GUIA PARA EL ANÁLISIS DEL PROTOCOLO DE ENCAMINAMIENTO OSPF EN REDES INALÁMBRICAS APLICADO EN NUEVAS TECNOLOGÍAS.

FERNANDO FLÓREZ AGUILERA

UNIVERSIDAD SANTO TOMÁS DE COLOMBIA
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ-COLOMBIA
2019

GUIA PARA EL ANÁLISIS DEL PROTOCOLO DE ENRUTAMIENTO OSPF EN REDES INALÁMBRICAS, Y REDES APLICADAS EN NUEVAS TECNOLOGÍAS.

FERNANDO FLÓREZ AGUILERA

MONOGRAFÍA COMO REQUISITO PARA OPTAR POR EL TÍTULO DE INGENIERO DE TELECOMUNICACIONES.

Ing. PEDRO MANCERA
Asesor de proyecto

UNIVERSIDAD SANTO TOMÁS DE COLOMBIA
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ-COLOMBIA
2019

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

_____

Ciudad y Fecha de entrega

DEDICATORIA

Principalmente a Dios quien siempre me acompaña y es mi guía en cada uno de mis proyectos emprendidos, a mis padres, por su incondicional apoyo, comprensión y motivación, en todo momento, son ustedes núcleo de mi vida y mi mayor motivación para superarme día a día.

AGRADECIMIENTOS

Gracias a Dios por bendecirme día a día y darme la serenidad necesaria para cumplir cada uno de mis objetivos, a mi familia por su incondicional apoyo, a mi maestro Carlos, a mi tutor pedro mancera quienes siempre me guiaron en todo momento, y me motivaron a cumplir mi meta.

RESUMEN

Se expuso de manera específica el protocolo de encaminamiento OSPF, y su desempeño en redes de sensores inalámbricos aplicadas a nuevas tecnologías. Dentro del documento se analiza su funcionamiento en dichos entornos, para finalmente realizar una guía de aplicación que apoye al estudiante, en el análisis del protocolo en mención, profundizando en su aplicación.

Finalizando con el desarrollo por metodologías de resolución de problemas en ese tipo de redes basado en el Troubleshooting del protocolo.

Palabras clave

OSPF, Redes inalámbricas, Resolución de Problemas, metodología, competencias.

ABSTRACT

OSPF will be specifically exposed, and its performance in wireless sensor networks applied to new technologies, will be specifically exposed, analyzing its operation in these environments, to finally make an application guide that supports the student, in the analysis of the protocol in question, deepening in its application, consummated by methodologies of resolution of problems in this type of networks based on the Troubleshooting of the protocol.

Keywords

OSPF, wireless, Troubleshooting, methodology, skills,

Tabla de contenido

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

1. INTRODUCCIÓN

El avance en las Telecomunicaciones, se evidencia con la aparición de nuevas tecnologías en infraestructura e interconexión, especialmente en entornos inalámbricos, para dar soporte a los nuevos paradigmas de intercambio de información, por ejemplo, el concepto de conectividad entre dispositivos informáticos integrado en objetos cotidianos a través de redes inalámbricas. Existen varias aplicaciones de este tipo de tecnología, como la vigilancia de la naturaleza, aplicaciones para defensa, aplicaciones médicas entre otras.

Lo anterior muestra una clara necesidad de profesionales expertos en redes y entornos inalámbricos, evidenciando el reto que manejan los docentes para enseñar redes de computadoras y dispositivos de red, puesto que muchas veces la abstracción de conocimiento por parte del estudiante mejora exponencialmente al fundamentarse con la parte teórico-práctico en escenarios reales, ya que es muy difícil imaginar los conceptos de redes en escenarios actualmente aplicados, formatos de protocolos y comprensión del flujo de paquetes durante la enseñanza en el aula.

Por ende, se propone a lo largo del documento una revisión teórica del protocolo y su funcionamiento y las ventajas que se presentan al implementarlo en redes de sensores inalámbricos a lo largo del capítulo #, culminando con el capítulo 5, donde se refleja la implementación y discusión del funcionamiento de OSPF en entornos inalámbricos, y sus principales parámetros a tener en cuenta a la hora de diseñar o administrar este tipo de redes emergentes.

2. PLANTEAMIENTO DEL PROBLEMA

El considerable aumento de investigaciones en redes de sensores inalámbricos que permiten la implementación de nuevas tecnologías como lo es el Internet de las cosas, las cuales contribuyen con sus características a situaciones donde las adversidades de despliegue están siendo mitigadas. Se ha identificado que surge la necesidad de herramientas o material para la enseñanza de nuevas tecnologías que permitan al estudiante entender el concepto de las redes en entornos actuales y de constante crecimiento, dentro de las áreas de conocimiento del pensum encontramos a la telemática, área estudiada en la facultad de telecomunicaciones de la universidad santo Tomás, la cual tiene gran equivalencia a lo largo de la carrera profesional, es necesario establecer unos conceptos claros en el estudiante, para lograr un aprendizaje constructivo, a lo largo del semestre la universidad realiza guías de laboratorio excelentes para el desarrollo de competencias académicas según el currículum de la universidad, de igual forma el estudiante se interesa por entornos nuevos, además de la configuración del protocolo en dichos entornos es importante generar competencias que permitan entender al estudiante por qué y en qué situaciones aplicar el protocolo o si otro será más adaptativo y funcional.

¿Cómo entender OSPF para poder aplicarlo en tecnologías inalámbricas, donde el protocolo cumpla su función de una manera eficiente y se le permita al estudiante comprenderlo en escenarios actuales y emergentes dando herramientas para que el estudiante de cara a situaciones reales en su vida profesional?

Se propone un refuerzo con una guía que analice el protocolo OSPF y se destaque su mejor uso depende a una situación y tecnología que se esté llevando a cabo, perfilado al estudiante a estar preparado para confrontar situaciones del futuro.

3. OBJETIVOS

1. OBJETIVO GENERAL

Desarrollar una guía de análisis de funcionamiento del protocolo ospf para ser aplicado en entornos inalámbricos dirigido a nuevas tecnologías de comunicación.

2. OBJETIVOS ESPECÍFICOS

- Identificar los parámetros fundamentales del protocolo de encaminamiento OSPF para entornos inalámbricos y las nuevas tecnologías en que se puede aplicar.
- Analizar los parámetros de funcionamiento, configuración y rendimiento más relevantes de ospf en entornos inalámbricos.
- Seleccionar las metodologías de solución de problemas - Troubleshooting - en OSPF, de acuerdo con los requerimientos de Cisco.
- Proponer una topología referente para la guía, donde se lleve a cabo el análisis y TSHOOT del protocolo OSPF en una red basada en redes de sensores inalámbricos.
- Crear una simulación complementaria para explicar qué datos se configuran de lado de usuario final.

4. JUSTIFICACIÓN

1. Justificación Técnica.

Los protocolos de encaminamiento juegan un papel importante en las redes de computadoras, y para este caso nos referimos a una clase de protocolo que gracias a sus algoritmos encuentra rutas más favorables para la comunicación que se esté llevando a cabo, a través del tiempo las redes han cambiado por necesidad de implementar nuevos servicios, han tenido que transformarse. OSPF será el único protocolo vigente en las nuevas certificaciones de cisco, como protocolo de encaminamiento proactivo basado en el estado de enlace por ende se implementará en el desarrollo de estos escenarios y se analizaran sus características y beneficios presentados para varios tipos de redes, partiendo de la investigación encontraremos la implementación de las configuraciones aprendidas en el diplomado CCNP.

Para comprender el protocolo en redes influyentes en nuevas tecnologías, exponiendo al estudiante el análisis del papel del protocolo OSPF en redes que aporten a nuevas tecnologías.

Para que el estudiante entienda el uso correcto del protocolo y en qué tipo de redes, de acuerdo a sus necesidades técnicas, se puede llevar a cabo el uso de OSPF, entender sus características, ventajas y desventajas.

2. Justificación Académica

Académicamente se realizarán metodologías que faciliten al estudiante el proceso de desarrollo de las guías, además nutriendo de conocimiento al estudiante con bases y algo más para entender diferentes tecnologías y usos del protocolo en escenarios empresariales importantes para todo aquel que desea ejercer la profesión. El análisis y resolución de problemas dentro de redes que funcionen con el protocolo se verán reflejadas en el capítulo 2 donde veremos el protocolo y sus diferentes características.

3. Justificación Económica

Dentro de lo que toda empresa tiene como objetivo se encuentra la reducción de costos de infraestructura, sus servicios están garantizados gracias a las redes que se manejan, por eso dentro de las aplicaciones que se mencionan se quiere reflejar esto, topologías usadas actualmente que reducirán costos y que cumplirán con su papel para que cada uno del servicio, muchos emergentes que se están conociendo en el transcurso de los últimos años sean bien justificados.

4. Justificación Social

Por medio de esta monografía se busca generar una herramienta que facilite a los estudiantes, el aprendizaje de uno de los temas pertenecientes a la certificación profesional CCNP de CISCO.

5. ALCANCE Y LIMITACIONES

1. ALCANCE

El desarrollo del presente documento se centra en la identificación de los parámetros más importantes del protocolo OSPF, que deben ser tenidos en cuenta para su análisis en entornos inalámbricos, lo que se plasmará en una guía que permita, a través de una topología propuesta y su respectiva simulación, seguir unos pasos definidos para mostrar el funcionamiento, configuración y solución de problemas - TroubleShooting.

2. LIMITACIONES

Debido a las limitaciones en los simuladores para redes sensores inalámbricos, especialmente en la configuración de OSPF, se usa la similitud que existe en funcionamiento de este protocolo en entornos alambrados e inalámbricos, y se propone una simulación adicional en packet tracert para emular el comportamiento en tecnologías como IoT.

Packet tracert cuenta con una capacidad de dispositivos finales para medición limitadas, por ende, en la simulación complementaria de cara al cliente se utilizó un sensor de temperatura para demostrar cómo se genera la información que después será reenviada por la puerta de enlace a cada uno de los demás nodos plasmados en la topología desarrollada para la solución.

3. Metodología.

- La metodología planteada en este proyecto, tiene como primera fase llevar a cabo una conceptualización del protocolo OSPF, tanto en su diseño como en su implementación, teniendo en cuenta que el estudiante que realice la guia tenga nociones del protocolo, de manera que se utilizan habilidades teóricas lo más concisas y fáciles de entender.

- En la segunda fase se investigó sobre varios trabajos en las bases de datos de la universidad sobre redes de sensores inalámbricas, para contextualizar al estudiante de qué tipos de redes estamos hablando y por que se han vuelto tan importantes hoy en día. llevando la adecuada documentación de esta tecnología, para que así sea posible explorar escenarios donde se vea trabajando de manera eficiente y eficaz, que además no genere costos adicionales.

- En la tercera y última fase se llevó a cabo la guia en el capítulo 3, donde realizó una verificación de ejemplo del protocolo, donde se iba analizando paso a paso cada comando para que nos sirve y que se debe analizar de cada resultado. Posterior a esto se lleva a cabo una explicación detallada de como crear un entorno de virtualización para el funcionamiento de GNS3 y mitigar inconvenientes por requerimientos necesarios del PC, por último se explica la configuración de una solución basada en redes de sensores inalámbricos, el enfoque es en las comunicaciones más no en el acceso, puesto que para el caso será administrado por el usuario, a lo largo de estos últimos apartados se explica cada uno de los factores y se analiza el por que de las configuraciones, motivando al estudiante a diseñar sus propias redes rigiéndose de los factores estudiados.

TRABAJOS SIMILARES

Antecedentes

- Rodríguez, E. J., Deco, C., Petinari, M., & Burzacca, L. (2012). Protocolos de encaminamiento para Redes malladas Inalámbricas: un estudio comparativo. In XVIII Congreso Argentino de Ciencias de la Computación.

Este trabajo nos permite entender cómo funcionan las redes malladas inalámbricas, las cuales funcionan con varios protocolos de enrutamiento, entre ellos el que para esta ocasión analizaremos. OSPF utiliza el conocido algoritmo dijkstra,teniendo en cuenta como métrica estado de enlace, gracias a conocer este estudio se nos permite tener una periferia amplia, conociendo cómo funciona el protocolo en redes inalámbricas las cuales son elemento importante en el IOT.

.

- Rey Manrique, F. R. (2011). Diseño de un sistema de CCTV basado en red IP inalámbrica para seguridad en estacionamientos vehiculares.

Este trabajo permite conocer técnicas de redes inalámbricas, para nuestro caso de estudio es bastante importante conocer los protocolos bajo el estándar 802.11, el sistema de CCTV que propone en este trabajo el autor, expresa la importancia de los elementos intermedios como el router para comunicar los nodos que abstraen la información, en este caso las cámaras.

- Sánchez, J. R. P. (2016). Análisis y comparación de la seguridad utilizando dos protocolos de enrutamiento para IPv6. *Maskana*, *7*, 213-220.

Por medio de este trabajo realizado por el autor, podemos analizar las vulnerabilidades del protocolo, en este caso para este estudio OSPFv3, la seguridad en IPV6 es demasiado importante y más en escenarios futuros donde pasará a jugar un papel más exigente, el trabajo expone un análisis de los protocolos de enrutamiento RIPng y OSPv3, evaluando básicamente su Disponibilidad, integridad y confidencialidad.

- 10.1109/CONFLUENCE.2016.7508186

Este documento nos permite abstraer conceptos básicos y fundamentales de OSPF, una introducción interesante, aplicándolo en IPV6, puesto que se evaluaron dos desempeños trabajando en conjunto, se analiza el desempeño de OSPF teniendo en cuenta su ancho de banda y demás conceptos que nos dan a entender que OSPF será uno de las mejores opciones entre los protocolos de enrutamiento IPV6 en un futuro no muy lejano.

CAPÍTULO 2

6. PARÁMETROS FUNDAMENTALES DEL PROTOCOLO DE ENCAMINAMIENTO OSPF

Para que una red basada en IP se comunique con otras redes, es necesaria la implementación de un protocolo de encaminamiento, como lo son RIP, EIGRP, OSPF, y BGP. Para el caso de redes que poseen subredes es óptimo la implementación del protocolo OSPF, ya que, permite la actualización de la tabla de enrutamiento en cada uno de los dispositivos de enrutamiento de cada una de las redes y a su vez, también permite resumir rutas de máscaras de subred de longitud variable. Por lo tanto, la implementación de este protocolo de enrutamiento es se necesita conocer o fundamentar los parámetros de funcionamiento del protocolo.

1. PROTOCOLO DE ENCAMINAMIENTO.

Se define como un conjunto de mensajes, reglas y algoritmos utilizados por los enrutadores teniendo como propósito compartir información de enrutamiento. Este proceso incluye el intercambio y análisis de información de enrutamiento. Cada enrutador elige analiza y determina cuál de los diferentes caminos, tiene una métrica o coste bajo, es decir, que cual de las diferentes rutas tiene menos tiempo de enrutamiento para cada subred (selección de ruta) y finalmente registrar la ruta seleccionada tabla de enrutamiento IP. Los ejemplos incluyen RIP, EIGRP, OSPF y BGP.[1].

2. FUNCIONES.

Principalmente las funciones de los protocolos de enrutamiento son:

- Al tener bastantes elecciones de ruta el enrutador elige la mejor según su **métrica**.
- Cambiar de topología al percibir una falla, reaccionar al cambio y adaptarse, eligiendo la mejor ruta actualizada como se indica en el texto de CCNA Routing and switching ICND2 200-105 de Wendell Odom, este proceso se llama **convergencia**.
- Aprender información de encaminamiento de subredes de sus enrutadores vecinos.
- Informar encaminamiento sobre las subredes a enrutadores vecinos.
- Permite que los dispositivos de la red de enrutamiento puedan registrar en su tabla de enrutamiento rutas más usadas y hacer un canal único entre las rutas ya establecidas.

3. PROTOCOLOS DE ENCAMINAMIENTO INTERIORES Y EXTERIORES.

El conjunto de redes IP, que tienen políticas de rutas independientes es considerado un sistema autónomo, teniendo en cuenta esto existen protocolos internos y externos a estos sistemas.

4. PROTOCOLO DE PASARELA INTERIOR (IGP)

IGP: Se refiere a un protocolo de enrutamiento diseñado para ser implementado dentro de un único sistema autónomo (AS)[1].

5. PROTOCOLO DE PASARELA EXTERIOR (BGP)

EGP: Un protocolo de enrutamiento que fue diseñado y destinado a ser utilizado entre diferentes sistemas autónomos.

(AS)[1].

