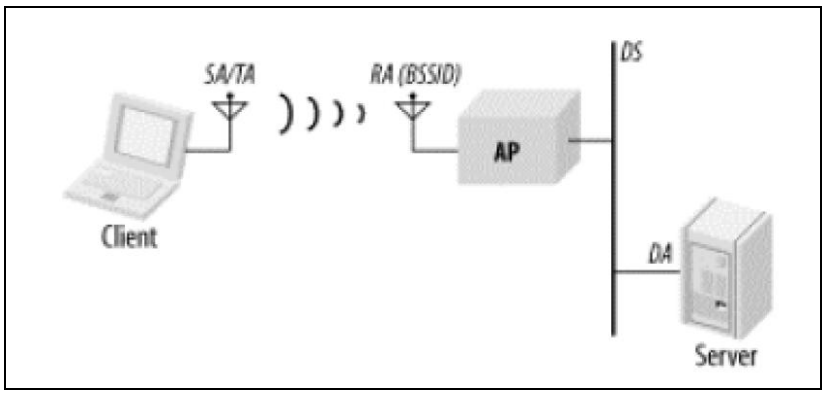


Figura. 2.18. Red de Infraestructura inalámbrica

Se puede apreciar una red en la que el cliente es a la vez fuente y transmisor (SA/TA, *Source Address / Transmitter Address*). El receptor de la trama radiada es el AP (*RA, Receiver Address* y usa el BSSID)

El AP es considerado solamente como un “destino intermedio”, el cual retransmite la información al DS (*Distribution System*) para que llegue al servidor. El destino final es el servidor (DA, *Destination Address*). [20]

Tabla. 2.7. Uso de los Campos de Dirección en las tramas de Datos

Función	ToDS	FromDS	Dirección1 (*RX*)	Dirección2 (*TX*)	Dirección3	Dirección4
IBSS	0	0	DA	SA	BSSID	No utiliza
To AP	1	0	BSSID	SA	DA	No utiliza
From AP	0	1	DA	BSSID	SA	No utiliza
WDS	1	1	RA	TA	DA	SA

Campos de Control de Secuencia

Contiene tanto el número de secuencia como el número de fragmento en la trama que se está enviando. Se utiliza para la desfragmentación y para descartar tramas duplicadas.

La composición del campo de control de secuencia es de la siguiente manera:

- 4 bits para indicar el número de fragmento usado en fragmentación y re-ensamblado.

- 12 bits para número de secuencia utilizado para numerar las tramas.

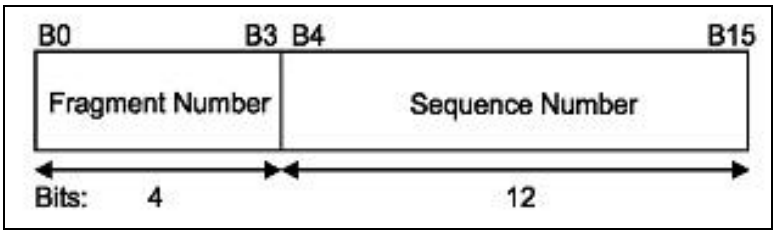


Figura. 2.19. Campos del Control de Secuencia

Cuando se recibe una trama, una estación puede filtrar tramas duplicadas monitoreando los números de frecuencia y de fragmentos, esto se puede evitar, especialmente en el control del número de secuencia ya que cuando se retransmite una trama, no se cambia el número de secuencia; la estación conoce si la trama está duplicada, si los números de fragmento y de secuencia son iguales a los de la última trama recibida (la inmediatamente anterior), o si el bit de *Retry* tiene el valor de “1”.

La duplicación de tramas puede ocurrir en los siguientes casos:

- Una estación recibe una trama sin errores y envía el ACK necesario.
- Ocurren errores de transmisión que destruyen la trama ACK en el camino.
- Al no recibir el ACK en un periodo de tiempo especificado, la estación transmisora retransmite la trama.

La estación destino envía un ACK de la trama retransmitida a pesar que la trama se descartó por filtrado de tramas duplicadas. [21]

Cuerpo de la Trama [22]

Varía según el tipo de trama que se quiere enviar. Contiene un MSDU o un fragmento de un MSDU (*MAC Service Data Unit*).

El MDSU puede ser un PDU de LLC (*Logical Link Control*) o información de control de la MAC, la cual cumple una función de segmentación y reensamblaje de tramas.

Para el funcionamiento con las Ethernet tradicionales, no tiene sentido la utilización de una WLAN que no sea capaz de manejar tramas de hasta 1518

bytes. Por otro lado, el medio físico de una WLAN es bastante propenso a errores, resulta conveniente manejar tramas más pequeñas para disminuir el efecto de las sucesivas retransmisiones.

Para evitar éste tipo de transmisiones, se procede a realizar una segmentación de la *"carga útil"* de una trama de nivel de enlace, en varios fragmentos más pequeños. Cada fragmento se compone de un encabezado de capa 2 y que debe ser confirmado positivamente para poder enviar el siguiente fragmento, mientras tanto en el receptor se lleva a cabo un proceso inverso y se vuelven a ensamblar los datos. El tamaño del campo de datos máximo es de 2304 bytes, pero las implementaciones deben soportar 2312 para acomodar el *overhead* de WEP

Control de secuencia de Trama (*Frame Control Sequence* – FCS) [23]

La cola de una trama 802.11 es el FCS *(Frame Control Sequence)* que es el CRC de grado 32, que corresponde al estándar IEEE CRC – 32.

Al igual que Ethernet y como ya se analizó previamente, 802.11 usa CSMA para lograr acceso al medio de transmisión. Las interfaces inalámbricas *(tranceivers)* normalmente son *half dúplex* y no se puede escuchar a la misma vez que se está transmitiendo, es decir no existe un control de detección de colisiones, hay que tener claro una idea importante que se debe tener en cuenta en 802.11 en la cual las colisiones no se detectan sino que se evitan.

2.7 ESTRUCTURA DE LAS TOPOLOGÍAS IEEE 802.11 [24]

Las topologías de red que definen el estándar IEEE 802.11 para una red inalámbrica son las siguientes:

- Ad-hoc

- De infraestructura

Red Ad hoc

Es una red compuesta de estaciones que se comunican mutuamente mientras se encuentren dentro de su rango de cobertura, sin la necesidad de un punto de acceso.

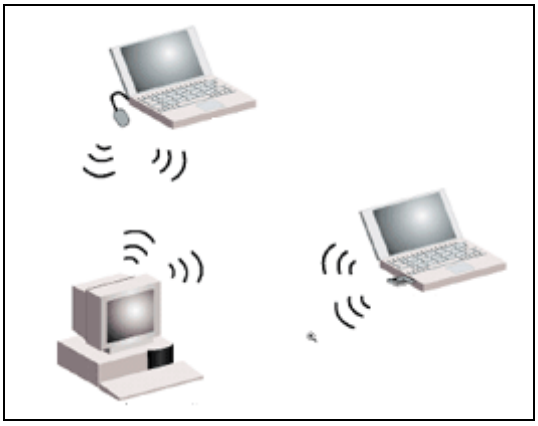


Figura. 2.20. Red Ad hoc

Ésta topología es de las más básicas del estándar IEEE 802.11, consiste en un grupo (mínimo 2) de estaciones que se pueden comunicar directamente entre sí, sin necesidad de ninguna infraestructura adicional. Éste tipo de redes son también conocidas como *"redes entre pares"*.

Éste tipo de red resulta ideal para conformar grupos de trabajo temporales en reuniones o conferencias.

Características:

- Transmisiones solo punto a punto.

- Fácil configuración.

- Conjunto de Servicio Básico Independiente (IBSS).

- No es necesario la utilización de Puntos de Acceso (AP)

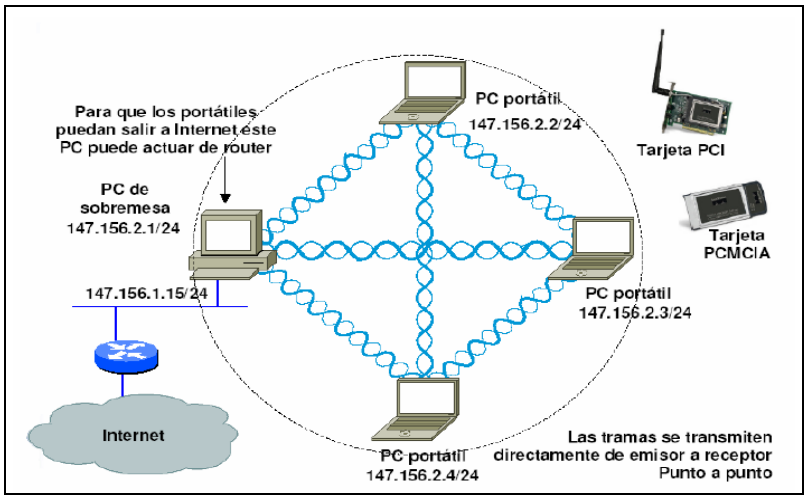


Figura. 2.21. Estructura y Funcionamiento de una red Ad hoc

Red de Infraestructura

Es una red que necesita de un punto de acceso para que todas las estaciones de la red se puedan comunicar. Para la comunicación entre dos estaciones, el punto de acceso recibe los datos de la estación transmisora y los envía a la estación de destino.

Como ventajas de este tipo de red se tiene que el área de cobertura está definida por el punto de acceso, es decir será toda el área dentro de la que una estación pueda mantener comunicación con el punto de acceso. Se puede tener un modo de ahorro de energía para las estaciones cuando no mantengan una comunicación, ya que el punto de acceso puede indicarles cuándo entrar o salir de este estado.

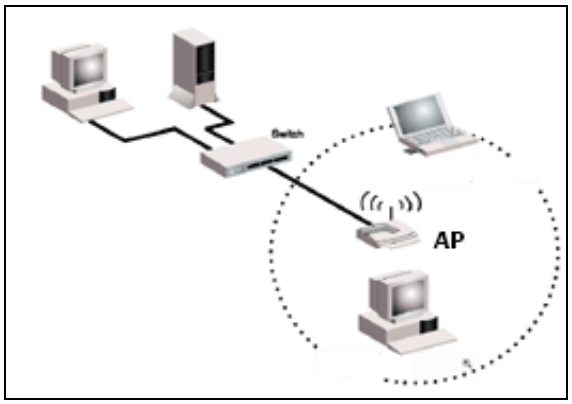


Figura. 2.22. Red de Infraestructura

Éste tipo de configuración es la más implementada en la actualidad, las WLAN se utilizan como una extensión a la infraestructura de red LAN que cuenta con la organización donde se instala la red.

Es frecuente que los nodos inalámbricos, a los cuales se les suele denominar estaciones remotas, actúen como clientes que solicitan servicios e información a servidores generalmente conectados a esa infraestructura cableada de red, a través de puntos de acceso llamados estaciones base.

Características:

- Es la red más común y más utilizada en la actualidad.
- Posibilidad de diseño a múltiples celdas.
- Cada celda opera sobre su propio canal.
- El sistema de distribución es usualmente la red cableada.
- Utiliza un dispositivo llamado *Access Point* (AP)

- La comunicación entre dos estaciones dentro de una misma área de servicios necesita dos saltos.

- El BSS se define por la distancia al AP.

- El AP está en condiciones de asistir a las estaciones móviles frente a problemas de energía.

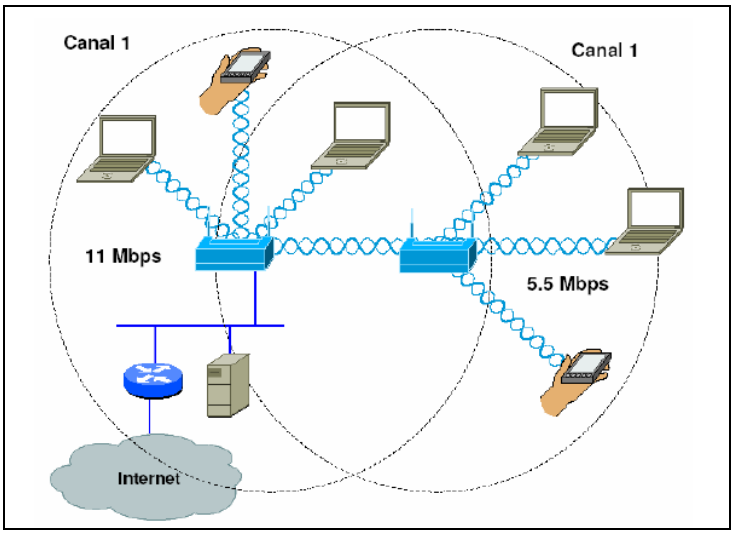


Figura. 2.23. Estructura de una Red tipo Infraestructura

Componentes de la Red:

Una red IEEE 802.11 está formada por los siguientes elementos:

- Medio Inalámbrico (*Wireless Medium* – WM): Es el medio utilizado para implementar una red inalámbrica.

- Estación (STA): Es el dispositivo que tiene una interfaz de red inalámbrica a través de la cual se accede a la red.

- Conjunto de Servicios Básicos (*Basic Service Set* – BSS): Es el bloque básico de construcción de una red LAN IEEE 802.11 y está formado

por un conjunto de estaciones controladas por una función de coordinación. Toda estación podrá comunicarse con los demás miembros del BSS mientras se encuentre dentro del mismo.

- Conjunto de Servicios Básicos Independiente (*Independent Basic Service Set* – IBSS): Es un BSS que no tiene relación con otros BSSs y las estaciones que lo componen se comunican directamente *(Ad hoc).*

- Área de Servicios Básicos (*Basic Service Area* – BSA): Es el área de cobertura de una BSS.

- Sistema de Distribución (*Distribution System* – DS): Sistema utilizado para interconectar múltiples BSSs e integrar otras redes de área local.

- Punto de Acceso (*Access Point* – AP): Es el dispositivo que permite la integración entre BSSs y el acceso a los servicios distribuidos.

- Portal: Es el punto de integración lógica entre una red LAN cableada y una red IEEE 802.11 para acceso a Internet. En la actualidad es muy común tener un solo dispositivo que actué como portal y punto de acceso a la vez.

- Conjunto de Servicios Extendidos (*Extended Service Set* – ESS): Es un conjunto de uno o varios BSSs y redes de área local integradas que aparecen como un BSS para la capa de control de enlace lógico (LLC) en una estación que se encuentre en un BSS asociado.

Servicios:

El estándar IEEE 802.11 no especifica la implementación del Sistema de Distribución, indica el conjunto de servicios que debe prestar y son utilizados por la subcapa MAC.

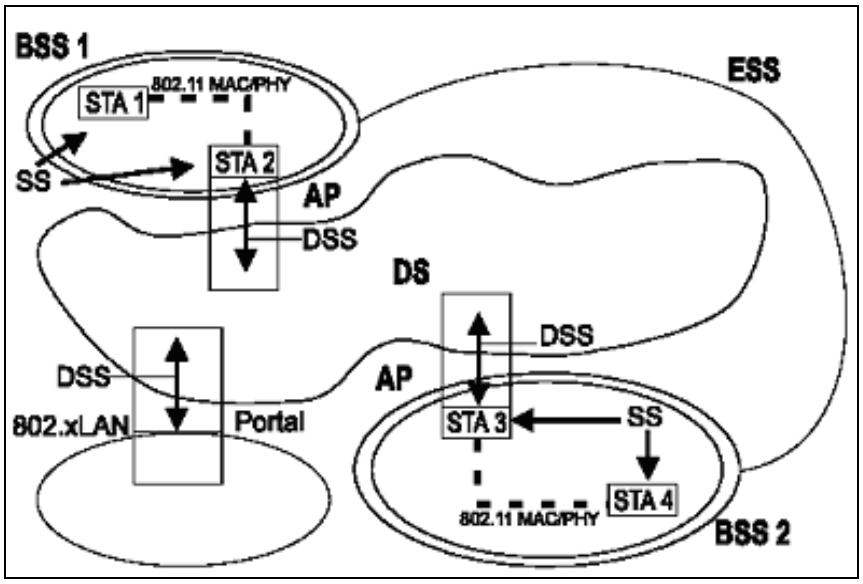


Figura. 2.24. Componentes de la arquitectura IEEE 802.11

Los servicios especificados bajo el estándar IEEE 802.11 se dividen en dos grupos:

- Servicios de Estación (SS)
- Servicios del Sistema de Distribución (DSS)

Servicios de Estación (*Station Service* – SS)

Éste tipo de servicios son aquellos provistos por las estaciones, incluyendo los APs. Estas estaciones adicionalmente soportan el transporte de MSDUs (*MAC Service Data Unit)* dentro de un BSS.

Los Servicios de Estación están divididos por:

- Autenticación: Utilizado para la identificación y autorización de las estaciones a la red inalámbrica.

- Desautenticación: Es utilizado para terminar una relación de autenticación.

- Privacidad: Es utilizado para asegurar y garantizar la confidencialidad de los datos transmitidos.

- Entrega de MSDU: Es utilizado para la entrega de los paquetes fragmentados y ensamblados desde la capa LLC hacia la capa física.

Servicios del Sistema de Distribución (DSS)

Son servicios provistos por el punto de acceso y utilizados para superar las limitaciones lógicas ofrecidas por el medio y el espacio de direcciones cuando la estación entra y sale del área de cobertura.

Los Servicios del Sistema de Distribución son los que se presentan a continuación:

- Asociación: Es utilizado para la asignación de una estación a un BSS. La estación realiza la petición y el punto de acceso puede aceptar o rechazar la solicitud. Una estación puede estar asociada solamente hacia un punto de acceso a la vez.

- Disociación: Es utilizado para terminar una asociación, eliminando la asignación de un BSS a una estación (en un ESS se indica al DS borrar toda la información existente de la asociación)

- Distribución: Permite la comunicación de datos entre estaciones de BSSs conectadas al mismo DS.

- Integración: Permite el intercambio de información entre la red IEEE 802.11 y otras redes que no pertenezcan al estándar IEEE 802.11 conectadas.

- Reasociación: Permite a las estaciones el cambio de un punto de acceso a otro, o del BSS asignado a otro.

Analizando los servicios citados previamente, se puede definir que una estación puede encontrarse en uno de tres estados posibles de acuerdo a los servicios de autenticación y asociación:

- No autenticado, no asociado: Esto significa que la estación está fuera de la red.

- Autenticado, no asociado: Significa que la estación está autenticada, pero la estación no puede intercambiar datos con la red.

- Autenticado, asociado: En éste punto la estación se encuentra en la red y es reconocida, además es capaz de enviar y recibir datos.

2.8 MODELOS DE PROPAGACIÓN EN NS-3

El Simulador *ns-3* tiene la capacidad de manejar diferentes modelos de propagación, que le permiten determinar el nivel de energía o potencia de recepción de la señal de un paquete en la capa física del receptor inalámbrico.

Dentro del simulador cada capa física de los diferentes nodos inalámbricos que forman parte de la infraestructura de la red tiene una variable que corresponde al umbral de energía con el que debe ser recibida una señal. Cuando la señal posee una potencia por debajo de los niveles determinados bajo dicho umbral, se considera una transmisión errónea, a lo cual la capa física envía esta

información a la capa MAC reportando el error y procediendo al inmediato descarte del paquete. [25]

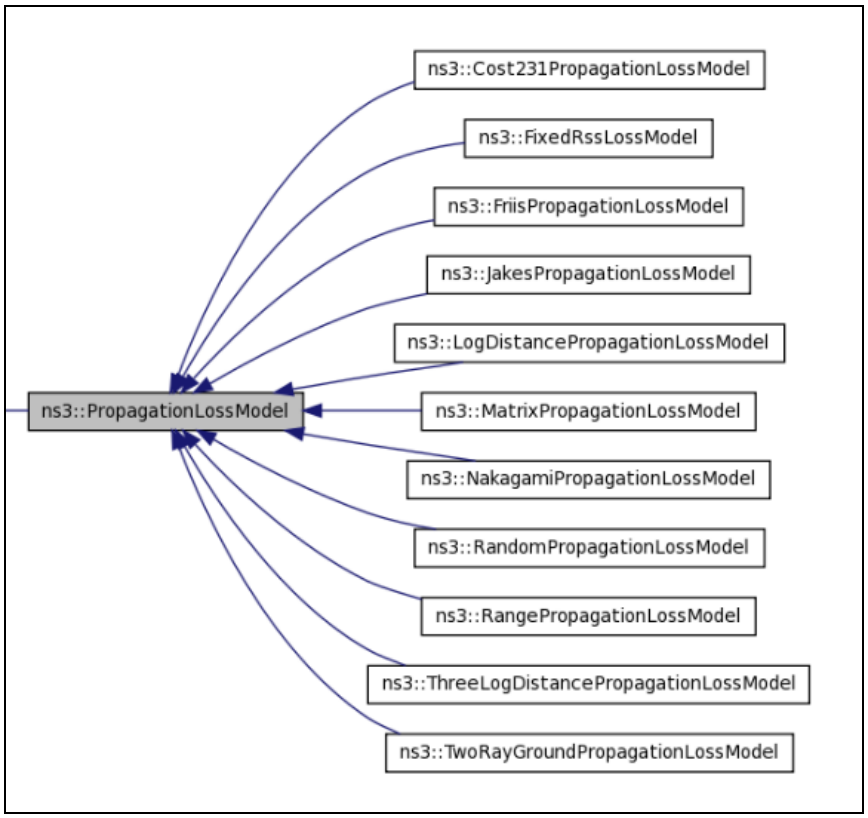


Figura. 2.25. Modelos de Propagación disponibles en *ns-3*

Bajo el estándar IEEE 802.11 que maneja el simulador *ns-3* existen varios modelos de propagación que se puede implementar y son los siguientes:

- *Free Space*
- *Two – Ray Ground Reflection*
- *Shadowing*
- *Nakagami – Rice*
- *Rayleigh*

- *Friis*
- *LogDistance*
- *FixedRss*
- *Random*

Los tres primeros son muy utilizados en el *Network Simulator 2*, adicionalmente hay que tener en cuenta el papel tan importante que manejarán las clases: *PropagationDelayModel* y *PropagationLossModel*, ambas para la configuración del canal Wifi que se aplicará durante las posteriores simulaciones.

2.8.1 Modelo de Propagación Nakagami

Este modelo de propagación describe situaciones típicas encontradas en entornos de comunicaciones inalámbricas, especialmente y más estudiadas aún en comunicaciones móviles. También conocida como distribución de Nakagami – Rice, es utilizada para analizar variaciones de la intensidad de campo de una señal formada por una componente determinista y varias aleatorias.

Éste modelo es utilizado tanto para situaciones multitrayecto LOS y NLOS, en el cual a un punto de acceso pueden llegar múltiples señales, una de las cuales tiene un valor fijo y claro por existir visión directa entre el transmisor y el receptor y otras consecuencias del multitrayecto existente.

La función densidad de probabilidad, ecuación 2.1, para ésta situación, siendo r la representación de la tensión será: [25]

$$f(r) = \frac{r}{b} e^{\left[\frac{(r^2+c^2)}{2b}\right]} I_0\left(\frac{cr}{b}\right) \qquad (2.1)$$

Siendo;

- 2b, el valor cuadrático medio de la componente aleatoria de la señal multitrayecto.

- c, es el valor eficaz de la señal directa LOS.

- I_0, es la función de Bessel modificada de primera especie y orden 0.

Existen ocasiones en las que se expresa la distribución como función de un parámetro, el parámetro k representado en la fórmula 2.2

$$k = c^2/2b \qquad (2.2)$$

- Si c = 0, resulta la típica función de Rayleigh.

- Si c >> $\sqrt{b}$, resulta una distribución gaussiana con media de la variable r; $\bar{r} = c$, y desviación típica $\sigma = \sqrt{b}$

$$f(r) = \frac{1}{\sqrt{2\pi}\sqrt{b}} e^{\left[\frac{(r-c)^2}{2b}\right]} \sqrt{\frac{r}{c}} \qquad (2.3)$$

La distribución de Nakagami – Rice es más general que la gaussiana o la de *Rayleigh* por separado, en tanto que puede convertirse en cualquiera de ellas con una adecuada configuración de los parámetros.

Como se analizó anteriormente, éste modelo ha sido utilizado para describir las propiedades estadísticas de un canal inalámbrico, que desde que la señal se propaga, se ve afectada específicamente por tres fenómenos estadísticamente independientes: pérdida determinista en el trayecto, decremento log-normal y rápido desvanecimiento multitrayecto. Luego de haber realizado estudios con éste modelo, el mismo ha sido descartado porque tomaba como referencia dos distancias y no tenía en cuenta la intensidad de la señal recibida. [25]

2.8.2 Modelo de Propagación Rayleigh

Es utilizada para describir la variación estadística de la envolvente de la señal resultante de la propagación multitrayecto, por superposición de señales de parecida amplitud y fase aleatoria, generadas en el caso de un entorno próximo al punto de acceso.

Si r, es una envolvente o amplitud en unidades naturales, la función densidad de probabilidad está definida por:

$$f(r) = 1.386\ \frac{r}{\hat{r}^2} e^{\left[-0.693\left(\frac{r_u}{\hat{r}}\right)^2\right]} = \int_{r_u}^{\infty} p(r)dr \qquad (2.4)$$

Se ha comprobado que este modelo de propagación representa de buena manera la condición en que no existe una componente dominante en la señal, lo que físicamente ocurre por lo general para terminales móviles en condiciones donde no existe línea de vista.

Al existir una componente dominante estacionaria (sin *fades*), como una trayectoria LOS, las componentes multitrayecto arriban en diferentes ángulos y se superponen a la señal dominante. Esto da lugar a una distribución de Rice. Si la señal tiende a cero, la distribución Rice degenera a una distribución Rayleigh. [25]

2.8.3 Modelo de Propagación Friis

Este es un modelo bastante sencillo, se deduce de las ecuaciones de Maxwell y permite calcular la potencia recibida a cierta distancia en condiciones ideales, es decir sin obstáculos de ninguna naturaleza. Es más conocido como un modelo en el que existe línea de vista *(line of sight – LOS)* entre el transmisor (Tx) y el receptor (Rx).

Como se indicó anteriormente, es un modelo que predice la potencia en función de la distancia entre el Tx y el Rx de acuerdo a la ecuación de Friis:

$$P_r(d) = \frac{P_t G_t G_r}{L}\left(\frac{\lambda}{4\pi d}\right)^2 \quad (2.5)$$

Siendo;

- P_t, el valor de la potencia transmitida.
- $P_r(d)$, el valor de la potencia recibida.
- G_t, la ganancia de la antena de transmisión.
- G_r, la ganancia de la antena de recepción.
- d, la distancia de separación entre Tx y Rx.
- L, las pérdidas del sistema no relacionadas a la propagación.
- λ, es la longitud de onda de la señal electromagnética.

2.8.4 Modelo de Propagación LogDistance

Éste es un modelo que permite calcular la intensidad de la señal recibida por cada antena utilizando el modelo *log – distance.* Para calcular la intensidad de la señal se utiliza la siguiente ecuación: [25]

$$L = L_0 + 10.n.log_{10}\frac{d}{d_0} \quad (2.6)$$

Donde;

- L_0, distancia de referencia (m).
- n, exponente de pérdida en la trayectoria.
- d, distancia entre las antenas (m)
- d_0, distancia de referencia de la antena (m)
- L, pérdida en la trayectoria.

Para utilizar este modelo es necesario estimar o calcular los valores de las variables y adaptarlo al banco de pruebas real.

Rappaport [21] entrega una tabla de valores estándar para el valor de n, en la siguiente tabla se especifica los valores más típicos.

Tabla. 2.8. Exponente de pérdidas para diferentes ambientes

Ambiente	Exponente de pérdidas, n
Espacio Libre	2
Área Urbana	2.7 a 3.5
Área Nublosa	3 a 5
En edificios con línea de vista	1.6 a 1.8
Obstruido por edificios	4 a 6
Obstruido por fábricas	2 a 3

2.8.5 Modelo de Propagación FixedRss

Con este modelo se puede modelar el fenómeno de la pérdida en la propagación, configurando la intensidad de la señal recibida (RSS, medida en dBm). Ha sido un modelo descartado, debido a que no se tomaba en cuenta la distancia entre nodos.

2.8.6 Modelo de Propagación Random

Éste modelo es utilizado cuando un parámetro se introduce dentro de un rango con valores específicos. Éste modelo no es muy utilizado cuando se utilizan variaciones de distancia, debido a que generalmente los nodos son estáticos y para éste tipo de redes se puede considerar un modelo ideal. Otro parámetro importante en el cual se utiliza éste modelo, es para la variación de la intensidad de la señal recibida.

2.9 PARÁMETROS DE DESEMPEÑO [26]

Para realizar el análisis de una red inalámbrica se debe tomar en cuenta ciertos parámetros que influyen directamente en el comportamiento y confiabilidad de las redes inalámbricas. Dichos parámetros se definen a continuación.

Throughput

Éste parámetro de desempeño bajo las redes de todo tipo es de gran importancia y permite llegar a conclusiones bastante reales tanto teóricas como prácticas. El *throughput* es considerado como el volumen de información que se transmite a través de un sistema, o que fluye sobre una red de datos. Ésta es una opción muy utilizada cuando se desea recuperar o almacenar información en sistemas en los cuales el rendimiento es medido en unidades como accesos por hora, o paquetes de datos por segundo.

El *throughput* puede ser calculado para un solo nodo, o para toda la red. La fórmula para el cálculo de éste parámetro es la siguiente:

$$Throughput\ de\ Red = \frac{Bytes\ totales\ transmitidos}{Tiempo\ de\ transmisión\ (seg)} \qquad (2.7)$$

Retardo de Extremo a Extremo ó *Delay*

Éste retardo es la representación del tiempo que transcurre desde que un paquete sale del nodo origen hasta que alcanza el nodo de destino. Éste parámetro es utilizado para realizar una medición de métrica para determinar el funcionamiento de la red y determinar si la red implementada se encuentra en condiciones aceptables de operación. La forma para calcular el tiempo promedio del retardo es la siguiente:

$$Promedio\ de\ Retardo = \frac{Suma\ de\ retardos\ de\ todos\ los\ paquetes}{Total\ de\ paquetes\ recibidos} \qquad (2.8)$$

Relación de Entrega *(Delivery Ratio)*

Éste parámetro indica el porcentaje de los paquetes que han sido recibidos con éxito, permitiendo obtener una perspectiva del congestionamiento presente en la red. La relación de entrega es muy importante ya que es un indicador que permite analizar el desempeño de los paquetes en un tiempo determinado. La siguiente fórmula permite calcular éste parámetro:

$$Relación\ de\ Entrega = \frac{Número\ de\ paquetes\ recibidos}{Total\ de\ paquetes\ transmitidos} x100 \qquad (2.9)$$

CAPÍTULO 3

MÉTODOS Y APLICACIONES

Con la utilización de un simulador de redes que maneja modelos físicos de propagación, una amplia gama de tipos de enrutamiento de datos, protocolos de comunicaciones, animación de eventos y simulaciones, etc., es indispensable una herramienta de tales características y capacidades para poder realizar diseños de redes inalámbricas que se acercan a la realidad.

Éste proyecto ha seguido la siguiente metodología de trabajo:

En una primera etapa, se ha realizado un repaso teórico del simulador que será utilizado para realizar el diseño de las redes inalámbricas propuestas, así como una revisión al estándar IEEE 802.11 para entender de una mejor manera su funcionamiento, capacidades y limitaciones en una red dependiendo de su configuración y disposición de elementos correspondientes a la red inalámbrica.

Acto seguido, se plantea un primer escenario que será el primer paso para posteriormente complementar ésta primera red realizando variaciones en sus parámetros de diseño y de funcionamiento.

La siguiente etapa es realizar un escenario más complejo que permita trabajar redes con el simulador de eventos discretos en el cual, con tan solo unas pequeñas modificaciones sobre un script principal comenzar un análisis de funcionamiento y desempeño de la red implementada en el simulador.

Existe una base importante para el simulador de red que se debe tomar muy en cuenta al momento de llegar a implementar una red, se puede tomar el siguiente procedimiento para empezar a realizar una simulación, independientemente del simulador que se esté utilizando:

- Creación y colocación de los nodos.
- Instalación de las interfaces WiFi, adoptando los parámetros necesarios para su operación, incluso a largas distancias si fuera el caso.
- Instalación de pilas de protocolos.
- Generación de tablas de enrutamiento.
- Instalación de un sistema de monitorización de tráfico en todos los nodos.
- Creación de flujos de tráfico.
- Ejecución de la simulación.
- Muestra de presentaciones de la red.

Éste último punto, es quizás el más importante a nivel de análisis de desempeño de la red, ya que la generación de resultados gráficos permite al usuario obtener una gran cantidad de información que permitirá mejorar y garantizar el funcionamiento de la red en base a los parámetros más importantes durante el análisis, tales como el throughput y el retardo, siendo los más destacables.

3.1 INTRODUCCIÓN AL DISEÑO DE REDES INALÁMBRICAS WIFI IEEE 802.11

3.1.1 Consideraciones para la Red Inalámbrica

Para el proceso de simulación y utilización de la herramienta de simulación ns-3 se va a simular redes inalámbricas utilizando el estándar IEEE 802.11, considerando los estándares y variaciones que dicho estándar presenta y pueden ser simulados e interpretados por el software ns.3.

Para el análisis de resultados se medirá el desempeño de la red en función del throughput y del delay que se podrá obtener mediante gráficas y con la utilización del analizador de protocolos Wireshark.

Para la simulación de una red inalámbrica bajo un script desarrollado en texto plano se debe considerar, en primer lugar la definición de variables globales que intervienen en el proceso de simulación y que podrán ser utilizados en cualquier momento de la simulación, además son los más importantes debido a su funcionalidad y facilidad de manejo de objetos.

En el diseño de las redes inalámbricas se debe tomar en cuenta varios parámetros como son:

- Elementos constituyentes de la topología

.

- Estándar inalámbrico

.

- Modelos de Propagación
- Tasas y Frecuencias de transmisión.
- Distancias entre nodos, tanto móviles como estáticos.
- Tráfico de datos generado durante la simulación.

Todos estos parámetros son configurables desde el código fuente de cada simulación que se plantee, incluso la herramienta ns-3 presenta una gran cantidad de aplicaciones y variaciones en todos estos parámetros, es así que se puede variar tanto el modelo de propagación, los protocolos de enrutamiento, la posición de los nodos, etc., todo esto de acuerdo al tipo de red que se implemente. [26]

3.2 ESCENARIOS DE SIMULACIÓN

3.2.1 Parámetros y criterios de diseño

Para el diseño de las redes inalámbricas que se pretende analizar se tomará en cuenta los siguientes parámetros de simulación:

- Nodos estáticos y móviles.
- Estándar Inalámbrico para IEEE 802.11
- Modelo de propagación
- Tasa de transmisión
- Frecuencia de transmisión
- Distancia entre nodos (mínima y máxima)
- Tráfico utilizado
- Tiempo total de simulación
- Número de paquetes transmitidos
- Tamaño de paquetes transmitidos
- Intensidad de señal (Transmitida y Recibida)
- Direccionamiento IPV4

Nodos Estáticos y Móviles

La movilidad en una topología inalámbrica, y en este caso en una red *Wireless*, es tan importante ya que éstas proporcionan las facilidades que no se disponen en redes cableadas, una de ellas, la movilidad sin perder conectividad. Así mismo los sistemas inalámbricos que presentan nodos estáticos representan gran importancia, en especial cuando se requiere ubicar un nodo estático en el cual su instalación cableada es de difícil implementación.

Dentro del script a realizar en el simulador *ns-3* se debe importar los módulos de Wifi así como los de movilidad para su correcto funcionamiento bajo el estándar IEEE 802.11. Dichos módulos son los siguientes:

```
#include “ns3/wifi-module.h”
#include “ns3/mobility-module.h”
```

Estándar Inalámbrico para IEEE 802.11 [27]

Este es un parámetro, quizás el más importante dentro de la diferenciación de todos los tipos de simulaciones que puede realizar el simulador *ns-3.* En el siguiente campo del script se identifica el estándar que se va a utilizar, en el caso de este proyecto se identificará los siguientes tipos de estándares con las características presentadas en la siguiente tabla:

Tabla. 3.1. Estándares IEEE 802.11 soportados en *ns-3*

NOMBRE DEL ESTÁNDAR	BANDA DE FRECUENCIA	TASA DE TRANSMISIÓN	MODULACIÓN
IEEE 802.11	2.4GHz	1 – 2 Mbps	DSSS
IEEE 802.11a	5.8GHz	6 – 54 Mbps	HR – DSSS
IEEE 802.11b	2.4 GHz	2 – 11 Mbps	OFDM
IEEE 802.11g	2.4 GHz	Hasta 54 Mbps	DSSS - OFMD

Para la definición del estándar inalámbrico se requiere configurar el módulo *Wifi* para diferenciar entre los tipos de estándar que define el IEEE 802.11, para lo cual:

```
WifiHelper wifi;
 if (verbose)
  {
    wifi.EnableLogComponents ();
  }
 wifi.SetStandard (WIFI_PHY_STANDARD_80211b);
```

En el código anterior, se requiere una explicación adicional, especialmente sobre variables y comandos utilizados para comprender el funcionamiento de las mismas.

La variable *verbose*, es una variable lógica o *booleana* la cual representa valores que normalmente representan falso o verdadero. Para el presente caso, *verbose* ha sido determinado con un valor de *false*, el mismo que si llega a cumplir la condición que se indica, presentará un reporte de fallo o error.

Se especifica el estándar a ser utilizado, se configura simplemente con el comando indicado anteriormente. Este comando es muy importante ya que la variación del mismo implica mayor o menor rendimiento de la red, de acuerdo a las características que presenta cada uno de los estándares.

Modelo de Propagación

Un modelo de propagación no es más que una predicción de las pérdidas de potencia (expresada en decibeles) en ambientes simulados. Existen modelos que se utilizan en la práctica y/o en la teoría, debido a que pueden ser utilizados en modelos más complejos.

Para la programación de este parámetro se debe primero especificar y llamar a la clase *ns3:: YansWifiPhyHelper* el mismo que se origina del núcleo de

simulación conocido como *yans (Yet Another Network Simulator)*. A continuación se detalla el método correcto que se debe seguir para configurar el modelo de propagación en la simulación.

```
1 YansWifiPhyHelper wifiPhy =  YansWifiPhyHelper::Default ();
2 wifiPhy.Set ("RxGain", DoubleValue (0));
3 wifiPhy.SetPcapDataLinkType
(YansWifiPhyHelper::DLT_IEEE802_11_RADIO);
4 YansWifiChannelHelper wifiChannel ;
5 wifiChannel.SetPropagationDelay
  ("ns3::ConstantSpeedPropagationDelayModel");
6 wifiChannel.AddPropagationLoss
 "ns3::FixedRssLossModel","Rss",DoubleValue(rss));
7 wifiPhy.SetChannel (wifiChannel.Create ());
```

En la línea número 2 del *script* se puede visualizar la configuración para la ganancia de recepción la cual se ubica en un valor de 0. Este valor es importante ya que si no se determina dicha valor se debe tomar en cuenta un aumento en la ganancia de recepción.

El simulador *ns-3* es compatible con extensiones .pcap, lo cual hace que la captura de datos y protocolos de comunicación sean más fáciles a la hora de interpretar este tipo de datos utilizando programas especializados en la lectura de los mismos, uno de ellos es Wireshark. En la línea 3 del *script,* se observa el parámetro que el auxiliar de *yans* utiliza para la configuración de este tipo de enlaces. Además existen dos variaciones para éste *helper* que son los siguientes:

- DLT_IEEE802_11.- Que muestra cabeceras y paquetes inalámbricos del estándar IEEE 802.11

- DLT_PRISM_HEADER.- Incluye información en modo monitor de *Prism*, la misma que no es muy completa respecto a la información que presenta *Radiotap.*

En las siguientes líneas del script simplemente se configura el parámetro de intensidad de señal recibida (rss) la misma que es independiente de la distancia y la potencia de transmisión. El valor que toma es el valor indicado previamente en la declaración de la variable rss.

Tasa y Frecuencia de Transmisión

La tasa y frecuencia de transmisión está dada por el tipo de estándar que se configura al momento de elegir el estándar inalámbrico que se va a utilizar para la simulación. Estos valores vienen definidos en la Tabla 3.1 en donde se especifican todos los estándares aplicables en el simulador ns-3. Adicionalmente el enfoque también es relacionado en la capa MAC, en donde se debe escoger un sistema sin *QoS* para lo cual utilizamos el objeto *NqosWifiMacHelper*, en éste configuramos los parámetros de la MAC de la siguiente manera:

```
WifiHelper wifi = WifiHelper::Default ();
wifi.SetRemoteStationManager ("ns3::AarfWifiManager");
NqosWifiMacHelper mac = NqosWifiMacHelper::Default ();
```

En éste se elige el algoritmo de control de tasa de transmisión, para el caso se ha elegido el modo *"ns3::AarfWifiManager"*, existen más algoritmos de control y son los siguientes:

- *ns3::AarfWifiManager*
- *ns3::AmrrWifiManager*
- *ns3::ArfWifiManager*
- *ns3::CaraWifiManager*
- *ns3::RraaWifiManager*
- *ns3::IdealWifiManager*

- *ns3::AarfWifiManager*

- *ns3::OnoeWifiManager*

Todos los algoritmos listados anteriormente son utilizados en la implementación de control de tasas de transmisión, las mismas que permiten incrementar o disminuir el *throughput* cuando las condiciones del canal cambian de acuerdo a la variación de las tasas de datos. Los más utilizados y que dan mejores resultados en la práctica son los siguientes:

- **Algoritmo ARF *(Auto Rate Fallback)***

  El transmisor usa un histórico de transmisiones realizadas y tasas de error para seleccionar futuras tasas de transmisión.

  - Si no existen errores, incrementa la tasa de datos.

  - Si existen errores, reduce la tasa de datos.

  Por ejemplo, si dos tramas ACK consecutivas no son recibidas correctamente, los siguientes intentos se realizarán con una menor tasa y se activa un contador. Cuando el número de tramas ACKs recibidas correctamente alcanza a 10 o el contador se desactiva, una trama de prueba es enviada con una tasa superior a la anterior. Sin embargo si un ACK no es recibido con esa trama, la tasa vuelve a reducirse y el temporizador se reinicia.

- **Algoritmo AARF *(Adaptative ARF)***

  Para evitar el escenario descrito anteriormente, AARF aumenta el umbral para decidir si aumenta la tasa actual de 10 a 40 u 80.

  Cuando el paquete de prueba falla, cambia inmediatamente a una tasa más baja, pero también se multiplica por dos el número de

transmisiones consecutivas exitosas para cambiar a una tasa más alta. [28]

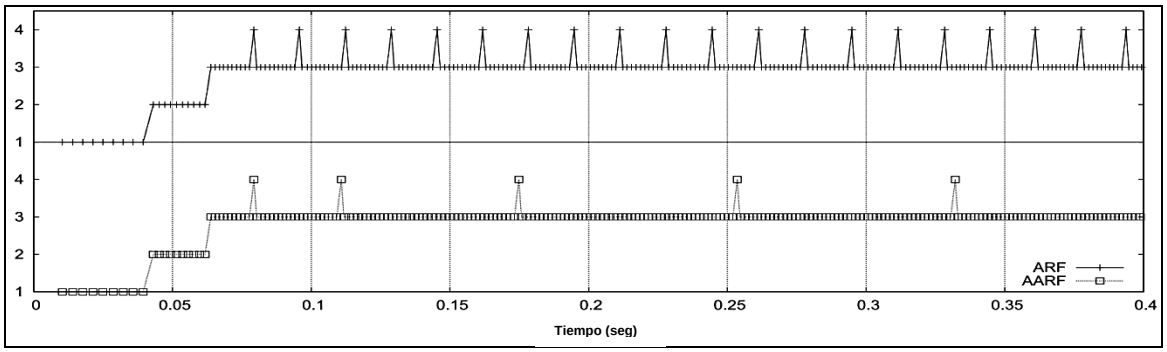


Figura. 3.1. Comparación entre los algoritmos ARF y AARF

- **Algoritmo CARA *(Collision Aware Rate Adaptation)***

Se caracteriza por ser un algoritmo en el cual las tramas de datos son transmitidas sin RTS/CTS, si la transmisión falla, RTS/CTS se activará para la siguiente retransmisión. En caso de que ésta retransmisión falle, la tasa es reducida. Si después ésta retransmisión es exitosa, mantiene la misma tasa y la siguiente trama la envía sin RTS/CTS.

- **Algoritmo RRAA *(Robust Rate Adaptation Algorithm)***

Mejora el rendimiento del *throughput* tomando en cuenta los siguientes componentes o factores en su funcionamiento:

1. Estimación de pérdidas.

   En lugar de una trama de prueba simple, RRAA usa una ventana de pérdidas la cual calcula la tasa de pérdida estimada por la ventana.

   Utiliza un umbral de pérdida superior e inferior para cada tasa y la tasa de pérdida estimada para decidir cuándo realizar el cambio de valor de tasa.

Tabla. 3.2. Implementación de RRAA con parámetros para IEEE 802.11ª

Tasa (Mbps)	Tasa de Pérdida Crítica (%)	P_{ORI}	P_{MTL}	Ewnd
6	N/A	50.00	N/A	6
9	31.45	14.34	39.32	10
12	22.94	18.61	28.68	20
18	29.78	13.25	37.22	20
24	21.20	16.81	26.50	40
36	26.90	11.50	33.63	40
48	18.40	4.70	23.00	40
54	7.52	N/A	9.40	40

En la tabla anterior, se especifica los valores de tasas predeterminadas de transmisión para el estándar IEEE 802.11a, los cuales pueden variar de acuerdo al estándar.

Aquí podemos observar los valores de tasa de transmisión en la primera columna, el porcentaje de tasa de pérdida crítica, el umbral máximo tolerable de pérdida (P_{MTL}), el umbral de aumento de tasa (P_{ORI}) y el tamaño de estimación de la ventana (Ewnd). Todos estos valores se encuentran tabulados y se requiere de cálculos previos para obtener los valores que se relacionan con dicha tabla.

2. Filtro Adaptativo RTS.

Este filtro realiza un uso selectivo de RTS/CTS, esto permite suprimir pérdidas en colisiones cuando se estima la tasa de pérdida.

Existe una ventana RTS (RTSwnd) la cual se incrementa en una unidad cuando la última trama se ha perdido sin utilizar RTS (lo más probable es que sucedió una colisión durante la transmisión)

Cuando la última trama se perdió y se utilizó RTS o cuando tuvo éxito sin utilizar RTS, la ventana RTS se reduce a la mitad, sin asumir ninguna colisión durante la transmisión. [28]

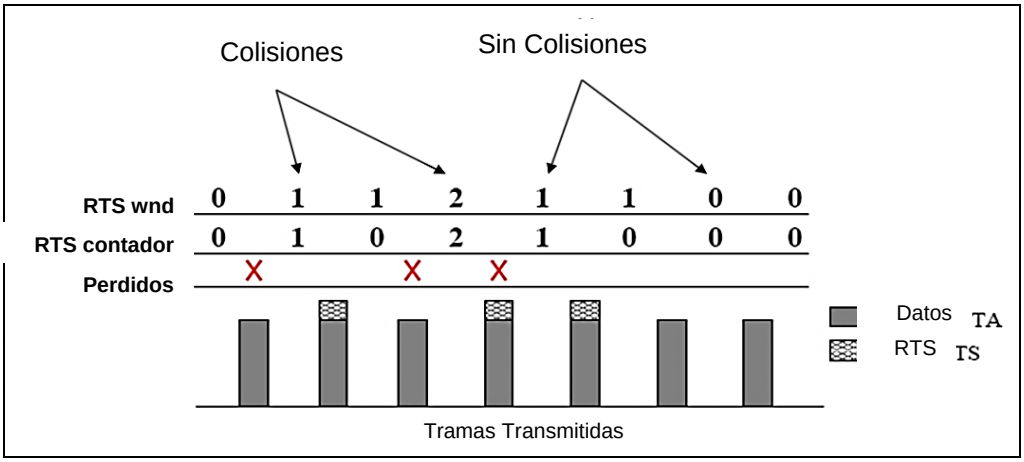


Figura. 3.2. Funcionamiento del Filtro Adaptativo RTS

- **Algoritmo RBAR (*Received – Based AutoRate*)**

El algoritmo RBAR escoge la tasa basándose en las medidas del SNR obtenidas en el receptor. Básicamente se centra en la medida de la calidad del canal desde el receptor para determinar si un paquete puede ser recibido. Cuando a un receptor le llega un paquete RTS (*Request To Send*), este calcula la máxima velocidad basándose en el nivel de señal medido y en rangos de SNR establecidos a priori con un modelo de canal. El receptor responde con un paquete CTS a la tasa calculada, y el emisor utilizará esta tasa para enviar los paquetes de datos.

RBAR fue diseñado para trabajar bien en entornos móviles donde las condiciones del canal cambian en el periodo de tiempo de envío de un paquete. RBAR supone que el dispositivo del receptor está preparado para poder calcular la mejor tasa de transmisión a partir del SNR de un paquete RTS.

Con este sistema surgen algunos inconvenientes, en primer lugar, se requiere un conocimiento previo del modelo del canal para calcular los valores del SNR, que no es trivial. En segundo lugar, se necesitan receptores que puedan medir el SNR, requerimiento difícil si queremos que los dispositivos de una WLAN sean de bajo coste. Finalmente, el algoritmo de adaptación de la tasa, no contempla los errores producidos por colisiones.

A continuación en el script se configura el tipo de MAC, el SSID de la infraestructura de la red se configura en las estaciones Wifi, tal como se indica en las siguientes líneas de código:

```
Ssid ssid = Ssid ("ns-3-ssid");
mac.SetType ("ns3::StaWifiMac",
                "Ssid", SsidValue (ssid),
                 "ActiveProbing", BooleanValue (false));
```

Inicialmente se crea un *Service Set Identifier* (SSID) el cual será utilizado para la implementación de la capa MAC, la cual se implementa mediante el atributo "ns3::StaWifiMac"

Una vez que todos los parámetros han sido totalmente configurados, tanto para la capa MAC como para la capa física, se procede a inicializar el método *Install* en donde se crearán los controladores *wifi* de las estaciones.

Distancia entre nodos

La distancia entre nodos se la ubica tal como en un plano cartesiano, se maneja un sistema de coordenadas rectangulares (x,y,z) las cuales deben ubicarse respectivamente en el mismo orden como se crearon los nodos. La sintaxis para la ubicación de los nodos es la siguiente:

```
MobilityHelper mobility;

Ptr<ListPositionAllocator>positionAlloc=CreateObject<ListPositionAllocator
> ();
positionAlloc->Add (Vector (0.0, 0.0, 0.0));
positionAlloc->Add (Vector (30.0, 10.0, 0.0));
positionAlloc->Add (Vector (-20.0, 20.0, 0.0));
```

Como se puede observar se inicializa un objeto *MobilityHelper*, el cual permite manejar el objeto de posición (*positionAlloc*) el cual se encargará de ubicar los nodos en las posiciones descritas en los atributos.

Tráfico utilizado

Generalmente el tráfico generado durante la simulación depende de factores como el tamaño de los paquetes, el intervalo de envío de los mismos, un contador que depende del tiempo de simulación y el manejo de sockets controlado por punteros que maneja el simulador ns-3.

Mediante una función estática se puede generar el tráfico que se requiere en cualquier simulación, claro que se puede variar los parámetros de simulación para que el tráfico también tenga un comportamiento diferente.

```
static void GenerateTraffic (Ptr<Socket> socket, uint32_t pktSize,
                                    uint32_t pktCount, Time pktInterval)
{
        if (pktCount > 0)
        {
        socket->Send (Create<Packet> (pktSize));
        Simulator::Schedule (pktInterval, &GenerateTraffic,
                                socket, pktSize,pktCount-1, pktInterval);
        }
         else
        {
                socket->Close ();
```

Con esta función se puede implementar un generador de tráfico para comunicaciones inalámbricas, en este caso para comunicaciones bajo el estándar IEEE 802.11 y sus varios tipos soportados por el simulador ns-3.

Tiempo total de Simulación, número y tamaño de paquetes e Intensidad de Señal (Transmitida y Recibida)

Estos son valores que fijos y que no varían a lo largo de la simulación. De los valores que se ubiquen en estos parámetros, dependerán tanto de velocidades de transmisión, tamaño de tráfico generado, e incluso el tamaño de los archivos de captura que se obtienen al final de cada simulación.

Direccionamiento IPV4

El direccionamiento de la red, es una parte fundamental durante la implementación de la topología. Para la asignación de direcciones IP a las interfaces de los dispositivos se requiere utilizar el módulo *Ipv4AddressHelper*.

```
Ipv4AddressHelper ipv4;
NS_LOG_INFO ("Assign IP Addresses.");
ipv4.SetBase ("10.1.1.0", "255.255.255.0");
Ipv4InterfaceContainer i = ipv4.Assign (devices);
```

En las líneas indicadas anteriormente del *script,* se configura el direccionamiento IP a los dispositivos inalámbricos creados previamente. Es importante manejar un método de direccionamiento lógico para que la topología que vaya a ser implementada funcione correctamente.

3.2.2 Tipos de Escenarios de Simulación

Durante el presente trabajo se han definido 4 tipos de escenarios, quizás los más utilizados y prácticos, así mismo son escenarios que permiten definir el funcionamiento del simulador *ns-3* y las aplicaciones gráficas que trabajan conjuntamente con el software.

Los escenarios definidos previamente, han sido realizados bajo el estándar de estudio el IEEE 802.11 con las variaciones que soporta el software. A continuación se listan los escenarios predefinidos:

- Simulación Tipo Infraestructura
- Simulación Tipo Ad-hoc
- Simulación Tipo Punto a punto (Fijo – Móvil)

Realizadas las simulaciones, el *script* es capaz de generar archivos de captura de red con extensión .pcap, los mismos que serán analizados utilizando el analizador de protocolos *Wireshark* para realizar el análisis de la red durante la transferencia de paquetes que se producen durante la simulación. Adicionalmente se manejará un sistema gráfico (*Pyviz*) para visualizar la topología de cada escenario y analizar también el envío y recepción de paquetes de cada nodo que constituye cada topología.

Simulación Tipo Infraestructura

En este tipo de simulación, la topología de la red presenta estaciones móviles o fijas, las cuales se comunican a través de un punto de acceso (AP). En este caso, se conoce también como BSS *(Basic Service Set)* la cobertura del AP, el cual es el responsable de gestionar la red, así mismo el BSSID *(BSS IDentifier)* es la dirección MAC del AP.

La simulación a realizar a continuación se resume en la Tabla 3.3 presentada con las características de la topología, así mismo se visualiza en la Fig. 3.3 la topología para el análisis posterior de esta simulación.

Tabla. 3.3. Características Principales del escenario Tipo Infraestructura

CARACTERÍSTICAS	VALORES
Número de Nodos Fijos	5

Tecnología de la Capa Física	DSSS a 11 Mbps
Tasa de Transmisión	8 Mbps
Intensidad de Recepción de Señal	-60 dBm
Tamaño de Paquetes Enviados	64000 B
Estándar Inalámbrico	IEEE 802.11b
Frecuencia de Transmisión	2.4 GHz
Modelo de Propagación	*FixedRssLossModel*
Distancia Promedio hacia el AP	30 m
Tráfico Generado	UDP
Tiempo de Simulación	120 seg.

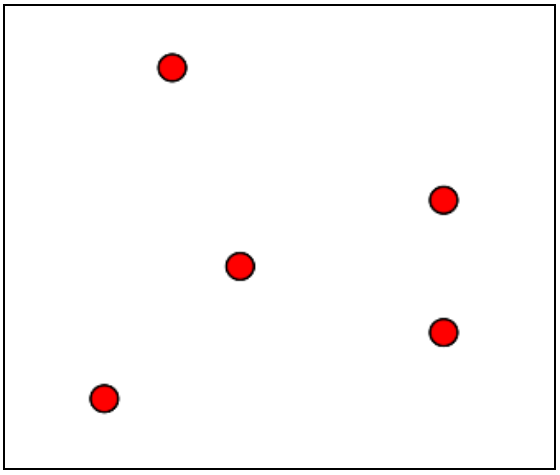


Figura. 3.3. Topología de la Red Tipo Infraestructura

A continuación se presenta una explicación de cada parámetro presentado en la Tabla 3.3 para el análisis de la red.

Número de Nodos Fijos.- Se han elegido cinco nodos, de los cuales cuatro son estaciones remotas y el quinto es el *Access Point* de la red. La topología soporta un número n de nodos, el funcionamiento de acuerdo al número de nodos depende de los parámetros que se presentan a continuación.

Tecnología de la Capa Física.- Se ha configurado un canal a 11 Mbps con el tipo de tecnología de espectro ensanchado conocido como DSSS (*Direct Sequence Spread Spectrum*). El IEEE ha desarrollado esta tecnología para su correcto funcionamiento en el estándar 802.11b obteniendo mejoras en seguridad así como el aumento de la velocidad hasta 11 Mbps, incrementando el rendimiento en las redes inalámbricas de tipo IEEE 802.11.

Tasa de Transmisión.- Tomando en cuenta el tipo de codificación del estándar IEEE 802.11b, las velocidades máximas de transmisión son de aproximadamente 5.9 Mbps con tráfico TCP y de 7.1 Mbps sobre tráfico UDP [29] La velocidad de transmisión elegida es de 1 Mbps tomando en cuenta la cantidad de paquetes enviados y el tamaño de los mismos los cuales son ideales para el análisis de los paquetes.

Intensidad de Recepción de Señal.- Este valor es importante especialmente para los nodos que reciban la información por parte del Punto de Acceso, dicho valor ha sido configurado de acuerdo a la Tabla 4.2 sobre los indicadores de RSSI. [29]

Tabla. 3.4. Valores de RSSI para ambientes WIFI

VALOR [dBm]	CARACTERÍSTICAS
-80	Señal mínima aceptable para establecer la conexión, pueden ocurrir caídas de enlaces.
-70	Enlace normal, señal medianamente buena, presenta problemas con lluvia y viento.
-60	Enlace bueno, se puede obtener una conexión estable al 80% modificando parámetros de tasas de transmisión.
-40 a -60	Enlace idóneo, con tasas de transferencia estables.
0	Enlace Ideal, difícil de lograr en la práctica.

Para este escenario se ha seleccionado el nivel de -60 dBm, de acuerdo a las características presentadas en la Tabla 4.2 se obtendrá un enlace bastante bueno con conectividad garantizada tomando en cuenta el parámetro de tasa de transmisión de 1 Mbps.

Número y Tamaño de Paquetes Enviados.- El número de paquetes enviados por cada nodo en respuesta a la información enviada por el *Access Point* es de un total de 100 paquetes y de acuerdo a la Unidad Máxima de Transferencia (*Maximum Transfer Unit - MTU*), que indica un valor de 1500 bytes el datagrama más grande que puede pasar por una capa de un protocolo de comunicaciones bajo el estándar combinado IEEE 802.3 – IEEE 802.11 (28), tomando en cuenta este último parámetro se puede enviar sin problema paquetes de 100 bytes.

Estándar Inalámbrico y Frecuencia de Transmisión.- Tomando en cuenta la tecnología del canal de transmisión utilizada como DSSS a 11 Mbps, el estándar IEEE 802.11b se acopla perfectamente soportando una velocidad máxima de transmisión de 1 Mbps en la banda de 2.4 Ghz para el correcto funcionamiento del estándar.

Modelo de Propagación.- Se ha configurado el modelo de propagación *FixedRSSLossModel*, en el cual el valor de RSSI es configurado en -60 dBm para todos los dispositivos que conforman la topología de red de éste escenario. Al utilizar un valor fijo de RSSI se garantiza la conectividad evitando la pérdida de paquetes durante la comunicación.

Distancia Promedio hacia el AP.- La distancia promedio hacia el *Access Point* se ha definido en 30 metros, tomando en cuenta los valores de zonas de cobertura del estándar proporcionadas en la Tabla 4.3.

Tabla. 3.5. Zonas de Cobertura para el estándar IEEE 802.11b

VELOCIDAD	RANGO EN AMBIENTES CERRADOS	RANGO AL AIRE LIBRE
11 Mbps.	50 m	200 m
5.5 Mbps.	75 m	300 m
2 Mbps.	100 m	400 m
1 Mbps.	150 m	500 m

Tráfico de Datos Generado.- El tráfico generado para este escenario esta basado en el protocolo UDP, esto debido a que se pretende presentar un ambiente similar al tráfico generado durante navegación en páginas Web,

sesiones de juegos *online* o simplemente realizar una descarga de algún archivo de música o video utilizando programas no orientados a la conexión o más conocidos como *torrents.*

Tiempo de Simulación.- El tiempo de simulación se ha seleccionado un total de 20 segundos, suficientes para realizar la captura del tráfico generado y obtener los datos necesarios para la presentación de las gráficas del *Throughput* y del *Delay*. Durante este tiempo se realiza un proceso de creación de un nodo que se encargará de recibir los paquetes de manera auxiliar. A partir del tiempo aproximadamente 2.034 hasta la finalización de la simulación se realiza la comunicación de los nodos que hacen parte de la topología así como el envío de los paquetes generados por cada nodo hasta que la aplicación es finalizada.

Simulación Tipo Ad-hoc

En la simulación configurada en este escenario se ha propuesto una red ad-hoc. Esta red es totalmente autónoma y no depende de un *Access Point* que conecte a los dispositivos inalámbricos que formarán parte de ésta, sino que dicho dispositivos o clientes formarán enlaces inalámbricos para compartir información entre ellos.

Este tipo de topología permite movilidad entre los clientes, es decir éstos se pueden movilizar libremente a lo largo de toda la zona de cobertura que posee cada dispositivo, de ésta manera la topología de ésta red no es considerada fija ya que los cambios de posición de los dispositivos inalámbricos pueden ser a cualquier momento.

La simulación correspondiente a la topología Tipo Ad-hoc se resume en la Tabla 3.4 en la cual se presentan las principales características de la red, y en la Fig. 3.4 se representa la topología a ser analizada.

Tabla. 3.6. Características Principales del escenario Tipo Ad-hoc

CARACTERÍSTICAS	VALORES
Número de Nodos Móviles	3
Tecnología de la Capa Física	DSSS a 11 Mbps
Tasa de Transmisión	8 Mbps

Tamaño de Paquetes Enviados	5000 B
Estándar Inalámbrico	IEEE 802.11b
Frecuencia de Transmisión	2.4 GHz
Modelo de Propagación	*FriisPropagationLossModel*
Distancia Promedio entre nodos	10 m
Tráfico Generado	UDP
Tiempo de Simulación	120 seg.

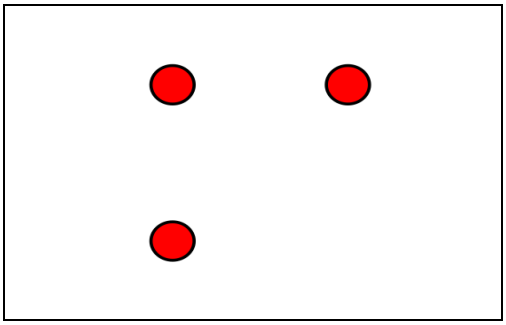


Figura. 3.4. Topología de la Red Tipo Ad-hoc

Número de Nodos Móviles.- Se han configurado tres nodos, en modo Ad-hoc, se han escogido tres nodos ya que los datos obtenidos son prácticamente los mismos y no se requiere de un mayor número de nodos para este caso y para el análisis del rendimiento de la red.

Tecnología de la Capa Física.- Se mantiene la misma tecnología referida en la topología Tipo Infraestructura, un canal a 11 Mbps con el tipo de tecnología de espectro ensanchado (Direct Sequence Spread Spectrum - DSSS).

Tasa de Transmisión.- Al mantener el tráfico de tipo UDP bajo el estándar IEEE 802.11b, se mantiene como velocidad de transmisión de 1 Mbps, tomando en cuenta las velocidades máximas soportadas con este protocolo que son de 7.1 Mbps.

Número y Tamaño de Paquetes Enviados.- El número y tamaño de paquetes enviados en este escenario es el mismo utilizado para el anterior escenario, es decir un total de 100 paquetes cada uno con un tamaño de 100 bytes, de la misma manera tomando en cuenta las características de MTU y la velocidad de transmisión utilizada para el envío de los paquetes.

Estándar Inalámbrico y Frecuencia de Transmisión.- Con la tecnología del canal de transmisión utilizada a 11 Mbps y utilizando el estándar IEEE 802.11b se realiza la transmisión en la banda de 2.4Ghz para el correcto funcionamiento del estándar.

Modelo de Propagación.- Se ha configurado el modelo de propagación *FriisPropagationLossModel*, o también conocido como Modelo de Espacio Libre, el cual es el más similar al de una conexión típica Ad-hoc en el cual la presencia de obstáculos es casi nula y su principal parámetro a tomar en cuenta es la distancia entre los nodos que forman parte de la topología.

Distancia Promedio entre nodos.- La distancia promedio entre los nodos que forman parte de la topología de este escenario es de aproximadamente 10 metros, el cual es un valor apropiado para las comunicaciones de éste tipo. El valor de 10 metros no es ni máximo ni mínimo, es un valor tomado desde el estándar, en el cual a dicha distancia se garantiza la conectividad durante la simulación.

Tráfico de Datos Generado.- El tráfico generado para este escenario esta basado en el protocolo UDP, teniendo en cuenta la simulación de un ambiente de intercambio de información bajo el protocolo especificado. Al igual que en el anterior escenario, un ambiente de simulación de juegos online es ideal para este tipo de ambientes.

Tiempo de Simulación.- El tiempo de simulación total es de 100 segundos, la aplicación inicia a partir del tiempo dos segundos, aquí se inicia el procedimiento para conocer la topología de la red bajo el protocolo de enrutamiento AODV (Ad Hoc On-Demand Distance Vector), este protocolo de enrutamiento permite trazar rutas sin necesidad de haberlas definido previamente, se requiere enviar un paquete denominado RREQ el mismo que incluye información del mismo nodo y de los nodos anteriores por los cuales pasó hasta llegar al nodo destino. Este protocolo de enrutamiento es ideal para este escenario debido a la movilidad del mismo, una de las ventajas de AODV es la corrección de errores en la red cuando un vecino detecta que un enlace se ha caído, éste tratará de ubicar una nueva ruta para llegar al nodo con el que perdió

el enlace, si encuentra otra ruta la cambia de manera local, sin notificar a los demás nodos para evitar utilizar el ancho de banda de la red.

Simulación Tipo Punto a Punto (Fijo – Móvil)

Esta simulación se la presenta para realizar una transmisión entre un nodo fijo y uno móvil. El procedimiento para la simulación se la realizará siguiendo el siguiente procedimiento:

- Se inicia la simulación y se transmite los paquetes de *beacon*.

- Ambos nodos comienzan a realizar la transmisión de datos mientras el nodo móvil comienza a alejarse del otro.

- La simulación se detiene segundos después de que se ha perdido la conexión entre ambos nodos.

En la Tabla 3.5 se presenta las principales características del escenario Tipo Punto a Punto.

Tabla. 3.7. Características Principales del escenario Tipo Punto a Punto

CARACTERÍSTICAS		**VALORES**	
Número de Nodos Fijos		1	
Número de Nodos Móviles		1	
Tecnología de la Capa Física		DSSS a 11 Mbps	
Tasa de Transmisión		8 Mbps	
Tamaño de Paquetes Enviados		2250 B	
Estándar Inalámbrico		IEEE 802.11b	
Frecuencia de Transmisión		2.4 GHz	
Modelo de Propagación		*LogDistancePropagationLossModel*	
Velocidad de Nodo Móvil	**Velocidad 1**	1 m/s	3.6 km/h
	Velocidad 2	2.5 m/s	9 km/h
	Velocidad 3	5 m/s	18 km/h
Tráfico Generado		UDP	
Tiempo de Simulación		150 seg.	