6. TIPOS DE PROTOCOLO IGP

Los tipos de protocolo IGP se clasifican teniendo en cuenta la lógica y los procesos utilizados por diferentes protocolos de enrutamiento para resolver el problema de aprender todas las rutas, la elección de la mejor ruta para llegar a la subred seleccionada y su convergencia a la hora de que algún router de la topología presente falla o inasistencia. Existen 3 principales ramas de algoritmos de protocolo de enrutamiento para protocolos de encaminamiento en el mismo sistema autónomo según el libro guía de Wendell Odom para la preparación del examen CCNA actual.

7. INTRODUCCIÓN OSPF

En la actualidad, las redes se utilizan para distintos servicios como acceder a páginas web, conversar mediante teléfonos IP, dar parte en videoconferencias, disputar en juegos interactivos, efectuar compras en Internet y entre otros servicios que puede ofrecer las redes conectas a internet.

Uno de los aspectos más importantes en el diseño e implementación de redes, es la configuración del protocolo de encaminamiento más eficiente, especialmente en topologías complejas y de gran extensión. El proceso de encaminamiento inicia cuando los dispositivos de red, que se encuentran en redes distintas, quieren comunicarse, por lo tanto, los paquetes IP se envían hacia el enrutador, el cual funciona como puerta de enlace, para poder acceder a otras redes, revisando parámetros como las tablas de enrutamiento, y correspondientes estados de enlace.

Comentado [JA1]: Esto no se entiende pues está mal redactado, qué es conocido?

la garantía en la comunicación entre distintas redes, depende en gran medida, de la capacidad de los enrutadores para reenviar paquetes del modo más eficaz. Es

aquí donde intercede el protocolo OSPF, el cual es un protocolo de encaminamiento dinámico, que utiliza como métrica el costo por interfaz, que se requiere para realizar una comunicación hacia otro nodo o enrutador. En la figura 2, se puede apreciar una topología configurada con OSPF, donde se evidencia manejo de distintos tipos de área, dentro de las cuales se permite excluir diferentes tipos de mensajes, en la imagen se evidencia un área 0, acompañada por tres áreas diferentes.

1. DEFINICIÓN

Protocolo de encaminamiento, basado en estado de enlace, que utiliza el costo de las interfaces del router y usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos, permitiendo la autenticación de actualizaciones de ruteo, máscaras de subred de longitud variable y resumen de rutas.

2. CARACTERÍSTICAS

A continuación, se pueden evidenciar las principales características del protocolo, las cuales serán vistas a mayor profundidad a lo largo del documento y como se refleja su importancia en cada uno de los parámetros a analizar del protocolo.

Comentado [JA2]: No describió las características como se solicitó.

Figura 1. OSPF características. Autoría propia: realizado en la APP: https://www.lucidchart.com/

Eficiencia.

Esta característica se refiere a como el protocolo rinde en varios tipos de redes, su rendimiento es destacable.

VLSM

OSPF permite llevar a cabo el método de máscara de subred de longitud variable

DE RAPIDA CONVERGENCIA

OSPF tiene la capacidad de adaptarse a cambios en la red de una forma rápida, la convergencia se refiere a el tiempo que el enrutador tarda en adaptarse a sus variaciones, y a editar sus tablas de encaminamiento.

Escalabilidad

Gracias a que OSPF es multiarea, le permite llevar acabo ampliaciones en la red, y llevar fácilmente la administración de redes complejas y de constante cambio.

MD5

OSPF tiene la ventaja de utilizar el algoritmo MD5 el cual por medio de una llave o hash, encriptan la información hasta que sea abierta por el receptor el cual conoce el mismo valor hash.

3. Cabecera OSPF

Para que un paquete pueda ser enrutado a su destino, el router introduce o agrega una cadena de bit que contiene la información de enrutamiento y de esa manera el paquete puede hacer su recorrido ya establecido.

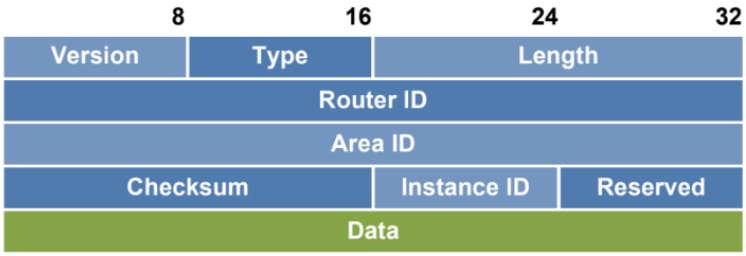


Figura 2. Cabecera de protocolo OSPF: packetlife.net

La cabecera del protocolo está compuesto por un total de 32 bits, la cual estos bits están distribuidos de la siguiente forma:

- Version: Los primero 8 bits de la cabecera indican la versión que se está usando, ya sea versión 2 o 3.
- Type: Estos 8 bits contiene la información de que tipo de paquete es enviado y recibido por los router vecinos, uno de estos mensajes son:
    1. Hello, mensaje de reconocimiento del router vecino.
    2. DB, descripción de la base de datos.

3. LS Request, solicitud del estado del enlace.
4. LS Update, Actualización del estado de enlace.
5. LS ACK, Acuse recibido del estado de enlace.

- Length: Tamaño del mensaje o paquete incluye la cabecera OSPF.
- Router ID: Es donde se almacena o se registra la dirección IP del router origen.
- Area ID: Es donde es registrado el número del área de donde es enviado el paquete.
- Checksum: Suma de la verificación del número de bits.

4. PROPIEDADES.

- Tipo de protocolo: estado de enlace.
- Algoritmo: Dijkstra
- Routes IP
- Routing Advertisements: Partial When Route Changes Occur
- Metric: es la valoración que hace el protocolo para identificar cual es la ruta más rapida, que es basado por los datos o el link del router origen (100,000,000/interface speed)
- Hop Count: None (Limited by Network)
- Variable Length Subnet Masks
- Summarization on Network Class Address or Subnet Boundary
- Load Balancing Across 4 Equal Cost Paths
- Router Types: Internal, Backbone, ABR, ASBR
- Area Types: Backbone, Stubby, Not-So-Stubby, Totally Stubby
- LSA Types: Intra-area (1,2) Inter-area (3,4), External (5,7)
- Timers: Hello Interval and Dead Interval (different for network types)
- LSA Multicast Address: 224.0.0.5 and 224.0.0.6 (DR/BDR) sin filtrar.
- Tipos de interfaces: punto a punto, difusión , No difusión, punto a multipuntos, y Loopback

Base de datos de estado de enlace (LSDB):

La estructura de datos mantenida por un enrutador OSPF para propósito de almacenar datos de topología[1]

Shortest Path First (SPF)

El nombre del algoritmo que OSPF usa para analizar el LSDB (Nota: el análisis determina la mejor ruta [de menor costo] para cada prefijo / longitud).[1]

Link-State Update (LSU)

El nombre del paquete OSPF que contiene la información de topología detallada, específicamente LSA. [1]

Link-State Advertisement (LSA)

El nombre de una clase de estructuras de datos OSPF que contienen información de topología (Nota: los LSA se guardan en la memoria en un LSDB y se comunican a través de una red en mensajes LSU). [1]

Parámetros claves en una red con OSPF.

Si hablamos de parámetros claves, es importante tener en cuenta que papel toma cada router (nodo), OSPF utiliza un nodo como DR(router designado), el cual es el encargado de redistribuir los enlaces de red, BDR el cual es el respaldo del DR(router designado), ABR qué es un nodo en el extremo de dos áreas, ASBR que es el nodo en frontera en áreas que utilizan otros protocolos de encaminamiento como (RIP,EIGRP,IS-IS).

-Estructura de datos, Base de datos de adyacencia, base de datos de, base de datos de estado de enlace (LSDB), Bases de datos de reenvía la cual es la encargada de general la tabla de routing

1. Mensajes.

El protocolo utiliza varios mensajes para detectar nuevos vecinos, compartir estados de enlace, después de los nodos estar en estado FULL, estos mensajes se volverán a enviar en dos únicos casos, al cambiar la topología y cada 30 minutos, Los mensajes HELLO funciona como un keepalive, esto significa que se utiliza para formar o reformar adyacencias, constantemente por medio de el se genera conocimiento a el enrutador si otro dispositivo se conecta a su red, un dispositivo de red capa 3. Los mensajes de paquetes de descripción de bases de datos o BDB, transportan la cabecera de los avisos de estado de enlace o LSA, para generar una consulta completa sobre los LSA, se envian mensajes LSR los cuales tienen como función es obtener información sobre nuevos LSA, o LSA no actualizados.

5. OSPF MULTIÁREA

OSPF Se puede implementar de dos maneras, OSPF de área única la cual se utiliza normalmente en redes más pequeñas, para las cuales funciona muy bien, no obstante, a medida que las topologías se extienden se presentas problemas de sobrecarga de procesamiento y de memoria. OSPF multiárea resuelve estos problemas utilizando varias áreas, para llevar así una administración distribuida de la información, cada área maneja una base de datos, las cuales son administradas por una sola en un área 0, es aquí donde se lleva la carga del almacenamiento y procesamiento que se necesita normalmente para volver a cargar tablas de encaminamiento nuevas, a continuación en la figura 3 podemos evidenciar un diseño típico de Múltiples áreas, en este caso 3 conectadas a un área 0.

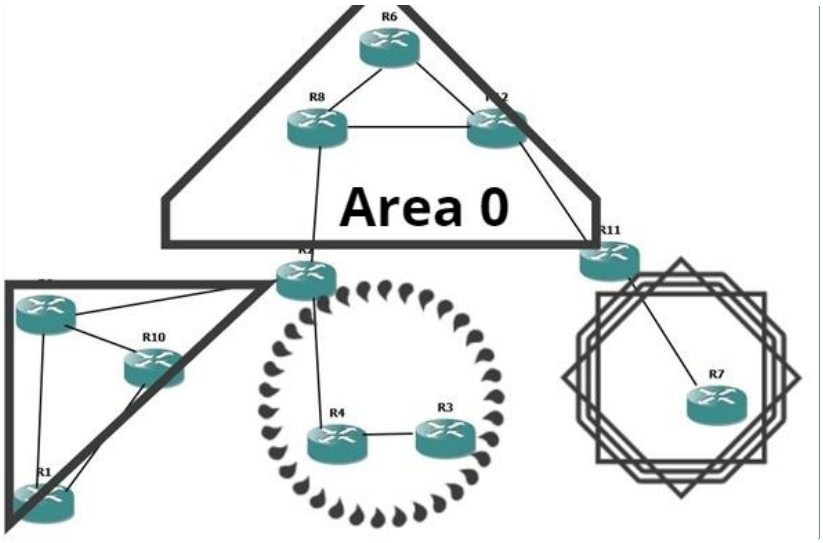


Figura 3. Diseño Típico. Autoría propia: software:GNS3, editor: https://www.fotor.com/es/

Comentado [JA3]: Sigue sin entenderse la imagen, en el texto se menciona la figura 2 (¿?) que muestra el área 0 y otras dos, pero en esta figura hay 4 agupaciónes, si son áreas no se entiende.

6. OSPF EN LAN'S

Para el OSPF tener redes adyacentes o vecinas es más complejo que los demás protocolos como EIGRP. Lo que hace complejo la coneccion entre diferentes redes LAN’s, como bien se sabe que en el protocolo EIGRP en el momento que se hace

un escaneo de redes vecinas o adyacentes, simplemente el protocolo comparte información entre las demas para asi hacer la comunicaciones.

Por lo tanto OSPF utiliza Máquina de Estado Finito Subyacente (FSM) la cual define a las redes vecinas en ocho estados, en donde permite conocer los estados de cada una de las redes. Para conocer cada uno de los estados actuales de las redes vecinas el protocolo OSPF tiene una serie de características.

- **Procedimiento del protocolo OSPF para el descubrimiento de redes vecinas**

Comentado [JA4]: Sigue estando mal la palabra

Para empezar al protocolo OSPF envía un mensaje multicast en interfaces LAN en busca de redes vecinas OSPF. Para que OSPF relación a otras redes como vecinas OSPF tiene que cumplir con los siguientes requerimientos:

- OSPF tiene que estar configurado en en la interfaz del enrutador.
- La interfaz del enrutador no debe ser pasiva.

En el momento que se cumplan las dos condiciones ya mencionadas, OSPF envía un mensaje (Hello) en multidifusión a una dirección exclusiva para enrutadores de que tenga configurado OSPF (dirección IP 224.0.0.5). El mensaje enviado contiene el OSPF RID (ID del router con OSPF) y el área OSPF que el enrutador le ha otorgado a la subred LAN. Se debe tener en cuenta que, si las interfaces que los enrutadores se encuentra en pasivo, en el momento en que dos enrutadores con OSPF se encuentre mutuamente, este dejará de enviar mensajes (Hello) ocasionando que no se descubra nuevas redes LAN.

- **Configuración que deben tener las redes LAN OSPF**

Cuando el enrutador local, envía el mensaje (Hello) de multidifusión a los demás enrutadores en distintas redes, estos últimos envían un mensaje de respuesta al enrutador local, y luego el enrutador local examina esos mensajes de respuesta provenientes de los demás enrutadores de las redes LAN vecinas, verificando que el mensaje cumpla con las siguientes condiciones:

Comentado [JA5]: Mal redactado

- ID del router OSPF
- Bande del área
- Los mensajes (Hello) en intervalos
- Intervalos muertos
- Máscara de la subnet
- Lista de las interfaces de las redes LAN vecinas
- ID del área
- Prioridad del router
- Dirección IP del enrutador de la red vecina

El procedimiento que sigue el protocolo OSPF para la conexión o reconocimiento de redes LAN adyacentes es de manera comparativa y estricta, ya que en el momento en que mensaje (Hello) de respuesta de un enrutador vecino es recibida

por el enrutador inicial, esté compara la dirección IP de origen del mensaje y el número de su máscara de la red LAN potencial. Luego calcula la dirección de subred, compara la dirección IP y la máscara que tiene configurada en su interfaz, estas tienen que coincidir junto con el ID de área de la subred. En caso que en el enrutador vecino no coincida el ID del área este lo rechaza.

OSPF usa un algoritmo complejo para el escáner y aceptación de redes LAN vecinas, ya que sus mensajes de difusión de saludo y respuesta poseen información que tiene que coincidir para que el enrutador potencial no sea rechazado.

7. OSPF EN WAN'S

Para la simulación de redes WAN'S los enrutadores con lenguaje OSPF puedan acceder a nuevas redes vecinas o adyacentes, deben cumplir con los mismos requerimientos OSPF en redes LAN. El protocolo funciona de la misma forma, pero algunos elementos cambian para varios tiempos de enlaces WAN, ya que algunos casos son pensados para el desarrollo de una implementación en particular de verificación.

Alguno de estos desarrollo de implementación se debe a elementos como, la configuración de tipo de red, servicio y tecnología.

- **Tipo de redes OSPF**

La configuración de la interfaz en un enrutador que va usar lenguaje OSPF es importante que tenga estas configuraciones.

- El enrutador puede esperar descubrir redes vecinas por medio de mensajes de difusión.
- Solo se pueden existir dos o más enrutadores OSPF en las subredes conectadas en la interfaz.
- El enrutador debe intentar elegir un DR OSPF en la interfaz.

Un tipo de red OSPF es por difusión, la cual encuentra de manera dinámica redes LAN vecinas usando mensajes de multicast y a su vez este tipo de red de transmisión permite dos o más enrutadores en la misma subred y eligen un ID dirección IP. Mientras los enlaces de punto a punto de una subinterfaz WAN están predeterminadas para usar un único tipo de red punto a punto, es decir que solo permite dos enrutadores en la subred, las redes vecinas pueden ser descubierta por medio de mensajes de difusión y no es necesario la selección estricta de un DR.

Interface Type	Uses DR/BDR?	Default Hello Interval	Dynamic Discovery of Neighbors?	More Than Two Routers Allowed in the Subnet?
Broadcast	Yes	10	Yes	Yes
Point-to-point[1]	No	10	Yes	No
Loopback	No	—	—	No
Nonbroadcast[2] (NBMA)	Yes	30	No	Yes
Point-to-multipoint	No	30	Yes	Yes
Point-to-multipoint nonbroadcast	No	30	No	Yes

Figura 4. Tipos de redes OSPF. Tomado de: CCNP Routing and Switching ROUTE 300-101

- **OSPF en enlaces punto a punto**

Es un tipo de red muy simple solo requiere que los dos extremos del enlace se encuentren conectados y las interfaces se configuren con el protocolo OSPF y habilitando la función de adquirir los valores de forma predeterminada.

- **Redes WAN vecinas con subinterfaces punto a punto con Frame Relay**

Para este caso se usa la opción de Frame Relay con el fin de agrupar en una sola subred por medio de configuraciones en la interfaz, las redes LAN vecinas y potenciales.