Número de Nodos Fijos y Móviles.- Se han elegido dos nodos, uno fijo que mantendrá su posición enviando y recibiendo datos de acuerdo a la configuración del *script* de programación. También se tiene un nodo móvil que se aleja del nodo fijo a una velocidad constante programada directamente en el *script* de programación.

Tecnología de la Capa Física.- Se mantiene la misma tecnología referida en la topología Tipo Infraestructura y Tipo Ad-hoc, un canal a 11 MBps con la tecnología de Espectro Ensanchado (*Direct Sequence Spread Spectrum* - DSSS).

Tasa de Transmisión.- Al mantener el tráfico de tipo UDP, bajo el estándar IEEE 802.11b, se mantiene la velocidad de transmisión de 1 Mbps, tomando en cuenta las velocidades máximas soportadas con este protocolo que son de 7.1Mbps.

Número y Tamaño de Paquetes Enviados.- El número y tamaño de paquetes enviados en este escenario es el mismo utilizado para los escenarios anteriores, es decir un total de 100 paquetes cada uno con un tamaño de 100 bytes, de la misma manera tomando en cuenta las características de MTU y la velocidad de transmisión utilizada para el envío de los paquetes.

Estándar Inalámbrico y Frecuencia de Transmisión.- Con la tecnología del canal de transmisión utilizada a 11 Mbps y utilizando el estándar IEEE 802.11b se realiza la transmisión en la banda de 2.4Ghz para el correcto funcionamiento del estándar.

Modelo de Propagación.- Se ha configurado el modelo de propagación *Log Distance Propagation Loss Model*, este modelo ha sido utilizado teniendo en cuenta los parámetros tanto de velocidad y variación de la distancia que se presentan durante la simulación. Hay que tomar en cuenta la Tabla 2.6 indicada en el Capítulo 2, para escoger el adecuado exponente de pérdidas y configurarlo en el script.

Velocidad del Nodo Móvil.- La velocidad del nodo es un valor constante a lo largo de toda la simulación, existen herramientas dentro del simulador *ns-3* que

permiten la variación de la velocidad, pero se requieren actualizaciones completas del software, por lo que en este caso las velocidades son contantes. Como se indica en la Tabla 3.5 los valores de velocidad son de 1 m/s, 2.5 m/s y 5 m/s. Se han escogido estos valores para evitar cambios pronunciados durante la simulación y ese no es el objetivo de este proyecto, lo que se pretende obtener son valores cercanos a la realidad y completos.

En la Figura 3.5 se observa la topología utilizada y la disposición de los nodos en cuestión.

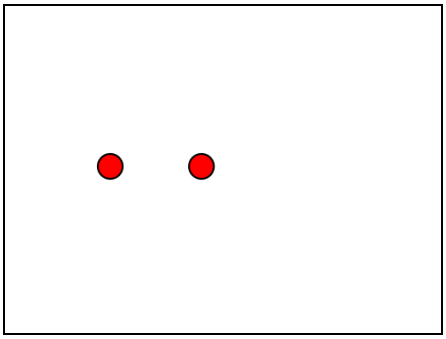


Figura. 3.5. Topología de la Red Tipo Punto a Punto

3.3 OBTENCIÓN DE DATOS DE SIMULACIÓN

Para la obtención de los datos de simulación, se utilizarán dos métodos. El primero proporcionado por la herramienta gráfica de simulación Pyviz la cual brinda información general y específica de los nodos configurados previamente en el script. El segundo método para el análisis de las redes inalámbricas propuestas puede ser mediante la herramienta de análisis de tráfico de red incorporada en la mayoría de sistemas operativos UNIX: Linux, Solaris, BSD, Mac OS X, HP-UX y AIX, ésta herramienta es conocida como tcpdump y la otra opción es utilizando el software analizador de protocolos Wireshark. Entre las dos herramienta se elegirá la más conveniente para el caso, la cual es el software Wireshark, debido a que la otra opción es bastante limitada especialmente en la presentación gráfica de los datos capturados y la presentación bastante básica de los datos que presenta. Debido a estas razones, el software que se utilizará será el analizador de protocolos denominado Wireshark, el mismo que muestra una amplia gama de opciones para analizar los paquetes transmitidos durante la simulación, opciones de organización y filtrado de información, de ésta manera permite ver todo el

tráfico que pasa a través de una red estableciendo la configuración en modo promiscuo (un equipo conectado a una red que captura todos los paquetes que ingresan a la red, incluyendo los destinados a él mismo y al resto de equipos que conforman la red)

3.3.1 Estudio y Análisis de las redes con Software Analizadores de Protocolos

Para el estudio y análisis de las redes propuestas anteriormente, se realizará un estudio y análisis individual de cada una de las topologías presentadas. Para realizar esto se tomará los datos de las dos herramientas mencionadas (*Pyviz y Wireshark*) diferenciando cada red, su funcionamiento y topología.

Simulación Tipo Infraestructura

En la simulación Tipo Infraestructura se puede observar en la Figura 3.6 los datos obtenidos directamente de los nodos ubicados en el plano de simulación, mediante la herramienta *Pyviz* se puede visualizar estos datos, en la Figura 3.6 se muestran los datos principales de un solo nodo y en la Tabla 3.6 se ubican los valores de los otros nodos, los cuales no difieren tanto del resto debido a que la configuración es muy similar en todos los nodos.

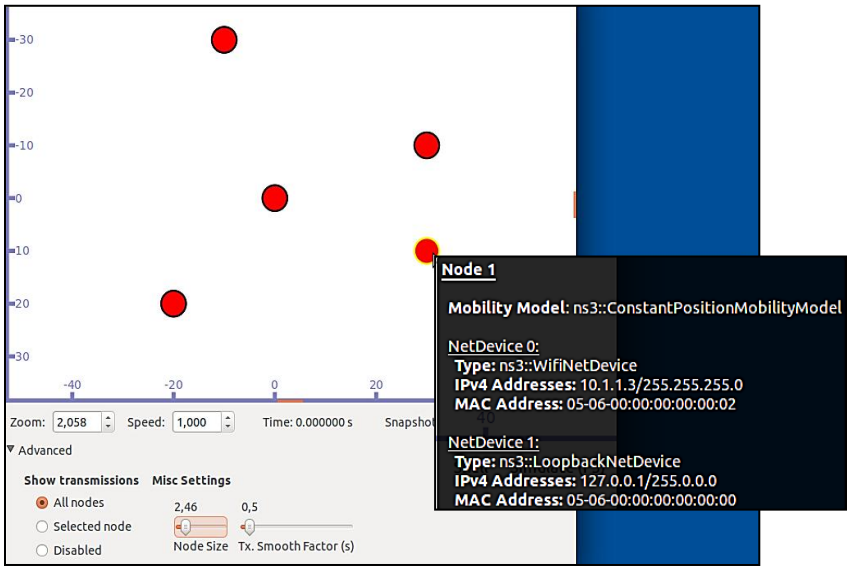


Figura. 3.6. Datos Obtenidos del Nodo 1

Tabla. 3.8. Valores de Configuración de los Dispositivos de Red

		Nodo 0	Nodo 1	Nodo 2	Nodo 3	Nodo 4
Mobility Model		ns3::ConstantPositionMobilityModel				
NetDevice 0	**Type**	ns3::WifiNetDevice				
	IPv4	10.1.1.2/24	10.1.1.3/24	10.1.1.4/24	10.1.1.5/24	10.1.1.1/24
	Mac	05-…00:05	05-…00:02	05-…00:03	05-…00:04	05-…00:01
NetDevice 1	**Type**	ns3::LoopbackNetDevice				
	IPv4	127.0.0.1 / 255.0.0.0				
	Mac	05-06-00:00:00:00:00:00				

En la Tabla 3.6 se muestran los valores de configuración predefinidos por el programador en el script, aquí cabe resaltar los valores más importantes a tomar en cuenta los siguientes factores:

Mobility Model.- El cual representa el tipo de movilidad que va a tener el nodo, en este caso se los ha ubicado como nodos estáticos (*ConstantPosition*), en caso de que se requiera nodos móviles se debe cambiar éste factor mediante la función:

mobility.SetMobilityModel ("ns3::RandomWalk2dMobilityModel");

Hay que recordar que para que esta función trabaje adecuadamente se requiere llamar a la clase *ns3::MobilityHelper* la cual gestiona las características de movimiento que se pueden configurar en los nodos que forman parte de la red en cuestión.

NetDevice 0.- Este se encarga de presentar el tipo de dispositivo que ha sido configurado (*Type*) en este caso se ha configurado dispositivos WIfi (*WifiNetDevice*), adicionalmente presenta la dirección IPv4 configurada previamente (*IPv4Addresses*) y finalmente la dirección de MAC que es única y exclusiva para cada uno de los nodos (*MacAddress*). En la Tabla 3.4 se presenta la dirección MAC del siguiente modo 05-…00:0X, debido a la extensión de la dirección que se visualiza de mejor manera en la Figura 3.3.

NetDevice 1.- En este se visualiza los datos del controlador de red del mismo dispositivo pero para su propia tarjeta de red, es decir, los datos que presenta son los de *localhost* el cual es un nombre reservado que tienen todas las computadoras, router o dispositivo independiente de que disponga o no de una tarjeta de red Ethernet, este nombre de *localhost* es traducido como un dirección IP de *loopback* o dirección de bucle de retorno 127.0.0.1.

Después de iniciar la simulación, se puede observar como se envían los paquetes desde el AP hacia los nodos de manera sincronizada. Para poder explicar y tener una mejor captura de los datos, se ha configurado al AP para que sea el principal elemento responsable en enviar información hacia los nodos, pero también se puede realizar un envío y recepción aleatorio para obtener una mayor cantidad de captura de datos. Mientras tanto en la Figura 3.8 se indica vía Terminal, la notificación de que el paquete ha sido recibido por cada unos de los nodos, hay que recordar que el programa se lo ejecuta siempre vía Terminal, en ésta se indicarán los procesos de *building* y compilación del programa, en caso de existir algún error se presentará el mismo en la ventana del Terminal, indicando el posible error en el script.

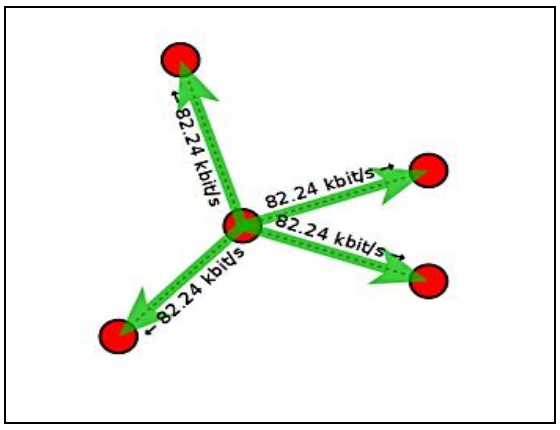


Figura. 3.7. Envío de Datos desde el AP visualizado en Pyviz

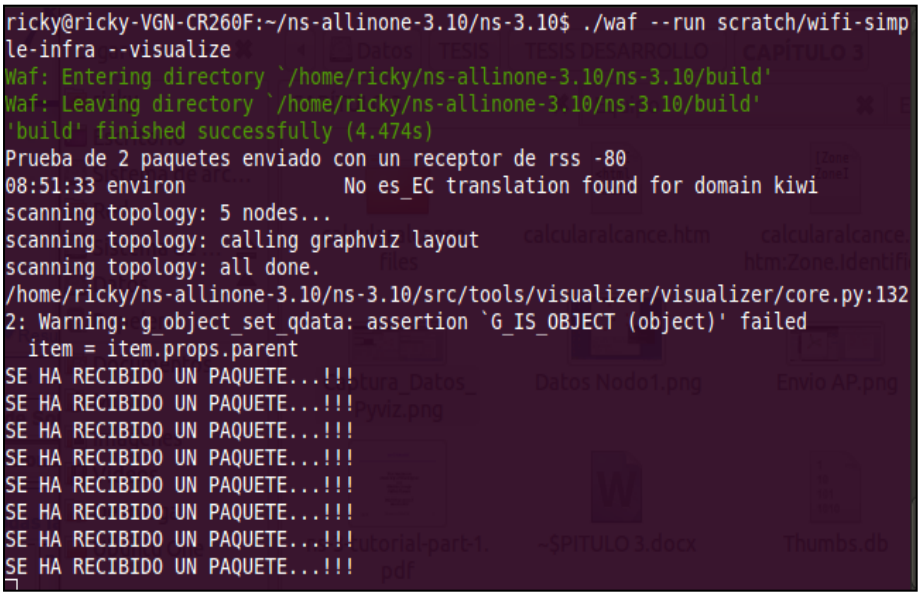


Figura. 3.8. Notificación de Recepción de datos en los nodos visualizado en Terminal

Al ejecutar la simulación, la herramienta gráfica *Pyviz*, permite verificar tres opciones que facilitan realizar el análisis de la red implementada.

- Estadísticas de las Interfaces
- Tabla de enrutamiento IPv4
- Últimos paquetes

Estadísticas de las Interfaces

Las estadísticas de las interfaces nos indican 9 parámetros tabulados en un resumen gráfico proveniente de la herramienta *Pyviz*, éste resumen se encuentra en la Figura 3.6. Se tabula tanto para el comportamiento del nodo ya sea como transmisor o receptor de la información. A continuación se listan los parámetros presentados y la función de cada uno de ellos.

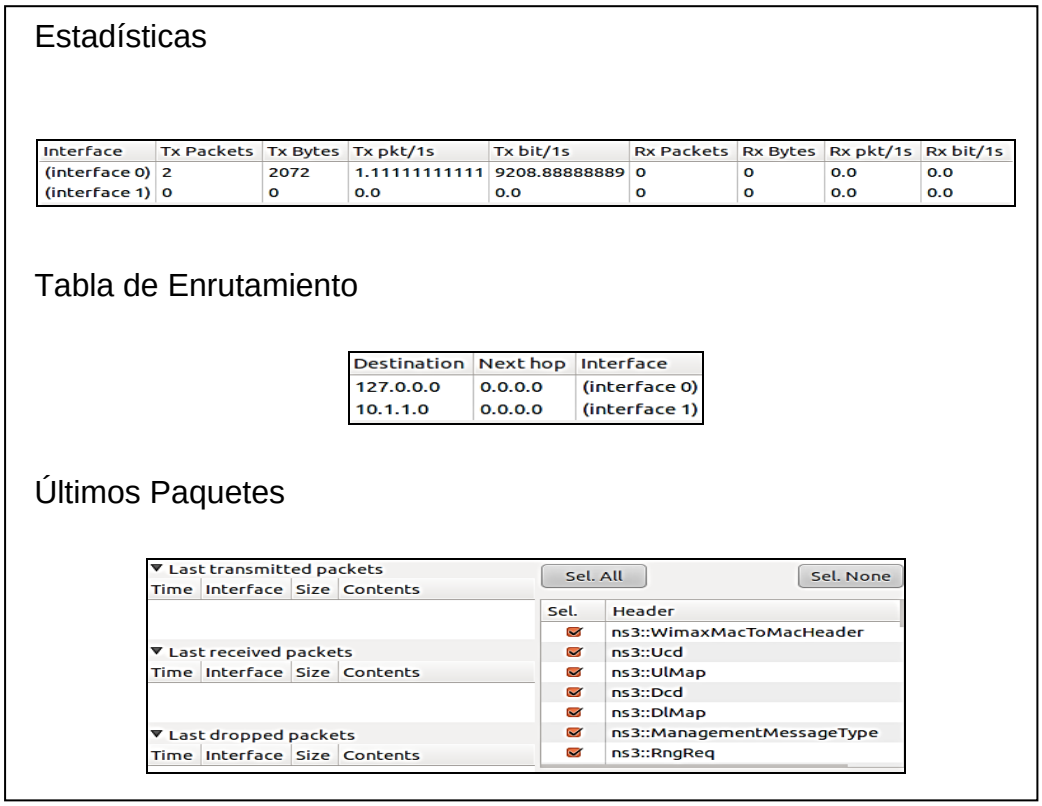


Figura. 3.9. Estadísticas del AP

Interface.- Identifica las interfaces del nodo seleccionado y que son configuradas previamente en el script, generalmente son las mencionadas en la Tabla 3.6.

Tx Packets.- Identifica el número total de paquetes transmitidos por el nodo, en el caso de que éste envíe los mismos, en caso de que sea este nodo sea receptor se identificaría éste valor en el campo *Rx Packets*.

Tx Bytes.- Indica el tamaño total de los paquetes que han sido enviados por el nodo seleccionado, este valor se configura en el script de la simulación a realizar, pero varía debido a que durante la transmisión se agregan cabeceras adicionales en los paquetes enviados.

Tx pkt/1s.- Identifica la transmisión de paquetes por unidad de tiempo que se da durante la transmisión de cada paquete involucrado en el intercambio de datos.

Tx bit/1s.- Indica la velocidad de transmisión y se encuentra identificada en el orden de número de bits por unidad de tiempo.

Interface	Tx Packets	Tx Bytes	Tx pkt/1s	Tx bit/1s	Rx Packets	Rx Bytes	Rx pkt/1s	Rx bit/1s
(interface 0)	0	0	0.0	0.0	2	2056	1.11111111111	9137.77777778
(interface 1)	0	0	0.0	0.0	0	0	0.0	0.0

Figura. 3.10. Estadísticas de un nodo Receptor

Para la explicación de los otros campos se ha tomado las estadísticas de otro nodo, en este caso el nodo 4, el cual es un nodo receptor de la información enviada por el AP.

Rx Packets.- Identifica el número total de paquetes recibidos por el nodo.

Rx Bytes.- Indica el tamaño total de los paquetes que han sido recibidos por el nodo seleccionado, éste valor como se observa es menor al tamaño de Bytes enviados por el transmisor, esto es debido al comportamiento de las cabeceras que se agregan durante la transmisión y que se eliminan o disminuyen en su tamaño, durante la recepción.

Rx pkt/1s.- Identifica la recepción de paquetes por unidad de tiempo que detecta el receptor durante la recepción de cada paquete involucrado en el intercambio de datos.

Rx bit/1s.- Indica la velocidad de recepción durante la simulación y se encuentra identificada en el orden de número de bits por unidad de tiempo.

Tabla de Enrutamiento IPv4

La tabla de enrutamiento almacena las rutas a las diferentes redes en una red inalámbrica. La Tabla de enrutamiento generalmente se almacena en un router o en una red en forma de una base de datos o archivo. Cuando los datos deben ser enviados desde un nodo a otro de la red, se hace referencia a la tabla de enrutamiento con el fin de encontrar la mejor ruta para la transferencia de la información.

Nodo 0

Destination	Next hop	Interface
127.0.0.0	0.0.0.0	(interface 0)
10.1.1.0	0.0.0.0	(interface 1)

Nodo 4

Destination	Next hop	Interface
127.0.0.0	0.0.0.0	(interface 0)
10.1.1.0	0.0.0.0	(interface 1)

Figura. 3.11. Tabla de Enrutamiento del Transmisor y Receptor

En la Figura 3.11 se identifica tres campos en la tabla de enrutamiento tanto para un nodo transmisor como para un nodo receptor, estos campos son:

- *Destination*
- *Next hop*
- *Interface*

Destination.- Identifica en primer lugar a la dirección de ruta de destino hacia la interfaz de red virtual (*loopback*) reconocida por la dirección 127.0.0.0, adicionalmente existe la otra ruta que es la de la red, en este caso la 10.1.1.0 la cual tomarán los paquetes como referencia para realizar el proceso de enrutamiento de la información.

Next hop.- Este campo sirve para identificar la ruta del siguiente salto, como no se ha configurado un protocolo de enrutamiento en los nodos inalámbricos la dirección del siguiente salto es la dirección 0.0.0.0 la cual es una dirección reservada para identificación local.

Interface.- Identifica la interface configurada por la cual los datos buscarán la ruta hacia el dispositivo de destino para enviar la información.

Últimos Paquetes

Este cuadro de resumen representado en la Figura 3.9 es una representación de las cabeceras que se agregan en cada paquete durante la transmisión y recepción de los datos.

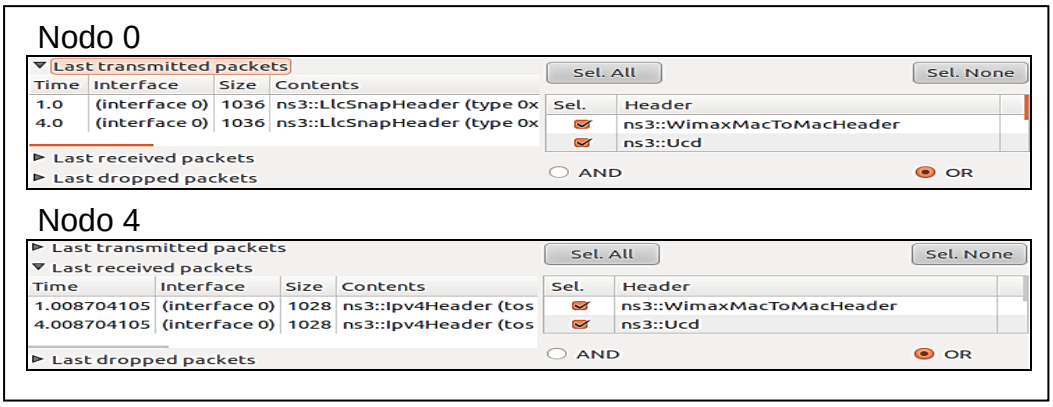


Figura. 3.12. Cabeceras para los paquetes transmitidos

Las principales cabeceras que se agregan durante la transmisión inalámbrica IEEE 802.11 son las siguientes:

- ns3::LlcSnapHeader
- ns3::Ipv4Header
- ns3::UdpHeader

*ns3::*LlcSnapHeader.- El protocolo LLC está basado en el protocolo de enlace HDLC[1], el protocolo de Control de enlace lógico LLC define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores. Adicionalmente en la *ns3::LlcSnapHeader* se añade el identificador del tipo de protocolo del paquete contenido, el valor de 0x800 corresponde al protocolo IP.

[1] HDLC (*High Level Link Control*) protocolo que utiliza los servicios de la capa física proporcionando un mejor esfuerzo y una mejor ruta de transmisión entre el transmisor y el receptor.

ns3::Ipv4Header.- Representa la cabecera del protocolo IP, en el cual se presenta la información de los campos utilizados durante la transmisión y recepción de la información. Los campos mostrados en esta cabecera con los valores en cada uno de los campos es el siguiente:

Tabla. 3.9. Valores de los campos de la Cabecera IPv4

TOS (*Type of Service*)	**TTL (*Time to live*)**	**ID (*Identification*)**		***Protocol***	***Offset***	***Flags***	***Lenght***
0x0	64	Paq.1	Paq. 2	17	0	-	1028
		0	1				

Type of Service.- Este parámetro contiene el valor de 0x0, lo cual representa que el campo de precedencia da una prioridad de carácter normal.

Time to live.- Este campo permite limitar el tiempo de vida del paquete, el valor que muestra este paquete es de 64 lo cual representa un contador que si disminuye hasta 0 se descarta dicho paquete.

Identification.- Este campo permite distinguir los fragmentos de un datagrama de los de otro. En la Tabla 3.7 se identifica a cada paquete con un ID único.

Protocol.- indica la capa de transporte a la que debe entregarse, en este caso se asignó el valor de 17, el cual corresponde a protocolo UDP (*User Datagram Protocol*) [2]

Offset.- En paquetes fragmentados indica la posición, en unidades de 64 bits, que ocupa el paquete actual dentro del datagrama original. En este caso el primer paquete de una serie de fragmentos se identifica con el valor 0.

[2] Soporte Microsoft, *Números del Protocolo Internet*, http://support.microsoft.com/kb/289892/es

Flags.- Especifica valores relativos a la fragmentación de paquetes. Como el paquete no ha sido fragmentado no se muestra ninguna indicación referente a la fragmentación del mismo.

Lenght.- Es la longitud total, tanto de los datos, como de la cabecera, para nuestro caso, la longitud total indica 1028 bytes.

ns3::UdpHeader.- Este campo representa los datos que viajan a través de la red utilizando el protocolo UDP (*User Datagram Protocol*) el cual es un protocolo no orientado a la conexión, pero sí orientado a datagramas. La cabecera UDP es muy simple, tan solo ocupa 8 bytes y los campos más representativos durante la transmisión de datos son los siguientes:

Tabla. 3.10. Valores de los campos de la Cabecera UDP

Length	**Puerto Origen**	**Puerto Destino**	***Payload***
1008	49153	80	1000

Lenght.- Es la longitud total, tanto de los datos, como de la cabecera, para este caso la longitud total indica 1008 bytes.

Puerto Origen.- El puerto origen para el caso se ha definido en el puerto número 49153, el cual es un puerto dinámico para uso privado que se utiliza simplemente para realizar la transmisión en la red por parte del nodo AP.

Puerto Destino.- El puerto destino que se maneja, de acuerdo al tipo de tráfico se tiene como puerto el designado al número 80, que es utilizado por los servidores de páginas web, en nuestro caso se utiliza dicho puerto de destino debido a la configuración de Internet realizada en el script de la simulación.

Payload.- El valor de *payload* es una porción de datos variable a diferencia del campo *lenght* el cual es un valor fijo. El tamaño de los datagramas varían de

acuerdo al ambiente de operación, tomando en cuenta que se tiene un tamaño máximo de 65535 bytes. Para este caso el valor se encuentra en 1000 bytes.

El análisis de las principales cabeceras para la recepción inalámbrica durante la simulación realizada en este caso es prácticamente la misma que se realizó para la transmisión de la información, debido a que ésta no varía desde que el nodo transmisor ubica sus cabeceras hasta que el nodo receptor las recibe.

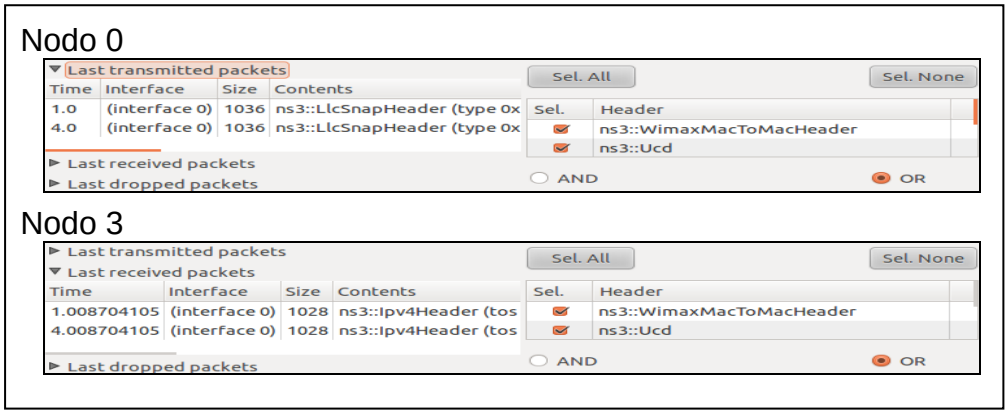


Figura. 3.13. Cabeceras para los paquetes recibidos

El análisis de la red Tipo Infraestructura se lo realizará utilizando la herramienta de análisis de protocolos *Wireshark*, la cual se la emplea para el análisis de los archivos de captura de datos generados durante la simulación.

Tabla. 3.11. Archivos de Captura para la Simulación Tipo Infraestructura

Archivo de Captura	Nodo
wifi-infraestructura-0-0.pcap	Nodo 0 (AP)
wifi-infraestructura-1-0.pcap	Nodo 1
wifi-infraestructura-2-0.pcap	Nodo 2
wifi-infraestructura-3-0.pcap	Nodo 3
wifi-infraestructura-4-0.pcap	Nodo 4

Análisis del archivo de Captura para el Nodo AP

Para el análisis del archivo de captura del nodo 0, que representa al punto de acceso de la red se realizará un análisis de los paquetes que se transmiten

durante la transmisión de los datos, así como de la recepción de la información cuando son enviados por los nodos que son parte de la red.

Durante el análisis hay que identificar tres procesos claves que suceden durante la simulación y que se deben tomar en cuenta para verificar el funcionamiento de la red, estos procesos son los siguientes:

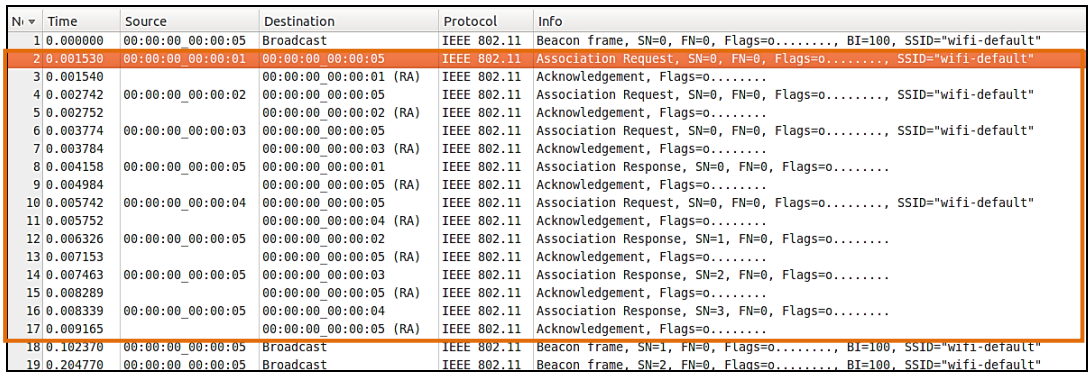
- Proceso de Negociación o Asociación
- Proceso de Sondeo o Monitoreo
- Proceso de Comunicación y Transferencia de Datos

Proceso de Negociación o Asociación

Este proceso es un proceso en el cual el nodo AP comienza a realizar un proceso de Sondeo que no dura más de una milésima de segundo en la cual envía un paquete de *beacon* por *broadcast* como se muestra en la Figura 3.14, este primer paso se lo hace para anunciar a otros dispositivos que se encuentren dentro de la cobertura del AP la presencia del mismo. Después de esto se puede alcanzar una conexión entre el cliente y el AP para comenzar el proceso de establecimiento de la conexión como se indica en la Figura 3.15 en la que se enmarca este primer proceso.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=0, FN=0, Flags=o........, BI=100, SSID="wifi-default"
2	0.001530	00:00:00 00:00:01	00:00:00 00:00:05	IEEE 802.11	Association Request, SN=0, FN=0, Flags=o........, SSID="wifi-default"
3	0.001540		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
4	0.002742	00:00:00_00:00:02	00:00:00_00:00:05	IEEE 802.11	Association Request, SN=0, FN=0, Flags=o........, SSID="wifi-default"
5	0.002752		00:00:00_00:00:02 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
6	0.003774	00:00:00_00:00:03	00:00:00_00:00:05	IEEE 802.11	Association Request, SN=0, FN=0, Flags=o........, SSID="wifi-default"
7	0.003784		00:00:00_00:00:03 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
8	0.004158	00:00:00_00:00:05	00:00:00_00:00:01	IEEE 802.11	Association Response, SN=0, FN=0, Flags=o........
9	0.004984		00:00:00_00:00:05 (RA)	IEEE 802.11	Acknowledgement, Flags=o........

Figura. 3.14. Proceso de Sondeo y envío de paquetes *Beacon*



No.	Time	Source	Destination	Protocol	Info
1	0.000000	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=0, FN=0, Flags=o........, BI=100, SSID="wifi-default"
2	0.001530	00:00:00_00:00:01	00:00:00_00:00:05	IEEE 802.11	Association Request, SN=0, FN=0, Flags=o........, SSID="wifi-default"
3	0.001540		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
4	0.002742	00:00:00_00:00:02	00:00:00_00:00:05	IEEE 802.11	Association Request, SN=0, FN=0, Flags=o........, SSID="wifi-default"
5	0.002752		00:00:00_00:00:02 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
6	0.003774	00:00:00_00:00:03	00:00:00_00:00:05	IEEE 802.11	Association Request, SN=0, FN=0, Flags=o........, SSID="wifi-default"
7	0.003784		00:00:00_00:00:03 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
8	0.004158	00:00:00_00:00:05	00:00:00_00:00:01	IEEE 802.11	Association Response, SN=0, FN=0, Flags=o........
9	0.004984		00:00:00_00:00:05 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
10	0.005742	00:00:00_00:00:04	00:00:00_00:00:05	IEEE 802.11	Association Request, SN=0, FN=0, Flags=o........, SSID="wifi-default"
11	0.005752		00:00:00_00:00:04 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
12	0.006326	00:00:00_00:00:05	00:00:00_00:00:02	IEEE 802.11	Association Response, SN=1, FN=0, Flags=o........
13	0.007153		00:00:00_00:00:05 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
14	0.007463	00:00:00_00:00:05	00:00:00_00:00:03	IEEE 802.11	Association Response, SN=2, FN=0, Flags=o........
15	0.008289		00:00:00_00:00:05 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
16	0.008339	00:00:00_00:00:05	00:00:00_00:00:04	IEEE 802.11	Association Response, SN=3, FN=0, Flags=o........
17	0.009165		00:00:00_00:00:05 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
18	0.102370	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=1, FN=0, Flags=o........, BI=100, SSID="wifi-default"
19	0.204770	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=2, FN=0, Flags=o........, BI=100, SSID="wifi-default"

Figura. 3.15. Proceso de Negociación o Asociación utilizando *Wireshark*

En la Figura 3.15 se muestra el proceso de Negociación para establecer la comunicación entre el AP y los nodos que se encuentren en el alcance de cobertura del AP. Para esto se observan los campos remarcados en el recuadro de la figura, estos paquetes enviados son los responsables de realizar el establecimiento de la sesión entre los clientes y el Access Point.

Como se puede observar en la Figura 3.15 tenemos 6 columnas de información que presenta *Wireshark*, la primera solamente es un identificador de cada proceso que se realiza durante la comunicación, éste identificador inicia por defecto en el valor de 1. En la segunda columna se muestra el tiempo transcurrido durante la simulación y en qué tiempo se realiza cada proceso, como se puede observar los tiempos son bastante precisos y se manejan 6 cifras decimales para mayor precisión. La tercera y cuarta columna muestran las direcciones MAC tanto del origen como la del destino, de ésta manera se identifica al equipo origen y al equipo destino. En una quinta columna se presenta el protocolo de comunicación que se aplica durante la simulación y que ha sido capturado en el archivo *.pcap*, para nuestro caso se muestra el protocolo WiFi IEEE 802.11. Finalmente en la sexta columna se presenta información general del proceso que se realiza en cada línea, en el caso del proceso de negociación se visualiza información de los paquetes de *Request, Response y Acknowledgement*, adicionalmente se presenta información de Número de Secuencia (SN), Número de Fragmento (FN), Banderas (*Flags*) y los SSID (*Service Set Identifier*).

Association Request.- Es el campo que indica que un dispositivo ha solicitado asociarse a la red después de que ha recibido un paquete de *Beacon*,

éste pedido es enviado al nodo AP para su posterior respuesta para poder establecer una comunicación entre estos.

Para el análisis de éste paquete se extrae la información de los detalles que presenta *Wireshark* para cada proceso realizado durante el establecimiento de la comunicación. En la Figura 3.15 se especifica los detalles más relevantes del paquete de *Request* que envían los nodos clientes hacia el nodo AP.

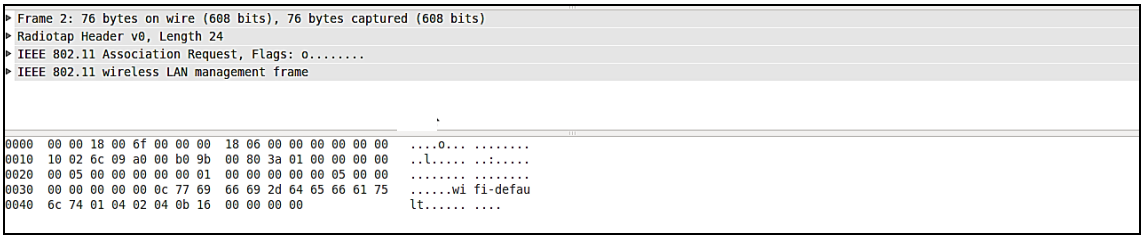


Figura. 3.16. Detalle del contenido del paquete *Request*

En la Figura 3.16 se tienen en la parte superior un panel de los detalles del paquete seleccionado en la lista de paquetes que se ubica en la Figura 3.15. En este panel se muestran los protocolos y campos que se manejan en este paquete, en este caso se tienen 4 campos con la información presentada en la Tabla 3.8.

Tabla. 3.12. Descripción del Paquete de *Request*

FRAME 2	*Time*	0.001530
	Frame Number	2
	Frame Length	76 bytes
	Protocols in Frame	radiotap:wlan
RADIOTAP HEADER	*Header Length*	24 bytes
	Data Rate	1,0 Mb/s
	Channel Frequency	2412 MHz
	Channel Type	802.11b
	SSI Signal	-80 dBm
	SSI Noise	-101 dBm

IEEE 802.11 ASSOCIATION REQUEST	*Destination Address*	00:00:00_00:00:05	
	Source Address	00:00:00_00:00:01	
	BSS Id	00:00:00_00:00:05	
IEEE 802.11 WIRELESS LAN MANAGEMENT FRAME	*SSID Parameter Set*	*Tag Number*	0
		Tag Length	12 bytes
		Tag Interpretation	wifi-default
	Supported Rates	*Tag Number*	1
		Tag Length	4 bytes
		Tag Interpretation	1,0 2,0 5,5 11,0 [Mbit/sec]

Association Response.- Este valor es exclusivo del nodo AP para el Modo Infraestructura del estándar IEEE 802.11, este campo es una notificación enviada al nodo que se ha unido a la red y que ha sido autentificado como parte del mismo producto del requerimiento realizado por el nodo cliente en el *Association Request*.

Al igual que en el paquete de *Request*, se tiene un detalle de los paquetes que se envían, en este caso por parte del nodo AP. Son muy parecidos y en el análisis se indicará las diferencias sustanciales con el paquete de *Request*. El detalle del paquete *Response* se encuentra tabulado en la Tabla 3.9 presentada a continuación.

Tabla. 3.13. Descripción del Paquete de *Response*

FRAME 8	*Time*	0.004158
	Frame Number	8
	Frame Length	62 bytes
	Protocols in Frame	radiotap:wlan
RADIOTAP HEADER	*Header Length*	22 bytes
	Data Rate	1,0 Mb/s
	Channel Frequency	2412 MHz

	Channel Type	802.11b	
IEEE 802.11 ASSOCIATION REQUEST	*Destination Address*	00:00:00_00:00:01	
	Source Address	00:00:00_00:00:05	
	BSS Id	00:00:00_00:00:05	
IEEE 802.11 WIRELESS LAN MANAGEMENT FRAME	*Supported Rates*	*Tag Number*	1
		Tag Length	4 bytes
		Tag Interpretation	1,0 2,0 5,5 11,0 [Mbit/sec]

Acknowledgement.- El conocido Acuse de Recibo o mensaje de ACK es el mensaje que envía inmediatamente el nodo AP después de haber establecido la asociación del nodo cliente y de hacerlo parte de la red. La estación receptora revisa el paquete recibido por si tiene algún error. Si lo encuentra correcto envía un paquete de "ACK", con lo cual el remitente sabe que el paquete llegó a su destino sin ningún error, caso contrario debe ser enviado nuevamente. Una vez que las demás estaciones capturan el paquete ACK, saben que el canal está libre y que pueden intentar enviar sus paquetes.

Los datos obtenidos se detallarán en dos paquetes ACK debido a que se realiza dos envíos durante el establecimiento de la comunicación entre el nodo cliente y el AP, similar a cómo se muestra en la Figura 3.14

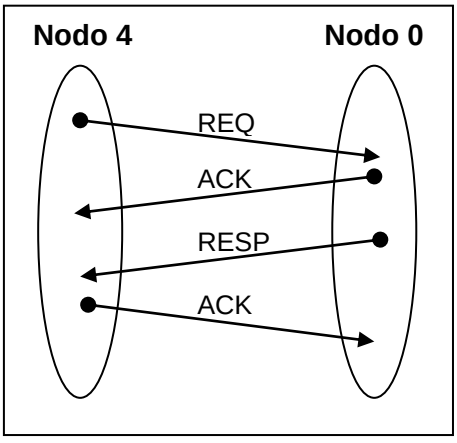


Figura. 3.17. *Handshake* válido para la conexión

Como se indica en la Figura 3.14 el nodo AP se encarga de enviar un primer paquete ACK después de recibir el pedido de asociación por parte del nodo cliente, éste paquete de ACK y la información que envía se detalla en la Tabla 3.10 y la información gráfica obtenida mediante el software *Wireshark* se lo demuestra en la Figura 3.18.

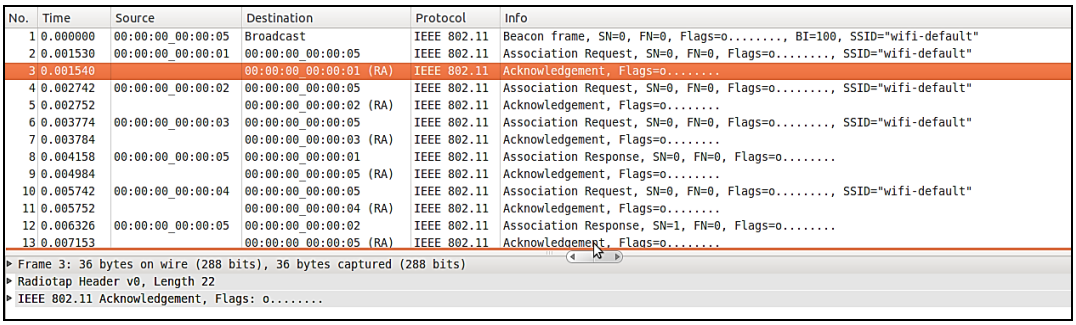


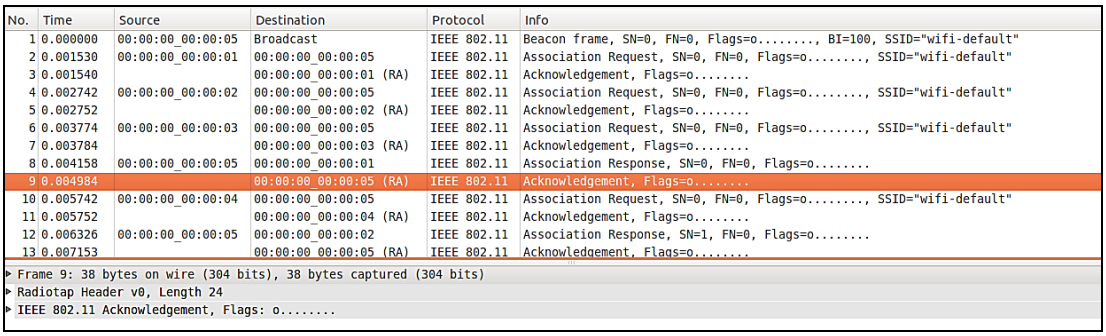
Figura. 3.18. Paquete ACK enviado al Cliente

En la Figura 3.18 se aprecia resaltado el paquete que se envía al Cliente y en la parte inferior el detalle del paquete enviado, en la Tabla 3.12 se detallarán los valores más importantes que este paquete registra en sus cabeceras.

Tabla. 3.14. Descripción del Paquete ACK enviado al Cliente

FRAME 3	*Time*	0.001540
	Frame Number	3
	Frame Length	36 bytes
	Protocols in Frame	radiotap:wlan
RADIOTAP HEADER	*Header Length*	22 bytes
	Data Rate	1,0 Mb/s
	Channel Frequency	2412 MHz
	Channel Type	802.11b
IEEE 802.11 ACKNOWLEDGEMENT	*Frame Control*	0x80D4 (Normal)
	Receiver Address	00:00:00_00:00:01

Mientras tanto, en la Figura 3.18 se puede observar el paquete de ACK que es enviado hacia el nodo AP y en la Tabla 3.13 se detallan los valores importantes para el análisis de éstos paquetes.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=0, FN=0, Flags=o........, BI=100, SSID="wifi-default"
2	0.001530	00:00:00_00:00:01	00:00:00_00:00:05	IEEE 802.11	Association Request, SN=0, FN=0, Flags=o........, SSID="wifi-default"
3	0.001540		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
4	0.002742	00:00:00_00:00:02	00:00:00_00:00:05	IEEE 802.11	Association Request, SN=0, FN=0, Flags=o........, SSID="wifi-default"
5	0.002752		00:00:00_00:00:02 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
6	0.003774	00:00:00_00:00:03	00:00:00_00:00:05	IEEE 802.11	Association Request, SN=0, FN=0, Flags=o........, SSID="wifi-default"
7	0.003784		00:00:00_00:00:03 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
8	0.004158	00:00:00_00:00:05	00:00:00_00:00:01	IEEE 802.11	Association Response, SN=0, FN=0, Flags=o........
9	0.004984		00:00:00_00:00:05 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
10	0.005742	00:00:00_00:00:04	00:00:00_00:00:05	IEEE 802.11	Association Request, SN=0, FN=0, Flags=o........, SSID="wifi-default"
11	0.005752		00:00:00_00:00:04 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
12	0.006326	00:00:00_00:00:05	00:00:00_00:00:02	IEEE 802.11	Association Response, SN=1, FN=0, Flags=o........
13	0.007153		00:00:00_00:00:05 (RA)	IEEE 802.11	Acknowledgement, Flags=o........

▸ Frame 9: 38 bytes on wire (304 bits), 38 bytes captured (304 bits)
▸ Radiotap Header v0, Length 24
▸ IEEE 802.11 Acknowledgement, Flags: o........

Figura. 3.19. Paquete ACK enviado al *Access Point*

Tabla. 3.15. Descripción del Paquete ACK enviado al *Access Point*

FRAME 9	*Time*	0.004984
	Frame Number	9
	Frame Length	38 bytes
	Protocols in Frame	radiotap:wlan
RADIOTAP HEADER	*Header Length*	24 bytes
	Data Rate	1,0 Mb/s
	Channel Frequency	2412 MHz
	Channel Type	802.11b
	SSI Signal	- 80 dBm
	SSI Noise	- 101 dBm
IEEE 802.11 ACKNOWLEDGEMENT	*Frame Control*	0x80D4 (Normal)
	Receiver Address	00:00:00_00:00:01

Número de Secuencia (SN).- Este campo junto al de número de fragmento forman parte del campo de la Trama MAC *Sequence Control*. Este campo es el responsable de numerar las tramas durante el proceso de comunicación. También sirve para verificar si existen tramas duplicadas de acuerdo a éste número se puede verificar si alguna trama no fue procesada completamente y se envió otra trama con el mismo número de secuencia. Esta duplicación de tramas puede ocurrir cuando:

- Una estación recibe una trama que no presenta errores y la toma como válida y realiza el envió del mensaje ACK aceptando dicha trama.

- Existen errores de transmisión los cuales intervienen en el contenido de la trama y destruyen el mensaje ACK en el camino.

- No se recibe el mensaje ACK después de haber transcurrido un periodo de tiempo específico, al tener este escenario la estación transmisora vuelve a transmitir la trama.

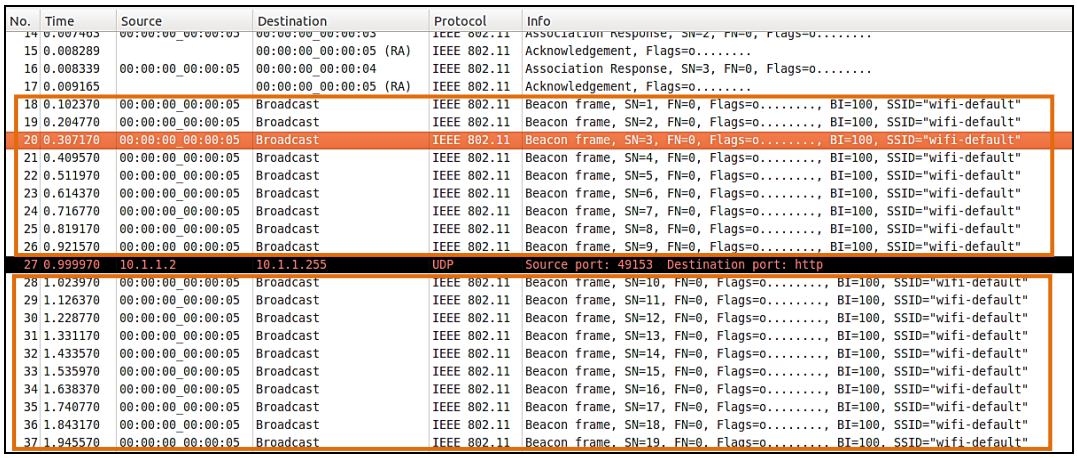
Número de Fragmento (FN).- El número de fragmento es un valor muy importante al momento de realizar el proceso de fragmentación y reensamblado, sin este valor los paquetes no podrían volver a ordenarse como el transmisor lo envió originalmente.

Banderas (*Flags*).- Las banderas o *Flags* como se presentan en el analizador de protocolos *Wireshark* son valores que se pueden utilizar para delimitar el inicio y final de una trama. Adicionalmente el comportamiento de éstas representa un valor que las tramas toman como señal para realizar un envío y/o recepción tanto del receptor como del transmisor.

SSID (*Service Set Identifier*).- Para el caso del Modo Infraestructura, en realidad debería presentar valores de ESSID, debido a que es un conjunto extendido el que se maneja para redes con punto de acceso. El SSID es un nombre incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red.

Proceso de Sondeo o Monitoreo

En este proceso, a diferencia del anterior, el *Access Point* realiza un envío periódico de "señales" denominadas *beacons*, para anunciar su presencia y que todas las estaciones que estén en el rango (100 ms aproximadamente) reconozcan éste AP como disponible para iniciar una comunicación. Estos paquetes "*beacons*" contienen varios parámetros entre ellos el SSID del Access Point y su Dirección MAC. Este proceso que realiza el *Access Point* se ejemplifica en la Figura 3.17.



No.	Time	Source	Destination	Protocol	Info
15	0.008289		00:00:00_00:00:05 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
16	0.008339	00:00:00_00:00:05	00:00:00_00:00:04	IEEE 802.11	Association Response, SN=3, FN=0, Flags=o........
17	0.009165		00:00:00_00:00:05 (RA)	IEEE 802.11	Acknowledgement, Flags=o........
18	0.102370	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=1, FN=0, Flags=o........, BI=100, SSID="wifi-default"
19	0.204770	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=2, FN=0, Flags=o........, BI=100, SSID="wifi-default"
20	0.307170	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=3, FN=0, Flags=o........, BI=100, SSID="wifi-default"
21	0.409570	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=4, FN=0, Flags=o........, BI=100, SSID="wifi-default"
22	0.511970	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=5, FN=0, Flags=o........, BI=100, SSID="wifi-default"
23	0.614370	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=6, FN=0, Flags=o........, BI=100, SSID="wifi-default"
24	0.716770	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=7, FN=0, Flags=o........, BI=100, SSID="wifi-default"
25	0.819170	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=8, FN=0, Flags=o........, BI=100, SSID="wifi-default"
26	0.921570	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=9, FN=0, Flags=o........, BI=100, SSID="wifi-default"
27	0.999970	10.1.1.2	10.1.1.255	UDP	Source port: 49153 Destination port: http
28	1.023970	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=10, FN=0, Flags=o........, BI=100, SSID="wifi-default"
29	1.126370	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=11, FN=0, Flags=o........, BI=100, SSID="wifi-default"
30	1.228770	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=12, FN=0, Flags=o........, BI=100, SSID="wifi-default"
31	1.331170	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=13, FN=0, Flags=o........, BI=100, SSID="wifi-default"
32	1.433570	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=14, FN=0, Flags=o........, BI=100, SSID="wifi-default"
33	1.535970	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=15, FN=0, Flags=o........, BI=100, SSID="wifi-default"
34	1.638370	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=16, FN=0, Flags=o........, BI=100, SSID="wifi-default"
35	1.740770	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=17, FN=0, Flags=o........, BI=100, SSID="wifi-default"
36	1.843170	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=18, FN=0, Flags=o........, BI=100, SSID="wifi-default"
37	1.945570	00:00:00_00:00:05	Broadcast	IEEE 802.11	Beacon frame, SN=19, FN=0, Flags=o........, BI=100, SSID="wifi-default"

Figura. 3.20. Proceso de sondeo en IEEE 802.11

Los paquetes *Beacon* también poseen campos característicos exclusivos los cuales se indican en la Tabla 3.12, estos datos obtenidos serán analizados posteriormente para verificar el comportamiento de los mismos.

Tabla. 3.16. Descripción del Paquete ACK enviado al *Access Point*

FRAME 20	*Time*		0.307170	
	Frame Number		20	
	Frame Length		82 bytes	
	Protocols in Frame		radiotap:wlan	
RADIOTAP HEADER	*Header Length*		22 bytes	
	Data Rate		1,0 Mb/s	
	Channel Frequency		2412 MHz	
IEEE 802.11 BEACON FRAME	*Frame Control*		0x8080 (Normal)	
	Sequence Number		3	
	Destination Address		Broadcast (ff:ff:ff:ff:ff:ff)	
	Source Address		00:00:00_00:00:05	
IEEE 802.11 WIRELESS LAN MANAGEMENT FRAME	*Fixed Parameters*	Beacon Interval	0.1024 (s)	
	Tagged Parameters	SSID	Tag Number	0
			Tag Length	12
			Tag Interpretation	wifi - default
		Supported Rates	1,0 2,0 5,5 11,0 [Mbit/sec]	

Proceso de Comunicación y Transferencia de Datos

Este proceso se da después de que un equipo cliente ha realizado todo el proceso de asociación y ahora forma parte de la red, adicionalmente el cliente se encuentra listo para poder enviar o recibir información desde o hacia el *Access Point* respectivamente. Para nuestro caso la transferencia de datos se hace a nivel de Capa 3 y esto se verifica con la captura de datos realizada con el software *Wireshark*, el cual demuestra esta comunicación y transferencia de datos a dicho nivel.

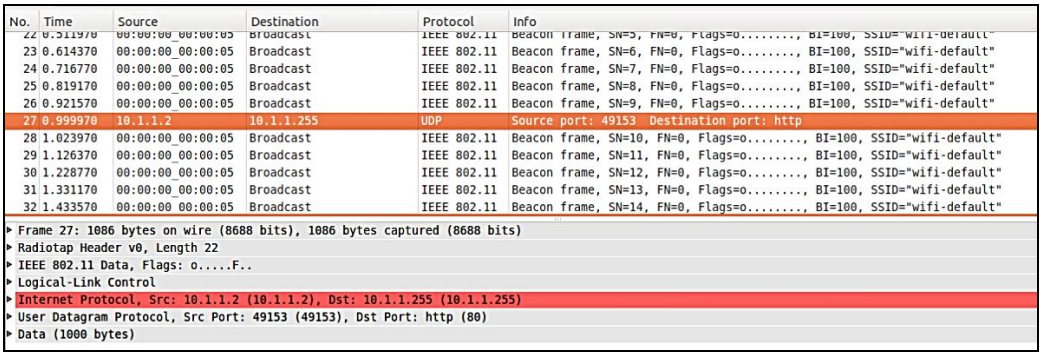


Figura. 3.21. Paquete enviado desde el AP a los nodos conectados

En la Figura 3.18 se indica que el paquete número 27 es el que contiene la información bajo el protocolo UDP que es enviada a todos los clientes que se encuentren conectados en la red debido a que realiza un envío por *broadcast*.

Adicionalmente se verifica los campos del paquete en el panel de detalles del paquete seleccionado, en este caso del paquete de información enviado por el AP. En la Tabla 3.15 se indica con más detalle los valores correspondientes a cada campo que contiene este paquete.

Tabla. 3.17. Descripción del Paquete de Información

FRAME 27	*Time*	0.999970
	Frame Number	27
	Frame Length	1086 bytes
	Protocols in Frame	radiotap:wlan:llc:ip:udp:data

RADIOTAP HEADER	*Header Length*	22 bytes	
	Data Rate	1,0 Mb/s	
	Channel Frequency	2412 MHz	
	Channel Type	802.11b	
IEEE 802.11 DATA	*Destination Address*	Broadcast (ff:ff:ff:ff:ff:ff)	
	Source Address	00:00:00_00:00:05	
	BSS Id	00:00:00_00:00:05	
LOGICAL–LINK CONTROL	DSAP[3]	SNAP	0xaa
	SSAP[4]	SNAP	0xaa
	Organization Code	Encapsulado Ethernet	
	Type	IP	
INTERNET PROTOCOL	*Version*	4	
	Header Length	28 bytes	
	Total Length	1028 bytes	
	Time to Live	64	
	Protocol	UDP	
	Source	10.1.1.2	
	Destination	10.1.1.255	
USER DATAGRAM PROTOCOL	*Source Port*	49153	
	Destination Port	http (80)	
	Length	1008	
DATA	*Length*	1000	

Simulación Tipo Ad-hoc

En la simulación Tipo Ad-hoc se han dispuesto los nodos de tal forma que mantengan una posición fija inicialmente y después comiencen a realizar movimientos aleatorios. En la Figura 3.19 se muestran los datos obtenidos directamente en cada nodo antes de realizar la simulación, mediante la herramienta *Pyviz* integrada con el simulador *ns*-3 se puede visualizar estos datos, en la Figura 3.19 se muestran los datos principales de un solo nodo y en la

[3] DSAP: *Destination Service Access Point*, Campo que permite a la capa LLC realizar un seguimiento de múltiples conexiones a través de la LAN.
[4] SSAP: *Source Service Access Point,* Identifica las entidades de protocolos de red que utilizan el servicio de capa de enlace.

Tabla se ubican los valores de los otros nodos, los cuales no difieren tanto del resto debido a que la configuración es muy similar entre estos.

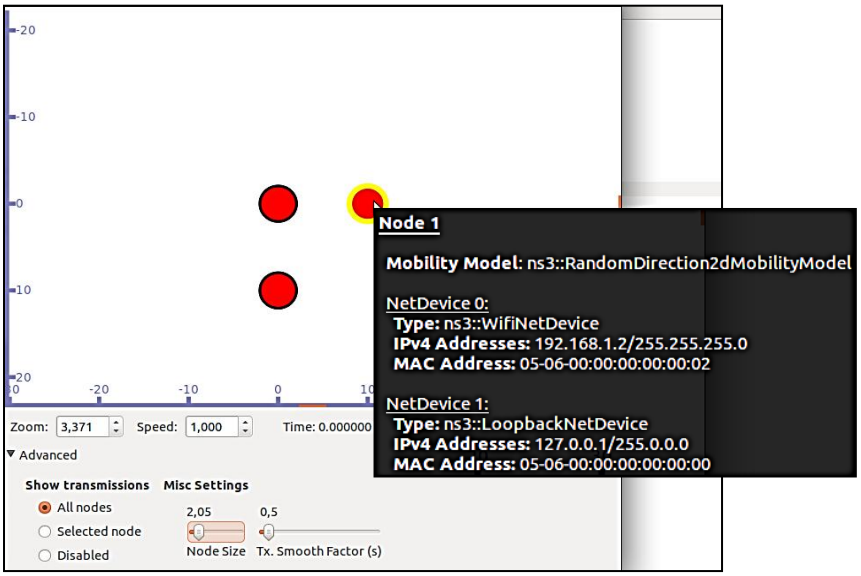


Figura 3.22. Datos Obtenidos del Nodo 1 en la Topología Ad-hoc

En la Figura 3.19 se muestran los valores principales de configuración de Red para el Nodo 1, si se ubica el puntero en otro nodo, se obtendrá los valores de configuración de los dispositivos de red para el nodo en el cual se haya ubicado el puntero. De esta manera funciona el simulador gráfico con cualquier dispositivo que forme parte de la red, y de esta manera se pueden obtener datos de forma más rápida y resumida para realizar estudios de análisis o corrección de errores durante la simulación.

Tabla.3.18 Valores de Configuración de los Dispositivos de Red en la Topología Ad-hoc

		Nodo 0	Nodo 1	Nodo 2
Mobility Model		ns3::RandomDirection2dMobilityModel		
NetDevice 0	**Type**	ns3::WifiNetDevice		
	IPv4	192.168.1.1/24	192.168.1.2/24	192.168.1.3/24
	Mac	05-06…00:01	05-06…00:02	05-…00:03
NetDevice 1	**Type**	ns3::LoopbackNetDevice		
	IPv4	127.0.0.1 / 255.0.0.0		

	Mac	05-06-00:00:00:00:00:00

En la Tabla 3.16 se muestran los valores de configuración predefinidos en el script, hay que resaltar los valores más importantes a tomar en cuenta que son los siguientes factores:

Mobility Model.- El cual representa el tipo de movilidad que se va a configurar a cada uno de los nodos, para este caso se ha configurado nodos móviles los cuales realizan movimientos aleatorios (RandomDirection2d) alrededor del área predefinida en el script.

Al igual que en las simulaciones anteriores, se debe tomar en cuenta la clase ns3::MobilityHelper la cual gestiona las características de movimiento que se pueden configurar en los nodos que forman parte de la red en cuestión.

NetDevice 0.- Este se encarga de presentar el tipo de dispositivo que ha sido configurado (Type) en este caso se ha configurado dispositivos WIfi (WifiNetDevice), adicionalmente presenta la dirección IPv4 configurada previamente (IPv4Addresses) y finalmente la dirección de MAC que es única y exclusiva para cada uno de los nodos (MacAddress). En la Tabla 3.16 se presenta la dirección MAC del siguiente modo 05-06…00:0X, debido a la extensión de la dirección que se visualiza de mejor manera en la Figura 3.19.

NetDevice 1.- Al igual que en las simulaciones anteriores en éste se visualiza los datos del controlador de red del mismo dispositivo pero para su propia tarjeta de red (localhost)

Iniciada la simulación en la Figura 3.20 se puede observar el envío de los paquetes desde todos los nodos, entre ellos los paquetes de enrutamiento de datos OLSR los cuales serán analizados en el correspondiente capítulo. Mientras tanto en la Figura 3.21 se indica vía Terminal, la notificación de que los paquetes han sido recibidos por cada unos de los nodos.

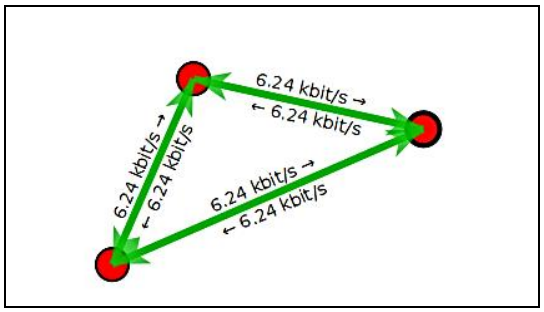


Figura.3.23. Envío y recepción de datos visualizado en Pyviz

```
Waf: Leaving directory `/home/ricky/ns-allinone-3.10/ns-3.10/build'
'build' finished successfully (4.668s)
Testing 10 packets sent
09:10:47 environ                No es_EC translation found for domain kiwi
scanning topology: 3 nodes...
scanning topology: calling graphviz layout
scanning topology: all done.
/home/ricky/ns-allinone-3.10/ns-3.10/src/tools/visualizer/visualizer/core.py:132
2: Warning: g_object_set_qdata: assertion `G_IS_OBJECT (object)' failed
  item = item.props.parent
/home/ricky/ns-allinone-3.10/ns-3.10/src/tools/visualizer/visualizer/core.py:116
2: Warning: g_object_set_qdata: assertion `G_IS_OBJECT (object)' failed
  gtk.main()
Se ha recibido un paquete...!!!
Se ha recibido un paquete...!!!
Se ha recibido un paquete...!!!
Se ha recibido un paquete...!!!
Se ha recibido un paquete...!!!
Se ha recibido un paquete...!!!
Se ha recibido un paquete...!!!
Se ha recibido un paquete...!!!
Se ha recibido un paquete...!!!
Se ha recibido un paquete...!!!
```

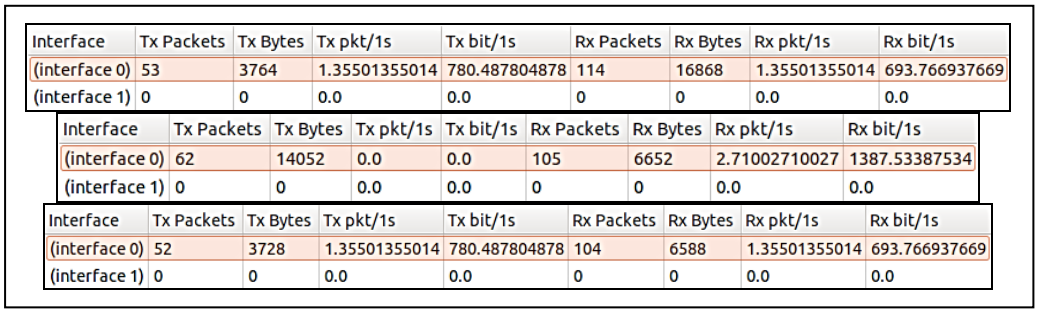
Figura.3.24. Notificación de Recepción de datos en los nodos visualizados en Terminal

La herramienta gráfica *Pyviz*, permite obtener datos de 4 configuraciones realizadas en el *script*, éstas facilitan el análisis de la red implementada y son las siguientes:

- Estadísticas de las Interfaces
- Tabla de enrutamiento IPv4
- Tabla de enrutamiento OLSR
- Últimos paquetes

Estadísticas de las Interfaces

Las estadísticas de las interfaces nos indica un resumen gráfico proveniente de la herramienta *Pyviz*, éste resumen se encuentra en la Figura 3.22, aquí se muestran las estadísticas para los 3 nodos que forman parte de la topología de red. Se tabula tanto para el comportamiento del nodo ya sea como transmisor o receptor de la información. A continuación se listan los parámetros presentados y la función de cada uno de ellos.



Interface	Tx Packets	Tx Bytes	Tx pkt/1s	Tx bit/1s	Rx Packets	Rx Bytes	Rx pkt/1s	Rx bit/1s
(interface 0)	53	3764	1.35501355014	780.487804878	114	16868	1.35501355014	693.766937669
(interface 1)	0	0	0.0	0.0	0	0	0.0	0.0

Interface	Tx Packets	Tx Bytes	Tx pkt/1s	Tx bit/1s	Rx Packets	Rx Bytes	Rx pkt/1s	Rx bit/1s
(interface 0)	62	14052	0.0	0.0	105	6652	2.71002710027	1387.53387534
(interface 1)	0	0	0.0	0.0	0	0	0.0	0.0

Interface	Tx Packets	Tx Bytes	Tx pkt/1s	Tx bit/1s	Rx Packets	Rx Bytes	Rx pkt/1s	Rx bit/1s
(interface 0)	52	3728	1.35501355014	780.487804878	104	6588	1.35501355014	693.766937669
(interface 1)	0	0	0.0	0.0	0	0	0.0	0.0

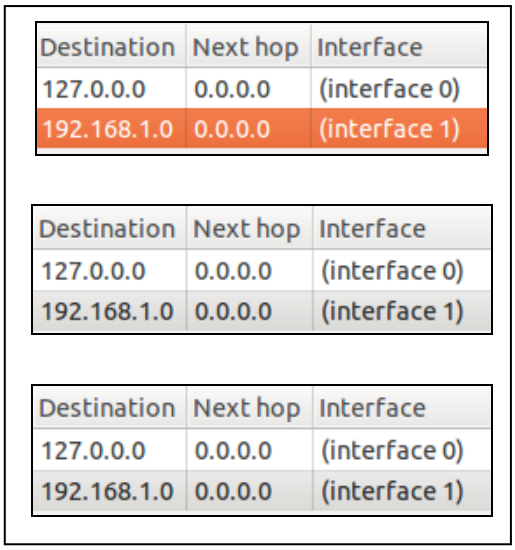
Figura.3.25. Estadísticas de las Interfaces

Como se puede apreciar en la Figura 3.22 se indican los datos obtenidos en cada nodo, respecto a las estadísticas de los paquetes enviados y recibidos, características de transmisión y recepción.