Con este tipo de configuración en las interfaces de los enrutadores, el protocolo OSPF ignora la comparación del DR y solo es necesario el uso del mensaje de multidifusión para el reconocimiento de redes vecinas.

Figura 5. Características de una red. Tomado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1.1.1.1

Esta sección inicia con una revisión de la terminología OSPF fundamental y la teoría del estado del enlace, posterior a esto una muestra de su configuración y verificación.

8. REDES DE SENSORES INALÁMBRICOS

Para hablar de redes de sensores inalámbricos es necesario tener en cuenta la importancia que estos pueden tener en la sociedad, actualmente por medio de sensores inalámbricos ya es posible detectar muchas situaciones en cualquier problemática que se pueda presentar cotidianamente y así evitar problemas futuros y hasta en algunos casos salvar vidas. Una prueba de ella es la utilización de estos sensores en el internet de las cosas (lot), el cual tiene como fin crear una conexión entre cualquier objeto con una o varias personas que permita por medio de la tecnología mejorar la calidad de vida de los seres humanos minimizando el tiempo que se utiliza para realizar ciertas actividades.

Para esto es necesario la implementación de sensores inalámbricos teniendo cuenta su vida útil tanto del sensor como de su red, su consumo de energía debido a que por medio de este es posible conocer los momentos en donde se ve más afectado generando problemas en el proceso de transmisión de datos.

Los sensores inalámbricos permiten recolectar diferentes datos que pueden ser útiles para gestionar, analizar, identificar cualquier tipo de información relevante para distintas áreas de desarrollo, actualmente es muy común encontrar redes de sensores en diferentes organizaciones, tanto en el sector industrial como en el sector educativo.

Es importante mencionar el modo de funcionamiento que se puede encontrar en la red de sensores, el manejo de sus nodos que son distribuidos por la región de control o monitorización tanto indoor (espacios cerrados) como outdoor (espacios

abiertos), lo cual hace muy factible abarcar cualquier tipo de condición para la recolección de datos.

9. OSPF EN REDES DE SENSORES INALÁMBRICOS

Los resultados experimentales confirman que el protocolo OSPF es útil principalmente durante el monitoreo de datos en tiempo real cuando se requiere la visualización continua de datos casi a cada segundo. [5]

El protocolo OSPF encuentra aplicaciones relacionadas con redes inteligentes en donde es ineluctable el monitoreo de datos en tiempo real. La detección de fallas de las redes y el equilibrio de carga en la red requiere una transferencia de datos rápida, el protocolo OSPF destaca por su convergencia y depende al entorno de redes inalámbricas en el que se esté manejando puede funcionar, ya que si se desea una mejora eficiente de la administración de la energía se podrían implementar protocolo como LBR. Dado que la recopilación de datos es la función principal de las redes de sensores, un protocolo de enrutamiento basado en el nivel de energía está diseñado para recopilar datos en condiciones de suministro de energía limitado [7].

1. Arquitectura

Existen dos arquitecturas: Arquitectura Centralizada en la que los nodos se comunican únicamente con el gateway y a Arquitectura Distribuida en la que los nodos sensores se comunican sólo con otros sensores dentro de su alcance. Otro aspecto es la Computación Distribuida, donde los nodos cooperan y ejecutan algoritmos distribuidos para obtener una ÚNICA medida global que el nodo que se establece como puerta de enlace se encarga de comunicar a la estación base. Los nodos llevan a cabo mediciones, donde el nodo recoge información suministrada por el dispositivo actuador que esté conectado digitalizando la información análoga recopilada, posterior a esto transmitirla hacia redes exteriores por medio de la puerta de enlace o gateway, donde finalmente la información será recibida por un servidor adecuado para guardar los datos y analizarlos si es necesario.

- Estación Base (server.)
- Nodos inalámbricos.

- Puerta de enlace(Gateway)

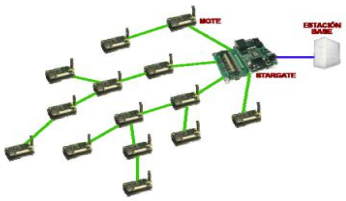


Figura 6. Red inalámbrica de sensores. [10]

2. **Costos de producción**:

Para que sea viable la implementación de una red es necesario tener en cuenta el costo, en el caso de una red inalámbrica se tiene que tener en cuenta cada uno de los nodos a diferencia de las redes cableadas, los costos siempre deben ser menores a los costos del despliegue.

3. **Topología**

Dentro de las topologías más usadas está la tipo malla, fundamental en este tipo de redes ya que todos los nodos están conectados a cada nodo incluido en la red y deben intercambiar información entre cada uno de ellos para cumplir sus rutas y llegar a sus destinos, No se utiliza infraestructura de red: Una red de sensores inalámbricos no depende de un infraestructura para poder operar, debido a que los nodos pueden tomar diferentes papeles; emisores, receptores o enrutadores. Es necesario tener muy en cuenta el nodo que funciona como puerta de enlace, que es el nodo que recolecta la información y por el cual se tiene alcance a otras redes. Esta información generalmente es adquirida por un ordenador conectado a este nodo y es sobre el ordenador que recae la posibilidad de transmitir los datos por tecnologías inalámbricas o cableadas según sea el caso.

CAPÍTULO 3

A continuación, se muestra el desarrollo de los pasos para realizar la guía de análisis de funcionamiento del protocolo OSPF, para ser aplicado en entornos inalámbricos. Iniciando con la identificación de los parámetros en la implementación de OSPF, en las redes de sensores inalámbricos, posterior a esto se analizan sus parámetros en comparación a otros protocolos conocidos, y como estos parámetros convienen en el las redes de sensores, se lleva a cabo el paso a paso de la configuración de una sola área. Por consiguiente teniendo claro el cómo realizar la configuración se procede con verificar el protocolo OSPF, culminando con la instalación del entorno por medio de una máquina virtual de GNS3, se realiza la implementación de una topología común en soluciones basadas en redes de sensores inalámbricos complementándola con la configuración de los dispositivos finales en packet tracert, por medio de este desarrollo se presenta la guía la cual permitirá al lector manejar los conceptos básicos del protocolo, implementarlo y analizar en que redes su funcionamiento será acorde y eficiente.

10. PARÁMETROS FUNDAMENTALES DEL PROTOCOLO DE ENCAMINAMIENTO OSPF PARA ENTORNOS INALÁMBRICOS.

OSPF está definido por varios parámetros los cuales nos permiten identificar en qué tipo de solución podemos usar este protocolo de encaminamiento, y que tan factible será su uso, en negrilla se desea resaltar los parámetros más sobresalientes a tener en cuenta en una red de sensores inalámbrica, es de suma importancia que el estudiante los identifique y genere sus propias conclusiones a partir de su significado en este tipo de redes.

PARÁMETROS	**DEFINICIÓN**
Número de nodos.	A diferencia de otros protocolos OSPF puede manejar N nodos en una topología, por ejemplo RIP solo puede manejar 16. Las redes de sensores normalmente esta constituidas por cantidades de nodos considerables, por lo que no se aconseja utilizar un protocolo como RIP en los sensores y/o nodos.
Información que comparte.	OSPF únicamente comparte el enlace, NO comparte su base de datos.
Cada cuánto envía información el Nodo	OSPF envía paquetes de saludo en cada 10 segundos.
Algoritmo que usa.	OSPF utiliza un algoritmo basado en el estado del enlace en cada uno de los nodos, este algoritmo es convenientes en las redes de sensores inalámbricos
Detección de errores	OSPF puede detectar errores.
Métrica	Costo, Es importante tener en cuenta que el costo es lo que ospf tiene en cuenta a la hora de elegir la mejor ruta, entre mas ancho de banda se tenga en una interfaz, menor será su costo, si si ancho de banda es menor su costo será más elevado, OSPF elegirá la

	interfaz con menos costo.
Sumarización	Manual
Latencia	La suma de retardos temporales en OSPF es poca en comparación a RIP.
Distancia administrativa	110
Velocidad	El rendimiento es superior desde que la latencia sea menor. Rendimiento = paquete tamaño / latencia.

Tabla 1. Parámetros OSPF

11. CONVERGENCIA DE OSPF EN REDES DE SENSORES INALÁMBRICOS

La convergencia del protocolo nos entrega facilidad a la hora de aumentar el área de cobertura añadiendo nuevos nodos, ya no es necesario cambiar infraestructuras como en el caso de las redes cableadas, además que al hablar de redes de sensores es importante tener en cuenta que las soluciones estarán ubicadas en lugares difíciles de acceder y que acomplejan el desarrollo de una infraestructura para redes alámbricas, la robustez que presenta ante fallos al disponer de rutas alternativas y la capacidad de transmisión que permiten aplicaciones a los usuarios en tiempo real de voz, video y datos son parámetros fundamentales que permiten a OSPF trabajar en entornos inalámbricos.

12. RENDIMIENTO DE OSPF EN COMPARACIÓN A EIGRP Y RIP

El rendimiento de OSPF en este tipo de redes en constante cambio como lo son las redes de sensores, se mide de acuerdo a la velocidad de la red, entre más rápido se genere la transferencia de datos entre los nodos, a continuación analizaremos el estudio generado por los autores M Athira; Lekha Abrahami; R. G. Sangeetha, quienes para la Conferencia internacional 2017 sobre tecnologías electrónicas de Nextgen (ICNETS2) donde se comparan los 3 protocolo, a continuación evidenciamos el retardo de extremo a extremo para una topología diseñada por los autores con las mismas características y nodos,

SL NO:	TYPE OF PROTOCOL	AVERAGE END TO END DELAY TIME(ms)
1	RIP	50.526
2	OSPF	42.189
3	EIGRP	46.82

Tabla 2. Retardo extremo a extremo, tomado de M Athira; Lekha Abrahami; R. G. Sangeetha(23-25 March 2017). Study on network performance of interior gateway protocols — RIP, EIGRP and OSPF

OSPF maneja un retardo menor a RIP y EIGRP, por 4 milisegundos es menor que EIGRP protocolo propiedad de Cisco quien maneja un rendimiento bastante interesante, de acuerdo, en las redes de sensores inalámbricas o en redes móviles donde actualmente se está manejando soluciones M2M.

En cuanto a la velocidad medida en bits por segundo, podemos evidenciar un rendimiento considerablemente mayor de OSPF sobre los demás protocolos con una velocidad de 622.912 kbps

TYPE OF PROTOCOL	THROUGHPUT(kbps)
RIP	424.079
OSPF	622.912
EIGRP	517.959

Tabla 3. Velocidad, tomado de M Athira; Lekha Abrahami; R. G. Sangeetha(23-25 March 2017). Study on network performance of interior gateway protocols — RIP, EIGRP and OSPF

La convergencia como se identificó en apartados anteriores es el tiempo que dura el router en adaptarse a un cambio en la red, en el estudio referencia llevado a cabo por M Athira; Lekha Abrahami; R. G. Sangeetha nos expone el resultado de análisis donde se compara dicho tiempo entre los 3 protocolos, realizando un bloqueo a la interfaz de los router 5 veces, a continuación se logra observar en la tabla y los resultados obtenidos para OSPF, es de suma importancia comprender que el autor utilizó un envío de Paquetes con tamaño de datagrama 100 y el tiempo de espera 2s se envía desde el origen al destino de destino con recuento 500, El número de paquetes perdidos es multiplicado con tiempo de espera para obtener el tiempo de convergencia y Este proceso continúa cinco veces y se toma el promedio.

.

	Packets received	Packet lost	Convergence time(ms)	Average convergence time(ms)
1	495	5	10	9.2
2	495	5	10	
3	495	5	10	
4	496	4	8	
5	496	4	8	

Tabla 4. Tiempo de convergencia, tomado de M Athira; Lekha Abrahami; R. G. Sangeetha(23-25 March 2017). Study on network performance of interior gateway protocols — RIP, EIGRP and OSPF.

13. VERIFICACIÓN DEL PROTOCOLO Y SOLUCIÓN DE PROBLEMAS.

13.1 CONFIGURACIÓN y VERIFICACIÓN DE OSPF PARA UNA SOLA ÁREA

A continuación, se lleva a cabo la identificación y análisis de la configuración estándar del protocolo ospf para este tipo de redes, nos apoyaremos de los comandos y sus características relevantes para llevar a cabo y verificar un correcto funcionamiento del protocolo OSPF, de lo cual dependerá la funcionalidad de la red para la solución que se esté llevando a cabo.

- De esta forma se puede iniciar el protocolo, dándole un número de identificación al proceso el cual lo mejor es configurarlo bien, para tener en cuenta el proceso ospf de cada router.

Router(config)#router ospf [process-id]

Router(config-router)#network [address] [wildcard-mask] area [area-id]

uno de los errores más comunes es definir las redes con una máscara normal, para este protocolo se definen las redes adyacentes con la wildcard.

- Para modificar el ancho de banda sobre la interfaz se utiliza el siguiente comando:

Router(config)#interface serial 0/0
Router(config-if)#bandwidth 64

Estando dentro de la interfaz se puede llevar a cabo el cambio del coste, como evidenciamos a continuación.

Router(config-if)#ip ospf cost [number]

Dentro del análisis de la configuración del protocolo se encontraron algunos comandos importantes a tener en cuenta a la hora de verificar el funcionamiento del protocolo, punto de partida para todo diagnóstico, entender en qué entorno y cómo está trabajando el protocolo en cuanto a las metas trazadas. El rendimiento del protocolo dependerá del uso que se le esté dando, y el escenario donde se esté llevando a cabo.

- Imprime la tabla de enrutamiento:

show ip route

- Imprime los parámetros del protocolo

show ip protocols

- Imprime la información de los vecinos OSPF

show ip ospf neighbors

El enrutador puede verificar qué interfaces están participando en el proceso OSPF con el comando **show ip ospf interface brief**, Mostrará qué interfaces participan en el proceso, en qué área están las interfaces, también puede verificar la dirección IP y las máscaras de las interfaces junto con el número de relaciones vecinas completas que se han formado fuera de la interfaz frente al número total de vecinos fuera de la interfaz decidimos iniciar con estas verificaciones porque nos permite revisar los parámetros fundamentales para que exista comunicación.

```
R5#sh ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Fa1/0        2     0               10.20.0.1/30       1     BDR   1/1
Fa0/0        2     0               10.10.0.2/30       1     DR    1/1
R5#
```

Figura 8 Verificación de interfaces OSPF, Autoría propia, realizado en GNS3

A continuación hacemos uso de debug ip ospf hello para identificar temporizadores no coincidentes, además se evidencian los mensajes Hello recibidos, fijémonos en la siguiente imagen.

```
R5#debug ip ospf hello
OSPF hello events debugging is on
R5#
*Mar  1 00:00:49.547: OSPF: Rcv hello from 44.44.44.44 area 0 from FastEthernet1
/0 10.20.0.2
*Mar  1 00:00:49.547: OSPF: End of hello processing
*Mar  1 00:00:50.307: OSPF: Rcv hello from 33.33.33.33 area 0 from FastEthernet0
/0 10.10.0.1
*Mar  1 00:00:50.307: OSPF: End of hello processing
*Mar  1 00:00:50.315: OSPF: Send hello to 224.0.0.5 area 0 on FastEthernet0/0 fr
om 10.10.0.2
*Mar  1 00:00:50.319: OSPF: Send hello to 224.0.0.5 area 0 on FastEthernet1/0 fr
om 10.20.0.1
R5#
*Mar  1 00:00:50.407: %OSPF-5-ADJCHG: Process 2, Nbr 33.33.33.33 on FastEthernet
0/0 from LOADING to FULL, Loading Done
*Mar  1 00:00:50.415: %OSPF-5-ADJCHG: Process 2, Nbr 44.44.44.44 on FastEthernet
1/0 from LOADING to FULL, Loading Done
R5#
*Mar  1 00:00:59.539: OSPF: Rcv hello from 44.44.44.44 area 0 from FastEthernet1/0 10.20.0.2
*Mar  1 00:00:59.539: OSPF: End of hello processing
*Mar  1 00:01:00.303: OSPF: Rcv hello from 33.33.33.33 area 0 from FastEthernet0/0 10.10.0.1
*Mar  1 00:01:00.303: OSPF: End of hello processing
*Mar  1 00:01:00.315: OSPF: Send hello to 224.0.0.5 area 0 on FastEthernet0/0 from 10.10.0.2
*Mar  1 00:01:00.319: OSPF: Send hello to 224.0.0.5 area 0 on FastEthernet1/0 from 10.20.0.1
R5#
*Mar  1 00:01:09.547: OSPF: Rcv hello from 44.44.44.44 area 0 from FastEthernet1/0 10.20.0.2
```

Figura 9 Identificación de mensajes HELLO, Autoría propia, realizado en GNS3

OSPF utiliza el concepto de áreas para convertirlo en un protocolo de enrutamiento dinámico extremadamente escalable. Un enrutador OSPF genera una adyacencia, si sus interfaces vecinas deben estar en la misma área. Entonces si se desea saber en qué área está la interfaz debemos ingresar el comando **show ip ospf interface [Tipo de interfaz] [número de interfaz]** Al determinar si las ID de área coinciden, use el método de detectar la diferencia entre las salidas en ambos enrutadores.

```
R5#sh ip ospf interface f0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 10.10.0.2/30, Area 0
  Process ID 2, Router ID 55.55.55.55, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 55.55.55.55, Interface address 10.10.0.2
  Backup Designated router (ID) 33.33.33.33, Interface address 10.10.0.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 3
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 33.33.33.33  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
R5#
```

Figura 10 Verificación de ID para las interfaces OSPF, Autoría propia, realizado en GNS3

14. INSTALACION Y CONFIGURACION GNS3 EN VMWARE PRO

Paso 1: Ingrese a gns3.com e ir a “download” y “Free download”

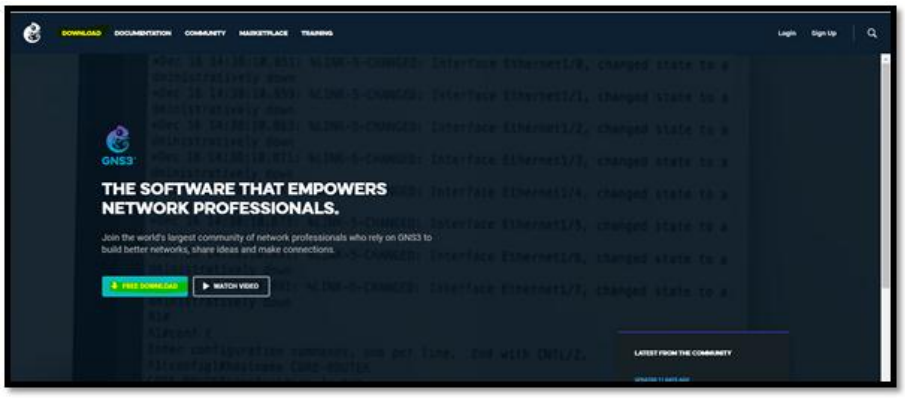


Figura 11. Pagina de GNS3, Recorte autoría propia.

Paso 2: Se deberá vincular alguna cuenta, y nos aseguraremos a descargar el GNS3 VM donde nos re-direccionará a otra página.

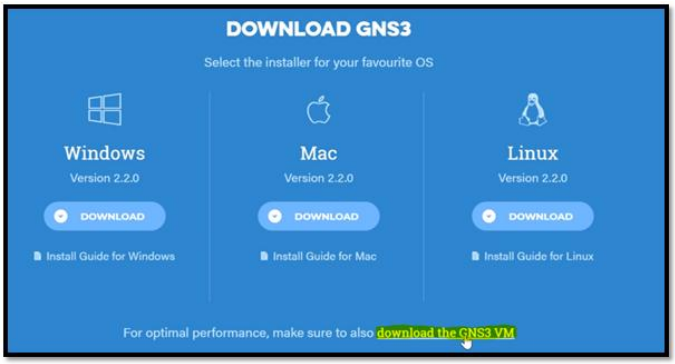


Figura 12, Descarga GNS3, Recorte autoría propia.

Paso 3: Elegiremos el VMWARE WORSTATION AND FUSION, asegurarnos que las versiones del VM y el GUI se han las mismas para evitar errores en la ejecución.

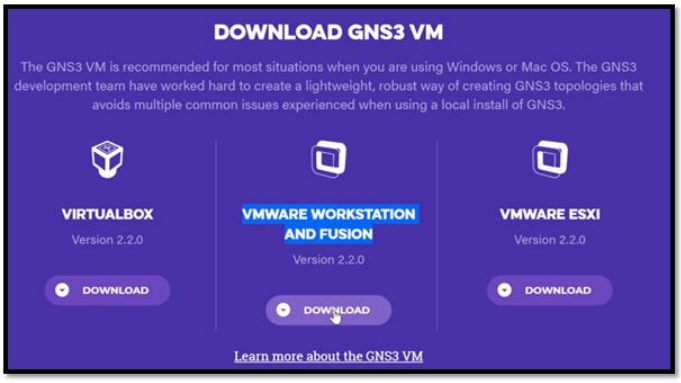


Figura 13 Descarga GNS3 VM, Recorte autoría propia.

Paso 4: Después extraer el documento descargado veremos un archivo .ova; no será reconocible porque nos hará falta descargar el VMWARE.

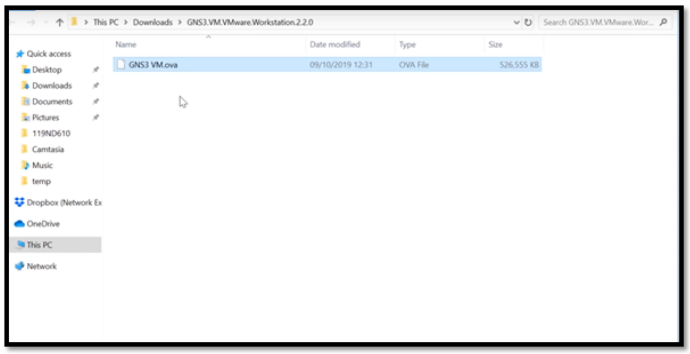


Figura 14 Imagen.ova GNS3 VM, Recorte autoría propia.

Paso 5: Para descargar VMWARE, iremos a la página vmware.com – dowloads y seleccionaremos Workstation Pro.

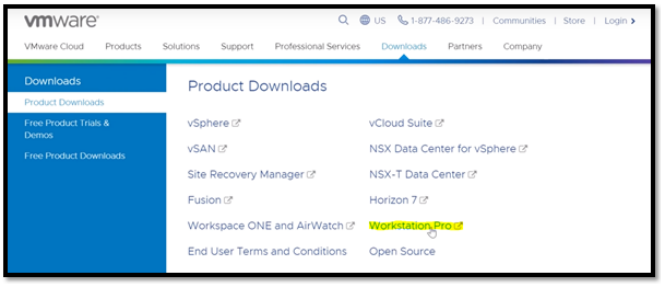


Figura 15. Descarga virtualizador workstation PRO, Recorte autoría propia.

Paso 6: Tendremos que elegir la descarga según nuestro sistema operativo (para este caso Windows).

Figura 16. Vmware Pro para windows, Recorte autoría propia.

Paso 7: Luego de oprimir “download now” tendremos que vincular una cuenta o crearla de ser necesario; posteriormente aceptar el acuerdo de licencia e iniciará la descarga posteriormente.

Figura 17. Licencia Vmware, Recorte autoría propia.

Paso 8: Luego de hacer doble clic en archivo descargado (VMware-workstation-full) aparecerá la ventana para iniciar la instalación.

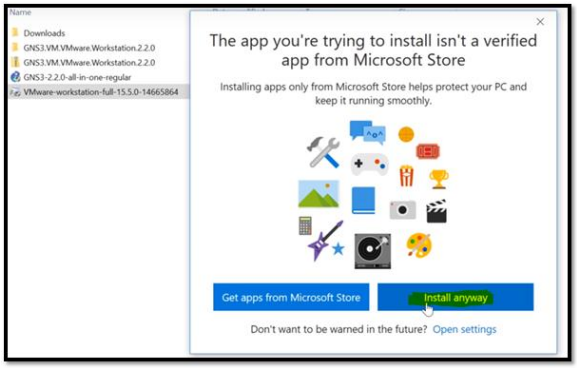


Figura 18. Ventana de inicio de instalación, Recorte autoría propia.

Paso 9: Luego de realizar la instalación requerirá un reinicio del sistema; ejecutamos nuevamente el archivo “VMware-workstation-full”.

Figura 19. Ventana emergente VMware 15.5, Recorte autoría propia.

Paso 10: Iniciará el asistente de configuración donde oprimimos “Next”

Figura 20 Inicio instalacion versión 15.5, Recorte autoría propia.

Paso 11: Aceptaremos el acuerdo de licencia.

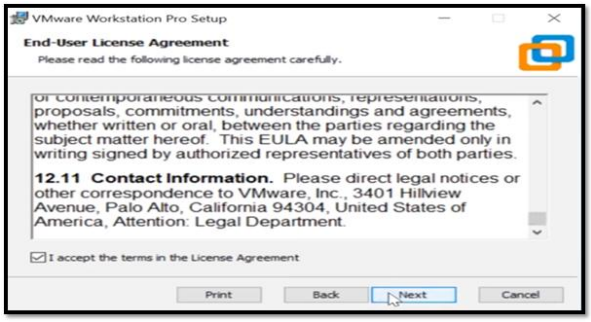


Figura 21 Acuerdo de licencia, Recorte autoría propia.

Paso 12: Dejaremos la dirección predeterminada (puede ser modificada).

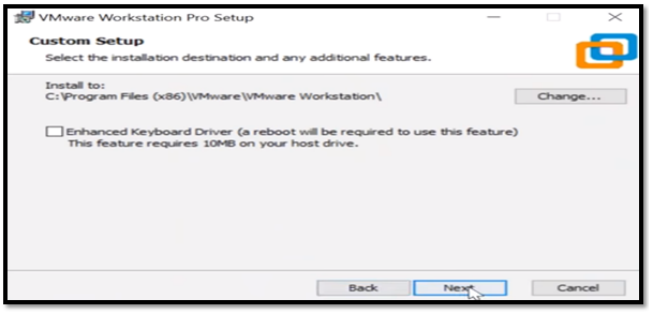


Figura 22 Dirección predeterminada, Recorte autoría propia.

Paso 13: Desmarcamos las casillas para no buscar más actualizaciones ni unirnos al programa de experiencia del cliente.

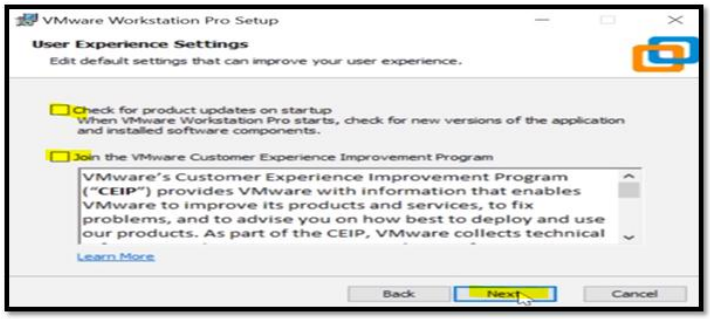


Figura 23. Ajustes de experiencia, Recorte autoría propia.

Paso 14: Marcaremos "Instalar" y también podremos ver cómo adiciona nuevos adaptadores de red.

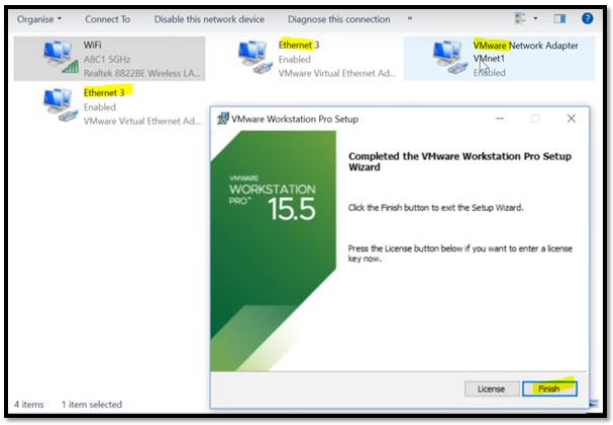


Figura 24 Finalización de la instalación, Recorte autoría propia.

Paso 15: Marcar la casilla de "30 días gratis"

Figura 25. Acuerdo de 30 días gratis, Recorte autoría propia.

Paso 16: Marcaremos si, en la siguiente ventana, y “Finish” para culminar la instalación y posteriormente aparecerá la ventana del VMware Workstation.

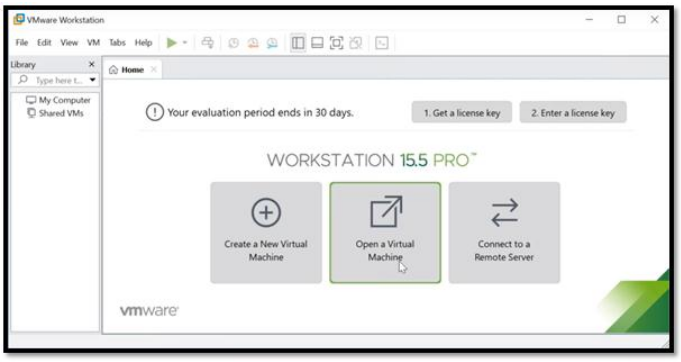


Figura 26. Opción abrir máquina virtual, Recorte autoría propia.

Paso 17: Se procede a abrir el GNS3 VM según la ubicación en la cual lo hayamos descargado.

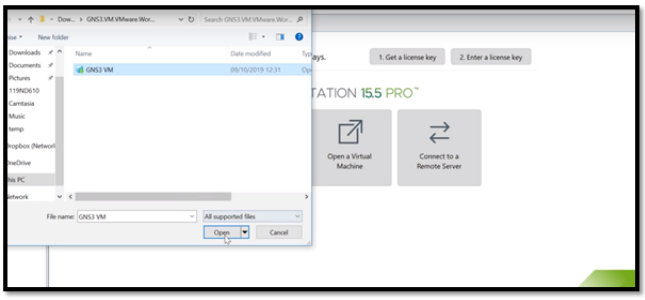


Figura 27. Elección de la máquina virtual antes descargada, Recorte autoría propia.

Paso 18: Se importará y observaremos la siguiente ventana.

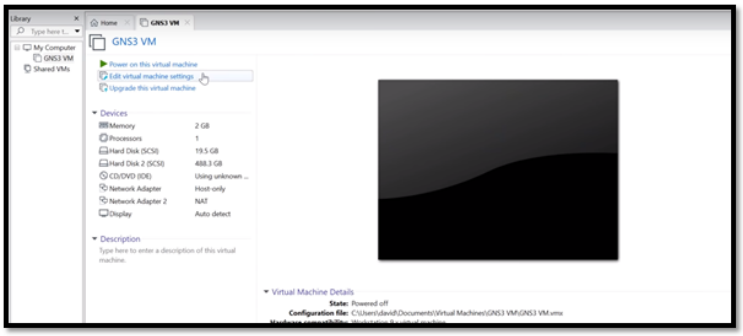


Figura 28. Máquina virtual, Recorte autoría propia.

Paso 19: Podremos cerrar y abrir el GUI GNS3 exitosamente.

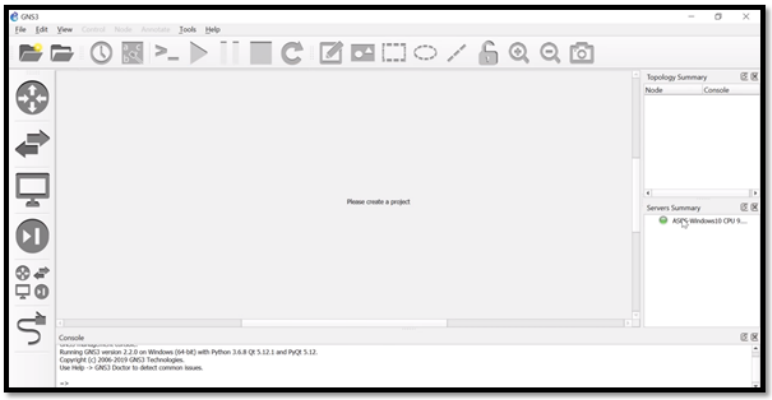


Figura 29, ventana de inicio GNS3, Recorte autoría propia.

Paso 20: Solo veremos un servidor y para ello iremos a Edit – Preferences abriremos el GNS3 VM y habilitaremos la casilla “Enable the GNS3 VM”; en esta ventana también podremos configurar la cantidad de RAM y CPU utilizable para su funcionamiento.

Figura 30 Habilitación GNS3 VM, Recorte autoría propia.

Paso 21: Se adicionará en Servers el VM GNS3, el cual ejecutaremos y empezará su procesamiento.