La interpretación de estos datos es similar a la realizada para las simulaciones anteriores por lo que su explicación resulta redundante.

Tabla de Enrutamiento IPv4

La tabla de enrutamiento almacena las rutas a las diferentes redes en una red inalámbrica. Para el caso presentado en la topología tipo Ad-hoc la ruta configurada es la ruta por defecto ya que es una topología bastante simple y suficiente para la explicación en el funcionamiento del enrutamiento de paquetes durante la simulación.



Destination	Next hop	Interface
127.0.0.0	0.0.0.0	(interface 0)
192.168.1.0	0.0.0.0	(interface 1)

Destination	Next hop	Interface
127.0.0.0	0.0.0.0	(interface 0)
192.168.1.0	0.0.0.0	(interface 1)

Destination	Next hop	Interface
127.0.0.0	0.0.0.0	(interface 0)
192.168.1.0	0.0.0.0	(interface 1)

Figura 3.26. Tablas de Enrutamiento de los Nodos

Como se puede apreciar en la Figura 3.23 se identifican los tres nodos respectivamente en el orden presentado, con sus respectivas tablas de enrutamiento, como se puede observar son exactamente los mismos valores para cada nodo, esto debido a que se manejan enrutamiento estáticos y topologías simples.

Los campos que se pueden apreciar en estas tablas de enrutamiento son las mismas que se presentan en todas las simulaciones anteriores, estos campos son las siguientes:

- *Destination*
- *Next hop*
- *Interface*

Tabla de Enrutamiento OLSR

La tabla de enrutamiento OLSR mantiene rutas estáticas del siguiente salto en el cual los paquetes serán enviados hacia toda la red. Esto quiere decir que simplemente este protocolo de enrutamiento permite enviar datos solamente al

siguiente salto o a su vecino más cercano para enviar información de datos y de control. En la sección correspondiente al análisis se profundizará éste estudio.

Destination	Next hop	Interface	Num. Hops
192.168.1.2	192.168.1.2	(interface 1)	1
192.168.1.3	192.168.1.3	(interface 1)	1

Destination	Next hop	Interface	Num. Hops
192.168.1.1	192.168.1.1	(interface 1)	1
192.168.1.3	192.168.1.3	(interface 1)	1

Destination	Next hop	Interface	Num. Hops
192.168.1.1	192.168.1.1	(interface 1)	1
192.168.1.2	192.168.1.2	(interface 1)	1

Figura 3.27 Tabla de Enrutamiento OLSR

En la Figura 3.24 se aprecian las tablas de enrutamiento de cada uno de los nodos que conforman la red simulada en este caso. En éstos se puede distinguir, al igual que en la tabla de enrutamiento para IPv4, cuatro campos que presentan la información de las rutas definidas por este protocolo. Estos campos son muy importantes a la hora del análisis, en especial para mantener la comunicación entre los nodos, estos campos son:

- *Destination*
- *Next hop*
- *Interface*
- *Num. Hops*

Los tres primeros campos son exactamente los mismos a los explicados anteriormente; el nuevo campo que presenta este protocolo es el campo de *Num. Hops* el mismo que simplemente indica el número de saltos que deben recorrer los paquetes para llegar hacia el dispositivo destino que se presenta en el primer campo.

Últimos Paquetes

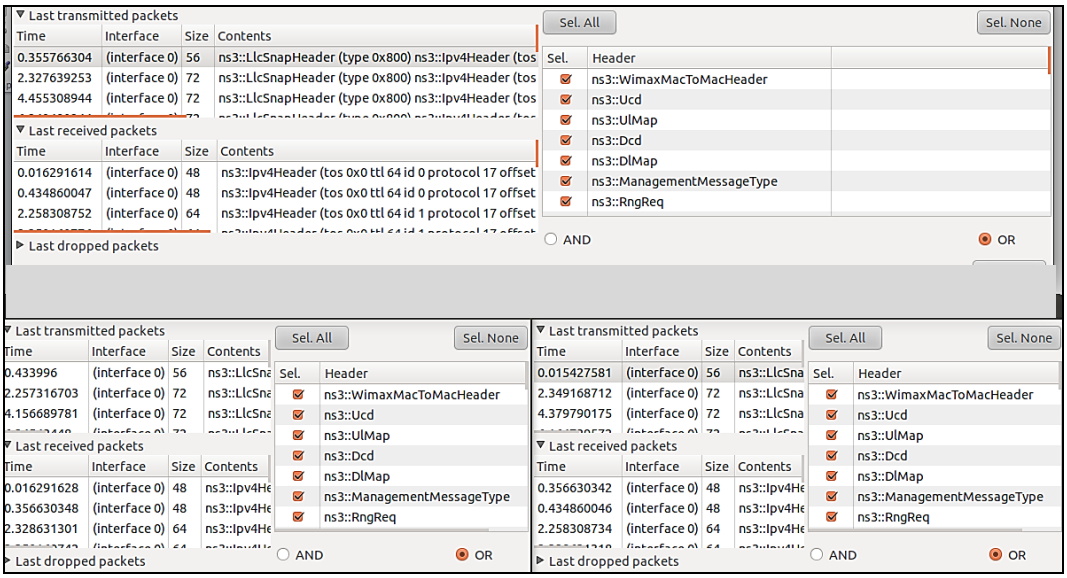


Figura 3.28. Estadísticas de los últimos paquetes enviados y recibidos

En la Figura 3.25 se detalla los valores de los últimos paquetes transmitidos y enviados por cada nodo. Este detalle divide a cada estadística en cuatro partes. La primera que es la de los paquetes transmitidos, una segunda con los paquetes recibidos, la tercera con los paquetes desechados y la cuarta que es una sección de selección o categorización de las cabeceras que se desea presentar en el resumen de contenido las primeras tres partes del resumen presentado en la Figura 3.25.

Las principales cabeceras que se agregan durante la transmisión inalámbrica IEEE 802.11 en la topología Ad-hoc son las siguientes:

- ns3::LlcSnapHeader
- ns3::Ipv4Header
- ns3::UdpHeader
- ns3::olsr::PacketHeader

- ns3::olsr::MessageHeader

*ns3::*LlcSnapHeader.- Este protocolo de Control de enlace lógico LLC define la forma en que los datos son transferidos sobre el medio físico,, de igual manera que en las simulaciones anteriores en la cabecera *ns3::LlcSnapHeader* se añade el identificador del tipo de protocolo del paquete contenido, el valor de 0x800 que corresponde al protocolo IP.

ns3::Ipv4Header.- Esta es la representación de la cabecera del protocolo IP, que presenta información de los campos utilizados durante la transmisión y recepción de la información. Estos campos se resumen en la Tabla 3.17 presentada a continuación.

Tabla 3.19. Campos de la Cabecera IPv4

TOS (*Type of Service*)	**TTL (*Time to live*)**	***Protocol***	***Offset***	***Flags***	***Lenght***
0x0	64	17	0	-	64

ns3::UdpHeader.- En este campo se muestran las cabeceras que viajan a través de la red utilizando el protocolo UDP (*User Datagram Protocol*). La cabecera UDP es muy simple, tan solo ocupa 8 bytes y los campos más representativos durante la transmisión de datos son los siguientes:

Tabla. 3.20. Campos de la Cabecera UDP

Length	**Puerto Origen**	**Puerto Destino**	***Payload***
1008	49153	80	1000

ns3::olsr::PacketHeader y ns3::olsr::MessageHeader.- Estos paquetes son simplemente paquetes de control que envía el protocolo OLSR por lo que el analizador gráfico de cabeceras de *Pyviz* no muestra mayor información y tan solo

indica que existen esas cabeceras más la información es nula para estas cabeceras. En la Figura 3.26 se aprecia la presentación de éstas cabeceras.

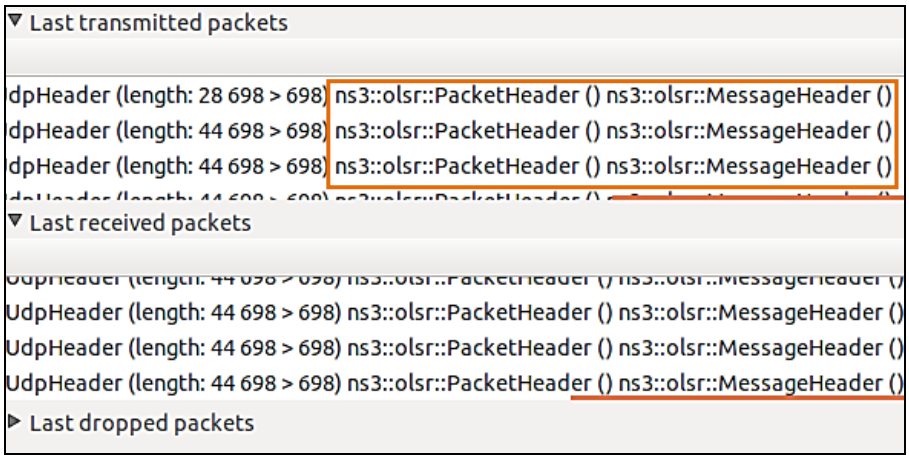


Figura. 3.29. Cabeceras del protocolo OLSR

Estos son los principales datos obtenidos utilizando la herramienta *Pyviz* implementada con *ns-3*, con todos estos datos se puede realizar el análisis respectivo de esta red sin antes recoger los datos obtenidos por el analizador de protocolos *Wireshark*, el cual se la emplea para el análisis de los archivos de captura de datos generados durante la simulación. Los archivos de captura son presentados en la Tabla 3.19.

Tabla. 3.21. Archivos de Captura para la Simulación Tipo Ad-hoc

Archivo de Captura	Nodo
wifi-adhoc-0-0.pcap	Nodo 0
wifi-adhoc-1-0.pcap	Nodo 1
wifi-adhoc-2-0.pcap	Nodo 2

Análisis del archivo de Captura para el Nodo 0

Para el análisis del archivo de captura del nodo 0, al igual que en los anteriores casos se realizará un análisis de los paquetes tanto los transmitidos como de los recibidos por parte de éste nodo.

Durante el análisis hay que identificar tres procesos claves que se presentan en la simulación y que se deben tomar en cuenta para verificar el funcionamiento de la red, estos procesos son los siguientes:

- Proceso de Control de Tráfico
- Proceso de Descubrimiento de la Red
- Proceso de Transferencia de Datos

Proceso de Control de Tráfico

Este es un proceso en el cual el protocolo de enrutamiento OLSR realiza el envío de paquetes de mensajes de control para el reconocimiento de vecinos en la topología y para reconstrucción de la base de datos topológica. Este proceso se lo realiza de manera repetitiva y se lo hace solamente cuando no se encuentran los nodos transmitiendo datos. En la Figura 3.27 se puede apreciar los paquetes que se envían desde cada nodo hacia sus respectivos receptores de estos mensajes.

No.	Time	Source	Destination	Protocol	Info	802.11 Tx rate	802.11 rssi
1	0.000000	192.168.1.3	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 20 Bytes	1.0	-60 dBm
2	0.339475	192.168.1.1	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 20 Bytes	1.0	
3	0.418569	192.168.1.2	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 20 Bytes	1.0	-63 dBm
4	2.242017	192.168.1.2	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-63 dBm
5	2.311348	192.168.1.1	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	
6	2.333869	192.168.1.3	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-65 dBm
7	4.141390	192.168.1.2	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-62 dBm
8	4.364491	192.168.1.3	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-60 dBm
9	4.439017	192.168.1.1	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	
10	6.149430	192.168.1.3	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-66 dBm
11	6.230125	192.168.1.2	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-59 dBm

Figura. 3.30. Proceso de Control de Tráfico

Al igual que en las anteriores simulaciones se tabulará los campos presentados durante esta simulación y la presentación de datos por parte del analizador de protocolos *Wireshark*. En la Tabla 3.20 se especifican las columnas que poseen los datos más importantes durante la simulación.

Tabla. 3.22. Campos de Información del Panel de Lista de Paquetes

Campo	Descripción
No.	Representa el número de paquete capturado durante la simulación.
Time	La marca de tiempo del paquete en el instante mismo en el cual fue capturado.
Source	La dirección del dispositivo que envió el paquete.
Destination	La dirección del dispositivo hacia donde esta destinado el paquete.
Protocol	Presenta el nombre abreviado del protocolo de comunicación utilizado.
Info	Información adicional que presente el paquete.
802.11 Tx rate	Información de la tasa de transmisión utilizada por el protocolo IEEE 802.11
802.11 rssi	Información sobre la potencia de señal de recepción en el protocolo IEEE 802.11

Los detalles para cada paquete de control se presenta en el panel de detalles que presenta *Wireshark* para lo cual en la Figura 3.28 se presentan los campos a ser tomados en cuenta durante el análisis posterior.

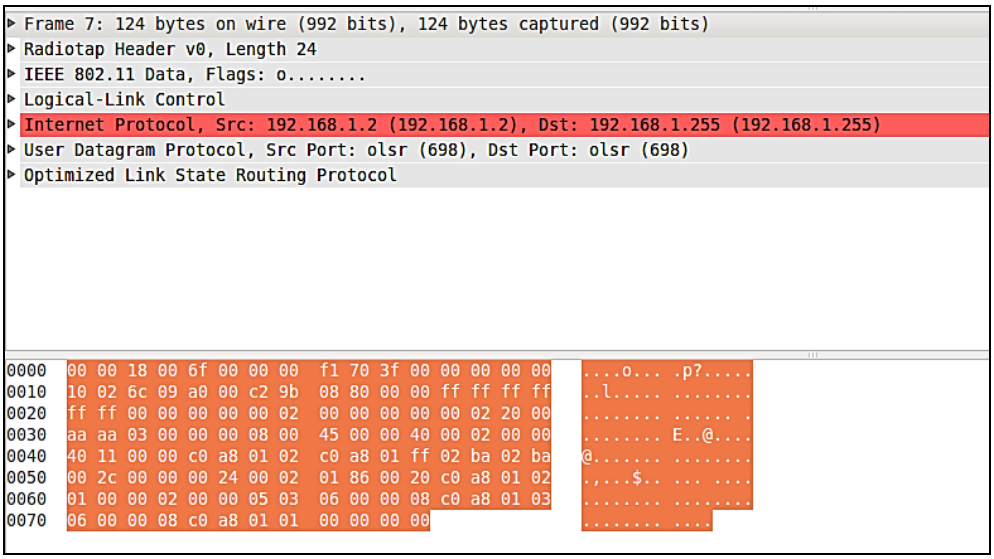


Figura. 3.31. Detalle del contenido del paquete de Control de Tráfico

A continuación en la Tabla 3.21 se ubican los valores obtenidos con cada campo presentado en el detalle del paquete seleccionado en la Figura 3.28

Tabla. 3.23. Descripción del Paquete de Control de Tráfico

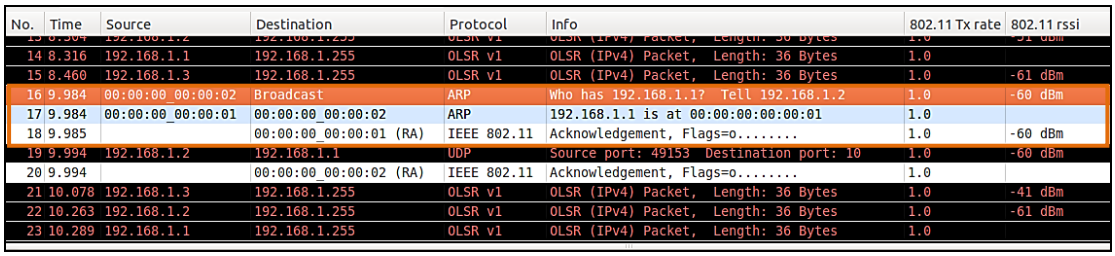
FRAME 7	*Time*	2.327
	Frame Number	5
	Frame Length	122 bytes
	Protocols in Frame	radiotap:wlan:llc:ip:udp:olsr
RADIOTAP HEADER	*Header Length*	22 bytes
	Data Rate	1,0 Mb/s
	Channel Frequency	2412 MHz
	Channel Type	802.11b
IEEE 802.11 DATA	*Frame Control*	0x8008
	Duration	0
	Destination Address	Broadcast (ff:ff:ff:ff:ff:ff)
	Source Address	00:00:00_00:00:01
	BSS Id	
	Fragment Number	0
	Sequence Number	1
LOGICAL-LINK CONTROL	DSAP	SNAP[5] (0xaa)
	IG Bit	*Individual*
	SSAP	SNAP (0xaa)
	CR Bit	*Command*
	Type	IP (0x0800)
INTERNET PROTOCOL	*Version*	4
	Header Length	20 bytes

[5] SNAP: *Subnetwork Access Protocol*, Permite transmisión de datagramas IP sobre redes IEEE 802.

<table>
<tr><td rowspan="5"></td><td>Total Length</td><td colspan="2">64 bytes</td></tr>
<tr><td>Time to Live</td><td colspan="2">64</td></tr>
<tr><td>Protocol</td><td colspan="2">UDP (17)</td></tr>
<tr><td>Source</td><td colspan="2">192.168.1.2</td></tr>
<tr><td>Destination</td><td colspan="2">192.168.1.255</td></tr>
<tr><td rowspan="3">USER DATAGRAM PROTOCOL</td><td>Source Port</td><td colspan="2" rowspan="2">olsr (698)</td></tr>
<tr><td>Destination Port</td></tr>
<tr><td>Length</td><td colspan="2">44 bytes</td></tr>
<tr><td rowspan="8">OPTIMIZED LINK STATE PROTOCOL</td><td>Packet Length</td><td colspan="2">36 bytes</td></tr>
<tr><td>Packet Sequence Number</td><td colspan="2">1</td></tr>
<tr><td rowspan="6">Message</td><td rowspan="6">HELLO</td><td>Message Type: Hello (1)</td></tr>
<tr><td>Validity Time: 6 (seg)</td></tr>
<tr><td>Originator Address: 192.168.1.1</td></tr>
<tr><td>TTL: 1</td></tr>
<tr><td>Hello Emission Interval: 2 (seg)</td></tr>
<tr><td>Link Type: Asymmetric Link</td></tr>
</table>

Proceso de Descubrimiento de la Red

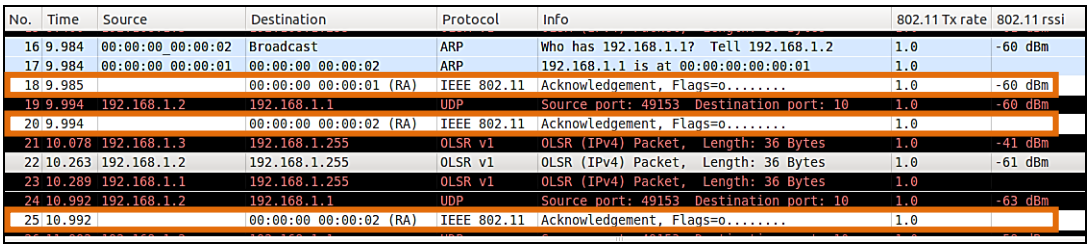
El proceso de descubrimiento de la red está basado en el protocolo de resolución de direcciones ARP (*Address Resolution Protocol*). Este protocolo se encarga de resolver una petición enviada por *broadcast* para encontrar la dirección IP que se busca durante el procedimiento de descubrimiento de la red, ésta IP pertenece a una dirección física de algún dispositivo el mismo que responde este pedido de ARP (ARP *request*) con un ARP *response* entregando la dirección que le corresponde. En la Figura 3.29 se puede observar este procedimiento en el recuadro indicado.



No.	Time	Source	Destination	Protocol	Info	802.11 Tx rate	802.11 rssi
14	8.316	192.168.1.1	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	
15	8.460	192.168.1.3	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-61 dBm
16	9.984	00:00:00_00:00:02	Broadcast	ARP	Who has 192.168.1.1? Tell 192.168.1.2	1.0	-60 dBm
17	9.984	00:00:00_00:00:01	00:00:00_00:00:02	ARP	192.168.1.1 is at 00:00:00:00:00:01	1.0	
18	9.985		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o.....	1.0	-60 dBm
19	9.994	192.168.1.2	192.168.1.1	UDP	Source port: 49153 Destination port: 10	1.0	-60 dBm
20	9.994		00:00:00_00:00:02 (RA)	IEEE 802.11	Acknowledgement, Flags=o.....	1.0	
21	10.078	192.168.1.3	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-41 dBm
22	10.263	192.168.1.2	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-61 dBm
23	10.289	192.168.1.1	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	

Figura. 3.32 Descubrimiento de la Red mediante el protocolo ARP

El protocolo IEEE 802.11 también realiza un proceso de reconocimiento, en especial con los dispositivos vecinos, el paquete que envía simplemente es un paquete de ACK el mismo que permite reconocer a los dispositivos con los cuales va a realizar el enlace y la posterior transmisión de datos. En la Figura 3.30 se remarca este paquete que se encuentra a lo largo de toda la simulación.



No.	Time	Source	Destination	Protocol	Info	802.11 Tx rate	802.11 rssi
16	9.984	00:00:00_00:00:02	Broadcast	ARP	Who has 192.168.1.1? Tell 192.168.1.2	1.0	-60 dBm
17	9.984	00:00:00 00:00:01	00:00:00 00:00:02	ARP	192.168.1.1 is at 00:00:00:00:00:01	1.0	
18	9.985		00:00:00 00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o.....	1.0	-60 dBm
19	9.994	192.168.1.2	192.168.1.1	UDP	Source port: 49153 Destination port: 10	1.0	-60 dBm
20	9.994		00:00:00 00:00:02 (RA)	IEEE 802.11	Acknowledgement, Flags=o.....	1.0	
21	10.078	192.168.1.3	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-41 dBm
22	10.263	192.168.1.2	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-61 dBm
23	10.289	192.168.1.1	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	
24	10.992	192.168.1.2	192.168.1.1	UDP	Source port: 49153 Destination port: 10	1.0	-63 dBm
25	10.992		00:00:00 00:00:02 (RA)	IEEE 802.11	Acknowledgement, Flags=o.....	1.0	

Figura. 3.33. Paquetes ACK bajo el protocolo IEEE 802.11

Cada uno de estos paquetes transmitidos por ARP tanto para el paquete de *Request* como para el de *Reply* presentan valores diferentes los mismos que son presentados en la Tabla 3.22 y la Tabla 3.23 respectivamente.

Tabla. 3.24. Descripción del Paquete de ARP (*request*)

FRAME 16	*Time*	9.984 (seg)
	Frame Number	16
	Frame Length	88 bytes
	Protocols in Frame	radiotap:wlan:llc:arp
RADIOTAP HEADER	*Header Length*	24 bytes
	Data Rate	1,0 Mb/s

	Channel Frequency	2412 MHz
	Channel Type	802.11b
	SSI *Signal*	- 60 dBm
	SSI *Noise*	-101 dBm
IEEE 802.11 DATA	*Destination Address*	ff:ff:ff:ff:ff:ff
	Source Address	00:00:00_00:00:02
	BSS Id	
LOGICAL-LINK CONTROL	DSAP	SNAP (0xaa)
	IG Bit	*Individual*
	SSAP	SNAP (0xaa)
	CR Bit	*Command*
	Type	ARP
ADDRESS RESOLUTION PROTOCOL	*Protocol Type*	IP (0x0800)
	Sender MAC address	00:00:00_00:00:02
	Sender IP address	192.168.1.2
	Target MAC address	ff:ff:ff:ff:ff:ff
	Target IP address	192.168.1.1

Tabla. 3.25. Descripción del Paquete de ARP (*reply*)

FRAME 17	*Time*	9.984 (seg)
	Frame Number	17
	Frame Length	86 bytes
	Protocols in Frame	radiotap:wlan:llc:arp
RADIOTAP HEADER	*Header Length*	22 bytes
	Data Rate	1,0 Mb/s
	Channel Frequency	2412 MHz
	Channel Type	802.11b
IEEE 802.11 DATA	*Destination Address*	00:00:00_00:00:02

	Source Address	00:00:00_00:00:01
	BSS Id	
LOGICAL-LINK CONTROL	DSAP	SNAP (0xaa)
	IG Bit	*Individual*
	SSAP	SNAP (0xaa)
	CR Bit	*Command*
	Type	ARP
ADDRESS RESOLUTION PROTOCOL	*Protocol Type*	IP (0x0800)
	Sender MAC address	00:00:00_00:00:01
	Sender IP address	192.168.1.1
	Target MAC address	00:00:00_00:00:02
	Target IP address	192.168.1.2

Adicionalmente para el protocolo IEEE 802.11 también se envía un paquete de ACK que permite reconocer a los dispositivos cercanos con quienes puede realizar transmisiones posteriormente.

Tabla. 3.26. Descripción del Paquete IEEE 802.11 (*Acknowledgement*)

FRAME 17	*Time*	9.984 (seg)
	Frame Number	17
	Frame Length	86 bytes
	Protocols in Frame	radiotap:wlan:llc:arp
RADIOTAP HEADER	*Header Length*	22 bytes
	Data Rate	1,0 Mb/s
	Channel Frequency	2412 MHz
	Channel Type	802.11b
	SSI *Signal*	- 60 dBm
	SSI *Noise*	-101 dBm

IEEE 802.11 DATA	*Destination Address*	ff:ff:ff:ff:ff:ff
	Source Address	00:00:00_00:00:02
	BSS Id	
LOGICAL-LINK CONTROL	DSAP	SNAP (0xaa)
	IG Bit	*Individual*
	SSAP	SNAP (0xaa)
	CR Bit	*Command*
	Type	ARP
ADDRESS RESOLUTION PROTOCOL	*Protocol Type*	IP (0x0800)
	Sender MAC address	00:00:00_00:00:02
	Sender IP address	192.168.1.2
	Target MAC address	ff:ff:ff:ff:ff:ff
	Target IP address	192.168.1.1

Proceso de Transferencia de Datos

Este proceso de transferencia se realiza utilizando un protocolo de comunicaciones como es el protocolo UDP (*User Datagram Protocol*). De acuerdo a la programación del *script* se puede ingresar la cantidad de paquetes que se requiere enviar durante la transmisión de datos.

En la Figura 3.31 se indica algunos paquetes UDP que se envían durante la transmisión, éstos paquetes adicionalmente tienen sus campos en las columnas siguientes se presentan valores adicionales los cuales se encuentran tabulados en la Tabla 3.25 con sus respectivos campos.

o.	Time	Source	Destination	Protocol	Info	802.11 Tx rate	802.11 rssi
18	9.985		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o........	1.0	-60 dBm
19	9.994	192.168.1.2	192.168.1.1	UDP	Source port: 49153 Destination port: 10	1.0	-60 dBm
20	9.994		00:00:00_00:00:02 (RA)	IEEE 802.11	Acknowledgement, Flags=o........	1.0	
21	10.078	192.168.1.3	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-41 dBm
22	10.263	192.168.1.2	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-61 dBm
23	10.289	192.168.1.1	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	
24	10.992	192.168.1.2	192.168.1.1	UDP	Source port: 49153 Destination port: 10	1.0	-63 dBm
25	10.992		00:00:00_00:00:02 (RA)	IEEE 802.11	Acknowledgement, Flags=o........	1.0	
26	11.992	192.168.1.2	192.168.1.1	UDP	Source port: 49153 Destination port: 10	1.0	-58 dBm
27	11.992		00:00:00_00:00:02 (RA)	IEEE 802.11	Acknowledgement, Flags=o........	1.0	
28	12.039	192.168.1.3	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-56 dBm
29	12.288	192.168.1.2	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-56 dBm
30	12.428	192.168.1.1	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	
31	12.992	192.168.1.2	192.168.1.1	UDP	Source port: 49153 Destination port: 10	1.0	-57 dBm
32	12.992		00:00:00_00:00:02 (RA)	IEEE 802.11	Acknowledgement, Flags=o........	1.0	
33	13.992	192.168.1.2	192.168.1.1	UDP	Source port: 49153 Destination port: 10	1.0	-63 dBm
34	13.992		00:00:00_00:00:02 (RA)	IEEE 802.11	Acknowledgement, Flags=o........	1.0	
35	14.062	192.168.1.2	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-63 dBm
36	14.124	192.168.1.3	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	-56 dBm
37	14.479	192.168.1.1	192.168.1.255	OLSR v1	OLSR (IPv4) Packet, Length: 36 Bytes	1.0	
38	14.992	192.168.1.2	192.168.1.1	UDP	Source port: 49153 Destination port: 10	1.0	-62 dBm
39	14.992		00:00:00_00:00:02 (RA)	IEEE 802.11	Acknowledgement, Flags=o........	1.0	
40	15.992	192.168.1.2	192.168.1.1	UDP	Source port: 49153 Destination port: 10	1.0	-47 dBm
41	15.992		00:00:00 00:00:02 (RA)	IEEE 802.11	Acknowledgement, Flags=o........	1.0	

Figura. 3.34. Paquetes enviados desde los nodos con paquetes UDP

Como se puede ver en la Figura 3.31 se resaltan los paquetes de UDP enviados por su dispositivo fuente hacia su dispositivo destino con la IP de cada uno de ellos. En el análisis respectivo se podrá indicar el comportamiento de cada valor presentado en cada campo en el detalle del paquete. Los valores que corresponden a cada paquete de UDP se detallan en la Tabla 3.25. .

Tabla. 3.27. Descripción del Paquete UDP

FRAME 24	*Time*	0.999970
	Frame Number	24
	Frame Length	1088 bytes
	Protocols in Frame	radiotap:wlan:llc:ip:udp:data
RADIOTAP HEADER	*Header Length*	24 bytes
	Data Rate	1,0 Mb/s
	Channel Frequency	2412 MHz
	Channel Type	802.11b
	SSI *Signal*	- 63 dBm
	SSI *Noise*	- 101 dBm
IEEE 802.11 DATA	*Destination Address*	00:00:00_00:00:01
	Source Address	00:00:00_00:00:02
	BSS Id	00:00:00_00:00:02

LOGICAL–LINK CONTROL	DSAP	SNAP	0xaa
	SSAP	SNAP	0xaa
	Organization Code	Encapsulado Ethernet	
	Type	IP	
INTERNET PROTOCOL	*Version*	4	
	Header Length	20 bytes	
	Total Length	1028 bytes	
	Time to Live	64	
	Protocol	UDP	
	Source	192.168.1.2	
	Destination	192.168.1.1	
USER DATAGRAM PROTOCOL	*Source Port*	49153	
	Destination Port	tcp (10)	
	Length	1008	
DATA	*Length*	1000 bytes	

Simulación Tipo Punto a Punto

En la simulación Tipo Punto a Punto se han dispuesto dos nodos de tal manera que el primer nodo mantiene una posición fija transmitiendo y recibiendo información hacia y desde el otro nodo, mientras tanto el segundo elemento de esta topología comienza a desplazarse a una velocidad constante en línea recta manteniendo una línea de vista hacia el otro nodo lo cual permite la comunicación entre ambos nodos durante un tiempo prolongado. En la Figura 3.32 se muestra la topología planteada para esta simulación, así mismo se indican los datos configurados previamente en el script para cada nodo, todo esto gracias a la utilización de la herramienta gráfica proporcionada por el simulador *ns*-3, *Pyviz* integra la herramienta instantánea con la cual solo con poner el cursor sobre el nodo se pueden obtener los principales datos configurados en la tarjeta de red inalámbrica.

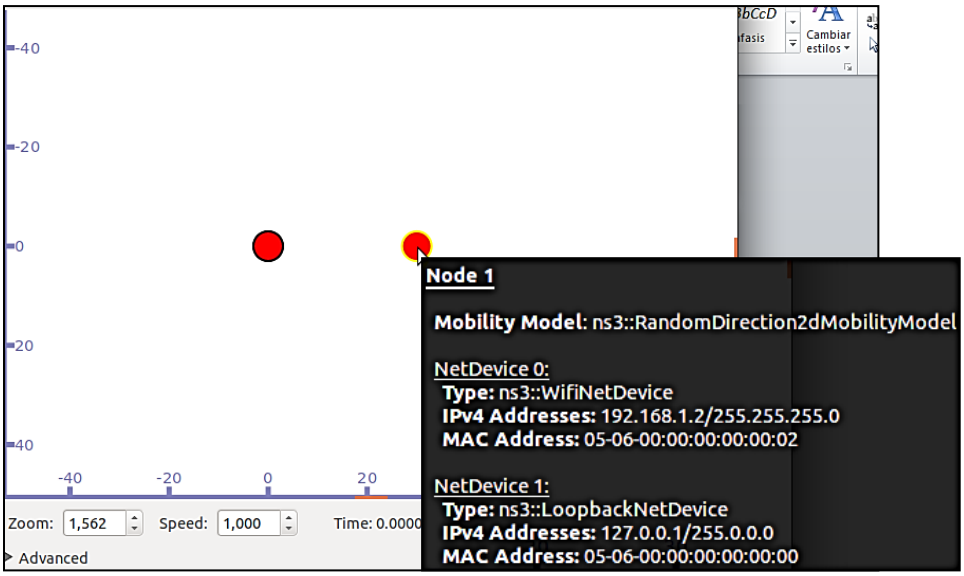


Figura. 3.35. Datos Obtenidos del Nodo 1 en la Topología Punto a Punto

En la Figura 3.32 se muestran los valores principales de configuración de la tarjeta de Red Inalámbrica para el Nodo 1, en el Nodo 0 obtendremos datos similares a los presentados anteriormente, la obtención de estos datos se tabulan en la Tabla 3.26 con todos los datos obtenidos por la herramienta Pyviz.