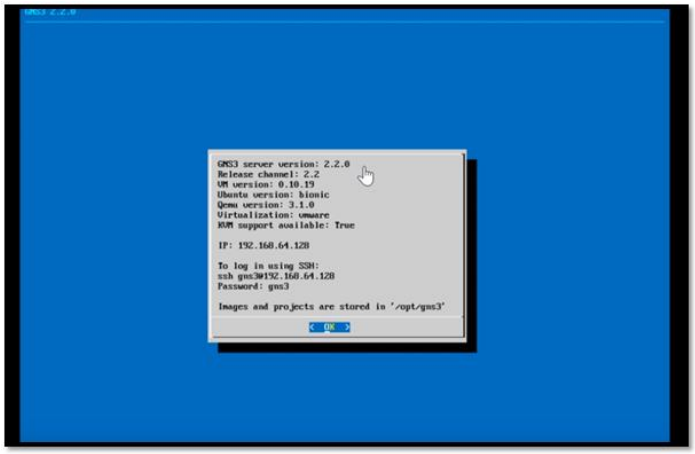


Figura 31. Ventana confirmación funcionamiento de GNS3 VM, Recorte autoría propia.

Paso 22: Apagaremos el pc y mantendremos oprimido el botón F2, iremos a la pestaña “Advanced” y nos aseguraremos que la “virtualización de Intel” este habilitado; para poder hacer la Virtualización anidada en VMware Workstation (guardamos y salimos).

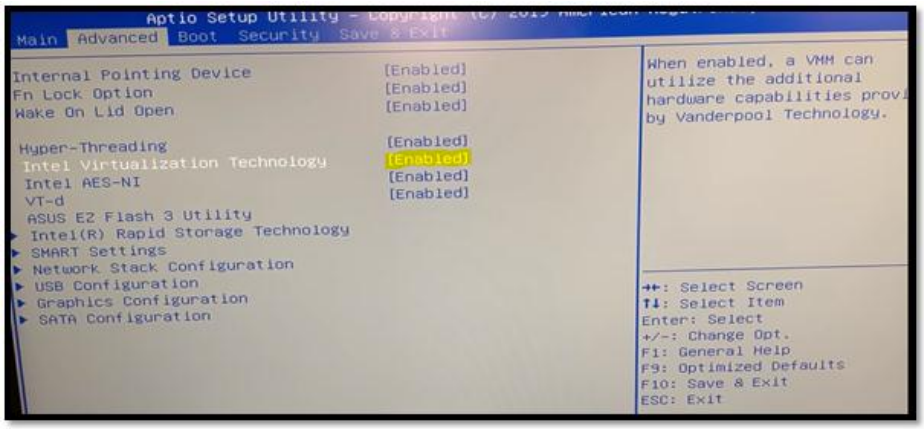


Figura 32. Virtualización habilitada en la BIOS.

Paso 23: Ejecutaremos GUI GNS3 y nos aseguraremos que el servidor del GNS3 también esté en verde y así confirmar que todo funciona correctamente (de no ser así reiniciar el VM, el GUI y reinicia el pc).

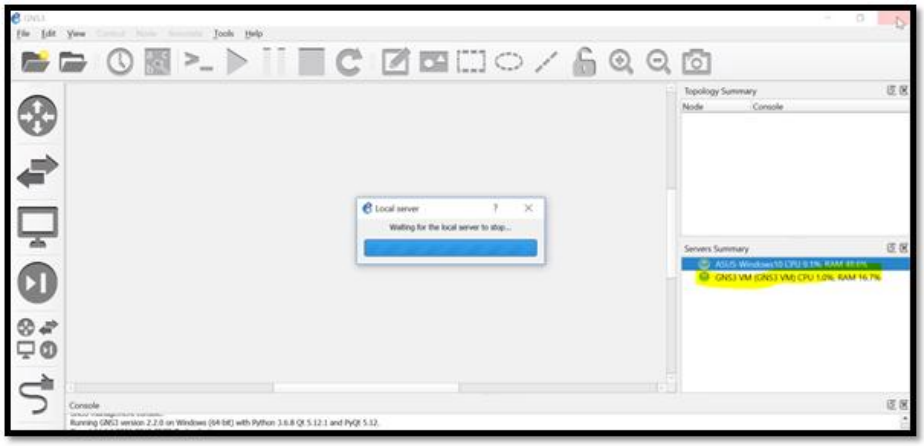


Figura 33. Servidor GNS3 , Recorte autoría propia.

Paso 24: Para asegurarnos que el VT-x está habilitado (que es necesario para el correcto funcionamiento) debemos abrir el VMware Workstation Pro – clic derecho en GNS3 – Configuración – Procesador y observaremos la casilla del VT-x.

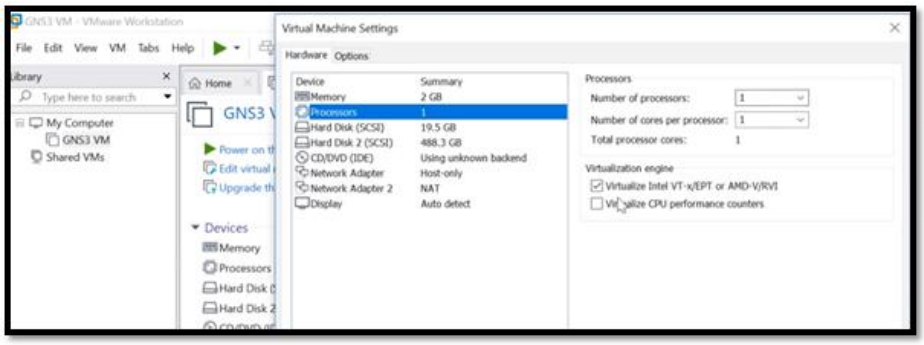


Figura 34 Configuración Máquina virtual, Recorte autoría propia.

Terminados los anteriores pasos a continuación se explica cómo descargar imágenes Cisco IOS (Cisco IOSv, Cisco IOSv capa 2) para configurar el protocolo OSPF en una red de malla.

Paso 1: Crearemos un proyecto nuevo en el GUI GNS3, y nos dirigiremos en el navegador a virl.cisco.com y nos redireccionaremos a “Get VIRL”.

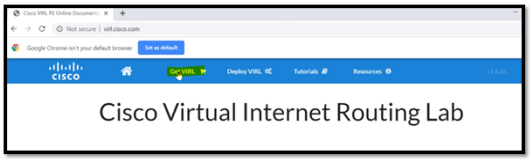
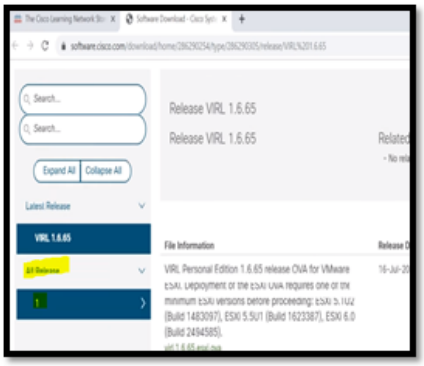
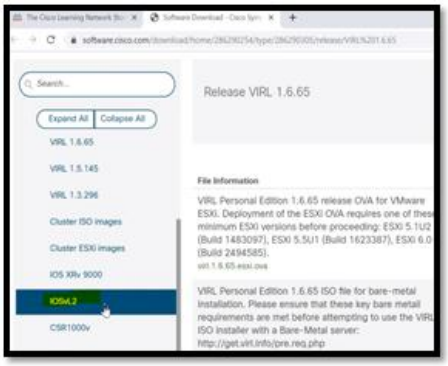


Figura 35 Imágenes IOS, Recorte autoría propia.

Paso 2: Vinculamos la cuenta, y daremos clic en “todos los lanzamientos”-“1”-y luego elegiremos las imágenes que queremos descargar (para este ejemplo utilizaremos IOS capa 2.





Paso 3: Descargamos y aceptaremos el acuerdo de licencia e iniciará la descarga de un archivo .qcow.

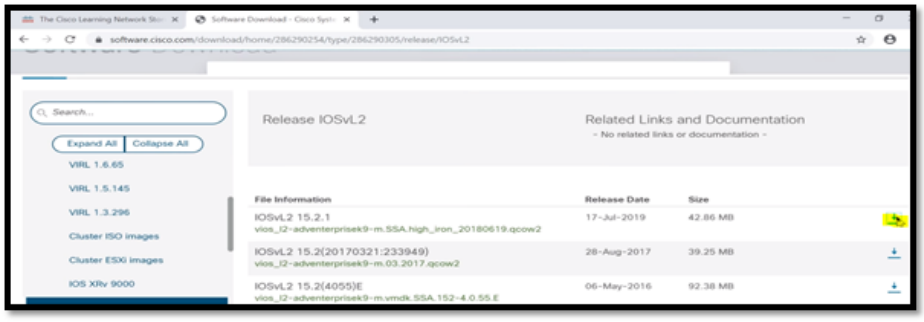


Figura 36. archivo .qcow, Recorte autoría propia.

Paso 4: Una vez descargados iniciaremos el GNS3 e intentaremos importarlos; iremos a los enrutadores y luego nueva plantilla.

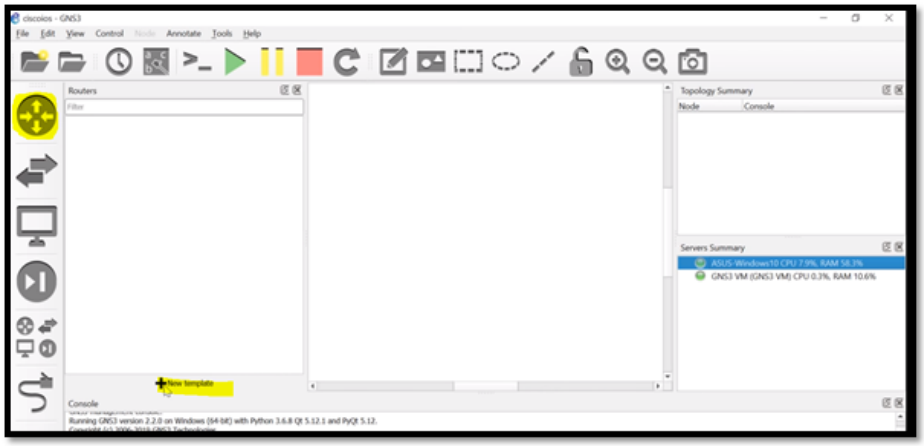


Figura 37. Importación enrutadores, Recorte autoría propia.

Paso 5: Instalaremos según lo recomendado.

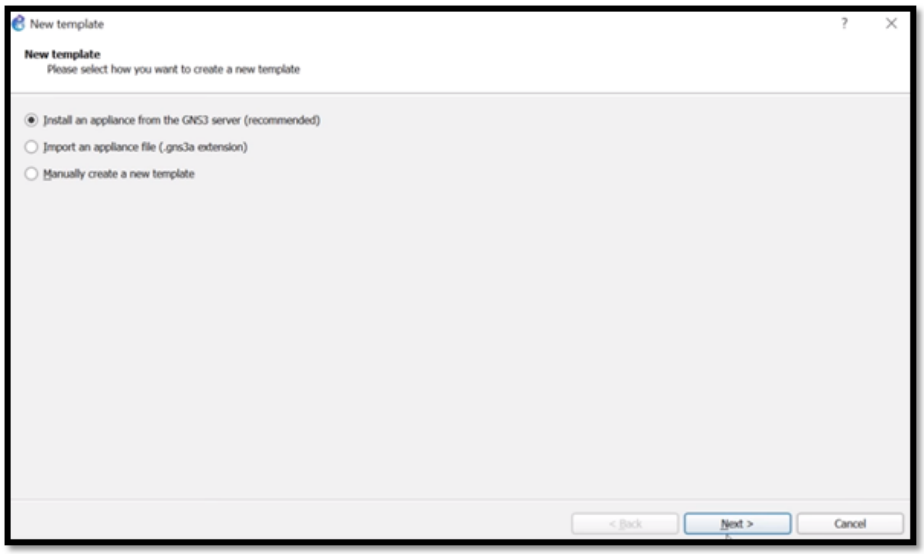


Figura 38 Instalación imagenes, Recorte autoría propia.

Paso 6: Seleccionamos Routers y elegiremos Cisco IOSv donde el emulador será Qemu que explica que lo queremos ejecutar en la VM GNS3.

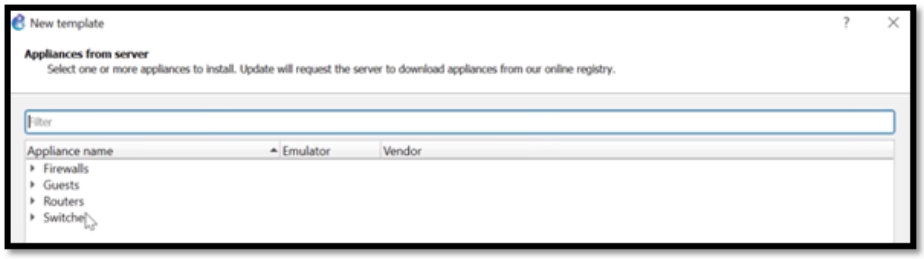


Figura 39. Aplicaciones, Recorte autoría propia.

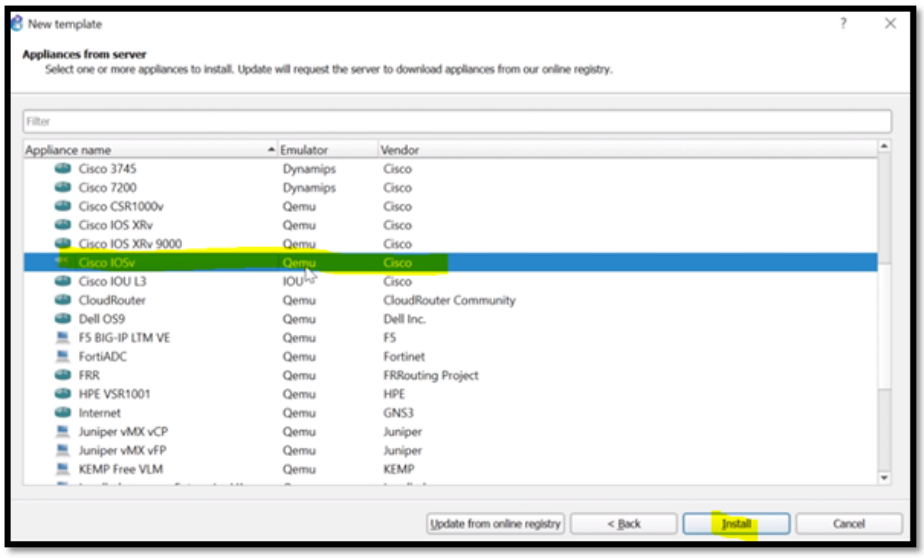


Figura 40, diferentes aplicaciones de varios fabricantes, Recorte autoría propia.

Paso 7: Daremos en recomendado por no tener un servidor remoto configurado.

Figura 41. Instalacion aplicación GNS3 VM, Recorte autoría propia.

Paso 8: Dejaremos la configuración del Qemu con los valores predeterminados.

Figura 42 Qemu, Recorte autoría propia.

Paso 9: El GNS3 escanea el directorio local y busca los archivos necesarios, que en este caso no posee la configuración de inicio así que al descargar, podremos seguir.

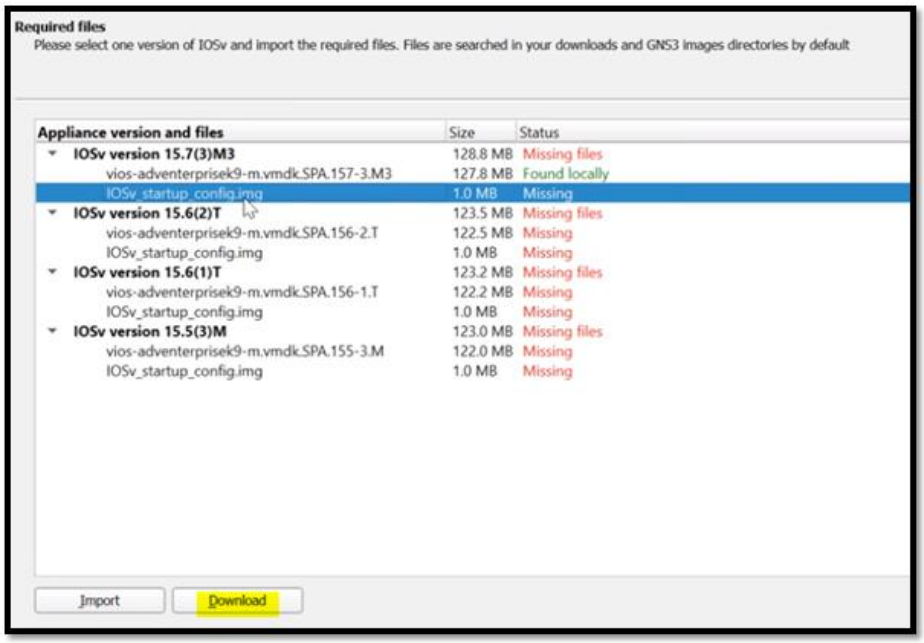


Figura 43 Proceso de descarga, Recorte autoría propia.