Tabla. 3.28. Valores de Configuración de los Dispositivos de Red en la Topología Punto a Punto

		Nodo 0	Nodo 1
Mobility Model		ns3::ConstantPositionMobilityModel	
NetDevice 0	**Type**	ns3::WifiNetDevice	
	IPv4	10.0.0.1/24	10.0.0.2/24
	Mac	02-06…00:01	02-06…00:02
NetDevice 1	**Type**	ns3::LoopbackNetDevice	
	IPv4	127.0.0.1 / 255.0.0.0	
	Mac	02-06-00:00:00:00:00:00	

En la Tabla 3.26 se muestran los valores de configuración predefinidos en el *script*, hay que resaltar los valores más importantes a tomar en cuenta que son los siguientes factores:

Mobility Model.- El cual representa el tipo de movilidad que se va a configurar a cada uno de los nodos, para este caso se ha configurado nodos de posición constante, esto debido a que se requiere que uno de los nodos mantengan un posición fija, mientras que el otro nodo logra la movilidad durante la simulación mediante un algoritmo implementado en el código.

Al igual que en las simulaciones anteriores, se debe tomar en cuenta la clase *ns3::MobilityHelper* la cual gestiona las características de movimiento que se pueden configurar en los nodos que forman parte de la red en cuestión.

NetDevice 0.- Este se encarga de presentar el tipo de dispositivo que ha sido configurado (*Type*) en este caso se ha configurado dispositivos Wifi (*WifiNetDevice*), adicionalmente presenta la dirección IPv4 configurada previamente (*IPv4Addresses*) y finalmente la dirección de MAC que es única y exclusiva para cada uno de los nodos (*MacAddress*). En la Tabla 3.26 se presenta la dirección MAC del siguiente modo 02-06…00:0X, debido a la extensión de la dirección que se visualiza de mejor manera en la Figura 3.33.

NetDevice 1.- Al igual que en las simulaciones anteriores en éste se visualiza los datos del controlador de red del mismo dispositivo pero para su propia tarjeta de red *(localhost)*

Iniciada la simulación en la Figura 3.33 se puede observar el envío de los paquetes desde ambos nodos, mucho de estos paquetes son los conocidos como paquetes de *Beacon* adicionalmente se envían paquetes de información los cuales serán analizados en el correspondiente capítulo.

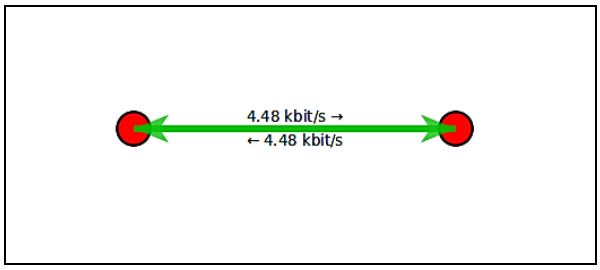


Figura. 3.36. Envío y recepción de datos en topología Punto a Punto

La herramienta gráfica *Pyviz*, permite obtener datos de 4 configuraciones realizadas en el *script*, éstas facilitan el análisis de la red implementada y son las siguientes:

- Estadísticas de las Interfaces
- Tabla de enrutamiento IPv4
- Tabla de enrutamiento OLSR
- Últimos paquetes

Estadísticas de las Interfaces

Las estadísticas de las interfaces nos indica un resumen gráfico proveniente de la herramienta *Pyviz*, éste resumen se encuentra en la Figura 3.34, aquí se muestran las estadísticas para los dos nodos que forman parte de la topología de la red. Se tabula tanto para el comportamiento del nodo ya sea como transmisor o receptor de la información.

Nodo 0

Interface	Tx Packets	Tx Bytes	Tx pkt/1s	Tx bit/1s	Rx Packets	Rx Bytes	Rx pkt/1s	Rx bit/1s
(interface 0)	4	248	1.11111111111	568.888888889	4	216	1.11111111111	497.777777778
(interface 1)	0	0	0.0	0.0	0	0	0.0	0.0

Nodo 1

Interface	Tx Packets	Tx Bytes	Tx pkt/1s	Tx bit/1s	Rx Packets	Rx Bytes	Rx pkt/1s	Rx bit/1s
(interface 0)	4	248	1.11111111111	568.888888889	4	216	1.11111111111	497.777777778
(interface 1)	0	0	0.0	0.0	0	0	0.0	0.0

Figura. 3.37. Estadísticas de las Interfaces en la Topología Punto a Punto

Como se puede apreciar en la Figura 3.34 se indican los datos obtenidos en cada nodo, respecto a las estadísticas de los paquetes enviados y recibidos, características de transmisión y recepción.

Es importante tomar en cuenta los datos presentados tanto para el Nodo 0 y el Nodo 1 ya que en el análisis se indicará la diferencia existente entre las velocidad de transmisión que cada nodo presenta respecto a la recepción. Como la configuración es realizada para que se envíen y se reciban datos al mismo tiempo la visualización de los paquetes enviados y recibidos son mas fáciles de explicar.

Tabla de Enrutamiento IPv4

La tabla de enrutamiento almacena las rutas a las diferentes redes en una red inalámbrica. Para el caso presentado en la topología tipo Punto a Punto se ha configurado una ruta por defecto debido a la simplicidad de la topología.

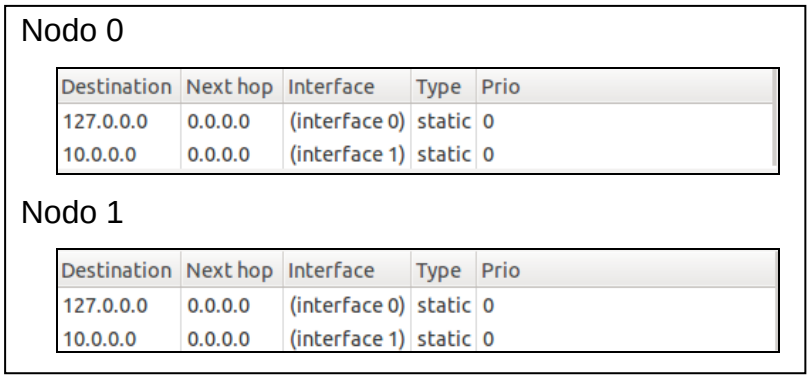


Figura. 3.38. Tablas de Enrutamiento de los Nodos para la Topología Punto a Punto

Como se puede apreciar en la Figura 3.35 se identifican los dos nodos con sus respectivas tablas de enrutamiento, aquí se observan exactamente los mismos valores para cada nodo, esto debido a que se manejan enrutamiento estáticos y topologías simples.

Los campos que se pueden apreciar en las tablas de enrutamiento son los siguientes:

- *Destination*
- *Next hop*
- *Interface*
- *Type*
- *Prio*

El campo *Destination* representa la red de destino que será utilizada para enrutar el paquete de acuerdo a la tarjeta de red que se encuentre utilizando.

El siguiente campo *Next hop* simplemente muestra la ruta por defecto que tomará el paquete en caso de que no encuentre el siguiente salto para la entrega de la información.

El campo *Interface* identifica a la interface utilizada por el nodo para realizar el envío o recepción de los datos.

El campo *Type* indica el tipo de ruta configurada en cada nodo, en este caso todas las rutas configuradas son estáticas debido a la simplicidad de la topología.

Finalmente el campo *Prio* indica la prioridad de la ruta a ser utilizada, mientras más bajo sea el valor configurado en este campo la ruta tiene mayor prioridad y el nodo elegirá ésta ruta para enviar el paquete, en caso de que existan prioridades iguales como se muestra en la Figura 3.35 el paquete es enviado por la interface que maneje una ruta por defecto como ambas interfaces en los dos nodos manejan esta ruta por defecto el paquete es enviado por la dirección destino de la red configurada en este caso la dirección 10.0.0.0 la cual identifica a la red de la topología.

Tabla de Enrutamiento OLSR

La tabla de enrutamiento OLSR mantiene rutas estáticas del siguiente salto, en este caso el siguiente salto de cada nodo es el otro nodo.

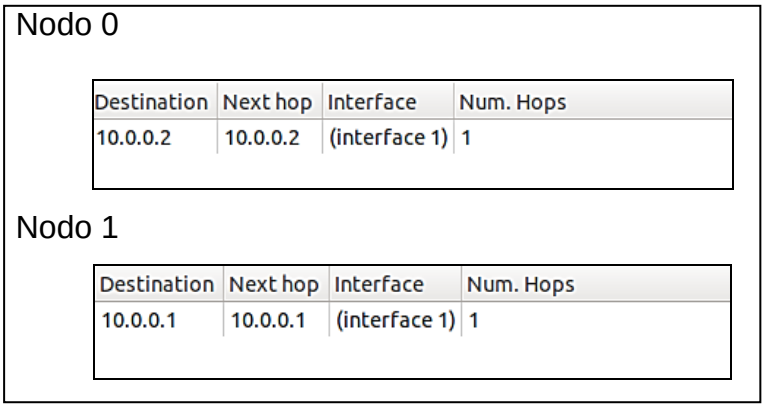


Figura. 3.39. Tabla de Enrutamiento OLSR para la Topología Punto a Punto

En la Figura 3.36 se aprecia las tablas de enrutamiento de los dos nodos que conforman la red simulada en este caso. En estas tablas se puede distinguir cuatro campos que presentan la información de las rutas definidas por este protocolo.

Los campos presentados en las tablas de enrutamiento OLSR son los siguientes:

- *Destination*
- *Next hop*
- *Interface*
- *Num. Hops*

A diferencia de los campos explicados para el enrutamiento de IPv4 es que ahora no se toma en cuenta las redes de destino sino específicamente el nodo del siguiente salto con su dirección IP al igual que en el campo de *Next hop* en el cual se especifica la dirección del siguiente salto, la cual es determinada por la IP del siguiente nodo al que se va a transmitir la información.

Últimos Paquetes

Figura. 3.40 Estadísticas de los últimos paquetes Topología Punto a Punto

En la Figura 3.37 se detalla los valores de los últimos paquetes transmitidos y enviados por cada nodo. Este detalle divide a cada estadística en cuatro partes. La primera que es la de los paquetes transmitidos, una segunda con los paquetes recibidos, la tercera con los paquetes desechados y la cuarta que es una sección de selección o categorización de las cabeceras que se desea presentar en el resumen de contenido de las anteriores tres partes.

Las principales cabeceras que se agregan durante la transmisión inalámbrica IEEE 802.11 en la topología Punto a Punto son las siguientes:

- ns3::LlcSnapHeader
- ns3::Ipv4Header
- ns3::UdpHeader

- ns3::olsr::PacketHeader

- ns3::olsr::MessageHeader

Prácticamente son las mismas cabeceras presentadas en la simulación Tipo Ad-hoc y su explicación resulta redundante, mas los datos obtenidos en cada campo son los importantes y son requeridos para el análisis posterior de la simulación.

En la Tabla 3.27 se presentan los valores obtenidos en el campo de la cabecera IPv4 (ns3::*Ipv4Header*)

Tabla. 3.29. Campos de la Cabecera IPv4 para el Tipo Punto a Punto

TOS (*Type of Service*)	**TTL (*Time to live*)**	***Protocol***	***Offset***	***Flags***	***Lenght***
0x0	64	17	0	-	56

Mientras tanto que para la cabecera UDP (*ns3::UdpHeader*) también se obtienen valores después de realizada la simulación, estos son importantes en especial para el análisis del tráfico “inyectado” en la red después de realizado el procedimiento de envío y recepción de la información. En la Tabla 3.28 se especifican los valores obtenidos desde la herramienta gráfica *Pyviz.*

Tabla 3.30. Campos de la Cabecera UDP para el Tipo Punto a Punto

Length	**Puerto Origen**	**Puerto Destino**
36	698	80

Finalmente los valores tanto para las cabeceras de los paquetes OLSR así como para las cabeceras de los mensajes OLSR son identificados en la Figura 3.38 tanto para el Nodo 0 como para el Nodo 1.

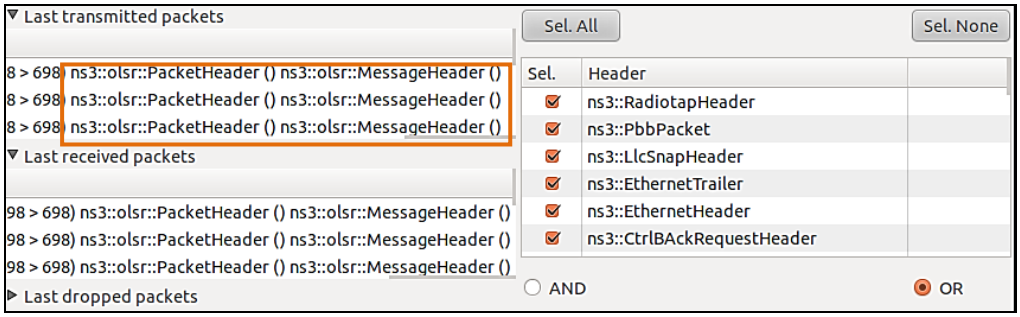


Figura 3.41. Cabeceras del protocolo OLSR

Es importante también la obtención de datos generados en el script mediante archivos de captura de protocolos, para poder interpretar dichos valores se requiere de una herramienta especializada en lectura de archivos de formato *.pcap*, para esto se utiliza el analizador de protocolos *Wireshark*, el cual se la emplea para el análisis de los archivos de captura de datos generados durante la simulación. Los archivos de captura son presentados en la Tabla 3.29.

Tabla 3.31. Archivos de Captura para la Simulación Tipo Punto a Punto

Archivo de Captura	Nodo
puntopunto-0-0.pcap	Nodo 0
puntopunto-1-0.pcap	Nodo 1

Para el análisis de estos archivos de captura es suficiente el análisis de un solo archivo ya que al ser una topología sencilla los datos capturados son prácticamente los mismos tanto para el Nodo 0 como para el Nodo 1.

Para el análisis se tomará el archivo de captura del Nodo 0 el mismo que representa al nodo fijo el cual realiza el envío y recepción de información por su tarjeta de red inalámbrica configurada previamente.

Análisis del archivo de Captura para el Nodo 0

Para el análisis del archivo de captura del nodo 0, al igual que en los anteriores casos se realizará un análisis de los paquetes tanto los transmitidos como de los recibidos por parte de éste nodo.

Durante el análisis hay que identificar dos procesos claves que se presentan en la simulación y que se deben tomar en cuenta para verificar el funcionamiento de la red, estos procesos son los siguientes:

- Proceso de Descubrimiento de la Red
- Proceso de Transferencia de Datos

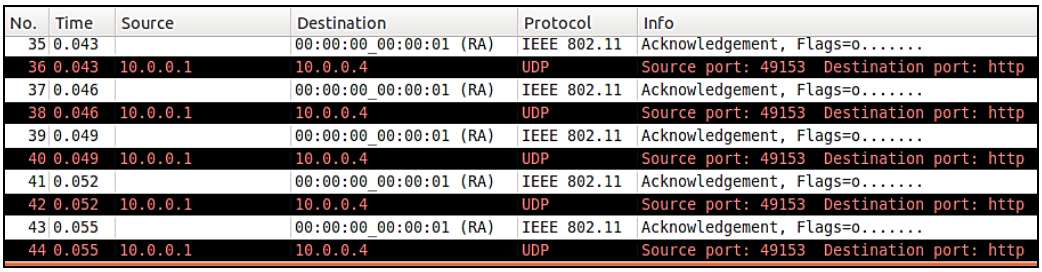
Proceso de Descubrimiento de la Red

El proceso de descubrimiento de la red está basado en el protocolo de resolución de direcciones ARP (*Address Resolution Protocol*). Este protocolo se encarga de resolver una petición enviada por *broadcast* para encontrar la dirección IP que se busca durante el procedimiento de descubrimiento de la red, ésta IP pertenece a una dirección física de algún dispositivo el mismo que responde este pedido de ARP (ARP *request*) con un ARP *response* entregando la dirección que le corresponde. En la Figura 3.39 se puede observar este procedimiento en el recuadro indicado.

No.	Time	Source	Destination	Protocol	Info
1	0.000	00:00:00_00:00:01	Broadcast	ARP	Who has 10.0.0.4? Tell 10.0.0.1
2	0.000	00:00:00_00:00:04	00:00:00_00:00:01	ARP	10.0.0.4 is at 00:00:00:00:00:04
3	0.000		00:00:00_00:00:04 (RA)	IEEE 802.11	Acknowledgement, Flags=o.....
4	0.000	10.0.0.1	10.0.0.4	UDP	Source port: 49153 Destination port: http
5	0.001		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o.....
6	0.001	10.0.0.1	10.0.0.4	UDP	Source port: 49153 Destination port: http

Figura. 3.42. Descubrimiento de la Red en la Topología Punto a Punto

El protocolo IEEE 802.11 también realiza un proceso de reconocimiento, al existir un único nodo con el cual puede establecer una conexión el paquete que se envía es un ACK que permite reconocer al dispositivo con el cual va a realizar el enlace y posterior transmisión de datos. En la Figura 3.40 se remarcan estos paquetes que se encuentra a lo largo de toda la simulación.



No.	Time	Source	Destination	Protocol	Info
35	0.043		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o.......
36	0.043	10.0.0.1	10.0.0.4	UDP	Source port: 49153 Destination port: http
37	0.046		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o.......
38	0.046	10.0.0.1	10.0.0.4	UDP	Source port: 49153 Destination port: http
39	0.049		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o.......
40	0.049	10.0.0.1	10.0.0.4	UDP	Source port: 49153 Destination port: http
41	0.052		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o.......
42	0.052	10.0.0.1	10.0.0.4	UDP	Source port: 49153 Destination port: http
43	0.055		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o.......
44	0.055	10.0.0.1	10.0.0.4	UDP	Source port: 49153 Destination port: http

Figura 3.43. Paquetes ACK bajo el protocolo IEEE 802.11 en simulación Punto a Punto

Cada uno de los paquetes transmitidos por el protocolo ARP tanto para el *Request* como para el de *Reply* presentan valores diferentes los mismos que son presentados en la Tabla 3.30 y la Tabla 3.31 respectivamente.

Tabla. 3.32 Descripción del Paquete de ARP (*request*)

FRAME 1	*Time*	0.00026(seg)
	Frame Number	1
	Frame Length	64 bytes
	Protocols in Frame	wlan:llc:arp
IEEE 802.11 DATA	*Destination Address*	ff:ff:ff:ff:ff:ff
	Source Address	00:00:00_00:00:01
	BSS Id	00:00:00_00:00:01
LOGICAL-LINK CONTROL	DSAP	SNAP (0xaa)
	IG Bit	*Individual*
	SSAP	SNAP (0xaa)
	CR Bit	*Command*

	Type	ARP
ADDRESS RESOLUTION PROTOCOL	*Protocol Type*	IP (0x0800)
	Sender MAC address	00:00:00_00:00:01
	Sender IP address	10.0.0.1
	Target MAC address	ff:ff:ff:ff:ff:ff
	Target IP address	10.0.0.2

Tabla. 3.33. Descripción del Paquete de ARP (*reply*)

FRAME 2	*Time*	0.00046 (seg)
	Frame Number	2
	Frame Length	64 bytes
	Protocols in Frame	wlan:llc:arp
IEEE 802.11 DATA	*Destination Address*	00:00:00_00:00:02
	Source Address	00:00:00_00:00:01
	BSS Id	
LOGICAL-LINK CONTROL	DSAP	SNAP (0xaa)
	IG Bit	*Individual*
	SSAP	SNAP (0xaa)
	CR Bit	*Command*
	Type	ARP
ADDRESS RESOLUTION PROTOCOL	*Protocol Type*	IP (0x0800)
	Sender MAC address	00:00:00_00:00:02
	Sender IP address	10.0.0.2
	Target MAC address	00:00:00_00:00:01
	Target IP address	10.0.0.1

Adicionalmente para el protocolo IEEE 802.11 también se envía un paquete de ACK que permite reconocer a los dispositivos cercanos con quienes puede

realizar transmisiones, en este caso es solamente para mantener la conexión con el otro nodo.

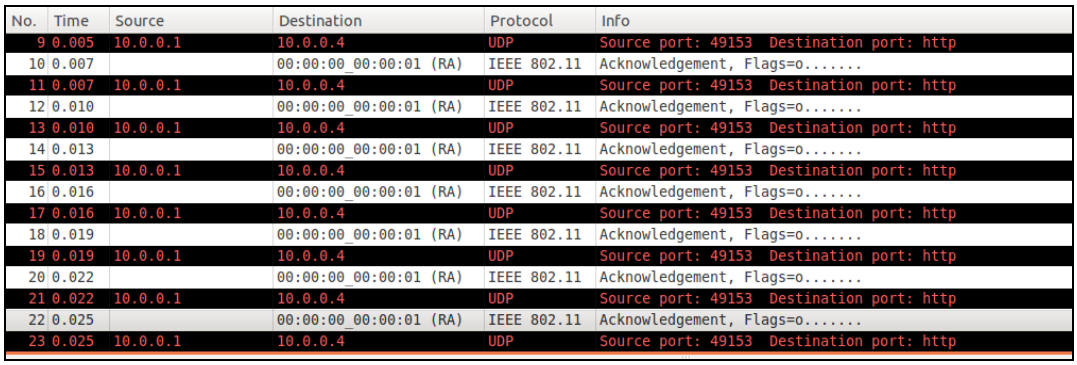
Tabla. 3.34 Descripción del Paquete IEEE 802.11 (*Acknowledgement*)

FRAME 22	*Time*	0.025 (seg)
	Frame Number	22
	Frame Length	14 bytes
	Protocols in Frame	wlan
IEEE 802.11 Acknowledgement	*Type / Subtype*	*Acknowledgement*
	Frame Control	0x80D4 (Normal)
	Receiver Address	00:00:00_00:00:01

Proceso de Transferencia de Datos

Este proceso de transferencia se realiza utilizando el protocolo de comunicaciones UDP (*User Datagram Protocol*). De acuerdo a la programación del *script* se puede ingresar la cantidad de paquetes que se requiere enviar durante la transmisión de datos.

En la Figura 3.41 se indica algunos paquetes UDP que se envían durante la transmisión, éstos paquetes presentan datos en cada campo por cada columna que se presenta en *Wireshark*, estos datos serán tabulados posteriormente para su respectivo análisis.



No.	Time	Source	Destination	Protocol	Info
9	0.005	10.0.0.1	10.0.0.4	UDP	Source port: 49153 Destination port: http
10	0.007		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o.....
11	0.007	10.0.0.1	10.0.0.4	UDP	Source port: 49153 Destination port: http
12	0.010		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o.....
13	0.010	10.0.0.1	10.0.0.4	UDP	Source port: 49153 Destination port: http
14	0.013		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o.....
15	0.013	10.0.0.1	10.0.0.4	UDP	Source port: 49153 Destination port: http
16	0.016		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o.....
17	0.016	10.0.0.1	10.0.0.4	UDP	Source port: 49153 Destination port: http
18	0.019		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o.....
19	0.019	10.0.0.1	10.0.0.4	UDP	Source port: 49153 Destination port: http
20	0.022		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o.....
21	0.022	10.0.0.1	10.0.0.4	UDP	Source port: 49153 Destination port: http
22	0.025		00:00:00_00:00:01 (RA)	IEEE 802.11	Acknowledgement, Flags=o.....
23	0.025	10.0.0.1	10.0.0.4	UDP	Source port: 49153 Destination port: http

Figura. 3.44. Paquetes UDP enviados desde el nodo Fijo

Como se puede ver en la Figura 3.41 se resaltan los paquetes de UDP enviados por su dispositivo fuente hacia su dispositivo destino con la IP de cada uno de ellos. En el análisis respectivo se podrá indicar el comportamiento de cada valor presentado en cada campo en el detalle del paquete. Los valores que corresponden a cada paquete de UDP se detallan en la Tabla 3.33.

Tabla 3.35. Descripción del Paquete UDP

FRAME 17	*Time*	0.017	
	Frame Number	17	
	Frame Length	2064 bytes	
	Protocols in Frame	wlan:llc:ip:udp:data	
IEEE 802.11 DATA	*Destination Address*	00:00:00_00:00:02	
	Source Address	00:00:00_00:00:01	
	BSS Id	00:00:00_00:00:01	
LOGICAL–LINK CONTROL	DSAP	SNAP	0xaa
	SSAP	SNAP	0xaa
	Organization Code	Encapsulado Ethernet	
	Type	IP	
INTERNET PROTOCOL	*Version*	4	
	Header Length	20 bytes	
	Total Length	2028 bytes	
	Time to Live	64	
	Protocol	UDP	

	Source	10.0.0.1
	Destination	10.0.0.2
USER DATAGRAM PROTOCOL	*Source Port*	49153
	Destination Port	http (80)
	Length	2008
DATA	*Length*	2000 bytes

CAPÍTULO 4

DISCUSIÓN DE RESULTADOS

En este capítulo se analizan los resultados obtenidos a partir de los escenarios de simulación planteados en el Capítulo III. Se han utilizado cuatro herramientas para el análisis; la primera es *Pyviz* que trabaja conjuntamente con el *ns-3* y presenta la topología de la red que permite visualizar elementos como paquetes enviados, recibidos y perdidos, así como datos básicos de cada nodo; dirección IPv4, dirección IPv6, dirección MAC, Modelo de Movilidad y tipo de adaptador de red. La segunda herramienta utilizada para el análisis es el analizador de protocolos *Wireshark* que presenta la captura de los paquetes enviados y recibidos durante las transmisiones. La tercera herramienta, *Gnuplot* permite realizar gráficas vía línea de comandos de los datos representados en un archivo con extensión *.dat* o ingresados directamente. Y la cuarta y última herramienta es la del *Terminal* de Ubuntu, en la cual se presentan los valores calculados de *Throughput* utilizados para graficar los resultados.

4.1 Análisis de Resultados

Los resultados de las simulaciones se obtienen ejecutando cada *script*, vía *Terminal*, esto provoca que se visualicen datos expresados en Mbps y que la aplicación gráfica *Pyviz* se ejecute obteniendo los datos tabulados en el Capítulo 3.

Finalmente desde el código del *script* se generan los archivos de captura *.pcap* que contienen una traza entera de cada ejecución. Los valores son generados en un archivo de extensión *.xml* y éstos son utilizados por la

herramienta *gnuplot* permitiendo graficar los resultados tanto del Rendimiento de la Red (*Throughput*) como del *Delay*.

4.1.1 Análisis del Rendimiento (*Throughput*)

El *Throughput* es definido como el volumen de la información que se transmite a través de un sistema o a la información que fluye en las redes de datos durante un tiempo determinado. (26) En este caso el tiempo depende del tipo de simulación.

Se realiza un análisis del Rendimiento de la Red para cada uno de los escenarios propuestos, todas sus gráficas son analizadas tomando en cuenta los valores más importantes durante la interpretación de los resultados.

Escenario Tipo Infraestructura

Para el escenario Tipo Infraestructura descrito en la Figura 3.3 del Capítulo 3, se han tomado los valores presentados en la Tabla 4.1. Estos datos de simulación son configurados directamente en el *script* de simulación para la obtención de los datos y su posterior análisis.

Tabla. 4.1. Datos de Simulación para el escenario Tipo Infraestructura

CARACTERÍSTICAS	VALORES
Número de Nodos Fijos	5
Tecnología de la Capa Física	DSSS a 11 Mbps
Tasa de Transmisión	8 Mbps
Intensidad de Recepción de Señal	-60 dBm
Tamaño de Paquetes Enviados	64000 B
Estándar Inalámbrico	IEEE 802.11b
Frecuencia de Transmisión	2.4 GHz
Modelo de Propagación	*FixedRssLossModel*

Distancia Promedio hacia el AP	30 m
Tráfico Generado	UDP
Tiempo de Simulación	120 seg.

Para el análisis de resultados se mide el desempeño de la red en función del *Throughput* Normalizado y del *Delay.* En la Figura 4.1 se visualiza el resultado de los datos obtenidos en función del tiempo y la velocidad de transmisión configurada inicialmente en el *script*.

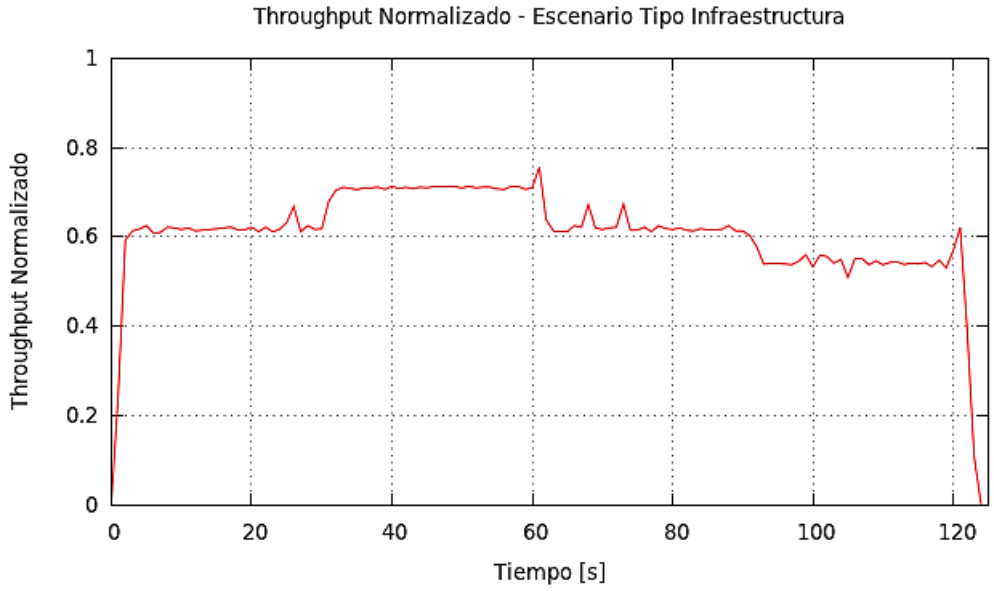


Figura. 4.1. *Throughput* Normalizado de la red para el escenario Tipo Infraestructura

En la Figura 4.1 se observa el comportamiento del rendimiento de la red durante el tiempo total de simulación. El canal configurado a 11 Mbps y la tasa de transmisión del nodo AP a 8 Mbps, permite obtener los resultados representados en la Figura 4.1 que alcanzan una eficiencia del 61.6%, lo cual se encuentra dentro de los parámetros de eficiencia establecidos para una red de este tipo.

Para el cálculo teórico del *throughput* de la red, η, se debe tomar en cuenta la relación entre el número de bytes enviados, *Ne*, y el tiempo total de simulación, τ utilizando la siguiente expresión:

$$\eta = \frac{8Ne}{\tau} \quad [bps] \qquad (4.1)$$

Con la expresión 4.1 se realiza el cálculo del *throughput* de la red, valor que será comparado con los datos obtenidos por la simulación.

$$\eta = \frac{8Ne}{\tau}$$

$$\eta = \frac{8(103435600)}{120}$$

$$\eta = 6895707 \ [bps]$$

$$\eta = 6.896 \ [Mbps]$$

Con el valor de *thorughput* calculado se realiza una comparación con los datos obtenidos durante la simulación. En la Tabla 4.2 se tabulan los datos calculados con los datos medidos.

Tabla. 4.2. Comparación de resultados para el escenario Tipo Infraestructura

RESULTADOS DEL *THROUGHPUT* DE LA RED	
Calculado	**Medido**
6.896 Mbps	6.776 Mbps

Con los valores presentados en la Tabla 4.2 es importante también realizar un cálculo del error para obtener el margen de variación entre ambos resultados. Para realizar este cálculo se utiliza la fórmula 4.2

$$(\%)\ Error = \frac{|Valor\ Medido - Valor\ Teórico|}{Valor\ Teórico} x100 \qquad (4.2)$$

$$(\%)\ Error = \frac{|6.776 - 7.829|}{7.829} x100$$

$$Error = 1.7271\ \%$$

Con el valor del error calculado de -1.7271%, se puede verificar que los valores obtenidos durante la simulación se acercan a los valores calculados, lo que permite tomar dichos resultados como válidos.

Para el escenario Tipo Infraestuctura y su análisis de rendimiento de la red (*Throughput*) se obtiene la siguiente interpretación de los resultados:

- El valor del *Throughput* no puede sobrapasar la capacidad del canal de 11 Mbps, tal como se muestran en los resultados obtenidos, mientras mayor sea el número de nodos que envían información por el mismo canal inalámbrico el rendimiento de la red asciende y el *throughput* tiende al valor máximo de capacidad del canal.

- En el caso de la transmisión de paquetes tipo UDP se toma en cuenta solamente los paquetes transmitidos desde el nodo origen hacia el nodo destino. A diferencia de una transmisión con paquetes tipo TCP, los cuales requieren de paquetes adicionales de reconocimiento (ACK) y los tiempos para el análisis del *Throughput* tienen que ser la suma del tiempo transcurrido entre la recepción y el envío del paquete de ACK y el tiempo que un nodo ocupa para escuchar el canal, estos paquetes de control afectan directamente al *throughput* ya que también son parte del canal de transmisión durante el establecimiento de una sesión TCP, lo cual no ocurre en UDP logrando obtener resultados máximos durante la simulación.

- La fuerza de la señal recibida (RSSI - *Receive Signal Strength Indication*) es un factor importante durante las comunicaciones inalámbricas, para este escenario de tipo Infraestructura se tiene un número pequeño de nodos, a pesar de eso cada uno es un factor de

interferencia que incide sobre los otros. Lo importante es que este factor RSSI, permite que la conexión permanezca estable durante la simulación tomando en cuenta el modelo de propagación configurado, de esta forma los valores obtenidos son constantes a lo largo del tiempo y se puede obtener los resultados esperados.

- Los cálculos tanto del *throughput* como del error permiten verificar que los resultados obtenidos desde la simulación comparados con los calculados son bastante cercanos, esto permite verificar que la funcionalidad del simulador *ns-3* es óptima para este tipo de estudios tanto a nivel académico como de investigación.

Escenario Tipo Ad-hoc

Para el escenario Tipo Ad-hoc descrito en la Figura 3.4 del Capítulo 3, se ha tomado los valores presentados en la Tabla 4.3. Estos parámetros de simulación son configurados directamente en el script de simulación para la obtención de los datos y su posterior análisis.

Tabla. 4.3. Datos de Simulación para el escenario Tipo Ad-hoc

CARACTERÍSTICAS	VALORES
Número de Nodos Móviles	3
Tecnología de la Capa Física	DSSS a 11 Mbps
Tasa de Transmisión	8 Mbps
Tamaño de Paquetes Enviados	5000 B
Estándar Inalámbrico	IEEE 802.11b
Frecuencia de Transmisión	2.4 GHz
Modelo de Propagación	*FriisPropagationLossModel*
Distancia Promedio entre nodos	10 m
Tráfico Generado	UDP
Tiempo de Simulación	120 seg.

Para el análisis de resultados se medirá el desempeño de la red en función del *Throughput,* el *Delay* y el análisis de los paquetes enviados, recibidos y perdidos durante las transmisiones realizadas en la simulación. En la Figura 4.2 se visualiza el resultado de los datos obtenidos en función del tiempo y la velocidad de transmisión configurada inicialmente en el *script*. Hay que tomar en cuenta que en este escenario los nodos son móviles y el *throughput* se verá afectado durante la simulación.

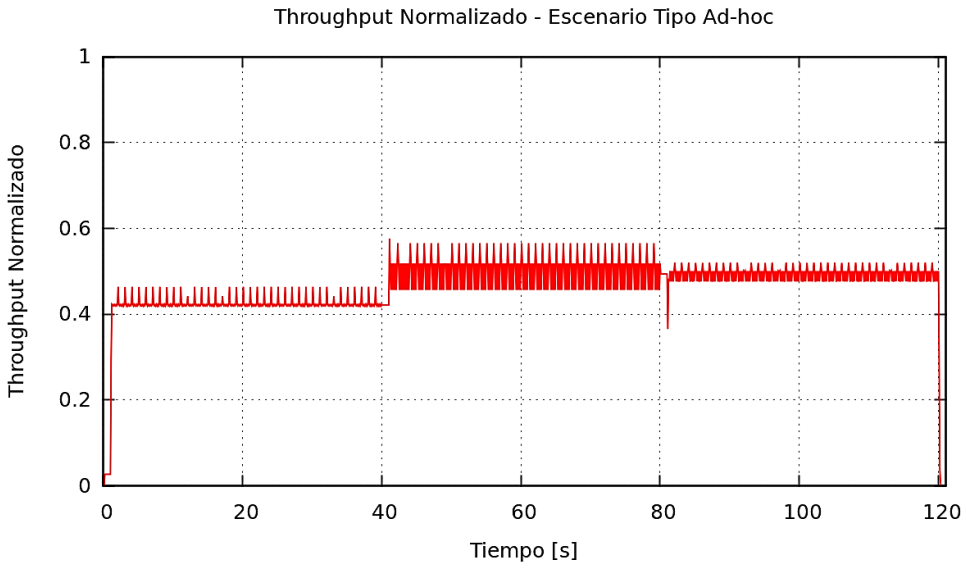


Figura. 4.2. *Throughput* Normalizado de la red para el escenario Tipo Ad-hoc

En la Figura 4.2, el comportamiento del rendimiento de la red presenta variaciones a lo largo del tiempo total de simulación, esto se debe principalmente al tipo de escenario que hemos planteado. Los valores presentados representan un 47% de eficiencia de la red, un valor inferior al analizado previamente en el escenario Tipo Infraestructura, estos eran los resultados esperados al momento de comparar ambos escenarios. Hay que tomar en cuenta los siguientes factores que influyen directamente en el comportamiento de esta red:

- Movilidad
- Velocidad de los nodos

- Tamaño y Cantidad de paquetes

La movilidad de los nodos repercute en el rendimiento de la red, especialmente en casos en que el transmisor está enviando información hacia un receptor destinado y otro se interpone entre estos por un lapso de tiempo corto o largo, existe una pérdida debido a la interferencia entre nodos.

La velocidad de los nodos para este escenario es constante, por lo que no es un factor que influya durante la simulación, pero si se cambia parámetros de velocidad y aceleración, el *throughput* se vería afectado en estos casos, lo cual requiere un estudio más amplio para el análisis en estos casos.

El tamaño y la cantidad de paquetes es el factor más importante para el cálculo del *throughput*, ya que de estos parámetros el rendimiento de la red disminuye o aumenta al ser un factor directamente proporcional en el cálculo a nivel teórico y práctico.

A continuación se realiza el cálculo del valor del *throughput* de la red para comparar con los valores obtenidos en la gráfica de la simulación presentada en la Figura 4.2.

$$\eta = \frac{8Ne}{\tau}$$

$$\eta = \frac{8(78302745)}{120}$$

$$\eta = 5220183\ [bps]$$

$$\eta = 5.220\ [Mbps]$$

Con este valor de *thorughput* calculado mediante la fórmula 4.1, se puede realizar una comparación con los datos obtenidos durante la simulación y que son

representados en la Figura 4.2. En la Tabla 4.3 se tabulan los datos calculados con los datos medidos.

Tabla. 4.4. Comparación de resultados para el escenario Tipo Ad-hoc

RESULTADOS DEL *THROUGHPUT* DE LA RED	
Calculado	**Medido**
5.220 Mbps	5.105 Mbps

Con los valores presentados en la Tabla 4.2 es importante también realizar el cálculo del error para tener una perspectiva de los resultados adquiridos a través de la simulación respecto de los calculados. Para realizar este cálculo se utiliza la fórmula 4.2 para realizar un cálculo porcentual del error.

$$(\%)\ Error = \frac{|Valor\ Medido - Valor\ Teórico|}{Valor\ Teórico} x100$$

$$(\%)\ Error = \frac{|5.105 - 5.220|}{5.220} x100$$

$$Error = 2.195\ \%$$

Con el valor del error calculado de 2.195%, se puede verificar que los valores obtenidos durante la simulación se acercan a los valores calculados, lo que permite tomar dichos resultados como válidos.

Para el escenario Tipo Ad-hoc y su análisis de rendimiento de la red, se obtiene la siguiente interpretación de los resultados:

- Al igual que en el primer escenario, tal como se analizó inicialmente el valor del *Throughput* no sobrepasa los valores de capacidad del canal, es decir no debe pasar el valor de 11 Mbps,

- En este tipo de escenarios, como son los de tipo Ad-hoc, se debe tomar en cuenta que los dispositivos que forman parte de la topología son móviles, incluso pueden ser algunos fijos, pero para el escenario presentado la utilización de nodos móviles es más práctico a la hora de realizar el análisis.

- El porcentaje de eficiencia de 47% constrasta con el del escenario Tipo Infraestructura (61.6%), lo cual es correcto, ya que una topología que mantiene estabilidad durante la conexión y que posee garantía para mantener conectividad va a ser mucho más eficiente que una red Tipo Ad-hoc la cual depende de cada uno de los nodos que forman parte de la red.

- Hay que tomar en cuenta que el parámetro de protocolo de enrutamiento también tiene su importancia, ya que de éste depende que cada nodo envié los paquetes por las rutas adecuadas. El protocolo de enrutamiento utilizado para este escenario fue el protocolo AODV.

Escenario Tipo Fijo – Móvil

Para el escenario Tipo Fijo – Móvil descrito en la Figura 3.5 del Capítulo 3, se han tomado los valores presentados en la Tabla 4.4. Estos datos de simulación son configurados directamente en el *script* de simulación para la obtención de los datos y su posterior análisis. Además en este escenario hay que tomar en cuenta las velocidades configuradas en el dispositivo móvil.

Tabla. 4.5. Datos de Simulación para el escenario Tipo Fijo – Móvil

CARACTERÍSTICAS	VALORES
Número de Nodos Fijos	1
Número de Nodos Móviles	1
Tecnología de la Capa Física	DSSS a 11 Mbps

Tasa de Transmisión		8 Mbps	
Tamaño de Paquetes Enviados		2250 B	
Estándar Inalámbrico		IEEE 802.11b	
Frecuencia de Transmisión		2.4 GHz	
Modelo de Propagación		*LogDistancePropagationLossModel*	
Velocidad de Nodo Móvil	**Velocidad 1**	1 m/s	3.6 km/h
	Velocidad 2	2.5 m/s	9 km/h
	Velocidad 3	5 m/s	18 km/h
Tráfico Generado		UDP	
Tiempo de Simulación		150 seg.	

Para el análisis de resultados se medirá el desempeño de la red en función del *Throughput, Delay* y un análisis de los paquetes enviados, recibidos y perdidos durante la transmisión. En la Figura 4.3 se visualiza el resultado del rendimiento de la red en función del tiempo. En esta figura se ha dispuesto los resultados de la simulación variando las velocidades para poder identificar el funcionamiento de la red durante el tiempo total de simulación.

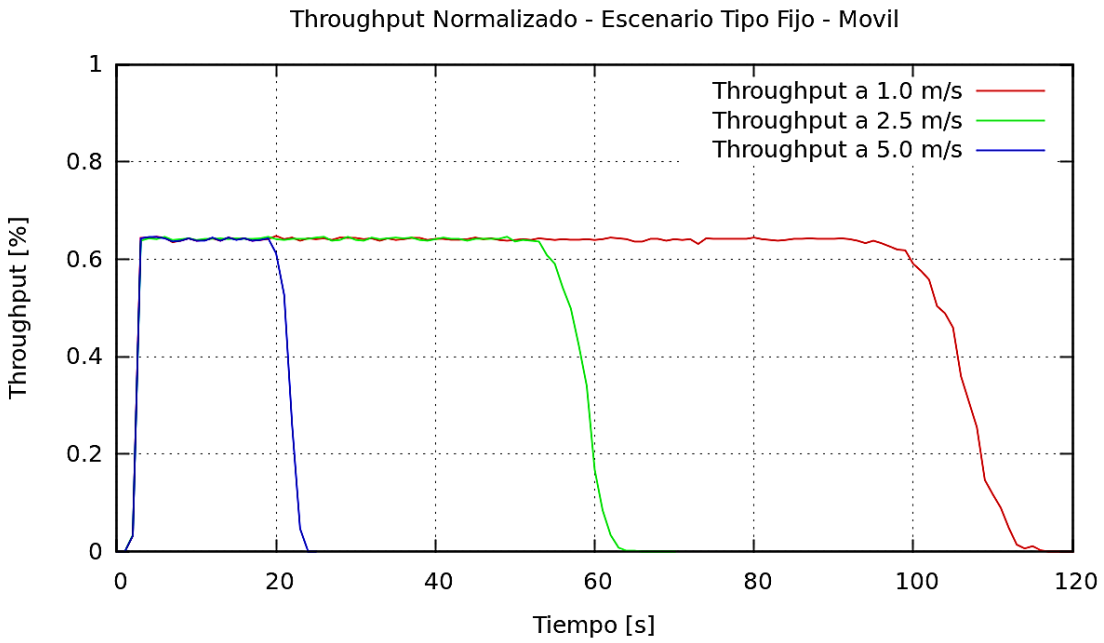


Figura. 4.3. *Throughput* Normalizado de la red para el escenario Tipo Fijo – Móvil

De acuerdo a los resultados obtenidos en la simulación mientras se varían las velocidades del dispositivo móvil se puede observar que el *throughput* para las tres simulaciones a las tres velocidades distintas se mantiene, es decir, los valores pico del *throughput* se mantienen constantes sin importar la variación de velocidad. Este valor del *throughput* total medio desde que inicia la simulación hasta que éste termina es de aproximadamente 6.414 Mbps, lo que representa un 60.45% de efectividad de la red, este es un valor de *throughput* efectivo, es decir, son valores de transmisión media cuando existe envío y recepción de datos sin problemas de conexión.

En la Figura 4.3 se puede observar que cuando el móvil se aleja a una velocidad de 1 m/s la conexión se mantiene durante 113 segundos, pasado este tiempo la conexión se pierde hasta que la simulación termina. Para el segundo caso, el móvil se traslada a una velocidad de 2.5 m/s, aquí la conexión se mantiene hasta los 62 segundos, mientras que para el último caso la velocidad del móvil es de 5 m/s, y la conectividad se mantiene hasta transcurridos 23 segundos. Con estos resultados podemos concluir que a menor velocidad mayor es el tiempo de conexión que se mantiene entre ambos nodos, al variar la velocidad y aumentarla, por efectos de distancia y propagación el tiempo de conexión disminuye, para solucionar estos problemas se procede a integrar nodos repetidores de señal a la red lo cual puede ayudar a mantener la conexión con el nodo móvil.

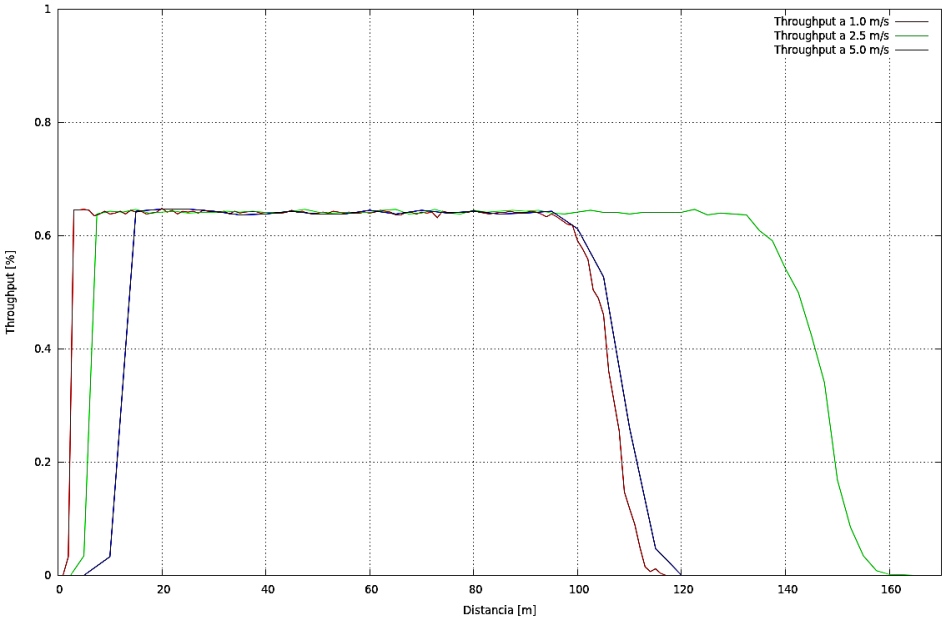


Figura. 4.4. *Throughput* Normalizado de la red para el escenario Tipo Punto a Punto respecto a la distancia recorrida.

Para el primer escenario, el móvil se desplaza a 1 m/s y en la Figura 4.4 se presenta la distancia máxima que alcanza el móvil con conectividad eficiente, es decir a 99 metros aproximadamente se mantiene dicha conexión. Para el segundo caso, la respuesta es superior a la anterior, en este escenario el móvil se desplaza a 2.5 m/s, una velocidad ideal para mantener buena conectividad y alcanzar mayor distancia, en este caso la distancia máxima alcanzada es de 135 metros aproximadamente. Finalmente para el último escenario, el móvil se desplaza a una velocidad de 5 m/s obteniendo resultados similares a los presentados en el primer caso cuando el móvil se desplaza a 1 m/s, para este caso la distancia es de apenas 1 metro de diferencia, con un móvil desplazándose a 5 m/s se obtiene una conectividad eficiente a una distancia máxima de 100 metros.

Con la gráfica presentada en la Figura 4.4 y el análisis del comportamiento de la red respecto a la distancia, se puede concluir que cuando un nodo presenta movilidad respecto a otro nodo fijo, la velocidad influye directamente en la distancia que puede alcanzar el nodo móvil y mantener conectividad durante un tiempo determinado.

En la Figura 4.5 se presenta la respuesta de los primeros segundos de simulación y las distancias que tiene el nodo que alcanzar para estabilizar la red hasta alcanzar el *throughput* máximo.

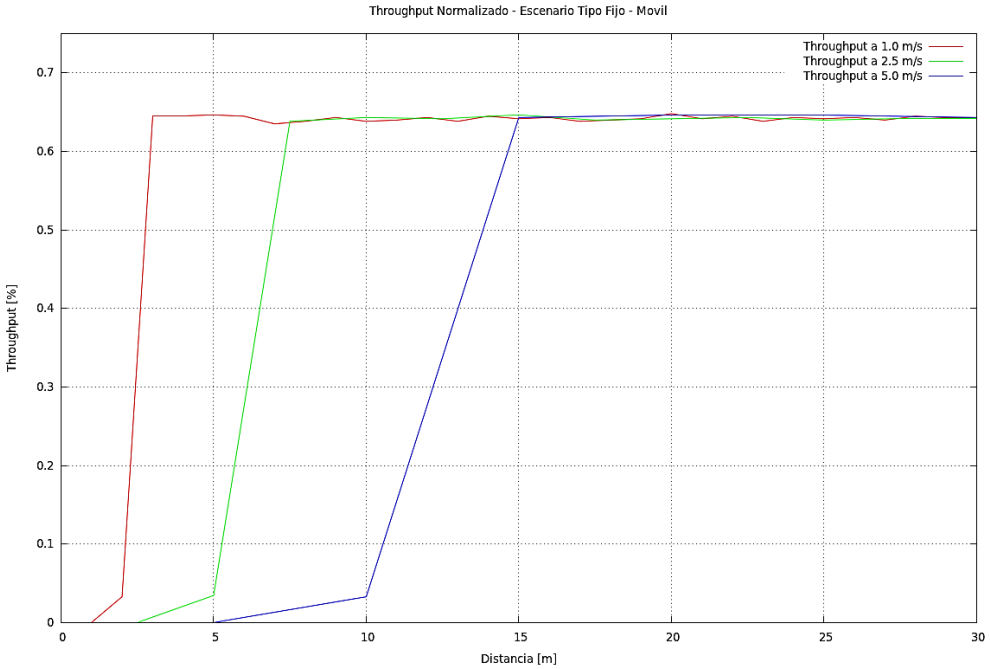


Figura. 4.5. Distancias para alcanzar la estabilización de la red en cada escenario.

Para el nodo que se desplaza a 1 m/s se puede apreciar que a los 3 metros de haber iniciado la transferencia de paquetes, el sistema llega a estabilizarse iniciando la conexión entre ambos nodos. En el segundo caso, para el móvil que se traslada a 2.5 m/s, la estabilidad de la red se obtiene a partir de los 7.5 metros de haber iniciado la simulación, finalmente para el tercer caso, en el cual el móvil se desplaza a 5 m/s, la estabilidad de la red se da cuando éste alcanza los 15 metros. Adicionalmente hay que destacar que el tiempo que toma la red para estabilizarse en los tres escenarios es de 3 segundos, esto se puede verificar en la Figura 4.3, a dicho tiempo se alcanza el *throughput* máximo de cada transmisión.

A continuación se realiza el cálculo del valor del *throughput* de la red para comparar con los valores obtenidos en la gráfica de la simulación presentada en la Figura 4.3.

Throughput para el Móvil a 1 m/s

$$\eta = \frac{8Ne}{\tau}$$

$$\eta = \frac{8(104151318)}{116}$$

$$\eta = 7182849.52\ [bps]$$

$$\eta = 7.1828\ [Mbps]$$

Throughput para el Móvil a 2.5 m/s

$$\eta = \frac{8Ne}{\tau}$$

$$\eta = \frac{8(41275796)}{47}$$

$$\eta = 7025667.4\ [bps]$$

$$\eta = 7.026\ [Mbps]$$

Throughput para el Móvil a 5 m/s

$$\eta = \frac{8Ne}{\tau}$$

$$\eta = \frac{8(28282230)}{32}$$

$$\eta = 7026640.99\ [bps]$$

$$\eta = 7.027\ [Mbps]$$

Con estos valores de *thorughput* calculado mediante la fórmula 4.1, se puede realizar una comparación con los datos obtenidos durante la simulación y

que estan representados en la Figura 4.3. En la Tabla 4.5 se presentan los datos calculados y los medidos para los tres escenarios.

Tabla. 4.6. Comparación de resultados para el escenario Tipo Punto a Punto

RESULTADOS DEL *THROUGHPUT* DE LA RED		
Velocidad	***Throughput* Calculado**	***Throughput* Medido**
1 m/s	7.1828 Mbps	6.7722 Mbps
2.5 m/s	7.0257 Mbps	6.7088 Mbps
5 m/s	7.0266 Mbps	6.4697 Mbps

Con los valores presentados en la Tabla 4.5 es importante también realizar el cálculo del error para tener una perspectiva de los resultados adquiridos a través de la simulación respecto de los calculados. La utilización de la fórmula 4.2 planteada anteriormente también puede ser utilizada para estos casos.

Cálculo del Error para el Móvil a 1 m/s

$$(\%)\ Error = \frac{|Valor\ Medido - Valor\ Teórico|}{Valor\ Teórico} x100$$

$$(\%)\ Error = \frac{|6.7722 - 7.1828|}{7.1828} x100$$

$$Error = 5.718\ \%$$

Cálculo del Error para el Móvil a 2.5 m/s

$$(\%)\ Error = \frac{|Valor\ Medido - Valor\ Teórico|}{Valor\ Teórico} x100$$

$$(\%)\ Error = \frac{|6.7088 - 7.0257|}{7.0257} x100$$

$$Error = 4.510\ \%$$

Cálculo del Error para el Móvil a 5 m/s

$$(\%)\ Error = \frac{|Valor\ Medido - Valor\ Teórico|}{Valor\ Teórico} x100$$

$$(\%)\ Error = \frac{|6.4697 - 7.0266|}{7.0266} x100$$

$$Error = 7.926\%$$

Estos valores de error calculados muestran la variación del rendimiento de la red respecto de los datos obtenidos con los datos calculados. Para los tres escenarios los valores calculados del error demuestran que la velocidad influye en la transmisión, verificando que cuando el móvil se desplaza a una velocidad de 2.5 m/s el margen del error es el menor entre los tres casos, un error de 4.51% demuestra que la conexión para este caso es casi similar a la del sistema ad-hoc a pesar del sistema móvil. Mientras tanto que para el caso en que el móvil se desplaza a una velocidad de 1 m/s el margen del error es del 5.71% demostrando también una estabilidad de la red respecto a los valores calculados. Finalmente para el último caso, el móvil se desplaza a una velocidad de 5 m/s obteniendo un error de 7.92%, el más alto hasta el momento lo cual representa un sistema menos estable a los anteriores en el cual la cantidad de paquetes perdidos va a ser superior al de los anteriores casos.

El análisis del parámetro de RSSI (*Received Signal Strenght Indication*) permite identificar el nivel de potencia de las señales recibidas durante las transmisiones entre ambos nodos.

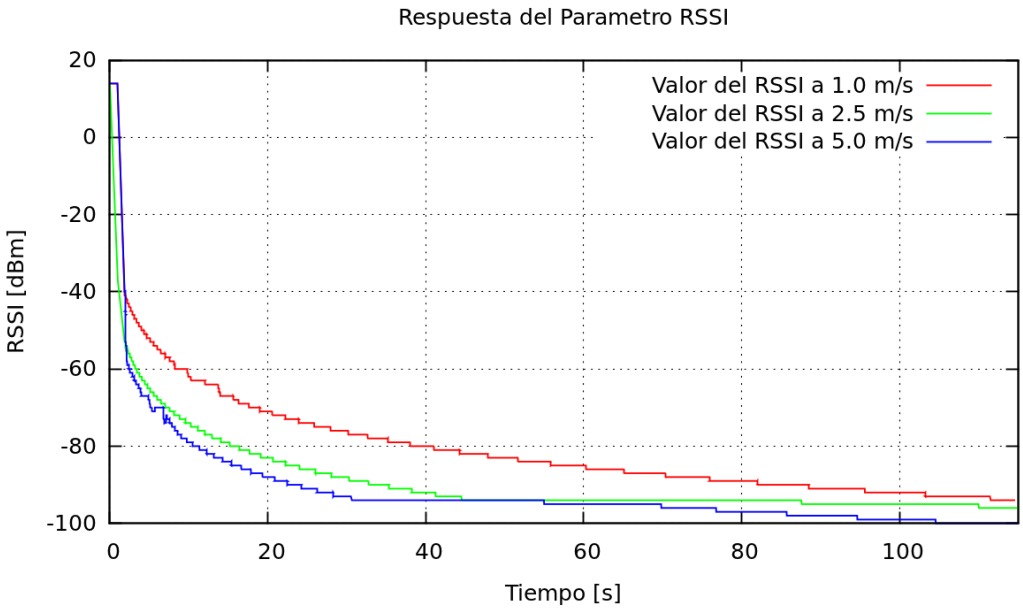


Figura. 4.6 Valores de RSSI de las simulaciones a diferentes velocidades respecto a la distancia entre los nodos.

En la Figura 4.5 se observan los valores obtenidos del RSSI para cada escenario presentado. Como se puede apreciar la tendencia de las curvas son similares debido a la variación de velocidades que sufre el nodo móvil, para el análisis de éste parámetro se puede observar que con el primer escenario en el cual el nodo móvil se desplaza a una velocidad de 1 m/s los valores de RSSI mantienen una estabilidad relativa, obteniendo una buena respuesta de la red durante el tiempo total de simulación. A diferencia de este primer escenario, para los casos en que la velocidad varía entre 2.5 m/s y 5 m/s el valor de RSSI aumenta aceleradamente respecto al tiempo de simulación, obteniendo una pérdida sustancial de paquetes transmitidos, debido a la mayor velocidad que se configura al nodo móvil, respecto al primer escenario, la cantidad de paquetes transmitidos también se reducen así como el tiempo de conexión que mantienen ambos nodos.

4.1.2 Análisis de Retardo (*Delay*)

El *Delay* o retardo se refiere al tiempo total trascurrido para que un paquete generado desde el nodo origen llegue hasta el nodo destino, de ésta manera se determina la eficiencia de la red.

Escenario Tipo Infraestructura

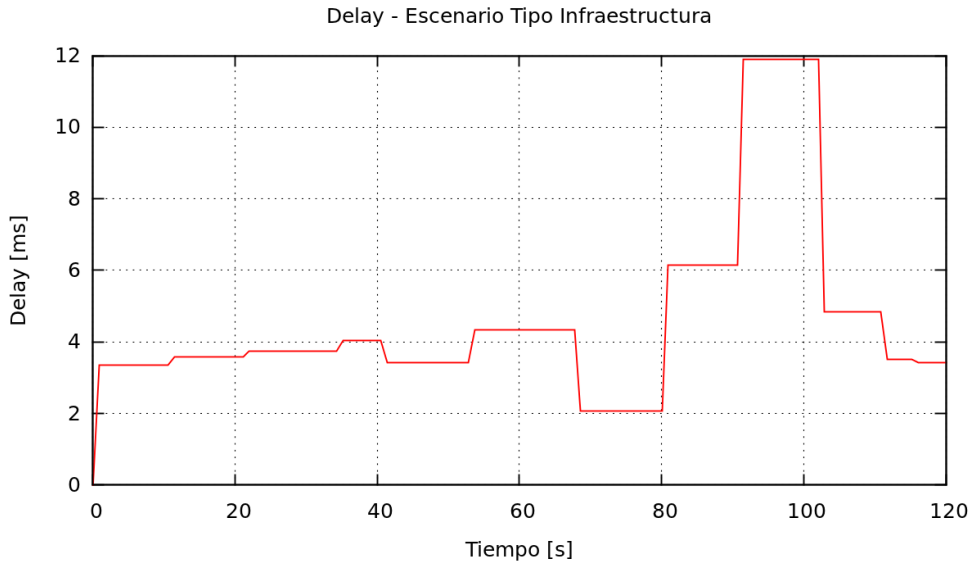


Figura. 4.7. *Delay* de la Red para el escenario Tipo Infraestructura

En la Figura 4.6 se puede apreciar la respuesta de los paquetes enviados desde el nodo origen hacia el nodo destino. Se representa los tiempos de retardo de toda la red en los rangos expresados en la Figura 4.6. En el primer intervalo de t = 0 segundos hasta el tiempo t = 80.95 segundos, el comportamiento de los retardos de tiempo se mantiene en una media de 3.58 ms., lo que indica que la eficiencia de la red durante este intervalo de tiempo corresponde a la calculada en el análisis del *throughput* que llegaba al 61%, para el tiempo restante de la simulación los retardos sufren un aumento mínimo hasta el tiempo t = 120 segundos obteniendo una media de 6.15 ms., la razón de este aumento se debe al tamaño de paquetes transmitidos y recibidos superior al de los flujos registrados en el primer intervalo.

Hay que tener en cuenta las siguientes observaciones dentro del análisis del *Delay* para el escenario Tipo Infraestructura:

- El análisis se lo realiza con un número fijo de nodos, al variar esta cantidad de nodos se puede obtener resultados similares ya que la configuración principal de la red no varía, los retardos del tiempo se mantendrían en el intervalo entre 3.58 ms. hasta los 12 ms., esto debido al protocolo utilizado UDP, en el cual el *delay* promedio no supera los 20 ms.

- En la Figura 4.6 el *delay* de la red muestra valores constantes a lo largo de toda la simulación, lo cual verifica que la respuesta de la red es bastante estable. Estos resultados eran los esperados tomando en cuenta la configuración inicial de la red, evitando forzar el funcionamiento de la misma y del simulador.

Escenario Tipo Ad-hoc

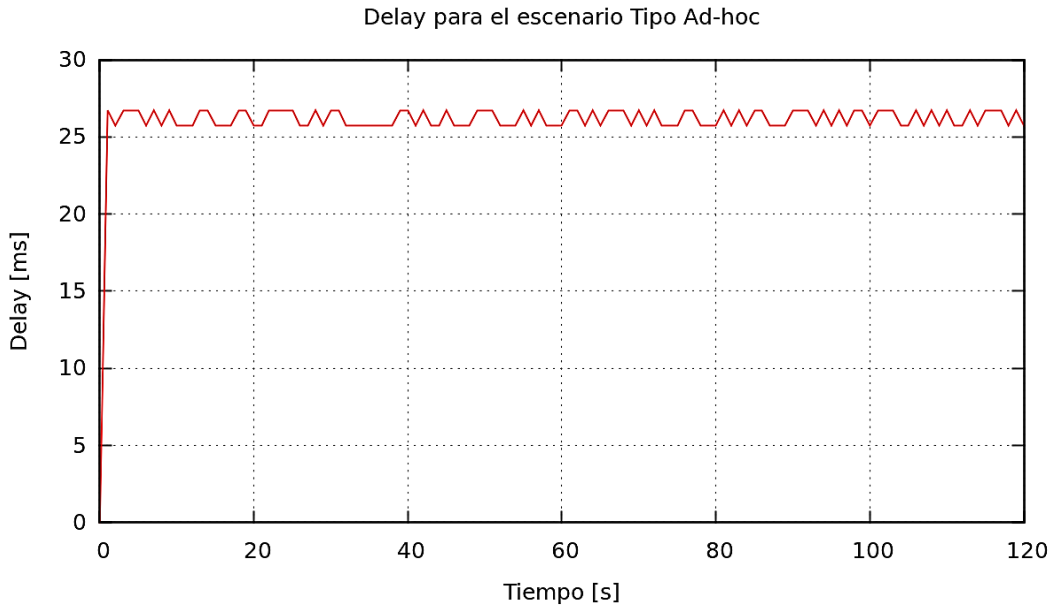


Figura. 4.8 *Delay* de la red para el escenario Tipo Ad-hoc

En la Figura 4.7 se puede apreciar la respuesta de los paquetes enviados desde el nodo origen hacia el nodo destino de los paquetes de datos que atraviesan la red durante el tiempo total de simulación. La media de estos valores de *Delay* obtenidos es de 26.221ms., un valor aceptable para transmisiones de éste tipo y como se puede apreciar en la gráfica los valores son casi constantes lo que permite verificar que el funcionamiento de la red es óptimo para las transmisiones de éste tipo con las condiciones establecidas inicialmente.

Hay que tener en cuenta las siguientes observaciones dentro del análisis del *Delay* para el escenario Tipo Ad-hoc:

- El análisis se lo realiza con un número fijo de nodos móviles bajo un escenario de dimensiones fijas, en este caso, los resultados del retardo del tiempo varía a lo largo del tiempo, tomando en cuenta los factores ya indicados anteriormente, distancia, protocolos de enrutamiento, tamaño de paquetes, y la velocidad de los nodos que forman parte de la topología.

- El *Delay* obtenido para esta simulación es mayor al obtenido en el escenario Tipo Infraestructura, debido a factores de movilidad y distancia variable entre nodos, principalmente, lo cual muestra una diferencia importante de aproximadamente 20ms. respecto del promedio en ambas redes.

Escenario Tipo Fijo – Móvil

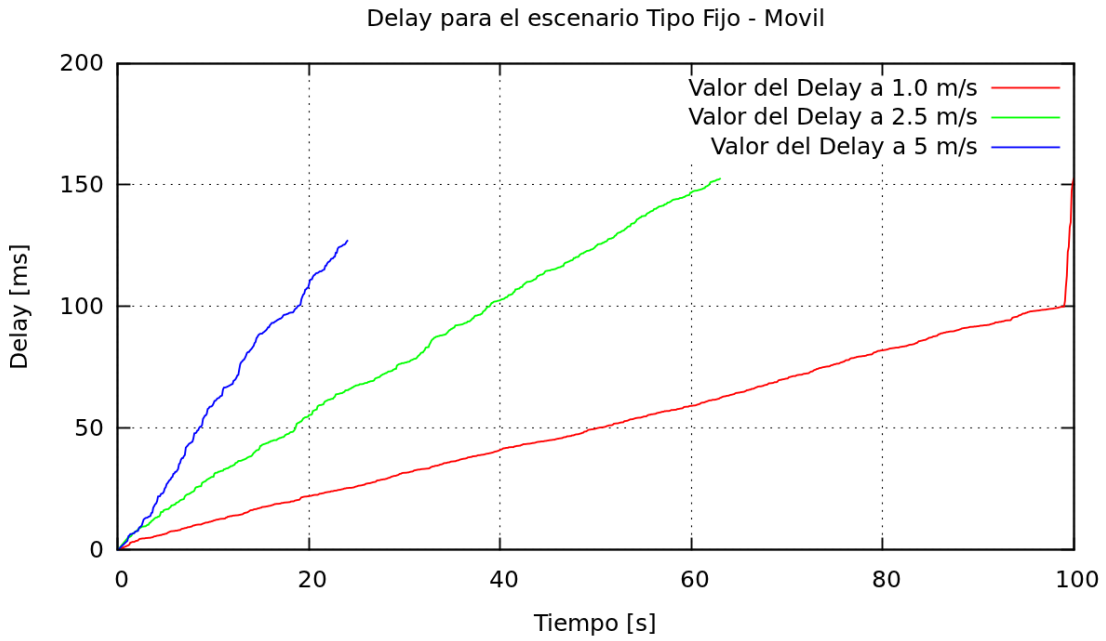


Figura. 4.9 *Delay* de la red para el escenario Tipo Fijo – Móvil

En la Figura 4.8 se ha planteado la respuesta del retardo de tiempos durante la simulación para los tres casos en que el móvil se desplaza a las velocidades indicadas en la gráfica.