Paso 10: La imagen cargará, y también menciona que no hay efecto de contraseña y habilitar contraseña y podremos finalizar.

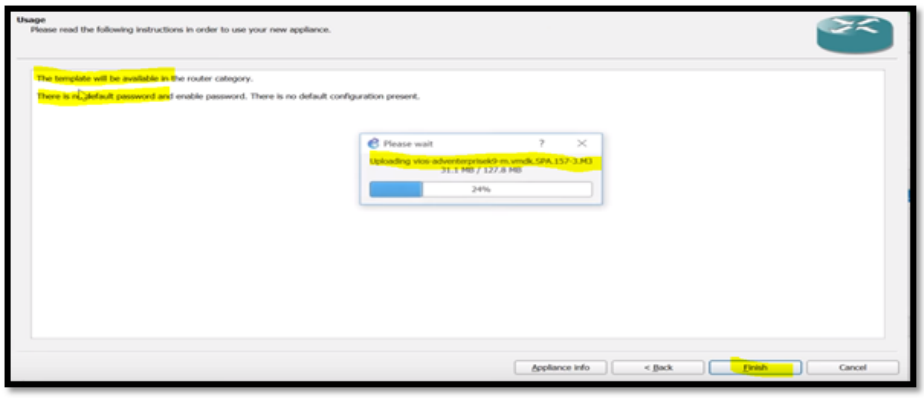


Figura 44. Imagen cargada, Recorte autoría propia.

Paso 11: Veremos que se ha instalado con éxito si observamos el símbolo del IOSV en la zona de filtros.

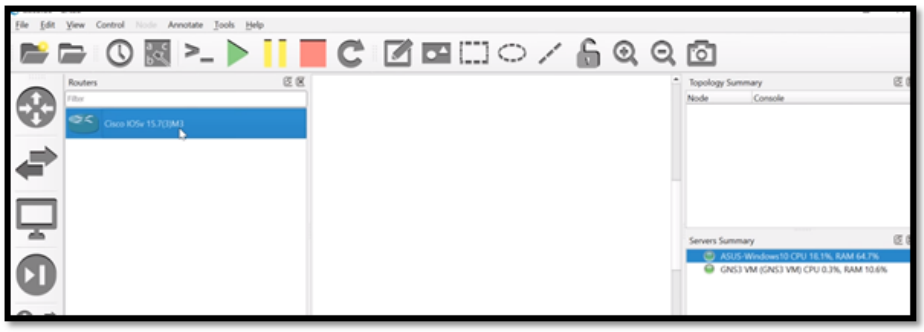


Figura 45 router cisco, Recorte autoría propia.

Paso 12: Iremos a interruptores y adicionamos una nueva plantilla.

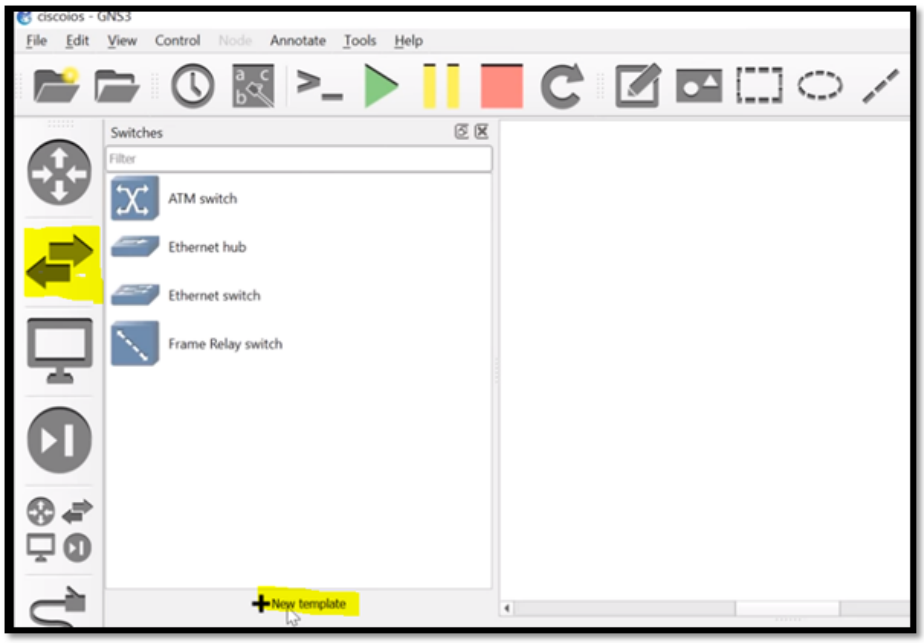


Figura 46 Nueva plantilla, Recorte autoría propia.

Paso 13: Instalaremos un nuevo dispositivo del servidor GNS3.

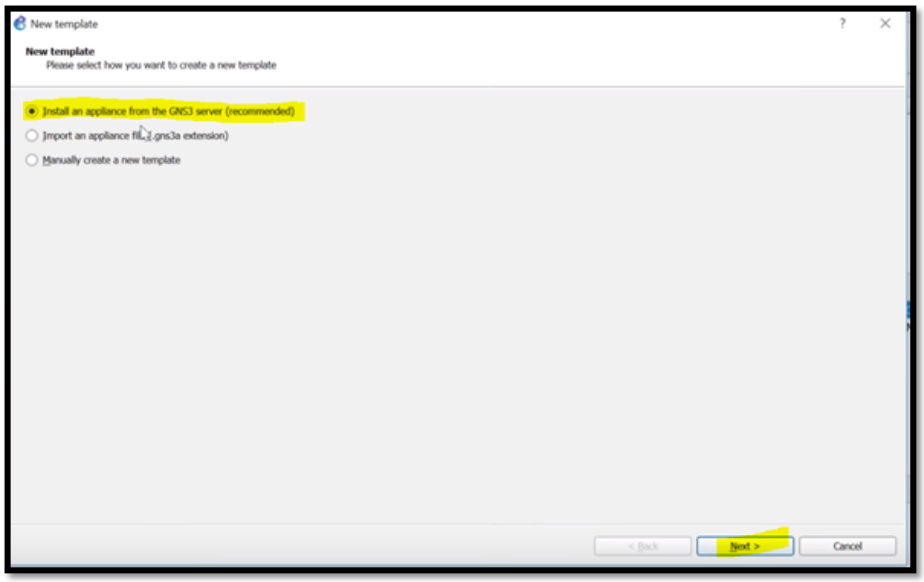


Figura 47 Proceso de instalacion de un nuevo dispositivo, Recorte autoría propia.

Paso 14: Clic en interruptores y elegiremos IOS de capa 2.

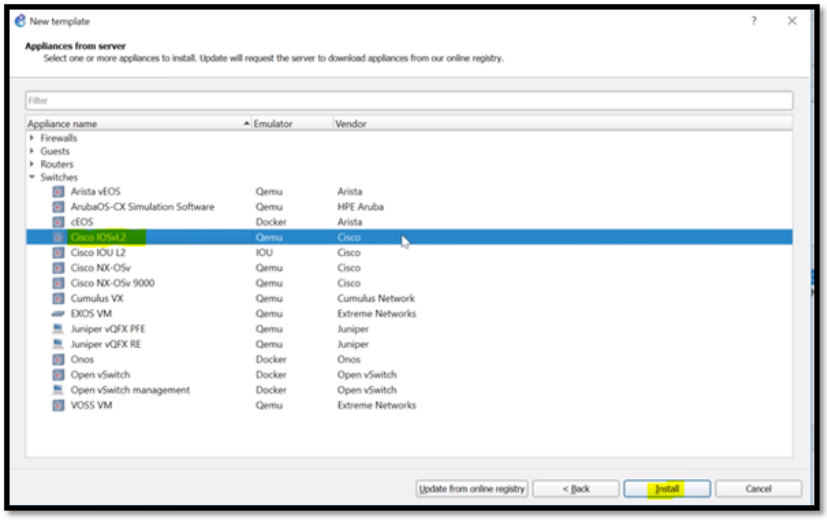


Figura 48. Selección equipo capa 2, Recorte autoría propia.

Paso 15: Aceptaremos de igual forma que el paso 7 y 8 sin modificaciones y posteriormente veremos que en este caso tendremos el dispositivo listo para instalar sin ningun archivo faltante así que proseguimos.

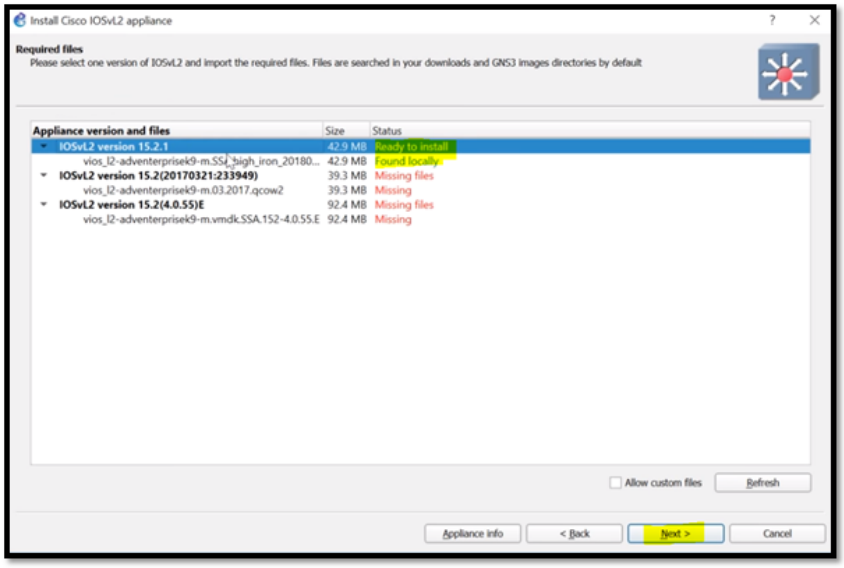


Figura 49. Log imágen equipo capa 2, Recorte autoría propia.

Paso 16: La imagen cargará de igual forma que en el paso 10 así que seguiremos con normalidad y podremos finalizar la instalación del dispositivo.

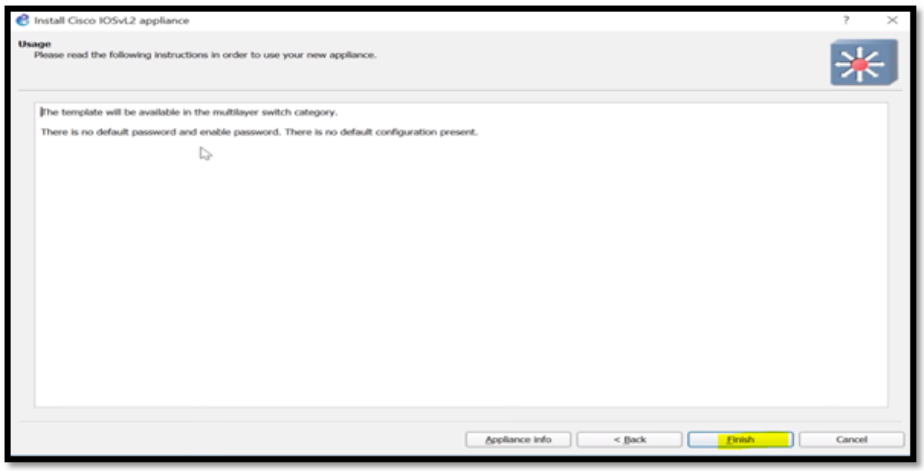


Figura 50. Ventana de finalización, Recorte autoría propia.

Paso 17: Observaremos el interruptor nuevo y lo adicionamos al espacio de trabajo

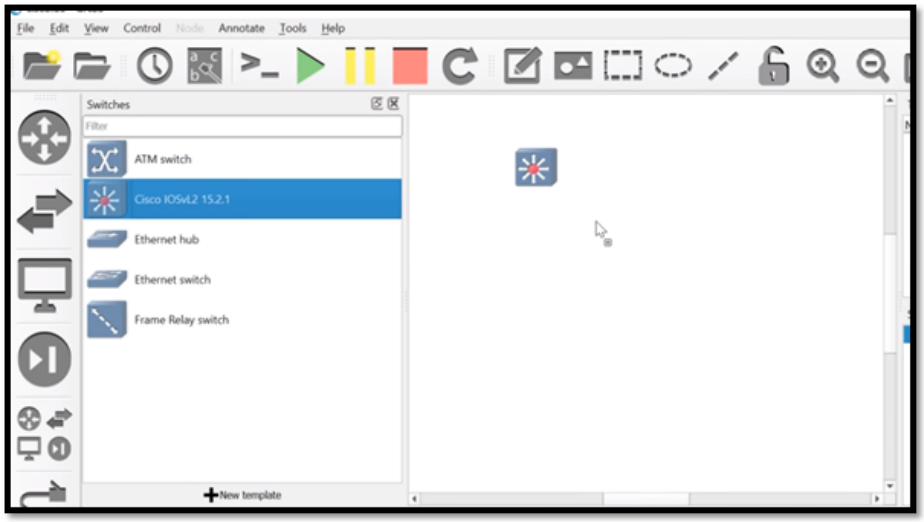


Figura 51. se evidencia el equipo capa 2 listo para usar, Recorte autoría propia.

Paso 18: De igual forma con el enrutador creado anteriormente (para este ejemplo agregaremos 2 enrutadores).

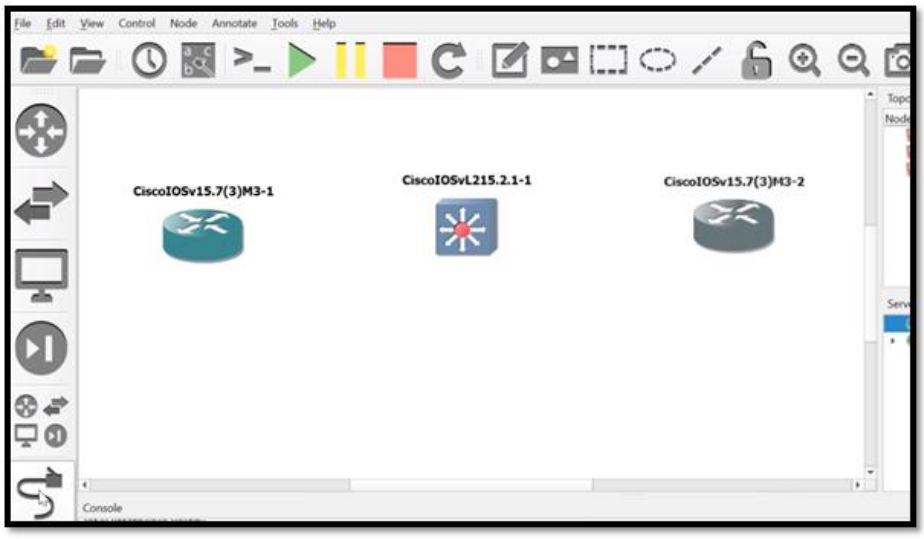


Figura 52. integración equipos capa 2 y 3, Recorte autoría propia.

Paso 19: Clic en el conmutador, daremos clic sobre el enrutador y elegiremos la opción Gi0/0.

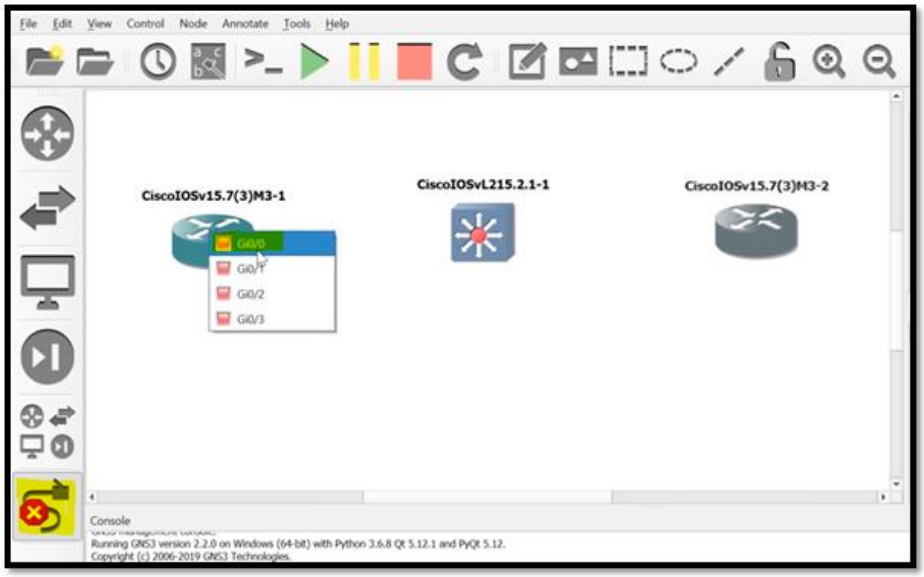


Figura 52. Conexión equipos capa 2 y 3, Recorte autoría propia.

Paso 20: Arrastramos hasta el interruptor y elegiremos nuevamente la opción Gi0/0

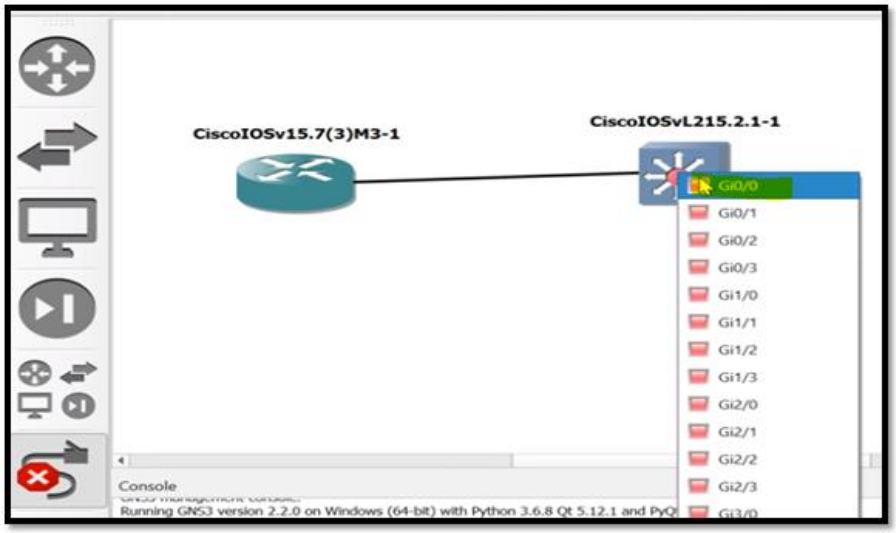


Figura 53. Conexión equipos capa 2 y 3, Recorte autoría propia.

Paso 21: Unificamos de igual forma el interruptor con el segundo enrutador pero eligiendo Gi0/1 de inicio y sobre el enrutador Gi0/0.

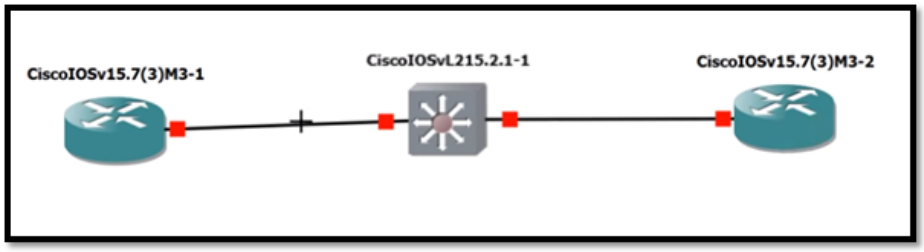


Figura 54. Conexión equipos capa 2 y 3, Recorte autoría propia.

Paso 22: Pondremos Play a nuestra plantilla de trabajo.

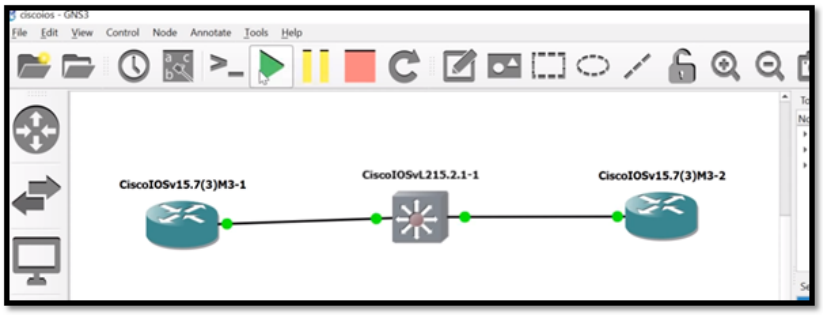


Figura 55. Enlaces disponibles entre los equipos capa 2 y 3, Recorte autoría propia.

Posterior a estos pasos, ya que hemos verificado en el paso 22 que los equipos encienden sin problema, procederemos con la simulación de una red malla de nodos, donde se configure y analice el protocolo OSPF en una red basada en redes de sensores inalámbricos, se seleccionó una topología en malla la cual se compone de varios nodos conectados entre sí y cada uno va asignado a una frontera o sitio de telemedida referido, todos los puertos de los nodos para este caso donde analizaremos el funcionamiento de OSPF son FastEthernet, a continuación en la siguiente imagen podemos observar cómo fue diseñada.

DISEÑO:

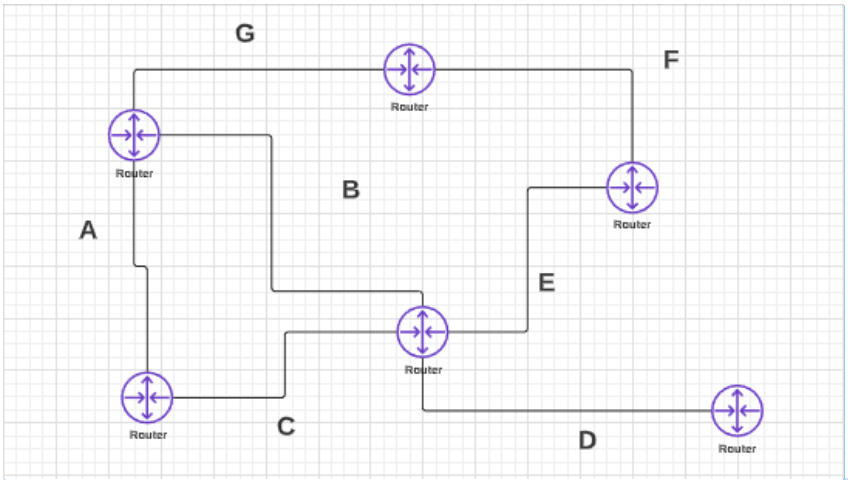


Figura 56. Diseño y direccionamiento, Topología propuesta, Realizado en Lucid chart.

Comentado [JA6]: Esta figura quedó sin numeración

A: 10.50.0.0 /30

B: 10.70.0.0 /30

C: 10.40.0.0 /30

D: 10.30.0.0 /30

E: 10.20.0.0 /30

F: 10.10.0.0 /30

G: 10.60.0.0 /30

TOPOLOGÍA EN CAMPO (GNS3)

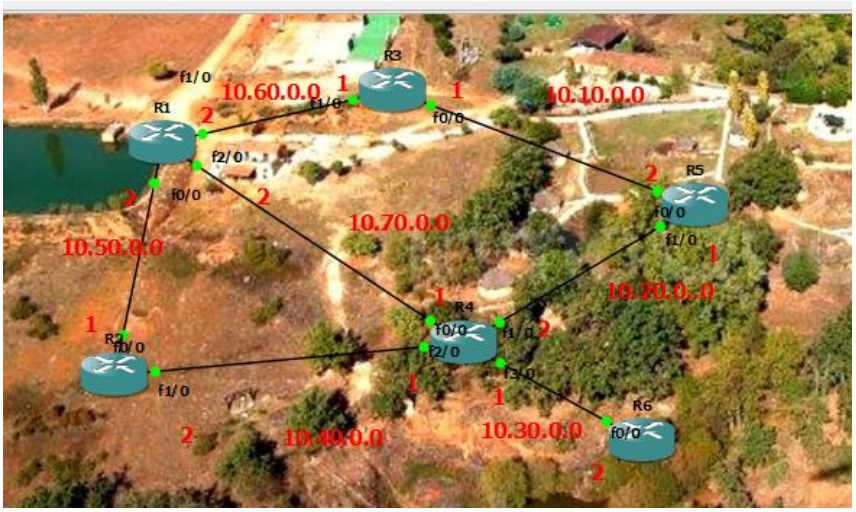


Figura 57. Topología Redes de sensores , Recorte autoría propia.

Posterior al montaje de todos los nodos procedemos con el direccionamiento para la red, para ello entramos a cada una de las interfaces de los nodos y asignamos las direcciones ip correspondientes, a continuación, configuraremos el nodo R3 el cual corresponde a un grupo de cultivos donde los sensores conectados al nodo miden temperatura y ph.

15. PROPUESTA DE TOPOLOGIA PARA ANALISIS Y SOLUCION DE PROBLEMAS DEL PROTOCOLO OSPF.

15.1 CONFIGURACIÓN Y DIRECCIONAMIENTO R3

Ingresamos a la consola del nodo haciendo doble click sobre él, se utilizó secureCRT como terminal en vez de putty, ahora dentro del router ingresamos a su configuración con el comando abreviado **Conf t,** direccionamos debidamente de acuerdo al nodo en el que estemos, es importante fijarse en el diseño de la figura anterior, para realizar esto en cada uno de los nodos, únicamente daremos espacio para dos direcciones puesto que configuramos la dirección con máscara /30, finalizando dejamos encendida la interfaz con el comando **no shutdown.**

R4:

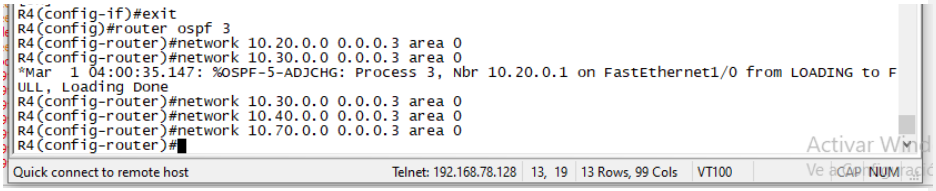


Figura 58. Configuración Router 4 , autoría propia en GNS3.

R6:

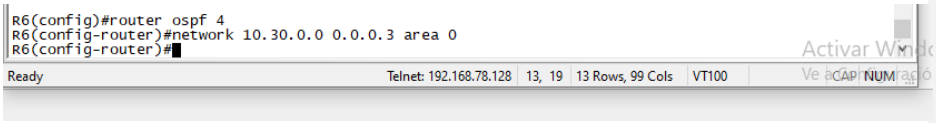


Figura 59. Configuración Router 6 , autoría propia en GNS3.

R2:

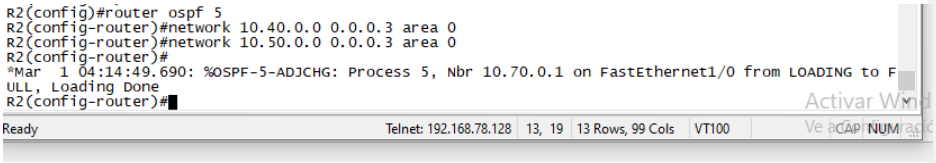


Figura 60. Configuración Router 2 , autoría propia en GNS3.

R1:

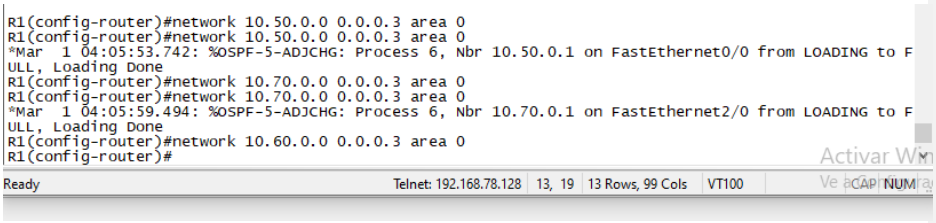


Figura 61. Configuración Router 1 , autoría propia en GNS3.

Posterior al direccionamiento de cada interfaz, verifiquemos con el comando Ping que alcanzamos las interfaces de los demás nodos, es muy importante verificar que se tenga alcance entre cada uno de ellos, es necesario crear una Loopback por cada nodo de la siguiente forma, lo cual facilitará las pruebas de comunicación, y por último el process ID el cual es necesario ya que como se vio en el apartado anterior en donde se analizó la configuración, y los parámetros de ospf el process id es el número que se usa internamente para identificar si existen múltiples procesos OSPF en ejecución dentro del router.

Como observamos en la siguiente imagen al ingresar en la configuración del enrutador debemos ingresar a la interfaz, con el comando **interface loopback** mas un numero que la identifique, posterior a ello añadimos una dirección ip para ella con su respectiva máscara. Es importante configurar la loopback ya que en transición normal de la red será clave para realizar validaciones de comunicación por parte del administrador de red.

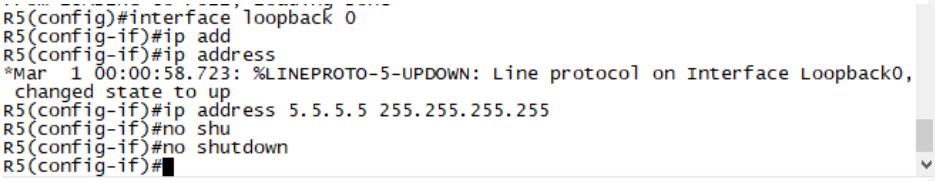


Figura 62. Configuracion Loopback 0 en router 5 , autoría propia en GNS3.

Posterior al proceso en cada uno de los nodos, procedemos a configurar el PROCESS-ID en cada router y los reiniciamos haciendo click izquierdo sobre ellos y seleccionamos la opción reload.

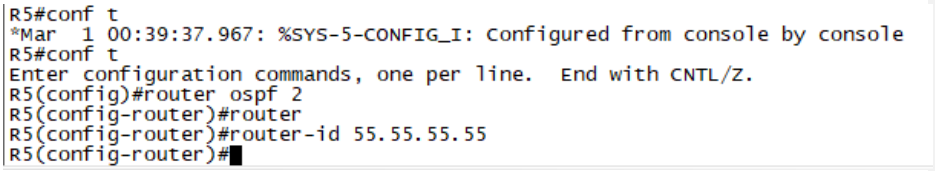


Figura 63 Configuración process ID , autoría propia en GNS3.

Posterior a la configuración del protocolo, debemos verificar que los datos configurados sean correctos, en el R5 se revisará el funcionamiento del protocolo en funcionamiento actualmente, ingresamos el comando SHOW IP PROTOCOLS, y encontramos el router ID, las redes adyacentes configuradas, lo cual nos servirá para entender qué posibles rutas puede tener el enrutador, y por último observamos la distancia administrativa de OSPF la cual es 110.

```
R5#sh ip prot
R5#sh ip protocols
Routing Protocol is "ospf 2"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 55.55.55.55
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.0.0 0.0.0.3 area 0
    10.20.0.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.70.0.1            110      01:02:46
    10.70.0.2            110      01:02:46
  Distance: (default is 110)
```


Figura 64. protocolos IP router 5 , autoría propia en GNS3.

Ahora valoraremos la interfaz de acuerdo al funcionamiento del protocolo OSPF, en donde podemos verificar y encontrar un posible error, ya que se imprime el área en que está trabajando la interfaz, el costo el cual en una red de sensores inalámbricas nos servirá para encontrar la mejor ruta, como vimos en el anterior apartado este valor se puede configurar para crear rutas a nuestro criterio.