Como se puede ver en la Figura 4.8 el sistema que tiene mejor respuesta del *delay* durante la simulación es cuando el móvil avanza a una velocidad de 1 m/s. los retardos de tiempo se presentan con cierta estabilidad mientras el *throughput* se reduce a lo largo del tiempo. El tiempo total de simulación como se indicó en la Tabla 4.4 es de 150 segundos para los tres escenarios, para el análisis del *delay* se toma en cuenta solo los tiempos en que existe conexión entre ambos nodos, así para el primer escenario a t = 99 segundos, el valor del *delay* alcanza los 100 ms., para el segundo escenario a t = 60 segundos el *delay* es de 146.816 ms. y finalmente para el tercer escenario a t = 24 segundos, el *delay* alcanza el valor de 127.035 ms. Como se puede observar en los resultados presentados, estos no superan los 150 ms., valor máximo para el estándar IEEE 802.11b y su correcto funcionamiento.

4.1.3 Análisis de Paquetes de Datos

El siguiente análisis se basa específicamente en los valores totales de paquetes enviados, recibidos y perdidos durante cada una de las simulaciones. Es importante destacar las estadísticas del simulador obtenidas desde la herramienta gráfica *Pyviz,* la misma que demuestra la cantidad de paquetes que se envían así como los paquetes que se reciben en cada uno de los nodos que forman parte de la topología de red de cada escenario.

Escenario Tipo Infraestructura

Los resultados obtenidos durante la primera simulación se presentan directamente en la herramienta *Pyviz* y los resultados generados en el archivo *.xml* desde el *script* de simulación. En la Figura 4.9 se muestran dichos resultados.

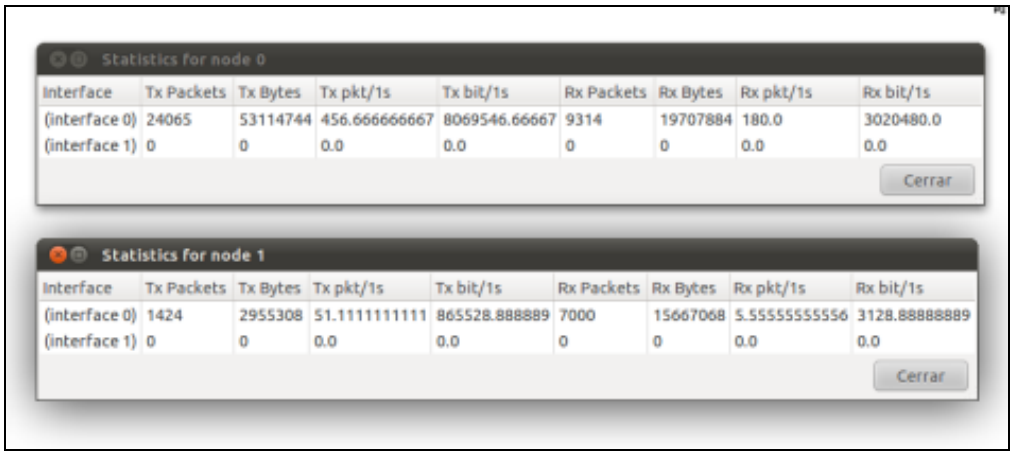
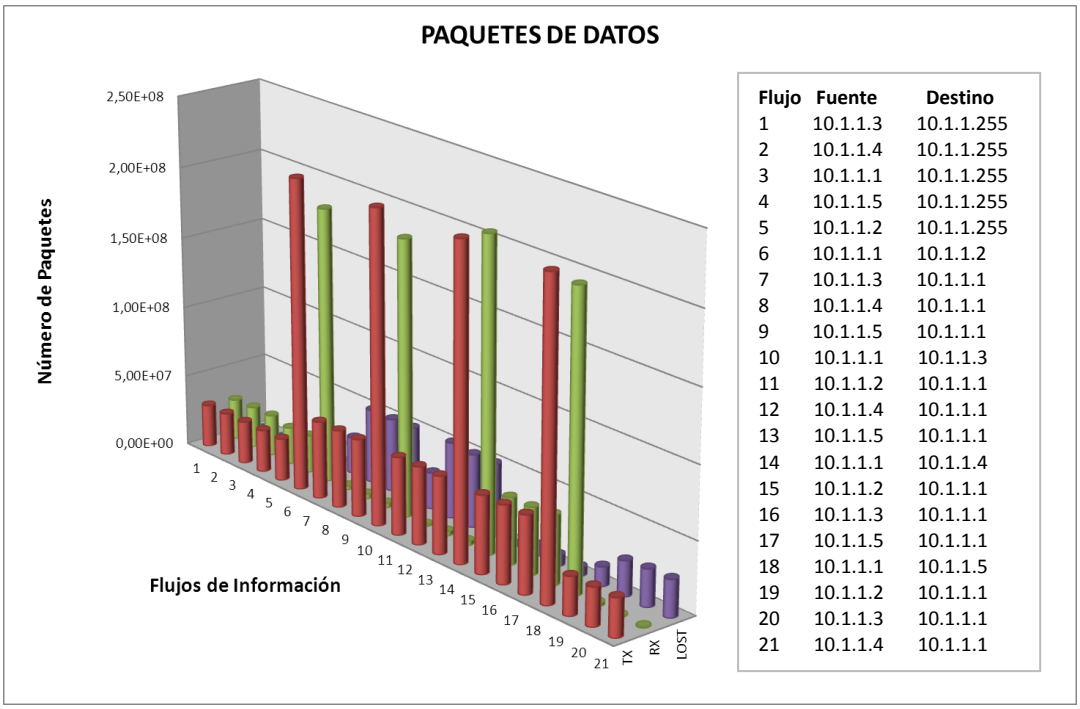


Figura. 4.10 Estadísticas de los Nodos AP – Nodo 1 durante la transmisión de Paquetes.

En la Figura 4.9 se puede destacar los valores de paquetes transmitidos y paquetes recibidos, en los primeros segundos de la simulación el Nodo 0, o nodo AP es el encargado de enviar la mayor cantidad de información a los Nodos clientes, por lo que la cantidad de paquetes transmitidos es mucho mayor a la de

los otros nodos que forman parte de la red, así mismo en la cuarta columna se indica que se realiza una transmisión promedio de paquetes de 456 paquetes por segundo. Al terminar la simulación se obtienen los resultados finales directamente desde el archivo generado, estos valores son representados en la Figura 4.10.



Flujo	Fuente	Destino
1	10.1.1.3	10.1.1.255
2	10.1.1.4	10.1.1.255
3	10.1.1.1	10.1.1.255
4	10.1.1.5	10.1.1.255
5	10.1.1.2	10.1.1.255
6	10.1.1.1	10.1.1.2
7	10.1.1.3	10.1.1.1
8	10.1.1.4	10.1.1.1
9	10.1.1.5	10.1.1.1
10	10.1.1.1	10.1.1.3
11	10.1.1.2	10.1.1.1
12	10.1.1.4	10.1.1.1
13	10.1.1.5	10.1.1.1
14	10.1.1.1	10.1.1.4
15	10.1.1.2	10.1.1.1
16	10.1.1.3	10.1.1.1
17	10.1.1.5	10.1.1.1
18	10.1.1.1	10.1.1.5
19	10.1.1.2	10.1.1.1
20	10.1.1.3	10.1.1.1
21	10.1.1.4	10.1.1.1

Figura. 4.11 Análisis de Paquetes Transmitidos, Recibidos y Perdidos para el escenario Tipo Infraestructura.

En la Figura 4.10 se representan los valores totales obtenidos de los paquetes que atraviesan la red durante la simulación. En la gráfica tridimensional se verifican los paquetes transmitidos, recibidos y perdidos, como era de esperar después del análisis del *throughput* y del *delay* de esta topología, los resultados eran los esperados también para este análisis. Tomando en cuenta la cantidad de paquetes enviados y recibidos obtenemos un rango de pérdidas de paquetes aceptable, que fluctúa entre el 0.66% y el 6.18%, valores que demuestran la confiabilidad de la red bajo el estándar IEEE 802.11.

Escenario Tipo Ad-hoc

Para este tipo de escenario el análisis es similar al anterior realizado, hay que tomar en cuenta que la cantidad de paquetes perdidos será superior debido a los factores de movilidad que se presenta en este escenario. Esto se complementa con los resultados obtenidos de *delay* para este escenario.

Los resultados de los paquetes que se envían y reciben se obtienen directamente desde un archivo generado con extensión *.xml* de los datos capturados durante la simulación los cuales permiten obtener los resultados descritos en la Figura 4.12, mientras tanto que la cantidad de paquetes enviados y recibidos en tiempo real, lo obtenemos desde la herramienta *Pyviz*, estos valores se presentan en la Figura 4.11.

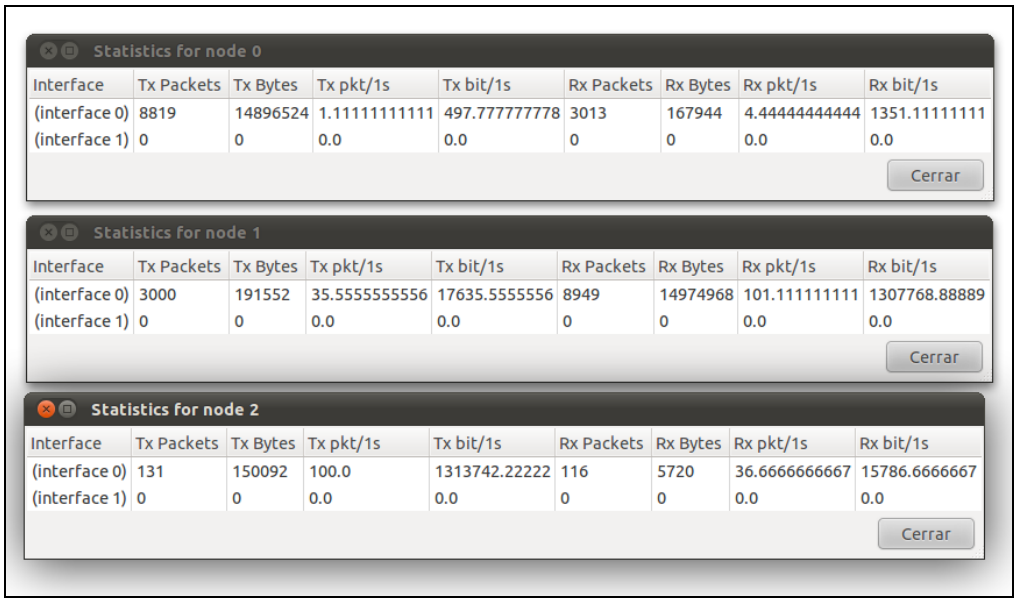


Figura. 4.12 Estadísticas de los Nodos 0, Nodo 1 y Nodo 2 durante la transmisión de Paquetes.

En la Figura 4.11 se presenta los resultados obtenidos utilizando la herramienta *Pyviz,* estos resultados verifican los paquetes transmitidos, recibidos y la cantidad de paquetes por segundo que transmite y que recibe cada nodo. En la gráfica se verifica que la cantidad de paquetes que transmitió el Nodo 0 al

momento de la captura era de 8819 paquetes y había recibido hasta el momento 3013 paquetes durante la transmisión. Mientras tanto en el Nodo 2 se muestra el promedio de los paquetes transmitidos por unidad de tiempo que es de 100 paquetes por segundo. Estos valores nos permiten verificar una tendencia de los posibles resultados, pero para obtener resultados más precisos se recurre al archivo generado *.xml.*

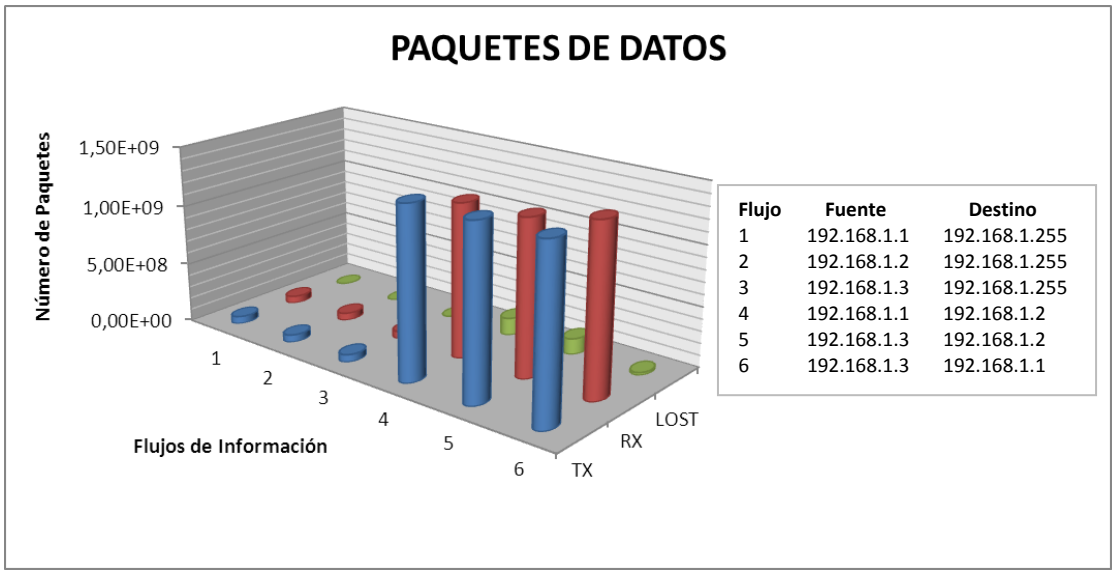


Figura. 4.13 Análisis de Paquetes Transmitidos, Recibidos y Perdidos para el escenario Tipo Ad-hoc.

En la Figura 4.12 se representan los valores totales obtenidos de los paquetes que atraviesan la red durante la simulación. En la gráfica se presentan los paquetes transmitidos, recibidos y perdidos, de acuerdo a cada flujo de información indicado en la leyenda de la misma gráfica. Tomando en cuenta los resultados obtenidos del *throughput* y del *delay* de esta topología, se puede verificar que ésta red presenta mayor cantidad de paquetes perdidos debido a los parámetros y condiciones de este escenario. Así los valores de pérdidas de paquetes se encuentra entre el rango del 0.81% al 10.09%, a pesar de estos datos, continúa siendo una red confiable bajo el estándar IEEE 802.11.

Escenario Tipo Fijo – Móvil

El análisis del siguiente escenario es más complejo pero las herramientas utilizadas para representar los resultados son las mismas. Para este escenario debemos tomar en cuenta la diferencia de velocidades que se configuran en cada caso, por lo que la pérdida de paquetes va a ser diferente para cada uno de ellos.

Los resultados de los paquetes que se envían y reciben se obtienen directamente desde un archivo generado con extensión *.xml* de los datos capturados durante la simulación. Antes de presentar los resultados desde el archivo generado, en la Figura 4.13 se indican los valores obtenidos desde la herramienta *Pyviz,* la cual muestra los datos de los mismos parámetros obtenidos para las anteriores simulaciones.

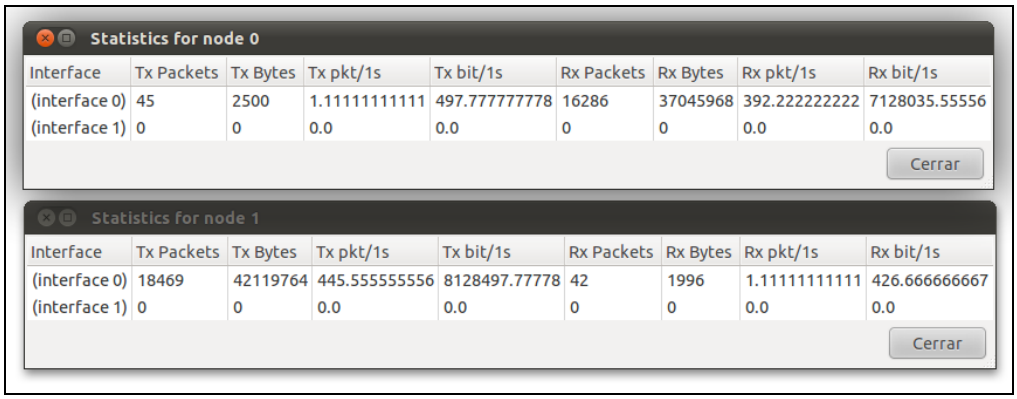
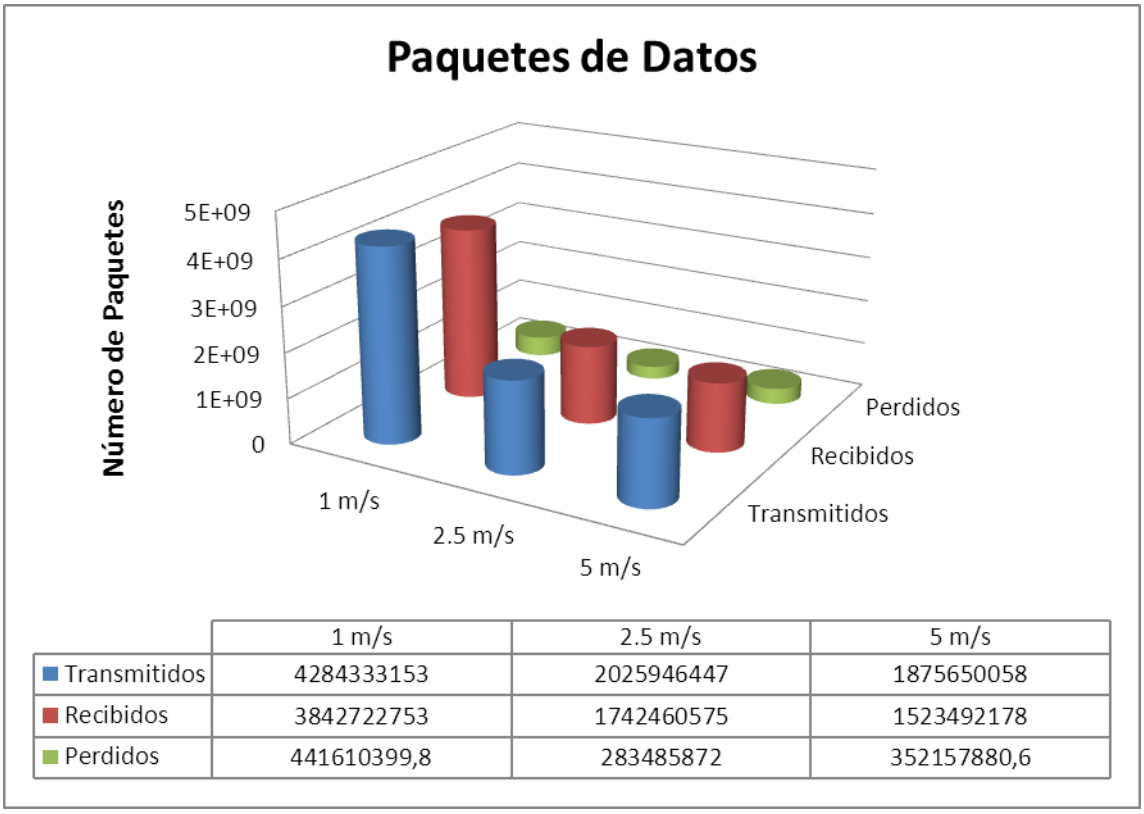


Figura. 4.14 Estadísticas de los Nodos 0 y Nodo 1 durante la transmisión de Paquetes.

En la Figura 4.13 se presenta los resultados obtenidos utilizando la herramienta *Pyviz,* estos resultados verifican los paquetes transmitidos, recibidos y la cantidad de paquetes por segundo que transmite y que recibe cada nodo. En la gráfica se verifica que la cantidad de paquetes que transmite el Nodo 1 al momento de la captura es de 18469 paquetes y ha recibido 42 paquetes durante la transmisión unidireccional. Respecto a la relación de los paquetes transmitidos se muestra que se envían 455 paquetes por segundo, estos valores cambian de acuerdo a la variación de velocidad de desplazamiento del nodo móvil. En la

Figura 4.14 se muestra, en contraste, los resultados obtenidos de las tres simulaciones en una sola gráfica, hay que destacar que los resultados se obtienen de diferentes archivos generados *.xml*, se requiere hacer esto ya que se necesita terminar la primera simulación, generar el archivo, cambiar la velocidad del móvil y nuevamente arrancar la siguiente simulación.



	1 m/s	2.5 m/s	5 m/s
Transmitidos	4284333153	2025946447	1875650058
Recibidos	3842722753	1742460575	1523492178
Perdidos	441610399,8	283485872	352157880,6

Figura. 4.15. Análisis de Paquetes Transmitidos, Recibidos y Perdidos para el escenario Tipo Fijo – Móvil.

En la Figura 4.14 se representan los valores totales obtenidos de los paquetes que atraviesan la red durante las tres simulaciones realizadas variando las velocidades del nodo móvil. En la gráfica se presentan los paquetes transmitidos, recibidos y perdidos. Como esta previsto la mayor cantidad de paquetes enviados se obtiene con la simulación cuando el móvil se desplaza a 1 m/s, de igual manera en este caso es cuando se obtiene la menor cantidad de paquetes perdidos, aproximadamente un 10% de pérdidas de paquetes durante la transmisión de estos. Para las siguientes dos simulaciones, el porcentaje de

pérdidas aumenta progresivamente, para el segundo caso cuando el móvil se desplaza a 2.5 m/s alcanza el 14% de pérdidas y para el tercer caso cuando el desplazamiento es a 5 m/s el porcentaje llega hasta el 18% de las pérdidas. Estos valores reflejan resultados similares al comportamiento de la red, tanto en el análisis del *throughput* como del *delay* ya que esto permite verificar el funcionamiento de la red tal como se esperaba.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- La evaluación del desempeño de la herramienta de simulación *ns-3*, bajo ambientes inalámbricos, específicamente el estudio realizado con el estándar IEEE 802.11 ha demostrado la potencialidad de este software sobre otras herramientas, entre ellas el *Network Simulator ns-2*, en el cual el desempeño tanto a nivel de simulación, resultados y funcionamiento es superior al obtenido con otros sistemas de simulación.

- El simulador *ns-2* es una herramienta potente, con muchos módulos disponibles (aunque no todos actualizados), pero compleja e incómoda de usar, además de arrastrar decisiones de diseño que con el tiempo se revelaron. Aunque sobre el papel es posible encontrar módulos para todos y cada uno de los escenarios que se necesitan, no es posible simular en un mismo escenario todas ellas, en cuanto a ns-3, cumple la necesaria e importante tarea de recoger la experiencia de ns-2 y desarrollarla logrando implementaciones a gran escala llegando a ser un simulador con un buen diseño desde su origen, muy potente y flexible.

- El simulador *ns-3,* representa una mejor alternativa para realizar estudios de investigación en comunicaciones inalámbricas, demostrando una arquitectura altamente flexible, permitiendo contribución de terceros para el diseño de nuevos modelos y la

posibilidad de incorporarlos en el código fuente de *ns-3* obteniendo un ámbito de continuo crecimiento.

- La implementación de estándares con alta disponibilidad como lo son WiFi, WiMax, GSM, GPRS, modelos de movilidad y protocolos de enrutamiento (OLSR, AODV, EIGRP, OSPF, etc.) hacen de *ns-3* un simulador muy adecuado para simular redes de manera eficiente y precisa, obteniendo resultados muy cercanos a la realidad con un margen de error bastante aceptable en el orden de las unidades, lo cual representa valores que pueden ser aceptados para una posterior implementación.

- El análisis de cada escenario de simulación ha permitido obtener resultados superiores a los que se puede obtener con otro simulador, interpretando resultados mediante la utilización de programas externos como *Wireshark* y *Pyviz*. Con el programa *WIreshark* se logró cargar archivos de captura generados durante las simulaciones presentadas, lo cual permitió interpretar resultados de acuerdo a los valores presentados en el archivo de captura. El análisis con estos datos son de gran importancia al momento de analizar el comportamiento de la red antes, durante y después de la simulación obteniendo un amplio estudio de análisis y recopilación de datos.

- Después de realizadas las implementaciones bajo el simulador *ns-3*, se generaron resultados para los tres tipos de simulaciones realizadas. Tipo Infraestructura, Tipo Ad-hoc y Tipo Fijo – Móvil, siendo ésta última la más utilizada en el mundo actual ya que los nuevos dispositivos inalámbricos poseen una alta movilidad y requieren de alta disponibilidad y conectividad durante la mayor cantidad de tiempo (aproximadamente 98% de conectividad). Con el tercer escenario se obtienen resultados bastante satisfactorios, ya que aquí se incluyen parámetros importantes dentro de la movilidad como son distancia y velocidad de los dispositivos móviles. Estos

resultados indican que tanto la distancia como la velocidad juegan un papel importante durante las transmisiones realizadas en la simulación, es decir son parámetros que hay que tomar en cuenta para su respectivo análisis. Finalmente los resultados fueron los esperados obteniendo un rendimiento de la red superior al 60%, tal como lo establece el estándar IEEE 802.11, manteniendo conectividad durante los intervalos de tiempo más críticos.

- La variación de parámetros de simulación fue uno de los principales métodos de análisis para las redes implementadas, se eligió dicho método para realizar comparaciones entre las tres simulaciones. Lo cual permitió llegar a obtener resultados óptimos para cada tipo de escenario planteado. Hay que tener muy en cuenta que la variación de dichos parámetros debe ser siempre acorde a los estándares inalámbricos implementados, tomando en cuenta rangos máximos y mínimos para su implementación. En caso de no tomar en cuenta dichos parámetros las simulaciones pueden variar drásticamente, obteniendo resultados incoherentes respecto a los obtenidos en este estudio.

5.2 RECOMENDACIONES

- El simulador *ns-3,* es una herramienta bastante potente, lo que permite seguir desarrollando nuevos módulos para poder ser implementados en el código fuente del simulador. Al tener una herramienta bastante estable, es recomendable utilizarla bajo el área de investigación ya que es un software que se acopla perfectamente para trabajos de investigación y manipulación de redes inalámbricas. El poder de esta herramienta es tal, que el investigador puede manejar los dispositivos a su conveniencia y de acuerdo a sus necesidades.

- A pesar de que la información es bastante limitada, actualmente se encuentran formados foros de investigadores en la nube, los cuales ofrecen una alta guía para la utilización de este simulador. Es importante continuar los estudios a nivel académico sobre esta herramienta, esto mantendrá un alto nivel de investigación permitiendo desarrollar nuevos sistemas de comunicaciones inalámbricas basados en los actuales, así como aumentar la capacidad de los estudiantes para poder comprender desde un ámbito mucho más profundo el funcionamiento de cada dispositivo móvil o estático al poder manipularlo.

REFERENCIAS BIBLIOGRÁFICAS

[1] Definición de Scripts, http://www.alegsa.com.ar/Dic/script.php., Recuperado el 15 de Junio de 2010

[2] Lacage, Mathieu, “Yet Another Network Simulator”, *7th ACM international symposium on Modeling*, New York, 2006.

[3] Sphinx, ns-3 Manual, http://www.nsnam.org/docs/manual/html/index.html,, 2010, Recuperado el 15 de Junio de 2010

[4] Sphinx, ns-3 Tutorial, http://www.nsnam.org/docs/tutorial/html/index.html, 2010, Recuperado el 15 de Junio de 2010

[5] Introducción a Wi-Fi (802.11), http://es.kioskea.net/contents/wifi/wifiintro.php3., Recuperado el 15 de Noviembre de 2010

[6] Redes Inalámbricas, http://www.slideshare.net/Comunicaciones2/espectro-ensanchado-por-secuencia-directa-dsss-unidad514, Recuperado el 26 de Noviembre de 2010

[7] Globalspec The Engineering Search Engine. (B. A. Forouzan, Editor), http://www.globalspec.com/reference/10510/121073/Chapter-6-2-3-Direct-Sequence-Spread-Spectrum, Recuperado el 31 de Noviembre de 2010

[8] TCP Models in ns-3, http://www.nsnam.org/docs/release/3.13/models/html/tcp.html, Recuperado el 31 de Noviembre de 2010

[9] Ponce, Enrique; Tortosa Enrique; Maicas Vicente, Redes Inalámbricas: IEEE 802.11, http://multingles.net/docs/Manual%20-%20Redes%20WiFi%20inalambricas.pdf, Recuperado el 15 de Diciembre de 2010.

[10] Bonastre, Juan Antonio, Modulación en redes inalámbricas, http://80.59.18.72/electron/franjagl/st/modem/04_Modulacion.pdf, Recuperado el 15 de Diciembre de 2010

[11] Gast, The Direct Sequence PHYs: DSSS and HR/DSSS (802.11b), http://www.canal-ayuda.org/a-informatica/inalambrica.htm, Recuperado el 20 de Diciembre de 2010

[12] Schwartz, Sorin, Frequency Hopping Spread Spectrum (FHSS) vs. Direct Sequence Spread Spectrum (DSSS) in Broadband Wireless Access (BWA) and Wireless LAN (WLAN), http://sorin-schwartz.com/white_papers/fhvsds.pdf, Recuperado el 20 de Diciembre de 2010

[13] Tramas 802.11, http://dns.bdat.net/seguridad_en_redes_inalambricas/x187 .html, Recuperado el 21 de Diciembre de 2010.

[14] Bernal, Iván, IEEE 802.11 MAC Management, http://clusterfie.epn.edu.ec/ibernal/html/CURSOS/Oct05Marzo06/Inalambricas/CLASES/802-11ParteIc.pdf, Recuperado el 21 de Diciembre de 2010

[15] Modulación PPM, http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/ valle_i_lf/capitulo1.pdf, Recuperado el 21 de Diciembre de 2010

[16] MAC frame formats, http://www.eefocus.com/article/08-06/43509s.html, Recuperado el 21 de Diciembre de 2010

[17] Siguencia, Hernán, Topologías y Requerimientos WLAN, http://dspace.ups.edu.ec/bitstream/123456789/221/3/Capitulo%202.pdf, Recuperado el 26 de Diciembre de 2010

[18] Bernal, Iván, Contention – Free Service with the PCF, http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/912/6/T10435CAP2.pdf, Recuperado el 28 de Diciembre de 2010

[19] Chiu, L, Procesamiento de Señales para Sistemas Inalámbricos, http://neutron.ing.ucv.ve/revista-e/No2/L_Chiu.html, Recuperado el 28 de Diciembre de 2010

[20] Modelos de Propagación, http://www2.elo.utfsm.cl/~elo352/2010/Exp1/marcoteo.pdf, Recuperado el 28 de Diciembre de 2010

[21] Descripción de IEEE 802.11, http://catarina.udlap.mx/u_dl_a/tales/ documentos/lem/soriano_m_jc/, Recuperado el 4 de Enero de 2011

[22] Dabbous, Walid Dr, Extensions du simulateur Omnet++ pour la validation de mecanismes de transmission multimedia dans les reseaux IEEE 802.11, http://www.memoireonline.com/07/08/1359/extensions-simulateur-omnet-tramsmission-multimedia-reseaux-ieee-802-11.html, Recuperado el 15 de Junio de 2011

[23] Vaduvur, Bharghavan, Robust rate adaptation for 802.11 wireless networks, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.126.7323, Recuperado el 15 de Junio de 2011.

[24] Valores RSSI para conexiones Wireless, http://jetclub.balearweb.net/post/8972, Recuperado el 27 de Julio de 2012

[25] Introducción a Wi-Fi (802.11), http://es.kioskea.net/contents/wifi/wifiintro.php3., Recuperado el 15 de Noviembre de 2012

[26] Delgado, Óscar, Nuevos Protocolos y Esquemas de Seguridad para Redes Ad-hoc Móviles Inalámbricas, http://e-archivo.uc3m.es/bitstream/10016/11576/1/Tesis_Oscar_Delgado_Mohatar.pdf, Recuperado el 15 de Noviembre de 2012

[27] Medina, Andrea, Familia de Estandares IEEE 802.11: Wireless Networking, http://ieeestandards.galeon.com/aficiones1573579.html, Recuperado el 25 de Julio de 2012

[28] Introducción al MTU, http://es.kioskea.net/faq/1557-introduccion-al-mtu, Recuperado el 26 de julio de 2012

[29] Villacrés, Santiago, Análisis del desempeño de una red WPAN Basado en el estándar IEEE 802.15.4 utilizando Network Simulator 2, http://repositorio.espe.edu.ec/bitstream/21000/120/1/T-ESPE-020306.pdf, Recuperado el 26 de julio de 2012

Autorización de publicación

ESCUELA POLITÉCNICA DEL EJÉRCITO

INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, Ricardo Javier Moreno Cadena

Autorizo a la Escuela Politécnica del Ejército la publicación, en la biblioteca virtual de la Institución del trabajo “Evaluación del desempeño de la herramienta *ns-3* en ambientes inalámbricos bajo el estándar IEEE 802.11”, cuyo contenido, ideas y criterio son de mi exclusiva responsabilidad y autoría.

_____

Ricardo Javier Moreno Cadena

FECHA DE ENTREGA

El proyecto fue entregado al Departamento de Eléctrica y Electrónica y reposa en la Escuela Politécnica del Ejército desde:

Sangolquí, _____ de 2012.

ELABORADO POR:

_____

Ricardo Javier Moreno Cadena

AUTORIDAD:

_____

Ing. Darío Duque
Coordinador de la Carrera de Ingeniería en
Electrónica y Telecomunicaciones