Nos muestra el estado en que está el enrutador, para este caso el R5 es elegido como el router designado, y el R3 como su backup, nos muestra también las adyacencias, en caso de no tener comunicación con un vecino debemos iniciar verificando este parámetro.

```
R5#sh ip ospf interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 10.10.0.2/30, Area 0
  Process ID 2, Router ID 55.55.55.55, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 55.55.55.55, Interface address 10.10.0.2
  Backup Designated router (ID) 33.33.33.33, Interface address 10.10.0.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:08
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 33.33.33.33  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```


Figura 65. Ospf en interface F0/0 , autoría propia en GNS3.

18. SIMULACIÓN COMPLEMENTARIA: CONEXIÓN A SENSORES PACKET TRACERT.

Como en el anterior apartado se revisó la configuración y su verificación para encontrar problemas en el funcionamiento de OSPF, es necesario complementar con configuración de cara a la solución, dentro de esta simulación utilizaremos un servidor, un sensor conectado a un nodo wireless quien transmitirá la información obtenida hacia el servidor, la información recolectada será interpretada por un software del usuario final, la intención es configurar el nodo que actuara como gateway, el server y el sensor de temperatura para este caso.

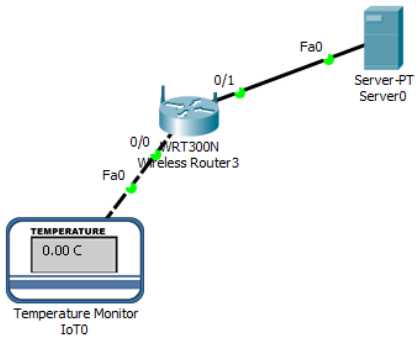


Figura 67. Sensor, Nodo, Servidor. , autoría propia en packet tracert.

Procedemos con el direccionamiento de todos los elementos, se decide iniciar por el servidor ejecutamos doble click sobre él y elegimos la opción **desktop** donde buscaremos la aplicación **IP configuración** la cual nos permitirá asignar una

dirección ip estáticamente o recibirla por DHCP, en la siguiente imagen se puede identificar el proceso que se debe llevar a cabo.

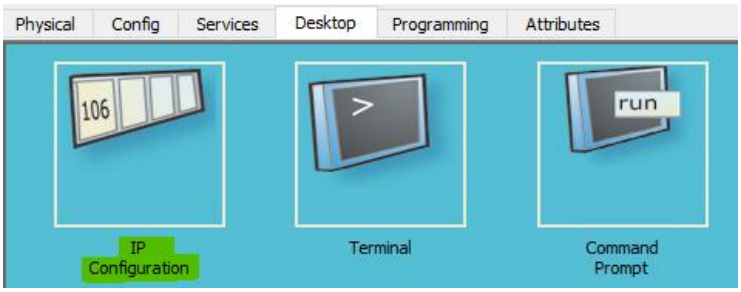


Figura 68. Configuración Ip servidor , autoría propia en Packet Tracert.

Al ingresar a IP configuration nos encontraremos con el siguiente menú:

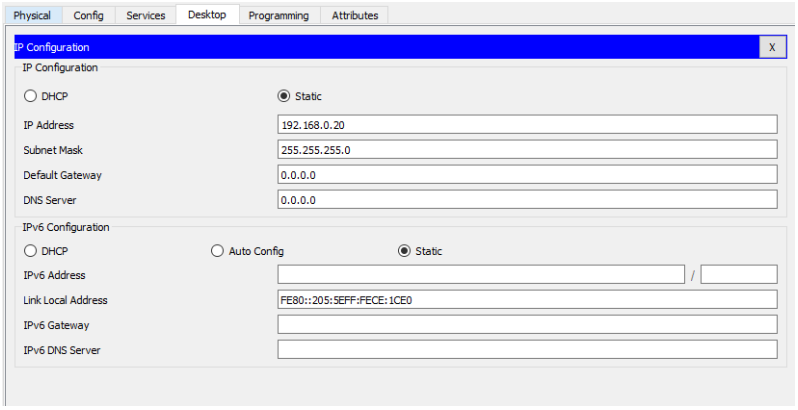


Figura 69 Direccionamiento servidor , autoría propia en Packet tracert.

En donde la dirección ip será configurada como 192.168.0.20 para este caso en especial.Ahora se continúa con la configuración del protocolo DHCP en el servidor

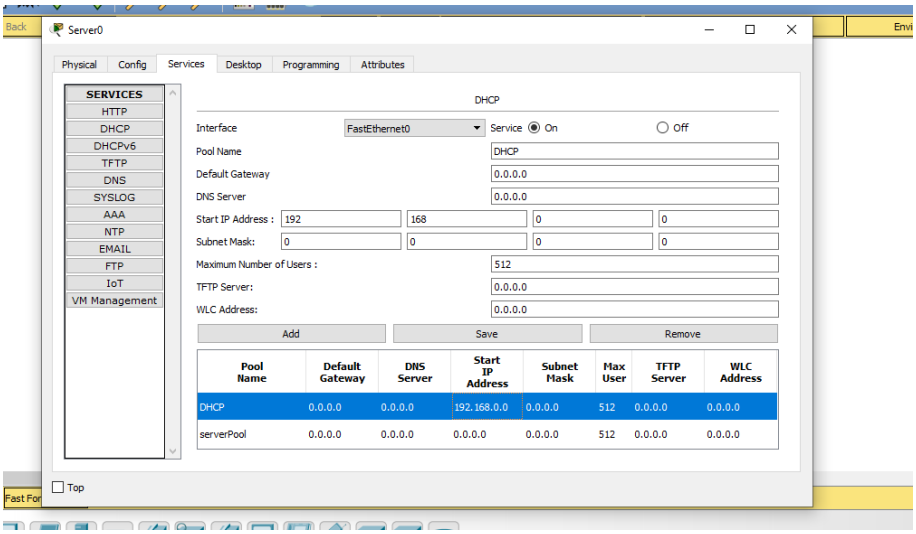


Figura 70. Direccionamiento server, autoría propia en Packet Tracert

Ahora vamos al sensor y oprimimos dos veces el click sobre el, ingresamos a configuración, seleccionamos la interfaz conectada al nodo y habilitamos el DHCP.

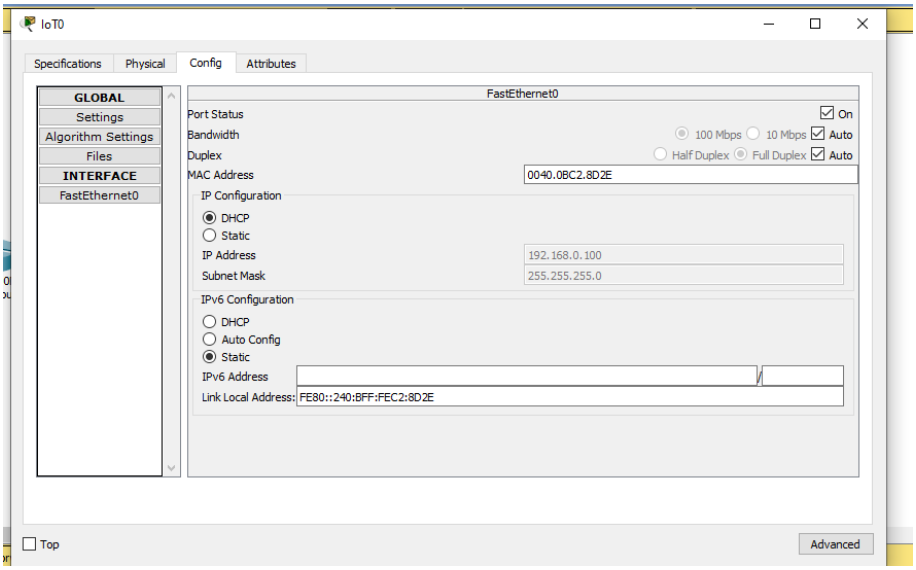


Figura 71. Dhcp server, autoría propia en Packet Tracert

Ingresamos al servidor, habilitamos la opción IOT,

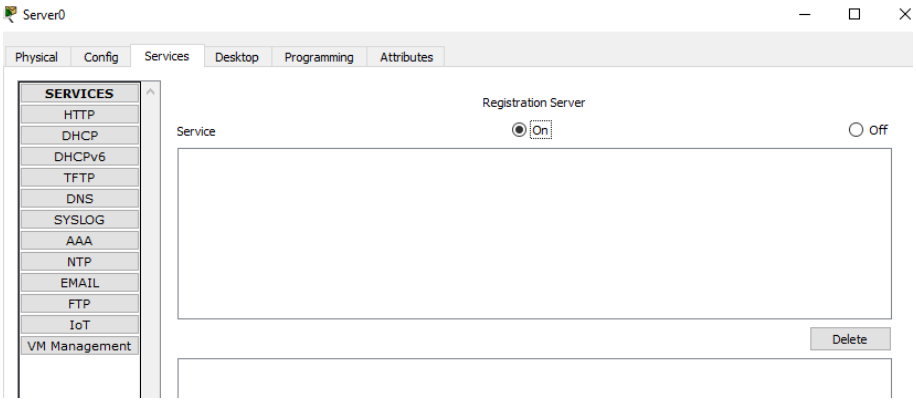


Figura 72. Direccionamiento server, autoría propia en Packet Tracert

y procedemos a seleccionar escritorio dentro del servidor, para seleccionar el server 192.168.0.20 como servidor principapal al cual le llegara la información obtenida por el sensor, cabe aclarar nuevamente que se representa esta simulación ignorando la red de transporte de comunicación antes configurada,

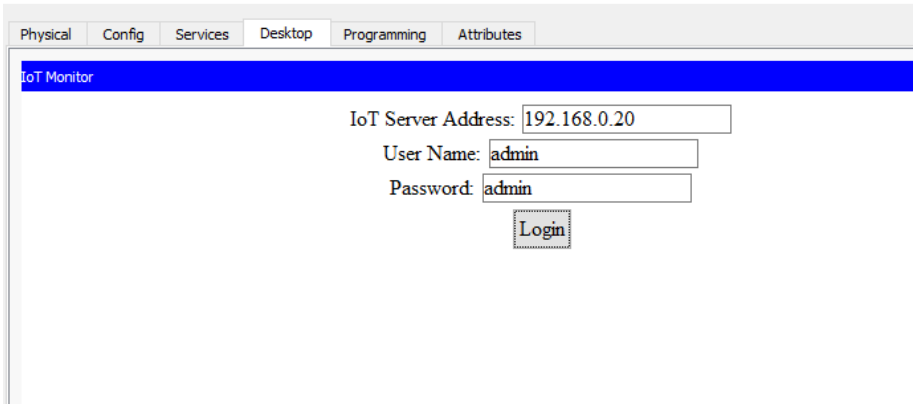


Figura 73. Configuración IOT monitor, autoría propia en Packet Tracert

Ahora dentro del sensor se configura el servidor remoto que estará conectado a cualquier de los 6 nodos anteriormente vistos y configurados en gns3.

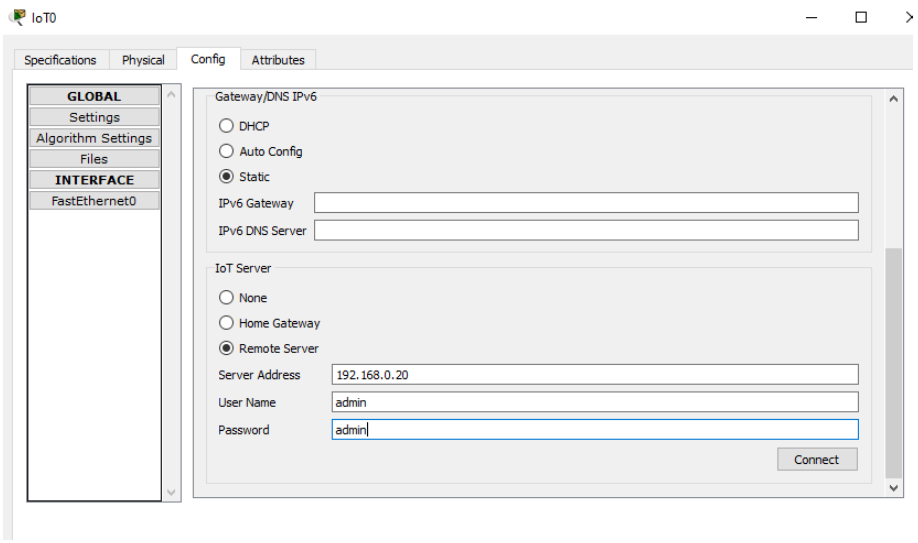


Figura 74.configuracion server monitor, autoría propia en Packet Tracert

Dentro de el sensor se pueden configurar condiciones y programar aplicaciones para llevar acabo análisis de los datos obtenidos por los sensores el manejo de información y configuración de cara al usuario final, está por fuera del trabajo del área de comunicaciones, por ende se ignoran estos pasos, es de suma importancia entender este tipo de arquitectura de cisco, capa de distribución, acceso y core, donde nos enfocamos directamente en la de distribución siendo OSPF un protocolo que trabaja para garantizar su perfecta operación.

19.CONCLUSIONES.

- Por medio de la guía se logra examinar y explicar el protocolo y su funcionamiento, además de los pasos que se deben realizar para encontrar problemas o anormalidades en la red.

- Se pudo identificar los parámetros a tener en cuenta en redes donde OSPF se implemente y que factores son importantes tener en cuenta a la hora de diseñar o administrar redes de sensores inalámbricos.

- Por medio del análisis llevado a cabo en la guía de implementación se logra identificar en uno de sus apartados que OSPF es el protocolo ideal para las redes de sensores inalámbricas y su rendimiento es acorde a las necesidades.

- Por medio de la Topología complementaria se explicó que configuraciones debe llevar a cabo el usuario final, puesto que la guía se basó únicamente en la comunicación de cada uno de los nodos, realizando esto se genera claridad y una perspectiva más clara y envolvente a este tipo de soluciones

- La guia expuesta en el capítulo 3 permite motivar al lector a realizar trabajos de investigación futuros con este tipo de redes inalámbricas en escenarios más adecuados.

20 Software de simulación

20.1 GNS3

La herramienta GNS3 permite emular gráficamente redes, a un nivel profesional compatible en windows, OS X, and Linux, permitiendo diseñar redes complejas, además de la combinación de dispositivos virtuales y reales.

Figura 68 *Software Gns3[15]*

20.2 Packet tracer

Cisco packet tracer de cisco es un programa de simulación de redes que permite a los estudiantes experimentar con el comportamiento de la red

Figura 69 *Software Gns3[16]*

21. REFERENCIAS

[1].*WENDELL ODOM, CCIE No. 1624 with contributing author SCOTT HOGG, CCIE No. 5133 ,"CCNA Routing and Switching ICND2 200-105",2013.*

[5]. *A. Ghosh and N. Chakraborty, "Performance study of routing protocols for power data transfer in Wireless Sensor Network," 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2017, pp. 2091-2095.*

doi: 10.1109/WiSPNET.2017.8300130

keywords: {energy conservation;radiofrequency interference;routing protocols;wireless sensor networks;performance study;power data transfer;power sector;time data monitoring;fast data delivery;model hardware implementation;conventional AC power data;data transmission pathways;energy efficient data delivery;wireless sensor network;routing protocols;shortest path first protocol;interference elimination;Peer-to-peer computing;Wireless sensor networks;Routing protocols;Voltage measurement;Monitoring;Wireless communication;Energy Efficient;Network Topology;Real Time Data Monitoring;Routing Protocol;Wireless Sensor Network},

URL: http://ieeexplore.ieee.org.crai-ustadigital.usantotomas.edu.co/stamp/stamp.jsp?tp=&arnumber=8300130&isnumber=8299705

[6]. *L. Veeravagu, L. Barrera, A presentation on Dijkstra's algorithm, 2010.*

[7].*Z. Wang, Y. Liu, "Data gathering routing algorithm based on energy level in wireless sensor networks", 2nd IEEE International Conference on Future Computer and Communiction, 2010.*

[8].*R. Singh Bisht y S. Budhani , «Performance analysis of hierarchical and nonhierarchical routing techniques in wireless sensor networks,» de Soft Computing Techniques for Engineering and Technology (ICSCTET), 2014 International Conference on, Bhimtal, 2014*

[9].*Raghav gathering in sensor inform the IEEE Aerospace, C.S.S. Lindsey, 2002*

[10]. *Roberto Fernández Martínez, Joaquín Ordieres Meré, Francisco -javier Martínez de Pisón Ascacíbar, Ana Gonzáles Marcos, Fernando Alba Elías, Ruben Lostado Lorza, Alpha verónica Pernía Espinoza, Integrantes del Grupo de investigacion EDMANS, "Redes inalámbricas de sensores teoría y aplicación práctica", 2009.*

[11]. *Rodríguez, E. J., Deco, C., Petinari, M., & Burzacca, L. (2012). Protocolos de encaminamiento para Redes malladas Inalámbricas: un estudio comparativo. In XVIII Congreso Argentino de Ciencias de la Computación.*

[12]. *Rey Manrique, F. R. (2011). Diseño de un sistema de CCTV basado en red IP inalámbrica para seguridad en estacionamientos vehiculares.*

[13]. *Sánchez, J. R. P. (2016). Análisis y comparación de la seguridad utilizando dos protocolos de enrutamiento para IPv6. Maskana, 7, 213-220.*

[15]. *URL https://sites.google.com/site/iosparagns3/to-dos*

[16]. *URL**:** https://notasinformaticas.com/curso-gratuito-de-cisco-packet-tracer/*

[17]. *M Athira; Lekha Abrahami; R. G. Sangeetha(23-25 March 2017). Study on network performance of interior gateway protocols — RIP, EIGRP and OSPF*